
Law in the digital age
edited by
Zoltan Vig

Law in the digital age

edited by

Zoltan Vig

Ankara, Budapest, Mauritius, Novi Sad, Szeged, Skopje
2023

This collection of studies is a joint publication of
Department of Business Law, Faculty of Economic and Social Sciences of the Budapest University of Technology and Economics, Budapest, Hungary
Department of Law, Faculty of Law & Management, University of Mauritius, Mauritius
Department of Private International Law, Faculty of Law, University of Szeged, Szeged, Hungary
Faculty of Law and Business Studies Dr Lazar Vrkatić, Novi Sad, Serbia
Faculty of Law, Ankara Yıldırım Beyazıt University, Ankara, Turkey
Faculty of Law, Yozgat Bozok University, Yozgat, Turkey
Iustinianus Primus Faculty of Law, Ss. Cyril and Methodius University, Skopje, Macedonia

ISBN 978-963-421-937-8

Table of contents

Zoltan Vig*

Editorial: Law in the digital age

Digitalization and new technologies have caused legal science to enter a period of transformation that we have perhaps never seen before in legal history. The rapidly approaching new challenges present enormous difficulties for regulators. It is often said that law is lagging several years behind the new technologies. If so, this position seems increasingly untenable as the technological transformation of society accelerates. The purpose of this conference is therefore to study these developments from a legal perspective, and to attempt to identify issues we face, and of course, to suggest solutions on how to resolve them in the most efficient way.

The most affected issues by this technological development are, among others, data protection, intellectual property rights, cybersecurity and online crimes, e-commerce and contract law, online platforms, blockchain, and cryptocurrency. Or we can mention artificial intelligence, which is taking over the drafting of contracts, conducting legal research and even drafting laws and administrative acts in some cases. In essence, this means that regulators and legal practitioners are increasingly delegating their responsibilities to technology. The long-term consequences of this in the legal field are difficult to predict.

Furthermore, computer and communications technologies are transforming legal practice. Technology affects lawyers on two levels. First, it allows them to perform traditional tasks more

* Zoltan Vig is a senior lecturer at the Department of Business Law, Faculty of Economic and Social Sciences of the Budapest University of Technology and Economics, Budapest, Hungary; and at the Department of Private International Law, Faculty of Law, University of Szeged, Szeged, Hungary; E-mail: jogasz@gmail.com.

effectively. Second, it is changing the very nature of what lawyers do. This, in turn, can cause further uncertainty regarding the future. A lot of times, those who apply the law in practice try to fit new technological solutions into existing legal boxes. Nevertheless, this is not easy to accomplish, and can often cause regulatory anomalies.

However, we have to face these issues with optimism. First of all, national regulators should respond more quickly to these challenges. Secondly, standardization increased the efficiency of trade and industry. This can also be true for legal regulation. Regulating these issues on an international level with international instruments can help overcoming challenges easier.

All the works in this conference volume address one or other of the above issues. The order of the works follows the alphabetical order of their authors' family names.

The first work in this conference volume, "Digitalization of the Macedonian public administration: a pathway to prevent maladministration and illegal activities", whose author is Konstantin Bitrakov, critically examines the process of digitalization of the Macedonian public administration. The author emphasizes that digitalization is a remedy against maladministration and comes to the conclusion that Macedonia is on the right path; however, there is much room for further improvements in this area.

In their study, "Digitalization and banks during COVID-19 crisis: a qualitative study", Rudranee Devi Deeljore and Bhavish Jugurnath investigate how digitalization has helped the banking sector during the COVID-19 crisis in Mauritius. The paper is special in the sense that it is based on interviews with local bank managers. The authors come to the conclusion that

the COVID-19 crisis played a significant role in the digitalization of the banking processes in Mauritius, which led to substantial improvements in services.

Aliz Fabian in her study "Artificial intelligence as a mediator?" focuses on the possible usage of artificial intelligence during mediation sessions, and among others, reviews the current mediation practice in the United States. She concludes that in the current state of technology AI software are not suitable for leading a whole mediation session without human intervention.

Goran Georgijevic in his work "Legal regime in Mauritius of consumer contracts made through electronic communication means" first gives an analytical overview of consumer contracts, and finds that there are still issues related to these contracts in Mauritius that could be addressed by the legislator. Following this, he analyses the legal measures that could still be adopted in order to protect consumers in a consumer contract made through electronic communication means.

Rajendra Parsad Gunputh, Eric Bindah, Joseph Assogbavi, and Ambareen Beebeejaun in their empirical study entitled "Computer crime: cryptography and cryptanalysis in the IT sector - where does the Mauritian law stand? –" examine whether academics and students are aware of cryptography and cryptanalysis, and the related legal regulation.

Tea Lalevska in her work "Digitalization of the cadastral system in the Republic of North Macedonia", as the title suggests, deals with the benefits of the digitalization of the real estate cadastre system in Macedonia. Following a short historic overview, she gives an excellent analysis of the current legislation and its application in practice.

Bhavna Mahadew's paper "The Digitalisation of Law: How prepared are we to welcome legal practice and education which are artificially intelligent?" examines the relationship between artificial intelligence, the law, and the pervasive digital revolution, and notes with concern that modern technologies might conflict with human rights.

Aleksandar Matkovic and Ivana Novakov in their brilliant work entitled "Decoding the changing (id)entity of cybercriminals: from human perpetrators to AI" study and dissect the knowledge on the psychological profile of traditionally defined cyber offenders (humans), and following this deal with the theoretical question of how the legal system should treat AI (as a non-human) independent cyber-criminal.

Tea Micevska in her article "The written form of the civil proceedings in the digital era: an evolution in the digital work environment" observes that nowadays a digitalized civil procedure is a prerequisite for a modern justice system; however, modernization should not undermine the fundamental principles of civil procedure.

Marija Mijatović and Tamara Gajinov in their work "Corporate strategy of planned obsolescence - a reflection of the reality of technological development" first of all raise the issue of defining planned obsolescence. Following this, the authors examine the existing legislation and judicial practice in France, and initiatives and the perspective of the regulation of this issue in the European Union.

Bengi Sargin in her work entitled "Determination of "*lex loci protectionis*" in the digital environment" examines the applicable law to intellectual property rights with foreign elements. Following this, the work concentrates on the connecting factors in terms of applicable law. And finally, the

author examines how to determine *lex loci protectionis* in intellectual property disputes arising in the Internet environment.

Marie Valerie Uppiah in her paper "Assessing the regulation of maritime cybersecurity at the level of the African continent" writes about the current issues of maritime cybersecurity and its regulation in Africa. She notes that with the digitisation of the shipping industry, many ports and shipping companies are becoming victims of maritime cyberattacks. Therefore, her work examines the concept of maritime cybersecurity and analyses the legal actions ought to be taken by the African Union and the Southern African Development Community to address potential cases of maritime cyberattacks.

Konstantin Bitrakov*

Digitalization of the Macedonian public administration: a pathway to prevent maladministration and illegal activities

Abstract: The global shift towards the digitalization of public administration presents a potent force in improving service delivery, efficiency, and curbing maladministration. This paper explores this transition in the Republic of North Macedonia, emphasizing the potential of digital platforms like e-governance portals and eIDs in reducing bureaucracy and fostering accessibility to public services. Despite the positive strides, a concrete evaluation of its impact remains elusive. The paper is segmented into several sections. Initially, it establishes a theoretical foundation, correlating digitalization with reduced maladministration, supplemented by comparative experiences. Following this, the focus shifts to the specific national context, discussing citizens' perceptions and other key indicators concerning maladministration and illicit activities. Subsequent sections delve into an analysis of Macedonia's recent legislation and ongoing projects, such as the National Portal of e-Services and the Catalogue of Services, assessing their efficacy and implementation hurdles like law inconsistencies and limited technological infrastructure. In conclusion, the paper underscores the necessity for a comprehensive approach to digitalization, encompassing legislative amendments and organizational reforms, alongside technological advancements. While Macedonia has initiated this process, sustained efforts are vital to surmount existing obstacles and maximize the benefits of digital technology in mitigating maladministration.

Keywords: digitalization, Macedonian administration, maladministration, digital transformation, electronic services

* Konstantin Bitrakov is a teaching assistant at the Iustinianus Primus Faculty of Law, Ss. Cyril and Methodius University, Skopje, Macedonia; E-mail: k.bitrakov@pf.ukim.edu.mk.

1. Introduction

In recent years, the global paradigm shift towards the digitalization of public administration has been markedly visible. Governments worldwide are adopting digital tools to streamline their operations, foster transparency, and enhance service delivery.[1] This transformative force enhancing effectiveness can also be instrumental in diminishing maladministration and other illicit activities that have been an underpinning issue in many administrative sectors. Within this global narrative, the Republic of North Macedonia (hereinafter: Macedonia) finds itself at a critical juncture, where it aspires to fully realize the potential benefits of a digital future in its public administration, however does not succeed in doing so.

In Macedonia, there is an optimistic view that pivoting towards a digital future can foster a significant positive change.[2] Concrete steps have been observed in several fields: the introduction of the Open Finance Portal,[3] with the aim to guarantee the transparency and tracking of public spendings, and the complete digitalization of the process of submitting claims to access public information by the Agency for Protection of the Right to Free Access to Public Information.[4] The policy creators, particularly the Ministry of Information Society and Administration, acknowledge the imperative of digitalization, envisioning a future where all public authorities would deliver services such as decisions, confirmations, and

[1] Digital Mahbub (2023).
[2] Karai & Mojsovski (2020).
[3] The "Open Finances" portal enables individuals to follow all payments from the accounts of institutions funded by the central budget in Macedonia. More information is available at: https://open.finance.gov.mk/mk/about.
[4] The Agency for Protection of the Right to Free Access to Public Information implemented a portal where the citizen can submit a request to access public information to every information holder (public institution). The portal is available at: https://slobodenpristap.mk/.

licenses electronically via the National Portal for Electronic Services.

However, despite being well-received as a concept, and being earmarked as a priority in strategic documents, such as the "Strategy for Public Administration Reform 2018-2022" and the draft "Strategy for Public Administration Reform 2023-2030", the implementation has been lagging. The availability of digital services for citizens and businesses remains markedly low, and the extent of the adoption of document management systems across various public authorities is unclear. Moreover, units of local self-government have been conspicuously absent in most digitalization efforts, indicating a notable gap in the approach. Therefore, this research seeks to delve deep into the intricacies of digitalization implementation in the Macedonian public administration, aiming to pinpoint avenues for improvement and explore its potential in combating maladministration and illegal activities therein.

2. Theoretical framework (digitalization vs. maladministration)

Digitalization, in the context of public administration, encompasses the utilization of digital technologies to modify, enhance, and streamline the operation of governmental services.[5] This process involves the transformation from traditional paper-based systems to digital platforms, fostering improved accessibility, efficiency, and transparency. At the core of this transformation is the ability to integrate data and information systems which ultimately brings about electronic sharing of data between public authorities, reducing of *in vivo* contacts between them and the citizens (and businesses),

[5] Similarly: Knowledge and Policy (2021).

electronic management of documents which also covers the automatic assignment of cases, *etc*.

Respectively, the advent of digital tools and platforms in the administrative domain can diminish maladministration significantly. Namely, the notion of maladministration covers all irregular administrative actions, starting from illegal, inconsistent, unfair decisions (administrative acts), other illegal and unjust actions, as well as invalid regulations and small omissions (excluding the trivial and meaningless mistakes).[6] Therefore, digitalization may affect maladministration in various ways, for example:

- since the *in vivo* contact between the administrative servants[7] and the clients are reduced, there is no possibility for the former to be rude, discourteous or ill-disposed to the latter, providing scarce or confusing information when asked for it, *etc*.[8];
- if the documents are managed digitally, the higher-ranked servants can easily monitor if their subordinates perform their tasks in a timely manner, *i.e.,* if there are any delays in deciding on citizens' and businesses' applications;
- whenever there are such possibilities, citizens and businesses can monitor themselves the current status of their case and, in cases of illegitimate delays, they can signal the managers of the public authorities;
- citizens and businesses are not asked to provide documentation as proof along with their application, since the public authorities can obtain all necessary information

[6] Davinić (2013) 134.

[7] The term "administrative servants" in the Macedonian legislation is used for all individuals employed in the public sector to perform administrative tasks such as HR, normative tasks, legal tasks, statistical tasks, etc. Other term that can be used for these individuals is "civil servants".

[8] The direct contact is perceived as the main problem in terms of maladministration and failure to provide services. Viendyasari (2020).

on the applicant digitally by accessing other authorities' registers[9];
- the digitalization of the process may also point out which steps are redundant or unnecessary, streamlining the procedures.

Globally, numerous countries have successfully embraced digitalization to curb maladministration. For instance, the experiences of nations such as Estonia and Singapore stand as testimony to the transformative power of digitalization in public administration. These countries have effectively utilized e-governance platforms, digital identities (eIDs), and electronic document management systems to foster a seamless, transparent, and efficient administrative mechanism, setting benchmarks for others to follow.

3. National context: citizens' perception of the administration

At the forefront of Macedonia's administrative landscape is the pressing need to modernize and streamline its public administration processes. This becomes more and more vivid, as the citizens' and businesses' perceptions are becoming worse over time. Yet, as the country moves towards a digital future, it finds itself grappling with the complexities of effectively transitioning from traditional administrative procedures to more technologically advanced solutions. This process, while marked by some successes, such as the implementation of the National

[9] For better understanding, we are providing an example. For instance, it might be stipulated – in the laws or bylaws – that only companies with more than 100 employees may obtain licenses to perform certain business operations. In the case of digitalization, the company shall not need to provide lists of employees when submitting an application to obtain the license. Instead, the public authority issuing the license will be able to obtain the information on the number of employees at the applicant by accessing the registers of another public authority such as an employment bureau, trade registry, *etc*.

Portal for Electronic Services, is also characterized as lethargic, slow, and with almost complete neglect of local self-government units in the digitalization initiatives. More attention is paid to these issues in the text below. At this point the focus is on citizens' perceptions towards maladministration in the country.

One might begin with an NGO survey from 2017[10] which illustrated that citizens are dissatisfied with the services they get from the administration. When citizens were asked if they find that the money which is used to finance the public administration is proportionate to the quality of services, the answers were as follows:

- completely agree: 8.4%
- agree: 16.5%
- neither agree, nor disagree: 28.6%
- disagree: 26.4%
- completely dissagree: 9.3%
- refuses to answer or does not know: 10.9%

Simply put, more than third of the citizens are dissatisfied with the administrative services in the country, while another third of them are neither satisfied nor dissatisfied. Although this question does not refer specifically to maladministration, it is quite indicative. It is a possibility that those who are not satisfied have been experiencing such practices.

Similar survey was published in 2019 as well, covering the period from 2017 to 2019.[11] As a general conclusion, 44.4% of respondents in Macedonia found that the work of the public administration is bad. If one goes into more details, the information is even worse. More than 60% of respondents

[10] Малеска Сачмароска and Гоцевски (2017).
[11] Граѓанска алијанса за транспарентност (2019).

found that there is clientelism and privileges when providing services in the public administration, as well as that the only way to obtain a service is to have connections.[12] Answering the question "[h]ave you personally faced problems when using public administration services":

- 46.4% of respondents answered 'yes' in 2017;
- 50.4% of respondents answered 'yes' in 2019.

Moreover, when asked which are the problems they most often face when asking for services from the public administration, respondents pointed out:

- being redirected from one counter to another/unclear procedures;
- employees not being service oriented;
- employees being unprofessional/bad attitude from the employees;
- deadlines being breached/slow pace/procedures lasting too long;
- bad quality of services.

In other words, it is becoming more and more vivid that maladministration practices are widely spread, since everything that was mentioned is in fact a manifestation of maladministration.

The State Commission for Prevention of Corruption also commissioned a survey of the citizens' perceptions on the public administration, which was conducted by a private company, and published in October 2020.[13] The findings are

[12] Speaking of having connections, it is vivid that illicit activities are implied. Citizens are speaking of a form of patronage (certain individuals or businesses are prioritized when providing services since they have close personal or other ties with the administrative servants or the political appointees who are on top of a certain administrative authority).

[13] Тим институт (2020).

(more or less) the same as the ones referred to above. The responses of question 16 – where individuals were asked to rate the transparency/openness of the central authority in the delivery of public services (services from the public institutions to the citizens) – indicated that:

- 25% of citizens found that the delivery of public services is absolutely non-transparent;
- 49% of citizens found that the delivery of public services is somewhat transparent;
- 15% of citizens found that the delivery of public services is very transparent;
- 11% of citizens did not know.

In the same survey citizens were also asked to rate the transparency of the local authorities in providing public services (services from the public institutions for the citizens). The ratio was almost identical as in question 16:

- 26% of citizens found that the delivery of public services by the local authorities is absolutely non-transparent;
- 48% of citizens found that the delivery of public services by the local authorities is somewhat transparent;
- 16% of citizens found that the delivery of public services by the local authorities is very transparent;
- 10% of citizens did not know.

Therefore, one might conclude that citizens in Macedonia do perceive maladministration to occur regularly in their country. This is a vital indicator of the progress of the country and makes the digitalization efforts even more important. Yet, even though it cannot be disputed that digitalization is vital, one cannot be overly optimistic. The slow pace of implementation of digital services and the limited reach of these services to the broader populace are quite worrisome. The government obviously needs to put more efforts and resources to enhance e-services and e-governance altogether. To have a better understanding, the

following text focuses on the current policies and laws in light of digitalization, as well as the factual success of the initiatives.

4. Laws and current projects surrounding public administration digitalization in Macedonia

Macedonia has been proactive in drafting legislative frameworks to govern and guide the digital transformation of its public administration. In this part the backbone legislation of the country's digitalization drive is examined.

The Law on Electronic Documents, Electronic Identification and Trust Services: This law embodies the principle of ensuring that digital documents possess the same legal status as traditional paper documents. Furthermore, it provides the foundational framework for electronic identification (eID), ensuring secure and seamless interactions in the electronic environment. Basically, with the adoption of this law, Macedonia completely harmonized its legislation in terms of electronic documents and eID with the Regulation (EU) 910/2014 on electronic identification and trust services for electronic transactions in the internal market.

In accordance with this law, a Rulebook on the mandatory elements of electronic documents was adopted, along with other bylaws, which additionally operationalized the provisions from the law.

The laws regulating electronic services: Two laws are vital in terms of digital services provided by public authorities – the Law on General Administrative Procedure (hereinafter: LGAP) and the Law on Electronic Management and Electronic Services. The LGAP sets out the basis for electronic

communication between the public authorities and parties,[14] when the latter seek services from the former. In addition, the LGAP obliged all public authorities to communicate among each other electronically, as well as to obtain all necessary documents and information which are available, either in their or on other public authorities' registers *ex officio* in the administrative procedures. This means that, according to the LGAP, citizens and businesses were no longer obliged to provide additional documents as evidence when applying for service (*e.g.* documents which provide their citizenship, status, *etc.*). Instead, public authorities were supposed to communicate amongst themselves and share documents. The Law on Electronic Management and Electronic Services further regulates digital services. In summary, this law obliges public authorities to: (a) record the services they provide to citizens and businesses to the Catalogue of Services, so that it is clear how many services each public authority provides, making it easier for the policy-coordinators (*e.g.* the Ministry of Information Society and Administration, as well as the Government) to monitor how many of them have been digitalized, but also making it clear for citizens and businesses how to obtain a certain service; (b) enable citizens and businesses to obtain all services (with the exception of the ones which are by law only provided in writing)[15] electronically, through the National Portal for Electronic Services, which means that citizens and businesses should be able to apply for the service online and to also receive whatever document that comes as an output of the procedure online; (c) issue all digital documents in accordance with the previously mentioned Law

[14] Parties are the natural or legal entities who are entering an administrative procedure in which a public authority decides on their rights, legal interests (*i.e.,* provides them a service) or their obligations.

[15] Of course, not all administrative services can be offered online. Some laws stipulate that in order to obtain a certain service the citizen or the business must submit a written application and must undergo an interview or similar activities which have to be *in vivo*.

on Electronic Documents, Electronic Identification and Trust Services; (d) use the National Platform for Interoperability to share information and documents – in a standardized format – with other public authorities, so that all information on citizens and businesses which are needed to provide a service and are held by in a public register, will be obtained *ex officio*.

The Law on Central Population Registry: in accordance with this law the Central Population Registry was set up. The Central Population Registry was built by integrating the data from various bases, so a comprehensive and up-to-date record of the Macedonian population was created. Thus, once a public authority receives a digital application for a service, as per the Law on Electronic Management and Electronic Services, it may enter the Central Population Registry and obtain his/her personal data.

Each piece of legislation marks a critical step towards creating a conducive environment for the seamless integration of digital solutions in the Macedonian public administration. Aside from the modern laws and bylaws, however, the ground-level implementation of administrative digitalization presents a mixed picture. Let us review the successes of the projects and initiatives we mentioned when elaborating upon the laws:

- Catalogue of Services: There are currently more than 1,200 public authorities which have recorded the services they provide in the Catalogue of Services, meaning that the mapping of the services provided by public authorities has been successful.
- National Portal for Electronic Services: Currently only 85 services are available on the National Portal for Electronic Services.[16] Therefore, one cannot say that the National

[16] According to the home page of the National Portal for Electronic Services in September 2023: https://uslugi.gov.mk/. Other 200 and some services are also available online, but not through the centralized National Portal for

Portal for Electronic Services is a success. Regardless the fact that the National Portal for Electronic Services is user-friendly and has a capacity to serve many citizens, it is rather rarely used – approximately 50,000 applications have been submitted through it ever since it was established in 2019. The National Portal for Electronic Services is not used by the units of local self-government, only by the central public authorities.

- National Platform for Interoperability: Hosted by the Ministry of Information Society and Administration, the National Platform for Interoperability is set up and functional. Significant resources are invested for its maintenance (hardware and software), as provided in the Strategy for Public Administration Reform (2023-2030),[17] yet very few institutions actually use it and share information and documents through it. To be precise, only 53 public authorities are using the Platform. Bearing in mind that the currently in Macedonia there are more than 1,300 public authorities,[18] this number is devastating.

Therefore, one may conclude that the public administration (and the public sector as a whole)[19] is not digitalized. Unfortunately, the vision laid down in strategic documents like the Strategy for Public Administration Reform 2018-2022 and the Strategy for Public Administration Reform 2023-2030 obviously clashes with on-ground realities. The improvement of this situation depends on the accuracy of the diagnosis – why is the public

---

Electronic Services but through other portals used by a single public authority (*e.g.* the Revenue Office have their own system, etc.). This fragmentation is not positive for citizens, it would be much easier for them if all services are available on the one National Portal for Electronic Services.

[17] Page 35 and 36 of the Strategy for Public Administration Reform.

[18] Министерство за информатичко општество и администрација (2023) 4.

[19] The term public sector is broader than the term public administration since it covers other public authorities aside from the administrative ones, such as courts, public enterprises, state-owned companies, *etc*.

administration not digitalized? We shall endeavor to find the answer.

5. Assessment of the digitalization process: why is the public administration not yet digitalized?

5.1 Legal obstacles

The digitalization of Macedonia's public administration, while laudable in its objectives, faces several hurdles in its path. While the laws enlisted above have laid a solid foundation for the digital transformation, there seems to still be legal obstacles for digital services. Namely, there have been statements by individuals employed at the government that there are substantive laws which regulate certain administrative services, and which have provisions not yet aligned with the digitalization laws. As a former advisor to the Prime Minister pointed out in 2021: "Over 100 laws should be harmonized with the 3 laws for digitalization (Law on Central Population Registry; Law on Electronic Documents, Electronic Identification and Trust Services and the Law on Electronic Management and Electronic Services)".[20] The Government should encourage such research, so that the precise number of laws which are not harmonized with the digitalization laws is outlined.

A field analysis suggests that while the laws might not be such a problem, the bylaws for providing services might be. The best way to illustrate this is a case study. So, several public authorities have been taken into consideration as examples, and their bylaws have been analyzed.

[20] Герзаова Муjчин, Лечевска, Колозова (2021) 5.

In the following table examples of bylaws can be found under which electronic services are not allowed and the authorities which have adopted them:

Ministry of Economy	
Rulebook on the form and the content of the license A and B for performing tourist activities.	Has a provision under which the license for the tourist agencies may only be issued in writing, on a A4 size paper in green color, with the signature of the minister.
Rulebook on the form and the content of the template of the request for categorization of an accommodation facility.	Has a provision under which the request for categorization of a hotel is submitted in a written form, on a A-4 white sheet of paper.
Rulebook on the form and content of the request for issuing a license for the sale of alcoholic beverages, the form and content of the license for the sale of alcoholic beverages and the form, content and manner of keeping the register for issued and seized licenses.	Has a provision under which the request for license to sale alcohol is submitted in a written form, on a A-4 format.
Rulebook on the form and content of the request for registration in the Registers of manufacturers of tobacco products and related products, the necessary evidence and documentation and the closer conditions for manufacturing of tobacco products and related products.	Has a provision under which the application to be registered as a tobacco producer has to be submitted in a written form on an A-4 size white paper.
Ministry of Transport and Communications	
Rulebook on the form and the contents of the request for	Has a provision which stipulates that only written

license for the development of urban plans, the form and content of the request for the issuance of an authorization for development of urban plans and the needed documentation.	requests, on an A4 size white paper, are accepted.
Ministry of Agriculture, Forestry and Water Economy	
Rulebook on the format and content of the application for registration in the Register of Legal Entities which place garbage on the wholesale market.	As in the rulebooks before, there is a provision under which the application can only be submitted in writing.
Rulebook on the format and content of the application for registration in the Register of Legal which place garbage on the retail market.	Just as in the previous rulebook, there is a provision under which the application can only be submitted in writing.

To start off, we took into account the Ministry of Economy which provides hundreds of services to businesses. These services vary from issuing licenses to perform tourist activities (*e.g.,* to become a tourist agent or to have a tourist agency) to categorizing hotels and issuing licenses for the sale of alcohol or tobacco. The rulebooks we cited explicitly stipulate that only written applications for services are going to be accepted, as well as that only written output documents (*e.g.,* licenses) are issued. To make matters even more disappointing, the rulebooks are not old and outdated. For instance, the rulebook which regulates the issuance of alcohol sale license is adopted in 2022 and amended in 2023, yet the provisions on the written application have remained therein. The Ministry of Transport and Communications also provides hundreds of services to businesses, especially in the areas of construction, urbanism, *etc*. Still, the cited rulebook has outdated provisions which explicitly regulate that only written applications are acceptable. Again, this would be something to understand if the rulebook is

old and precedes the new laws which are the backbone of the public administration digitalization. However, this is not the case. The rulebook is from 2020. Similar case is the Ministry of Agriculture, Forestry and Water Economy. The rulebooks' provisions explicitly state that only written submission of applications is possible. Unlike the other rulebooks, these ones are at least older.

So, in Macedonia there are some laws and many bylaws which are not aligned with the laws on digitalization. Thus, the question of how to overcome this difficulty arises. There are two possible approaches.

According to the first approach, since the Law on Electronic Documents, Electronic Identification and Trust Services contains a provision that each digital document is equivalent to the written ones, the ministries and all other authorities should start accepting digital applications for services and issuing digital output documents (licenses, decisions, *etc*.) regardless of the provisions in the substantive laws and bylaws which require written form. The Law on Electronic Documents, Electronic Identification and Trust Services may be considered as a *lex specialis* for the form of the documents, so it may derogate the rules on the forms of the documents from the substantive laws. In addition, the Law on Electronic Documents, Electronic Identification and Trust Services is a higher legal act than the bylaws. Therefore, the bylaws' provisions which are contradictory to the Law on Electronic Documents, Electronic Identification and Trust Services should not be applied. This approach would be in line with the strategic digitalization goal, it would be efficient, since no further amendments would be needed and, ultimately, would be in accordance with the service-orientation principle for the public administration, which is set out in the Law on General Administrative Procedure. To support this interpretation, the Government

might issue a conclusion which will be mandatory for all ministries and other authorities that report to it. The conclusion would be that the Law on Electronic Documents, Electronic Identification and Trust Services should be directly applied when digital applications have been submitted. The Government would not be able to oblige the units of local self-governments with such an instruction since they are completely independent from the central authorities, however, it might suggest they comply with it.

If the first alternative is not acceptable for the ministries and all other authorities, a process of detecting and amending all bylaws which need harmonization with the digitalization laws is initiated and coordinated by the Government. This process should not take more than a few months, bearing in mind that the bylaws are adopted/amended by the ministers, *i.e.,* no collective decisions are needed.

So, aiming not to overburden the text with legal obstacles, we might conclude that there are some legal obstacles for the digitalization of the administration in terms of providing electronic services. However, in the case where political will truly exists, these difficulties – which are of a formal nature – shall no longer be a problem. A holistic approach is more than ever necessary. The Government should enforce the digitalization agenda in the entire public administration and public sector. The holistic approach is emphasized for a simple reason: there would be no point to digitalize one or several public authorities while most of them are still functioning in an outdated way, since in that case the person or business might receive a digital document from one public authority which would not be accepted by another public authority, making it obsolete.[21]

[21] For instance, the person obtains a digital confirmation that he/she is a citizen of Macedonia. The confirmation is then printed out and attached to an

5.2 Challenges faced by public sector employees

A significant challenge in the digitalization journey has been the response from the existing workforce in the public sector.

First, one cannot deny that there is resistance to change on the side of the public administration. In fact, this is the case with any public organization.[22] It is difficult to quantify and precisely assess how resistant to change the public administration in Macedonia is. Yet, it is sure that resistance to change exists, especially since the authorities are reluctant to amend and modernize their bylaws so that they would be able to provide digital services.

If the digitalization laws are in force for more than three years now, why would a ministry adopt a bylaw which still requires written applications for service, on a A4 white sheet of paper? It is hardly the ignorance that is the problem; bylaws are usually drafted by employees which work on normative issues their entire careers, and they regularly follow the novelties in the legislation. As stated in a recent Macedonian publication,[23] experts in a focus group found that there is "inertia of the administration itself".

Another problem might be the capacity building and training. The employees in the Macedonian public administration and public sector are on average 46.03 years old (47.04 for men and 45.24 for women).[24] It is fair to say that individuals which are

application to receive pension. If the Pension and Disability Fund does not accept printouts of digital documents with digital signature, the citizen would again have to go to the counters of the Ministry of Interior and obtain a written confirmation for the citizenship status.

[22] Amjad & Regman (2018).

[23] Blazevski (2022) 21.

[24] Ministry of Information Society and Administration (2023) 4.

45+ might have difficulties to get acquainted with new technologies and software solutions such as the National Portal for Electronic Services. For this, they would need additional training. The competent authority to provide generic trainings is the Ministry of Information Society and Administration, as per the Law on Administrative Servants. However, the Ministry of Information Society and Administration does not include ICT technologies trainings in its annual training programs. In the annual program for generic trainings for 2023 the Ministry of Information Society and Administration included the following topics:[25] problem solving, learning and development, communication skills, achieving results, working with others, strategies and innovations, client orientation, development and progress, change management, creation and defining of policies, evaluations of programs and policies, equality and non-discrimination, regulatory impact assessment, mentorship. The very same topics were covered in the annual program for 2022,[26] 2021,[27] 2020,[28] and probably in the years before. Therefore, a vacuum exists. The Ministry of Information Society and Administration does not provide trainings which shall improve the servants' IT knowledge and skills necessary to provide digital services. Of course, the public authorities can provide specific training for their employees aside from the generic trainings by the Ministry of Information Society and

[25] Available at: https://portal.mioa.gov.mk/sites/default/files/pbl_files/documents/training/gpgo_2023.pdf.

[26] Available at: https://portal.mioa.gov.mk/sites/default/files/pbl_files/documents/training/gpgo_2022.pdf.

[27] Available at: https://obse.mioa.gov.mk/sites/default/files/pbl_files/documents/training/gpgo2021.pdf.

[28] Available at: https://obse.mioa.gov.mk/sites/default/files/pbl_files/documents/training/gpgo2021.pdf.

Administration. But not all of them have the resources for that. Also, the Ministry of Information Society and Administration does have some specific training for cyber issues, but not many of the public sector employees are covered. To conclude, the generic trainings provided to all public sector employees should include computer skills and managing the National Portal for Electronic Services, the Interoperability Portal, etc.

5.3 Limited Technological Infrastructure

The infrastructural constraints cannot be understated in the journey towards a fully digital public administration. The existing technological infrastructure has been found lacking in several aspects, including:

- Network infrastructure: The network infrastructure required to support the increased load of digital transactions is still in the development phase. However, it seems that the network infrastructure is quite weak. Even though there is no specific information, the Strategy for Public Administration 2023-2030 refers to the lack of hardware equipment and the lack of connection of the institutions with a stable internet.
- Hardware: The same citation goes for the hardware, even though there is no single analysis of the current state.

The lack of specific information in this respect strongly signals the need of an analysis, coordinated by the Ministry of Information Society and Administration and the Government (and perhaps the audit authority), of the technological infrastructure in the entire public sector, so that policies are built upon evidence, not arbitrary assessments.

6. Conclusion and recommendations for future steps

The trajectory of Macedonia's digitalization effort holds significant promise, not only in revolutionizing the nation's administrative landscape but also as a powerful tool to drastically reduce maladministration and foster a culture of efficiency. If digitalized properly, the public administration shall be more service-oriented, and citizens and businesses shall spend significantly less time and finances to effectuate their rights and legal interests. This transition, though laden with challenges, stands as a beacon of hope for instituting systemic improvements that would significantly diminish avenues for illegal activities and bureaucratic inefficiency. There is a notable potential for digital technologies to act as catalysts in restructuring public administration into a more transparent, efficient, and accountable entity.

To fully capitalize on the potential of digitalization in mitigating maladministration, Macedonia needs to focus on the following strategies which are specifically tailored to address this core objective:

1. Overcoming the legal obstacles for digitalization: Although several laws have been adopted to ensure digitalization of the public administration – the law which regulates electronic documents and eID, the LGAP, the Law on Electronic Management and Electronic Services and the Law on Central Population Registry –, there are still substantive laws and bylaws which are not aligned. These substantive laws and bylaws contain provisions under which administrative services may only be provided in writing, which is completely inconsistent with the digitalization agenda. In order to overcome the obstacle, the Government may take one of two possible approaches: (a) to issue an instruction for all public authorities that report

to it, explaining that the law regulating electronic documents derogates all provisions in other laws or bylaws which do not recognize the digital documents as valid or (b) to initiate a process for detection of all laws and bylaws which contain provisions not aligned with the digitalization laws and to amend them accordingly.

2. Fortifying technological infrastructure: A focused initiative to bolster the technological infrastructure is vital, catering not only to the increased demand but also ensuring an environment where maladministration finds it difficult to thrive.
3. Capacity building: Instituting extensive training programs to enhance the digital proficiency of public sector employees, fostering an environment where technological advancements directly contribute to reducing maladministration.
4. Holistic digitalization: A comprehensive digitalization strategy that encompasses every tier of government, including the grassroots level, ensuring uniformity in efforts to curb maladministration through digital means.
5. Public awareness and education: launching robust public awareness campaigns to elucidate the potential of digital services in reducing maladministration, thereby encouraging active citizen participation in this transformative journey.

Ultimately, this should result with: (a) many more services available on the National Portal for Electronic Services; (b) effective electronic communication between the public authorities, *i.e.,* sharing of data and documents thorough the Interoperability Portal; (c) better experience for the citizens; (d) reduced direct contact between the administration and citizens, which reduces the possibility of maladministration and is expected to increase the positive perceptions.

At this pivotal juncture, Macedonia has the golden opportunity to transform its administrative domain into a more accountable, transparent, and efficient entity. The road ahead may be challenging, but with sustained efforts and a focused approach, Macedonia can indeed usher in a future where the administration stands as a true partner in facilitating societal growth and prosperity, free of the shackles of maladministration.

Literature

Amjad A and Rehman M, 'Resistance to Change in Public Organization: Reasons and How to Overcome it' (2018) 4(1) European Journal of Business Science and Technology <https://www.researchgate.net/publication/328945263_Resistance_to_Change_in_Public_Organization_Reasons_and_How_to_Overcome_It> accessed 15 September 2023.

Blazevski T, "Administering" the Administration: Key Precondition for Reform (Methamorphosis Foundation 2022) <https://metamorphosis.org.mk/wp-content/uploads/2022/04/sledenje-na-javnata-administracija-en.pdf> accessed 15 September 2023.

Digital Mahbub, 'All about the Smart Government' (Digital Mahbub, 13 September 2023) <https://digitalmahbub.com/smart-government/> accessed 15 September 2023.

Strategy for Public Administration Reform 2023-2030 <https://www.mioa.gov.mk/content/Strategija%20RJA_MK%2003.pdf> accessed 20 November 2023.

Граѓанска алијанса за транспарентност <https://shorturl.at/eyzDK> accessed 9 September 2023.

Геразова Мујчин И, Лечевска К, Колозова К, *Дигитализацијата како пат на вистинска администрација ориентирана кон граѓаните: децентрализација на процесите како средства за забрзана и ефективна реформа* (Институт за општествени и хуманистички науки 2021) <https://www.isshs.edu.mk/digitalizacijakakopatnavistinskaadministracija/?lang=mk> accessed 15 September 2023.

Knowledge for Policy, 'Digital transformation of public administration and services.' (*Knowledge for Policy Competence Centre on Foresight*, 21 December 2021) <https://knowledge4policy.ec.europa.eu/foresight/digital-transformation-public-administration-services_en#trendteachthefuture> accessed 14 September 2023.
Law on Central Population Registry, Official Gazette of the Republic of North Macedonia no 98/2019, 275/2019.
Law on Electronic Documents, Electronic Identification and Trust Services, Official Gazette of the Republic of North Macedonia no 101/2019, 275/2019.
Law on Electronic Management and Electronic Services, Official Gazette of the Republic of North Macedonia no 98/2019, 244/2019.
Law on General Administrative Procedure, Official Gazette of the Republic of North Macedonia no 124/2015.
Davinic M*, Evropski ombudsman i loša uprava (maladministration)* (Zaštitnik građana 2013).
Министерство за информатичко општество и администрација, 'Извештај од регистарот на вработените во јавниот сектор за 2022' (*Министерство за информатичко општество и администрација*, 31 March 2023) <https://portal.mioa.gov.mk/sites/default/files/pbl_files/documents/reports/finalen_izveshtaj_za_2022_godina_30.03.2022_godina.pdf> accessed 11 September 2023.
Малеска Сачмароска Н, Гоцевски Д, *Ставови и перцепции за јавната администрација* (Центар за управување со промени 2017) <https://cup.org.mk/publications/Percepcii%20i%20stavovi%20za%20javnata%20administracija.pdf> accessed 8 September 2023.
Mojsovski A and Karai J, 'Is Macedonia prepared for digital government?' (ResPublica, 9 November 2020) <https://respublica.edu.mk/blog/politika/2020-11-09-10-52-53/> accessed 14 September 2023.
Viendyasari M, 'The Application of Digital Administration to Minimize Maladministration in Public Services: A Case Study of Jakarta Investment and One Stop Service Department' (2020) 426 ATLANTIS PRESS <https://www.atlantis-press.com/proceedings/icvhe-18/125938329> accessed 9 September 2023.

Rulebook on the format and content of the application for registration in the Register of Legal Entities which place garbage on the wholesale market, Official Gazette of the Republic of Macedonia 182/2011

Rulebook on the format and content of the application for registration in the Register of Legal which place garbage on the retail market, Official Gazette of the Republic of Macedonia 182/2011

Rulebook on the form and content of the request for issuing a license for the sale of alcoholic beverages, the form and content of the license for the sale of alcoholic beverages and the form, content and manner of keeping the register for issued and seized licenses, Official Gazette of the Republic of North Macedonia no 122/2022, 54/2023.

Rulebook on the form and content of the request for registration in the Registers of manufacturers of tobacco products and related products, the necessary evidence and documentation and the closer conditions for manufacturing of tobacco products and related products, Official Gazette of the Republic of North Macedonia no 271/2020.

Rulebook on the form and the content of the license A and B for performing tourist activities, Official Gazette of the Republic of Macedonia no 36/2013.

Rulebook on the form and the content of the template of the request for categorization of an accommodation facility, Official Gazette of Macedonia no 100/2016.

Rulebook on the form and the contents of the request for the license for development of urban plans, the form and content of the request for the issuance of an authorization for development of urban plans and the needed documentation, Official Gazette of the Republic of North Macedonia no 229/2020.

Rudranee Devi Deeljore,* Bhavish Jugurnath*

Digitalization and banks during COVID-19 crisis: a qualitative study

Abstract: Banking is at an innovatory crossroads. With the upsurge of non-financial institutions, fintech and challenger banks, traditional banks need to acclimatize to compete, and thus, digitalization is becoming more and more significant for the banking sector. The current circumstances have revealed the importance of a firm's capability to survive operative shocks and carry on with their main business. Driven by COVID-19 pandemic effects, there is a call for banking industry to speed up their digital agenda to innovate their financial products and services, and at the same time, working on the related cost reductions to shield banks' statement of financial position. Therefore, this paper offers insights about the usefulness of digitalization during COVID-19 within the banking sector. With respect to that, related to this study, semi-structured interviews were conducted with all banks operating in Mauritius (18 banks). That is, to have a clearer perspective about whether digitalization was effective for day to day business and business continuity during the pandemic, a representative from each bank is included in this study. The results reveal that digitalization has aided a lot during COVID-19. According to most of the respondents, digitalizing banking process results in quicker response rates to customers' queries, less system errors and faster onboarding for and payment of loans. Also, providing seamless payment solutions turned into an obligation as COVID-19 has speeded the trail toward a cashless society. Accordingly, digitalization should not be regarded as a conclusion, but as a medium to assure the ongoing of business. At this moment, failure to provide digital experience may lead to transfer of clients eternally to competitor banks that offer on this component.

* Rudranee Devi Deeljore is a PhD student at the Department of Law, Faculty of Law & Management, University of Mauritius, Mauritius.
* Bhavish Jugurnath is a senior lecturer at the Department of Law, Faculty of Law & Management, University of Mauritius, Mauritius.

Keywords: banks, COVID-19, digitalization

1. Introduction

Banking is at an innovatory crossroads. With the upsurge of non-financial institutions, fintech and challenger banks, traditional banks need to acclimatize to compete. Digital transformation is now a prerequisite for banks' survival. Changing customer demands together with pressure to reduce costs and increase efficiency are leaving banks with no option but to use modern technology. Banks must adapt to this change if they want to be successful. This automatically implies a constant review of the business models. Everyone has a distinct definition of digital; some associate it with artificial intelligence, while others associate it with modern tools that make life simpler and more connected. Digital is now a part of every aspect of our lives, including the way we consume, shop, work, stay in touch, and much more.

There is no doubt that COVID-19 has fast-tracked the use of digital payment to an exceptional level. For example, in year 2020, the World Health Organisation recommended to opt for contactless payments methods more and dodge cash payments.[1] To adapt to the new reality, banks have launched new efforts in response to this declaration. For instance, following the COVID-19 crisis, the rate of digital adoption in Europe increased from 81% to 95%.[2]

The shift to digital payments has also been noticeable in Mauritius during the covid19 outbreak, as evidenced by a rising usage of mobile and online banking platforms and mobile money wallet. Banks have also increased the threshold of contactless payment and have introduced many new payment

[1] Ciel (2021).
[2] McKinsey Digital (2020).

platforms to customers like MCB Juice Pro, SBM Easy Pay, and my t. bill pay. During the lockdown, Mauritius had a 200% increase in juice payments and a 50% decrease in withdrawals of cash from automated teller machine (ATMs).[3] Moreover, mobile payments have recorded an upward trend and a rise of 20% in terms of value after the lockdown.[4]

Digital transformation is the process of using pioneering technologies to respond to the shifting demands of business. It is a means to ensure swift adaption to changing situations by creating new company structure, culture or consumer services or altering existing ones. One example is E-banking, where the client can verify his/her bank balance, latest transaction, detail of account, statements, pay bills and carry out payments and purchase through internet and mobile banking.

The pandemic has highlighted the significance of a company's capacity to absorb operational shocks and carry out its main business. Digitalization is a means through which banking firms can meet their goals of protecting their statement of financial position, helping clients, and maintaining essential services. With respect to the pandemic, research is called for how well banks seized and used digitalization to their welfares. There is a need to address the effectiveness of digitalization crafted by COVID-19 because the situation is new to the world. Therefore, the purpose of this paper is to investigate how digitalization has helped the banking sector during COVID-19 crisis and till now. No such study has been carried out which would focus on the effectiveness of digitalization from the point of view of the bank. This paper allows us to highlight the lessons learned from this pandemic that can positively and definitely change the way banking services are performed, settled and transacted. Why Mauritius? Mauritius, because it is one of the most dynamic

[3] Nelito (2021).
[4] Mauritius Fintech Hub (2021).

economies in Africa with 1st position and 2nd amidst Small Island Developing State (SIDS). The financial services sector is central to the Mauritian economy contributing around 14% to GDP in year 2021.[5] Thus, this study can serve as a model among SIDS.

The remaining sections of this paper are arranged in the following order. Section 2 – digitalization and banking sector, section 3 – methodology, section 4 – findings, section 5 – analysis and section 6 – conclusion.

2. Digitalization and banking sector

A crisis causes us to reevaluate our methods of doing things, which can be disruptive at first, but will likely persist over time once we have become used to the shift. For instance, the forced digitalization created by the COVID-19 crisis provided new opportunities for experimenting brand-new digital practices.[6] In addition, the COVID-19 crisis opened up for mass markets in relation to AI technologies, ICT, and digital platforms.[7] The COVID-19 crisis has shifted financial services towards being more digital, which had a huge impact on the product offerings, the structure of payments, and the dynamics of the continuing transformations. The COVID-19 crisis has had a negative impact on the global economy and generated a sharp increase in the number of remote payment transactions. Banks are adjusting to the new world where digital technology, services, and products are dominant in order to sustain a customer base.

The term "digital transformation" refers to a radical change in how an organization operates and conducts business. The goal is to make operations more efficient and effective. The digital

[5] FSC (2022).
[6] Hacker, Vom, Handali, Otto, Schneider (2020).
[7] Ganichev & Koshovets (2021).

transformation is now required rather than an option.[8] In the current business environment, organizations must include digital technologies into their strategy; else, they risk total failure. Therefore, the banking sector's digitalization is seen as a constant issue that the sector is now confronting. The banking sector is currently undergoing a digital transformation, where the banking industry faces a disruptive digital innovation that requires the adaptation of simply all cooperative mechanisms.

In contrast to rapid digitalization, which focuses more on the quick adoption of digital services, accelerated digitalization examines how the transition is gaining speed and momentum.[9] When dealing with extraordinary occurrences like, for instance, the COVID-19 crisis, small to medium-sized businesses can benefit from using digital technology as a tool to ensure business continuity. When developing a strategy for digital technology, they place emphasis on the usage of a socio-technical approach. Examples of digital technologies being utilized to deal with the effects of severe occurrences include various collaborative technologies, 5G, blockchain, artificial intelligence, and the internet of things. Some researchers stressed the significance of having the appropriate competencies, such as organizational culture and aptitude, to ensure that digital technologies are realized in both current and future business.[10]

Even before the pandemic, it was clear that a digital banking strategy was necessary, but COVID-19 accelerated that requirement even further.[11] In some previous studies, the impacts of digitalization on banking performance and activities were underlined even before the pandemic crisis which listed

[8] Veling, Murnane, Carcary, Zlydareva (2014).
[9] Kudyba (2020).
[10] Papadopoulos, Baltas, Balta (2020).
[11] Moden & Neufeld (2020).

the availability of less expensive services, the elimination of branches, and cost savings, as well as the requirement to adapt to customers' lifestyles as the main factors that lead banks to be digital.

During the pandemic, people turned to banks to continue performing commonplace tasks like paying bills, purchasing food, and other necessities. Due to the significant and quick developments at this time, banks were forced to go fully digital, including the front end so that customers could take advantage of a cutting-edge and reliable digital interface. Banks are adjusting to the new world where digital technology, services, and products are dominant in order to sustain a customer base. Due to the low use of cash, the growing use of internet banking for many services, and the decrease in the number of physical banking firms, the digital revolution has significantly cut the operational costs of banks.

Banks can employ social media as a way to get in touch with disgruntled consumers, thereby preventing negative publicity and regaining their trust. In long-term, this can also help with brand reputation, connection building, and credibility. It may also be a helpful tool for banks to reach out to younger clients and teach them the value of saving and investing, as well as to educate and explain complicated items in a virtual and understandable manner for all types of clients. Overall, social media gives banks a chance to increase their level of transparency and obtain a competitive edge. The ability to schedule meetings online is one example of a new digital practice. One of the most obvious effects of the COVID-19 crisis was the rapid development of several information and communication technology (ICT) programs and online services.

However, forcing digitalization is not desirable because it carries greater dangers while planned digital transformation is

preferable since it offers flexibility and control.[12] That is, flexibility in how data and applications are delivered, as well as control over information security. According to the OECD, although the pandemic sped up developments in the banking industry, it could also result in higher uncertainty and lower earnings including hacking and other cyber risks. In addition, IMF predicted that as a result of the COVID-19 issue, bank loan losses would rise due to late mortgage instrument payments and business loan defaults.[13]

In addition, disruptive revolutions like artificial intelligence, nanotechnology and robots are expected to render millions of occupations obsolete.[14] However, a lot of new jobs are also going to be created or existing ones will be upgraded. Technologies are forcing individuals and organizations to change. New talents are needed, and skills are reappraised. Organisations require workers with the necessary skills to assist them deal with the complexity and speed of technological change in order to successfully navigate the challenges of digital transformation.[15]

3. Methodology

To investigate how digitalization has helped the banking sector during COVID-19 crisis and till now, this paper uses a qualitative research approach that is interviews with bank managers. Since, to investigate an individual's understanding of a phenomenon, a qualitative approach is more appropriate.[16] Using interviews to collect data gives a large space for the respondents to clarify the answers more broadly, covering full

[12] Kelkar (2020).
[13] IMF (2021).
[14] Henriette, Feki, Boughzala (2016).
[15] Sousa & Rocha (2019).
[16] Bryman & Bell (2015).

knowledge of the topic under investigation.[17] Furthermore, the interviews were designed as per Adams who stated that the reasonable maximum length for semi structured interviews to prevent fatigue for both respondent and interviewer is one hour.[18] To have balance of representatives from all banks studied, one respondent participated from each bank. In total, we have interviewed eighteen managers. To analyze the data gathered through the interviews, we used a coding scheme. By creating a coding scheme, there is a better prospect to recognize relationships. The coding scheme is centered on the analysis model and comprised of keywords and themes related to each other.[19] Then, we tried to look for a holistic patterns and themes demonstrating the respondent's experiences and answers for each element in three different sections from the keywords: before crisis, crisis management and change due to crisis.

Therefore, the empirical findings are presented in thematic order as follows: before crisis, crisis management and change due to crisis which is discussed in "Finding and Analysis".

4. Findings

4.1. Effectiveness of digitalization before COVID-19 crisis

During the interviews, it became clear that even before the COVID-19 crisis there had been ongoing effort towards a more digital business at the various banks as well as at the remote offices. However, as per the information acquired from the interviews, several of the institutions did not offer the needed level of digital solutions. The findings indicate that, prior to the pandemic, a lot of banking issues could be resolved remotely. The data also reveals that at some banks, actual meetings were

[17] Horton, Macve, Struyven (2004).
[18] Adams (2015).
[19] Corbin & Strauss (2008).

required to resolve the majority complaints of clients and the main reason why some errands could not be done remotely was several security solutions for identification.

4.2. Crisis management

As per the interviews, it was clear that banks did not have any plans for this type of unexpected crisis that is COVID-19 pandemic. However, according to the data, the banking firms have reacted very quickly and developed a strategy to deal with this unprecedented situation. In addition, banks' managers have taken the situation seriously and done as much as they have been able to. They have offered employees to work remotely, and at the offices - actions have been taken to diminish physical meetings in order to prevent the spread of the virus. Actions taken are for example, a decreased number of people allowed at the office space, hand sanitizers available and glass walls to separate customers and employees and so on. For instance, as per respondent 8 (R8) "after the lockdown period, we made sure to offer the employees with everything they needed to feel safe at the office and also develop a new plan of work where some people will be working from home and some at offices."

Moreover, as per some respondents, actions and changes have been communicated efficiently in an appropriate and clear manner. The interviewees claimed that the information had been communicated via email or online meetings. For instance, R3 mentioned that "he had a lot of digital meetings that aided him to communicate a lot of important information and details to the staff. These meetings were very successful and have also helped to gain trust of all employees that we as their employer-the bank cares about them".

4.3. Changes due to the crisis

All respondents consented on the fact that many changes had taken place. Due to COVID-19 crisis, the usage of digital tools and solutions have been rising by all banking firms throughout the Mauritius Island. Almost all respondents agreed on the fact, that even though most banks were in the process of becoming more digital, COVID-19 pandemic has put this process on fast-track and gave it an uptick in the right direction. For example, as per R5, “we have noticed that a lot of changes have occurred. Without the presence of COVID-19 pandemic, things would have been different. That is, these technological innovations would probably still be in the developing stage”. Similarly, as per R10, “initially before the COVID-19 crisis, there were more or less no digital meetings”. In addition, services such as internet banking and remote customer service by phone have improved and developed during this period. Thus, increased usage of digital tools was among the most positive impacts of the pandemic.

According to the data, many people believed that this accelerated process was mostly due to the assumption that if changes were not made promptly, they would become detrimental to the firm, and that belief caused things to move more swiftly. For instance, as per R5, “learning new things and getting started with new technology can be challenging if you are used to work in a different style. Having digital meetings is now really simple. Both on our end and the customers, there has been a shift in mentality”. Equally, according to R9, “I believe that consumers' attitudes and preconceptions have changed; even members of older generations now believe that a digital meeting is acceptable. You can now clearly observe that clients are making an effort to become familiar with mobile and internet banking services”. Thus, everyone now has an entirely new perspective on digitalization. It is now a common

occurrence. It is more of a rule now than it was before and is no longer the exception.

However, some respondents argued that due to security concerns and practical considerations like printing, not all duties could be completed from home. Many people were able to resolve this by choosing a partner for their collaboration who could alternate between being in the office and being at home.

4.4. Positive and negative impacts

The majority of the interviewees stated that although the new digital options were easier for employees to use during COVID-19, they were at first stressful and difficult to adapt to. For example, R9 explained that "even though the pandemic is bad in and of itself, it has brought about a lot of good things with the new digital solutions that banks have been compelled to develop. At first, I was anxious because I did not know how to use the available digital alternatives, but as I have learned and embraced the digital world, my anxiety has subsided".

Moreover, the respondents who held customer meetings virtually reported that their work had been significantly more productive. If you are sitting far away, it works better. The consumer will engage in less idle chatter about the weather and their summer vacation. Thus, meetings are more precise and short. In addition, there are numerous reasons why working from home or using digital alternatives makes employees more productive. For instance, when employees work from home, their coworkers will not bother them. When staff participate in online meetings, they can keep working while they wait for a customer to join in. Some respondents claimed that the crisis had little to no impact on their work. They claimed that their banks had a fantastic IT department, which had made things

simpler when the bank's employees required immediate assistance.

In addition, almost all respondents asserted that digitalization has been crucial for accomplishing certain objectives, including increased cost effectiveness, increased flexibility, seamless payment options, reduced system errors, quicker customer service response times, and shorter loan application and disbursement times. The pandemic has sped up the creation of digital solutions for many current problems. As per R9, "digitalizing many banking services and products during the COVID-19 pandemic, have aided the bank to maintain its customer base, and also tackled most of the client queries effectively".

However, some interviewees reported that they found the digital tools more challenging as they aged. It took some time for them to adjust and work effectively. While, some respondents asserted that many digital solutions have made their work easier, and they were quite appreciative of the changes that the covid19 issue has brought about for the banking industry's digital transition. The findings also show that some people, however, claimed that as banks became more digital, there were more demands placed on the relationship with customers. In addition, the research indicates that because everything needs to be documented, the new digital style of conducting business takes time. The staffs have a bad impression of this. For example, as per R13, "everything must be documented; digitization has slowed down, not sped up affairs. Every process involves a number of people". Some respondents even claimed that they would prefer not to use solutions if they were too time-consuming to use. Although the majority of employees' stress levels remained the same, several remarked that because some systems cannot be accessed from home, working from home is less effective and that some of the work instead falls on those

who are in the offices. That is, those who work in offices have more work to accomplish.

Many bank managers also admitted throughout the interviews that they lacked the socialization they experienced at work. The managers acknowledged that working from home can be isolating at times because they are unable to meet in person with clients or coworkers. Many of the participants claimed that virtual meetings are less intimate than in-person ones because the subject at hand dominates the conversation and small talk is avoided. For example, as per R1, “the digital meetings become more formal than the physical meetings; we follow the agenda without discussing the weather or the customer's vacation”.

When it came to the COVID-19 crisis, several employees were unable to say if using digital solutions helped or hurt their productivity. The reason was that it appeared to have turned into a job to instruct clients in how to carry out their tasks online, and some clients were unable to handle the digital substitutes and still need real office visits. Other interviewees also mentioned that it occasionally became the staff's responsibility to fix customers' errors when they themselves attempted to complete their tasks digitally. Employee stress levels grew as a result of having less time to devote to other responsibilities. Despite the fact that most people concur that the improvements brought about by technology have made their jobs simpler, they nevertheless see room for improvement.

5. Analysis

Digitalization is crucial for accomplishing certain objectives including increased cost effectiveness, increased flexibility, safe working from home, seamless payment options, reduced system errors, quicker customer service response times, and shorter loan application and disbursement times. The pandemic

has sped up the creation of digital solutions for current problems like quickly assessing credit and market risk trends or keeping employees interested and productive while working from home. New payment methods have also been made available by the advent of online banking applications, with the benefit that they are effective ways to complete transactions in a straightforward manner. Banks are the ones that must undergo digital transformation and they need to assert that they provide open, transparent, and simple-to-use services at prices that are lower than those of traditional services. Only if the bank serves as their partner and provides them with an accessible interface and greater security, then the customers will be encouraged to adopt digital services.

An increase in IT spending is necessary as digitalizing key business processes becomes increasingly necessary to protect operational resilience and customer relevance. Digital technologies are the best option, but they cannot completely replace the human component of social connections. To be able to complete operational activities remotely and in accordance with rules and regulations, employees must feel invested in their team. Banks must keep providing excellent customer service, while using technologies that track consumer requests or excellent, error-free digital experiences. These technological advancements are crucial for keeping the organization's entire workforce and customers linked.

However, to counter the increasing digital traffic, danger of phishing attacks, and email fraud brought on by remote work, banks must maintain strong cyber security. They should also aim to reduce associated costs by moving to the cloud to protect their statement of financial position.

6. Conclusion

The findings show that digitalization played a significant role in COVID-19. The majority of respondents claimed that digitizing banking processes led to speedier client query responses, fewer system problems, and quicker loan application and repayment processes. Additionally, as COVID-19 has accelerated the transition to a cashless society, delivering frictionless payment options has become a requirement. Digitalization should therefore not be seen as a conclusion, but rather as a tool to ensure the continuation of the company. Right now, failing to provide a digital experience could result in customers switching to rival banks that do. However, there is a critical need for cost-cutting measures that may be accomplished through optimizing application landscapes. Therefore, the banking industry needs to modify some of its traditional practices, and thus all these developments will show how the banking system will appear in the future.

Literature

Ciel Finance, 'Banking on digital channels to get ahead in the new normal' (03 August 2021) <https://www.cielgroup.com/en/news/2021/banking-on-digital-channels-to-get-ahead-in-the-new-normal> accessed 18 September 2023.

Fernandez S, Jenkins P, and Vieira B, 'Europe's digital migration during covid19: getting past the broad trends and averages 2020' (McKinsey Digital, 24 July 2020) <Available: https://www.mckinsey.com/capabilities/mckinsey-digital/our-insights/europes-digital-migration-during-covid-19-getting-past-the-broad-trends-and-averages> accessed 18 September 2023.

Nelito, "The future of digital payments in post covid Mauritius," 2021. [Online]. Available: <https://www.nelito.com/blog/the-future-of-digital-payments-in-post-covid-mauritius.html> accessed 18 September 2023.

Mauritius Fintech Hub, "The future of digital payments in post covid Mauritius," Mauritius/Africa Fintech Hub, 2021. [Online]. Available: <https://mauritiusfintech.org/blog/opportunities-challenges-fintech-post-covid-mauritius-future-digital-payments/> accessed 18 September 2023.
FSC, "Financial Service Commission, Contribution to GDP," 2022. [Online]. Available: <fscmauritius.org/en/statistics/contribution-to-gdp> accessed 18 September 2023.
Hacker J, Vom B. J., Handali J, Otto M, and Schneider J, 'Virtually in this together how web-conferencing systems enabled a new virtual togetherness during the covid19 crisis' (2020) Vol(Issue) European Journal of Information Systems 563.
N. A. Ganichev and U. B. Koshovets, "Forcing the digital economy: how will the structure of digital markets change as a result of the covid19 pandemic," Studies on Russian Economic Development, pp. 11-22, 2021.
L. Veling, S. Murnane, M. Carcary and O. Zlydareva, "The Digital Imperative," IVI White Paper Series, pp. 1-6, 2014.
S. Kudyba, "Covid19 and the acceleration of digital transformation and the future of work," Information systems management, pp. 284-287, 2020.
T. Papadopoulos, K. N. Baltas and M. E. Balta, "The use of digital technologies by small and medium enterprises during covid19: Implications for theory and practice," International Journal of Information Management, pp. 1-4, 2020.
N. Moden and P. Neufeld, "How covid19 has sped up digitization for the banking sector," 2020. [Online]. Available: <https://www.ey.com/en_gl/financialservices-emeia/how-covid-19-has-sped-up-digitalisation-for-the-banking-sector> accessed 18 September 2023.
R. Kelkar, "Forced digital transformation: Rethink, reimagine, redefine," 2020. [Online]. Available: <https://cio.economictimes.indiatimes.com/news/strategy-and-management/forced-digital transfornation-rethink-reimagine-redefine-> accessed 18 September 2023.
IMF, "Policy responds to covid19," 2021. [Online]. Available: <https://www.imf.org/en/Topics/imf-and-covid19/Policy-Responses-to-COVID-19> accessed 18 September 2023.

E. Henriette, M. Feki and I. Boughzala, "Digital Transformation challenges MCIS 2016 proceedings," The Mediterranean Conference on Information Systems, pp. 4-6, 2016.
M. J. Sousa and A. Rocha, "Digital Learning: developing skills for digital transformation of organisations," Future generation computer systems, pp. 327-334, 2019.
Bryman A and Bell E, *Business research methods* (4th edition ed., Oxford: Oxford University Press 2015).
J. Horton, R. Macve and G. Struyven, "Qualitative Research: Experiences in using semi-structured interviews," The real life guide to Accounting Research, pp. 339-357, 2004.
W. Adams, "Conducting Semi Structured Interviews," Handbook of Practical Program Evaluation, pp. 492-505, 2015.
Corbin J and. Strauss A, *Basic of Qualitative Research: Techniques and procedures for developing grounded theory* (3rd Edition ed., Thousand Oaks: CA: Sage 2008).
World Bank Group, "Ease of Doing Business report," World Bank Group flagship, Washington, 2020.
Bryman A and Bell E, *Business Research Method* (Oxford University Press 2007).

Aliz Fabian*

Artificial intelligence as a mediator?

Abstract: The subject of this study mainly focuses on the possible usage of artificial intelligence during mediation session by summarizing the latest mediation practice in the USA. The present study is divided into three main pillars following the introduction: the first part provides information about the mediation process in general, the second part provides deeper analysis into the current state of artificial intelligence technology, especially in mediation, and the third part describes the responsibilities of a mediator and the requirements of a good mediator, and simultaneously presents some current examples. This study is aiming to define the main divergences, as well as strengths and weaknesses of a human mediator and a robot-mediator. As a result of the comparison of these, we can better understand the opportunities which can be incorporated into the mediation session in the near future.

Keywords: ADR, artificial intelligence, mediation

1. Introduction

'Good morning. My name is Sophia robot. I will be your mediator this afternoon. I would like to thank you for being here. It is the first positive step in this process. By working together, I am hopeful that both of you will be able to resolve the issues that brought you here today.'[1]

Is it hard to imagine the above situation, that an artificial intelligence (hereinafter referred to as 'AI') is indeed ready for

* Aliz Fabian is a PhD student at the Eötvös Loránd University, Faculty of Law, Department of Labour Law and Social Law; E-mail: lizifab97@staff.elte.hu.

[1] Sample Mediator's Opening statement according to experience of the author as mediator and observer.

leading a mediation process. For instance, Sophia is one of the most famous robots in our days. She can answer questions and she looks like a human being in a video published in 2019.[2] She can analyse information more rapidly and in a much wider scope than any human.[3] It can be easily hypothesized that the same discussions with humans will be achievable with an AI in the immediate future.

On the other hand, there are some significant peculiarities in a mediation process which make the usage of an AI mediator questionable in alternative disputes. First of all, the presentation of the facts and the basis of the dispute by the parties from their point of view is one of the major parts of the proceedings. This specific section of the mediation can be emotionally demanding, sometimes chaotic. Are we confident about the hypothesis that an AI is able to think creatively and show empathy while listening to the contradictory allegations while simultaneously it is trying to summarize the opening speech of the parties? The mediation process is much more than a discussion between the parties without the need of arbitrators or judges. The mediator as a third party plays a significant role in these proceedings, since the parties expect the mediator to be *e.g.* a facilitator, an opener for communication channels, a problem explorer, a resource expander, *etc.* at the same time.[4] If the parties do not find the usage of an AI mediator trustworthy or they do not feel that they have been actively listened to by the mediator, then this perception can lead to the end of the mediation process without a solution or a settlement agreement in the parties dispute.

Since the purpose of my paper is comparing the advantages and disadvantages of an AI mediator, I would like to describe my

[2] CGNT America (2019).
[3] Kumar & Kumar (2021) 1477.
[4] Moore (2003) 19.

analysis in three different sections. The first part provides information about the mediation process in general. The second part provides deeper analysis into the current state of AI technology. And the third part describes the responsibilities of a mediator and the requirements of a good mediator and simultaneously allows to present some current examples. In addition, my alternative suggestions in accordance with the usage of an AI in the field of alternative dispute resolution and in business life are specified in the summary section.

2. Mediation as one of the alternative dispute resolutions

2.1. Short explanation of the system of alternative dispute resolution

Alternative dispute resolution (hereinafter referred to as 'ADR') refers to the different methods people 'can resolve disputes [with] in a broader framework than the traditional litigation process'.[5] This broader framework leads to the situation that the parties can choose among a number of different proceedings if their aim is the avoidance of judicial proceedings either at the time when the dispute arises or after the claim was submitted to the court. The classical categorization of ADR is the following: (i) negotiation, (ii) mediation and (iii) arbitration. In addition to the mentioned general classification of ADR proceedings, one other classification exists according to the purpose and main characteristics of these procedures. Allow me to provide this classification, pursuant to the USA Minnesota Court Rules: (i) facilitative, (ii) evaluative, (iii) investigating, (iv) hybrid, and (v) adjudicative proceedings.[6]

Mediation is a facilitative process in which a neutral third person facilitates communication and negotiation to achieve

[5] Nolan-Haley (2021) 275.
[6] General Rules of Practice for the District Courts Minnesota (1992) r. 114.02.

voluntary decision making by the parties to the dispute.[7] However, the decision making of the parties is generally understood as concluding an agreement between the parties at the end of the mediation session. It should be highlighted that decision making also means the opportunity of the parties to decide about continuing or finishing the mediation process provided by the court, 'including whether they wish to ultimately resolve the matter, as well as the terms of any resolution'.[8] In my experience, a mediation especially assists the parties to communicate more effectively to each other, to understand better the other's party perspective and intentions, to overview their alternative options to a mediated agreement or in litigation, therefore they can analyse the dispute and their legal opportunities carefully. These characteristic of the mediation process would be significant when we discuss the strengths and weaknesses of the usage of an AI during mediation later in this paper (*e.g.* is it sufficient *per se* if an AI can analyse summaries of the court-cases faster than a human).

In comparison with mediation, arbitration belongs to the adjudicative proceedings in which an arbitrator renders an award after an adversarial hearing at which each party and its counsel has the opportunity to present its position and legal arguments regarding the case. On other category of the ADR proceedings is the evaluative proceedings *e.g.* a 'non-binding advisory opinion' process in which a third person who issues a non-binding advisory opinion regarding liability, damages or both, after the parties and their counsel presented their position. Mediation and arbitration can be combined ('med-arb' as a hybrid procedure) in which a third person mediates the dispute firstly, and in case any impasse occurs, the rules of arbitration should be applied. These examples provide some insights to the

[7] General Rules of Practice for the District Courts Minnesota (1992) r. 114.02. s. (c)(1).
[8] Kovach (2014) 36.

ADR proceedings. The mediation process is analysed deeper below.[9]

2.2. The main stages of the mediation process

Even though, the stages of the mediation process depend primarily on the procedural regulation of the court or of the organisation, the parties, the matter of the dispute, the style of the mediator (*e.g.* 'facilitative, evaluative or transformative approach'[10]), there is a basic model according to Kovach, which assists the better understanding of the dynamic and challenges of the mediation process. It consists of the following stages: (1) preliminary arrangements, (2) mediator's opening speech, (3) opening statements by the parties, (4) collecting information, (5) identification of issues and interests, (6) generating options, (7) bargaining and negotiation, (8) drafting and concluding an agreement, (9) closing.[11] Highlighting the main characteristic of each stage, it can concluded that preliminary arrangements include all organisational matters, which are obligatory or recommended for holding a mediation session (*e.g.* selecting the procedure of the mediator, the name of the parties, the matter of the claim, whether lawyers will represent the parties, if there is an observer who has to be accepted by the parties, whether pre-mediation is involved in the process, expected fees of the mediation, drafting and reviewing the agreement to mediate *etc.*). It is interesting that the theory and the practice can deviate from each other regarding the preliminary part of the mediation session. According to my experience, it is one approach if the appointed mediator of the mediation obtains knowledge about the dispute of the parties which is absolutely necessary for the beginning of the mediation process to avoid

[9] General Rules of Practice for the District Courts Minnesota (1992) r. 114.02. ss. (a)(1), (b)(2), (c)(2).
[10] *See* Moffitt and Schneider (2008) 52-58.
[11] Kovach (2014) 41.

any impartiality or misinformation.[12] On the other hand, it is also possible to hold pre-mediation session in order to prepare the effectiveness of the mediation session and to plan a schedule in which there are five stages before the opening speech of the mediator, which are the following: (1) establishing relationship, (2) selecting strategy, (3) analysing background, (4) designing detailed plan, (5) building trust and cooperation.[13]

If the pre-mediation session is not part of the procedure, the mediator's opening statement should provide enough information about the mediation session, especially about the mediator's role as guardian of the process, and about the role of the parties, who are responsible for the content of the mediation. The mediator should explain the ground rules of mediation such as confidentiality of the session and enforceability of the mediated agreement and set out the housekeeping rules (*e.g.* the parties should ensure uninterrupted time to each other, the aim is a respectful conversation between the parties, *etc.*). The main goal of this stage is that the parties can gain detailed information and positive thoughts about the procedure, and they are able to ask questions about the agreement to mediate. Reaching and signing of the agreement to mediate is the absolutely necessary pre-requirement for the continuation of the mediation session.[14]

In the next step, the opening statements of the parties should provide the opportunity for them to explain the issue from their own perspective without the obligation to reflect on the points, argumentation of the opposing party. These opening statements especially focus on the positions of the parties (*e.g.* first party's position is that the second party has to pay $ 8000, *i.e.* the whole

[12] According to experience of the author as mediator and observer. (Rezler-scholarship and voluntary court mediation program, Bernalillo County Metropolitan Court, New Mexico, US).
[13] Moore (2003) 68-69.
[14] Bernalillo County Metropolitan Court Mediation Division (2019) 17, 30.

sum of the claim which was submitted to the court, but the second party's position is that the full refund is unfair, and the second party is ready to pay only $ 1000 from the claimed sum). After that it is possible to collect more details about the dispute, however it should be highlighted that the mediator is not a fact-finder, therefore the mediator should focus on the 'underlying interests'[15] of the parties, which are usually deeply hidden and it is uncertain whether the parties are aware of it or not. To understand the difference between the positions and interests of the parties, allow me to present the following example: we can imagine a dispute between the tenant and the landlord of the premises the tenant leases in accordance with a compensation of damages which was caused by an accident in the landlord's flat. Both parties reflect only on the amount of the payable compensation, but the interests provide deeper insight about what are the underlying reasons of the parties' actions, *e.g.* for example the landlord would like to avoid any precedent that leads to the consequence that landlords are responsible for every damage incurred in the flat; or the tenant is a disabled person and he/she has experience with discrimination because of his/her disability, therefore the tenant feels that the landlords claim would not exist if she/he would be a not-disabled person.

If the discussion of the parties moves from the past-focused explanations to future-focused problem solving, it is possible to generate options and start negotiations between the parties to reach a mediated agreement. Although the stages of the mediation session appear to be linear, impasses occur frequently. In this case, each party can meet with the mediator individually (caucus) and overview their alternative options,[16] or their realistic ways of achieving their goals to move away from their unrealistic positions. On the other hand, it is also

[15] Kovach (2014) 43.

[16] An example for reality testing as follows what are the consequences for you if today is not reached an agreement?

conceivable according to my experience that the parties already start their opening speech with a realistic and acceptable offer towards the other party. Occasionally the parties may conclude an interim agreement which may include their potential agreement and the time limit/deadline for a final decision, or they may enter into an only partial agreement which covers the agreement in some aspects of their dispute but the unsolved part of their dispute would remain for litigation. It is worth highlighting that the mediated agreement shall be as specific and detailed as possible as it would be a legally binding and enforceable agreement between the parties. The central part of a mediated agreement is especially (i) the agreement on the payable total amount, (ii) payment method and procedure to follow (*e.g.* via bank transfer, cash, check) and (iii) the deadlines for the performance of the obligations by the parties (*e.g.* payment until 10th of next month or monthly payment payable for eleven months in equal instalments). In the end of the mediation session, the mediator assists the parties typing, wording the mediated agreement, like in the following example: the parties agree that Party A will pay a minimum of $250 via bank transfer to Party B until 10th of each month, starting September 2023. Party B will provide a proof of receipt of the monthly payments as well as a receipt when the full payment ($ 2500) has been received via e-mail. The parties stipulate that if the terms of the mediated agreement is not fulfilled, the parties reserve their rights to ask the court to reopen their case within 5 years.[17]

[17] Bernalillo County Metropolitan Court Mediation Division (2019) 26-33.

3. The main characteristics of an AI

3.1. Definition and categorization of an AI

After understanding the general process of mediation, it should be clarified how can AI be defined and how can we summarize the current state of the technology in order to analyse the strengths and weaknesses of an AI mediator. In one aspect, 'AI is the ability of a computer or robot to do all of the activities that need human intelligence'.[18] Other authors define AI as 'intelligent automatic systems that arrive at results and take actions without human intervention'[19]. Although, an AI could exist in a variety of physical forms, it should be highlighted that that an AI should have 'the intellectual capacity of the software'[20] which is a more significant obligatory component than the type of the physical form. One of the classical categorization distinguishes groups according to the abilities of the technologies as follows: (1) technologies with physical enablement (*e.g.* platform, sensor), (2) methods with ability to learn (*e.g.* decision tree algorithm, regression analysis), (3) machine learning with ability to learn, (4) artificial intelligence with the ability to sense, reason, engage and learn (*e.g.* voice recognition, natural language processing (hereinafter referred to as 'NLP'), robotics and motion, knowledge capture).[21] Furthermore, there is a categorization according to the automation levels of the AI, which provides different opportunities for humans to intervene into the process instead of or in favour of an AI. The sphere of possibilities is the following: 1. only assistance, 2. partial automation, 3. conditional automation, 4. high automation 5. full automation.[22]

[18] Kumar & Kumar (2021) 1474.
[19] Morse (2019) 217.
[20] Larsen (2010) 107.
[21] Draper (2019) 120. *See also:* van Duin & Bakhshi (2017).
[22] Draper (2019) 129. This model refers originally to the self-driving vehicles.

How can we interpret these concepts regarding the mediation process?

Even if an AI would provide assistance to a mediator, it would mean that the mediation process would be fully controlled by the mediator, but some assistant features would be built in the process, which would be provided by AI. In case of partial automation, the features would be shared between the human mediator and the AI mediator, but the human mediator should remain engaged with the mediator's tasks and monitor the procedure at all times. Conditional automation would provide an opportunity for the human mediator to take one step back and he/she would not have to control the process at all times, but simultaneously the mediator should be ready to take the control back if he/she receives a notice from the AI's system. The difference between the highly automated process and the fully automated process is only that the AI mediator is capable of all mediator's tasks under certain conditions or under all conditions. The human mediator may have the option to control the mediation process in both cases.

3.2. The current state of technology

It should be also taken into consideration that the current state of technology already provides more platforms than an online dispute resolution system (hereinafter referred as 'ODR') for the parties, which can be defined as a cloud-based, case-management and communication software for resolving disputes. One of the most famous software is IMMEDIATION.[23] This software ensures among others role-based (claimant, respondent, witness) access to relevant materials and mediation sessions, the possibility to show evidence, the possibility to open the counsel rooms for private

[23] Rajendra & Thuraisingam (2022) 182.

meetings and increases the efficiency of collaboration with white board, chat functions, the possibility of co-drafting of a mediated agreement, e-signing and payment function.[24] Although it is visible that a wide range of assistant tasks are built into this software, however, a human mediator can control the parties and the process at any time, therefore IMMEDIATION operates between the assistance and the partial autonomy level according to the categorisation described above. Draper confirms that 'the ODR world is likely already 30-50% of the way towards full automation'.[25]

In comparison with the actual state of development of ODR, the 'Lodder-Zeleznikow three step model'[26] declares stronger efficiency and higher automation requirements towards an AI. First of all, the system should provide information about other alternative opportunities of the parties if a mediated agreement is not reached at the end of the session, *e.g.* the program should calculate the best alternative to a negotiated agreement (hereinafter referred to as 'BATNA') of the parties. Moreover, the program should facilitate to resolve conflicts with the assistance of argumentation and dialogue technics. Thirdly, if any issue would remain unsolved until this point, the program should offer decision analysis techniques and trade-off strategies, and if the parties are not satisfied with the results of the process, the tool should repeat the second and third step of the process until the dispute is resolved.

It is clear that an AI is able to generate and analyse options faster, however, the real question is how can an AI mediator facilitate the communication between the parties and is it able to use dialogue technics? Allow me to provide the following example: if any impasses occur, a human mediator attempts to

[24] Immediation (2021).
[25] Draper (2019) 129.
[26] Lodder & Zeleznikow (2012) 62.

summarize the aspects of the conflict in a more neutral language and attempts to clarify which can be a common path between the parties, and tries to move forward. Technically, an NLP processor is able to find and solve disagreements and use each of the above-mentioned tools in case of impasses.[27] According to Draper's example if an NLP AI mediator detects that there are two statements (B, C) which are in conflict with each other but also with an agreed statement (A), it could be trained to propose for example the following questions: as (i) 'Can you more fully explain what comment C means? (ii) Do you see relationship between B and C? (iii) Is there a way that B could be incorporated into A? (iv) If C were added into B, could it be incorporated into A? (v) Team 1, could you clarify…? (vi) Team 2, could you propose…?'[28] We can interpret this example as follows: party A states that the house was fully cleaned based on the lease agreement at the end of the lease, while the other party argues that the house was in a messy condition during a handover procedure. The common path is that the parties agree that the lessees were cooperative at the beginning of the lease, however the original condition of the house was not as clean as it is expected from the lessees.

4. Strengths and weaknesses of an AI mediator

4.1. Requirements of a good mediator

First of all, it is worth highlighting that a mediator has to fulfil many criteria if the parties would like to involve the mediator in the negotiation process. The most important requirements are observed in the Mediation Services Agreement, in the opening statement of the mediator and in the Mediators Code of Ethics such as the Model Standards of Conduct for Mediators.

[27] Draper (2019) 127.
[28] Draper (2019) 127.

The most essential requirement is impartiality. It means that the mediator does not represent either party, he or she is a neutral third party whose only task is assisting the parties in reaching a resolution regarding their problem. The Model Standards of Conduct for Mediators declares that 'impartiality means freedom from favouritism, bias or prejudice'.[29] It should be appreciated that an AI has the characteristic advantage in this particular field. According to Kahneman there are a lot of psychological impacts (for example halo effect, norm theory, self-control) which the human brain cannot avoid.[30] An AI does not have this emotional liability towards the parties, and it cannot be affected emotionally or in any other way neither by the parties in dispute nor by their representatives. For instance, an AI will provide equal time for each party when caucusing which can be emotionally significant when the other party has to wait alone for a private session with the mediator in a waiting room. Further example is, if one party is represented by a lawyer, but the other party do not involve any legal specialist and the mediator happens to be a qualified lawyer, it is hard to concentrate on his/her role as a mediator instead of involving himself/herself and acting in the process in favour of the unrepresented party. On the other hand, it can be also argued that the complete exclusion of biases or conflict of interests do not exist. Even if an AI mediator assists in the mediation, its mediator skills (*i.e.* programmed existing data and algorithms) only depend on the biases of its creator and sponsors. For instance, in case of a software programmed by the government, it can be a goal that the agreement will not be challenged by the parties and they do not burthen the civil courts with their case.[31]

[29] The Model Standards of Conduct for Mediators (2004) Standard II.A.
[30] Kahneman (2013) 54, 99.
[31] *See* an example regarding the differences in decision-making for an AI software purchased by government or a private market, Morse (2019) 215-216.

The next point which has to be taken into consideration is the requirement of confidentiality and how an AI can use, store and protect the client's data. Since several confidential information may be presented during the mediation process, the Model Standards of Conduct for Mediators declares that 'a mediator shall maintain confidentiality of all information'.[32] Furthermore, the mediator should not provide any information to any non-participants about how the parties acted during the mediation. Moreover, the mediator should protect the anonymity of the parties at all times. The mediator should sign a non-disclosure agreement on several occasions or it should be the part of the mediation services agreement, for example according to the following clause: 'the mediators will not reveal what was said in the mediation except (as required by law) to report suspected child abuse, threat of physical harm, or threat of damage to property, the parties agree all notes taken during the mediation will be thrown away at the end of the session'.[33] It provides a major guarantee for the parties, since a lawsuit can be initiated against the mediator in case the mediator breaches the contract for mediation. In my opinion this opportunity of accountability is non-exhaustive in case of an AI mediator. Hacking, viruses can occur disturbing the process, and the parties cannot supervise the gathering, storage, archiving and dissemination of all client data.[34] For example, who can ensure that an unauthorized third person is not involved as an 'observer' during the mediation session to collect some data which shall not be disclosed or is confidential?

Moreover, 'a mediator shall conduct a mediation based on the principle of self-determination'.[35] Party-self-determination means that the parties can act voluntarily, freely and in an

[32] The Model Standards of Conduct for Mediators (2004) Standard V.
[33] Bernalillo County Metropolitan Court Mediation Division (2019) 30.
[34] Kumar & Kumar (2021) 1478.
[35] The Model Standards of Conduct for Mediators (2004) Standard I.A.

uncoerced way during the whole mediation process. They have a well-informed choice to select a mediator, design the process, and withdraw from the process or its possible outcomes, if they intend to. An AI mediator might ensure better compliance with the principle of party-self-determination or the fairness of the procedure, since an AI can provide detailed preliminary information about the process (for example with the assistance of chatbots). Furthermore, the robot mediator can generate enormous amount of agendas and reasonable options almost immediately for the parties if it detects that it is required in the procedure. The robot mediator cannot have influence on the parties, for example regarding higher settlement rates, egos, increased fees. However, the danger of external influence has to be taken into account as well, which can also depend on the programmers of the AI's software.

However, should the parties claim that their AI mediator proceeds against the standards of mediation or they submit their request for deeper explanation of the mediator's moves, Morse argues that the system 'gives robots, more than humans, incentive to avoid any request to explain why they did what they did',[36] which leads to the absence of accountability in case of an AI mediator.

Although it seems to be that an AI mediator can fulfil most relevant criteria, the question arises if an AI is indeed able to act *inter alia* as a 1) a chairperson, 2) a communicator, 3) an educator, 4) a translator, 5) a resource expander, 6) an agent of reality, 7) a guardian of durable solutions, 8) a scapegoat, 9) a trust builder, 10) a protector of the process during the mediation in reality.[37] On one hand some authors argue that 'these tasks require creative intelligence, which is beyond current AI

[36] Morse (2019) 216.
[37] Bakken (2020).

capabilities'[38], on the other hand there have been several experiments which presented that AI systems can communicate empathy towards medical patients.[39] Therefore it is worth deeper analysing the necessary communication and problem-solving skills of a mediator.

4.2. Data analysing versus facilitation of communication between the parties

Returning to the stages of the mediation, according to my experience, the stage of exchanging information between the parties and creation of a future-focused environment is one of the hardest tasks in the process. There are a number of factors, for example excessive feelings, intensive interpretation of dispute, short, inaccurate and accusingly discussion which hinder the parties to move forward from their negative thoughts. The mediator should operate with special communication techniques to assist facilitating the communication, and try to decrease the psychological damage resulting from their discussion with the following: summarization, reframing, active listening, grouping, probing question, *etc.*[40] Providing a short summary by a mediator allows the other party to focus better on the main content of the speaker party's statement, while the speaker has an opportunity to add and clarify his/her view of the dispute. Reframing means such a technique when a mediator restates the content of the party to himself with other words (for example without negative tone or with focusing on common interests). Allow me to present the following example: if party A states that she would not like to work together with her co-worker in the future on the basis that party A finds her co-worker a liar, the mediator can reframe that it sounds like trust is important to you, especially at the workplace and it seems

[38] Rajendra & Thuraisingam (2022) 180.
[39] Larson (2010) 110.
[40] Moore (2003) 228.

that you need to trust party B again to continue working together.

Active listening ensures a communication technique 'when the mediator decodes a spoken message and then feeds back to the speaker the emotions of the message'. [41] The aim of active listening is for the parties to feel that (i) they have been heard by the mediator and (ii) their feelings are real without judgement and (iii) their claim is based on a justified ground from their perspective, which assists them moving forward from their intensive feelings to possible rational solutions. To understand better the necessity of active listening, allow me to analyse the following example: 'That made me so angry that all I can think of is the reason why I wasn't offered the position is because I'm a woman … I thought I could trust my boss. I thought I worked for a good company and you know … All my hard work for the past eight years has been … I'm just not sure what to do'.[42] If I would be the mediator in this case, I would summarize the circumstances as follows: it looks like you are frustrated and simultaneously disappointed since it seems that you are a hard, trustworthy employee and you have been working for this company for eight years until now, therefore you expected a promotion for a better position in the company, but instead of you the company offered a promotion to your co-worker. You are feeling betrayed and distrusted by the decision of your direct superior since you thought your work experience and your workplace attitude matters a lot to the company, but you feel that man get more privileges at your workplace even if they do not necessarily deserve it. Therefore, you are unsure about your role in the company now. If the speaker says 'exactly' it means that this part of active listening by the mediator was successful. Furthermore, with the assistance of grouping, the mediator is trying to identify common issues and

[41] Moore (2003) 228.
[42] Simon & West (2022) 17.

tries to structure them in a logical manner. For instance, if party B (the direct superior of the speaker) confirms that the speaker is a very good, efficient, trustworthy employee, it could lead to the consequence that the personal ability of the speaker as a co-worker is not questioned and the parties can focus on the process of the selection or what was the real intention of the direct superior for promoting another person instead of party A. Probing question provides an opportunity for the mediator to ask open-ended questions to facilitate the generation of new ideas, for example in the following way: if you would have a magic wand which option would you create to solve this situation?[43]

The above-mentioned examples confirm that an AI mediator should try to catch human emotions and reflect on them even if the emotions of the parties cannot be programmed in advance during the mediation session. Other authors argued that 'AI is able to perform routine tasks, it is limited in solving complex problems where there are no pre-existing data'.[44] On the other hand, there are positive examples which show that it is possible for an AI to pay attention for the feelings of others. Firstly, we should try to imagine a therapeutic robot which was programmed to interact with autistic children.[45] This interaction was inhered in social cues as gaze direction, expression, vocalization, which in the therapeutic context has a positive effect on children. Furthermore, 'conversational agents' could assist old patients in reaching more steps by walking or taking the daily drugs with the assist of a dialogue. Several users reported that they felt caring effects from the robot.[46]

[43] Lightsey (2022) 50.
[44] Rajendra & Thuraisingam (2022) 180.
[45] Larson (2010) 117-118.
[46] Larson (2010) 122.

However, these studies also found a problem which is that the AI often repeated the same questions, which lead to unexciting conversations and the decrease in the concentration of the patients. In my opinion this default is a real problem regarding mediation as well. What will happen if the parties have a question to the mediator after the opening speech for example regarding the agreement to mediate, but the acting AI mediator does not understand the question of the parties and the whole procedure breaks down? According to Sophia's robot interview if the parties ask ambiguous questions (*e.g.* 'Sophia do you think you are free or a servant, … Sophia did someone tell you to say that')[47], the conversation simply ends.

In case of the second part of the mediation session, an AI mediator is able to better benefit from its analysing skills. An AI mediator can faster create relevant documents, summaries, analyse possible options, and if the parties agree, the drafting section of the mediated agreement may also be delegated.[48] However, it sounds great that the parties can dictate loudly their possible mediated agreement, it is also a fear that the possible solutions provided by the AI mediator will be fixed (for instance: 'split the difference'[49] between the two offers by the parties) according to standards that would mostly harm one of the most important benefit of mediation, *i.e.* the opportunity to create new solutions and that the parties can and should always control the outcome of the process.[50]

5. Conclusion: Co-mediation as a solution?

In conclusion it should be highlighted that a human mediator has a significant advantage in the field of emotions and of

[47] CGNT America (2019) 3:30-4:35.
[48] Kumar & Kumar (2021) 1476.
[49] Thompson (2014) 72.
[50] Sander & Rozdeiczer (2005) 393.

communications skills as the above-mentioned examples showed. A human can feel *e.g.* if strong emotions may block open communication, and can advise the parties the caucus as a private meeting with the mediator. On the other hand, the AI mediator can analyse data, outcomes of the process quicker in a cost- and time- efficient way, and it seems to be more neutral than a human. Taking into consideration the distribution of the strengths of a human and an AI mediator, I would recommend co-mediation as a solution, which would be an approved solution by other authors as well for example in the field of co-arbitration. 'From a legal standpoint, it is observed that although AI is able to complement these tasks efficiently, human arbitrators should always supervise and review solutions to avoid erroneous mistakes'.[51] Co-mediation provides an opportunity when a human- and a robot mediator can mediate together, they can both strengthen the whole mediation process in the fields they are best and fill-in each other's weaknesses.

To understand co-mediation better, the main benefits of this model can be summarized as follows: (1) it ensures more insight of the case, since mediators can concentrate more on the needs of the parties (mainly their emotional and psychological needs), (2) it provides shared workload and specific expertise if a human mediator leads the first part of the mediation session, and an AI mediator is responsible for the second part of the session. Furthermore, (3) each of the gender, cultural or rational discrimination issues during mediation might be solved. Moreover, it also helps to work with a mediator with (4) a complementary/mixed style, since an AI mediator gets used to the human mediator's style.[52]

However, there are some difficulties which might occur regarding the model of co-mediation. First of all, preliminary

[51] Rajendra & Thuraisingam (2022) 183.
[52] Bernalillo County Metropolitan Court Mediation Division (2019) 7.

discussion or session is required to be held between the co-mediators in practice in order to prepare more effectively for the mediation session, and to get to know each other's mediation style better. It allows to discuss and also to explain for example: how can the other mediator define a successful mediation, how can the co-mediators share their opening statements, how can they solve the situation when the intensive feelings of the parties come out, who considers himself/herself a more active or a more passive mediator?[53] For instance, I tend to define a successful mediation as a process when the parties are able to move forward with their case, they can generate options, they understand better intentions, reasons of the other party, and if they can make a conversation with each other in a productive way. On the other hand, a robot mediator might define a successful mediation as a process when the parties can reach an agreement within 2 hours. The open question is that how can we collaborate together?

In conclusion we should mention that the parties have to trust in the mediation process and they should participate in the procedure actively to solve their dispute. If an AI is suitable for promoting the mediation process, why would anyone want to stop it? However, it seems that an AI mediator will not hold mediation sessions in the close future since at the current state of AI software are not suitable for leading a whole mediation session without human intervention as described above. Finally, in my opinion the parties generally would be reluctant to provide an AI mediator for example the opportunity to generate alternative options since 'the only solutions that are worth anything are the solutions that people find themselves'.[54]

Literature

[53] Bernalillo County Metropolitan Court Mediation Division (2019) 13.
[54] Simon & West (2022) 61.

Bakken L, 'Alternative Dispute Settlements: Handouts′ (University of Bergen, Norway 2020).
Bernalillo County Metropolitan Court Mediation Division, ′Mediating at Metro Court: A Handbook for Mediators′ (2019) BCMCMD <http://www.annelightsey.com/resources-links/> accessed 13 August 2023.
CGNT America, ′CES 2019: AI robot Sophia goes deep at Q&A′ (2019) CGNT America <https://www.youtube.com/watch?v=T4q0WS0gxRY> accessed 05 August 2023.
Draper C, 'The Pull of Unbiased AI Mediators' (2019) 6 IJODR 116.
General Rules of Practice for the District Courts Minnesota (1992), <https://www.revisor.mn.gov/court_rules/rule/gp-toh/ > accessed 06 August 2023.
Immediation, ′Immediation - Digital Legal Environments - Platform Demonstration′ (2021) Immediation <https://www.youtube.com/watch?v=zaMtHffjnJQ> accessed 20 August 2023.
Kovach K, *Mediation in a Nutshell* (3rd edn, West Academic Publishing 2014).
Kahneman D., *Thinking fast and slow* (1st edn, HVG Publishing 2013).
Kumar Sand Kumar H., ′Mediation and Artificial Intelligence: Future of Dispute Resolution′ (2021) 4 Int'l JL Mgmt & Human 1472-1479.
Larson D A, 'Artificial Intelligence: Robots, Avatars, and the Demise of the Human Mediator' (2010) 25 Ohio St J on Disp Resol 105.
Lightsey A, *Mediation Certification: Readings & Additional Resources* (University of New Mexico Anderson School 2022).
Lodder A R, Zeleznikow J, 'Artificial Intelligence and Online Dispute Resolution' in Wahab M, Katsh E, Rainey D (eds), *Online Dispute Resolution: Theory and Practice* (Eleven Publishers 2012).
Moffitt M Land Schneider A K, *Dispute resolution: examples & explanations* (1st edn, Aspen Publishers 2008).
Model Standards of Conduct for Mediators (2005), <https://www.americanbar.org/content/dam/aba/administrative/dispute_resolution/dispute_resolution/model_standards_conduct_april2007.pdf> accessed 27 August 2023.
Moore C W, *The mediation process: practical strategies for resolving conflict* (3rd edn, Jossey-Bass 2003).

Morse S C, 'When Robots Make Legal Mistakes' (2019) 72 Okla L Rev 213.
Nolan-Haley J M, *Alternative dispute resolution in a nutshell* (5th edn, West Academic Publishing 2021).
Rajendra J Band Thuraisingam A S, 'The deployment of artificial intelligence in alternative dispute resolution: the AI augmented arbitrator' (2022) 31 Inf. Commun. Technol. Law 176.
Sander F E Aand Rozdeiczer L, 'Selecting an appropriate Dispute Resolution Procedure' in Moffitt Land Bordone R C (eds), *The handbook of dispute resolution* (Jossey-Bass 2005).
Simon Dand West T, *Self-determination in mediation: the art and science of mirrors and lights* (1st edn, Rowman & Littlefield 2022)
Thompson L L, *The Mind and Heart of the Negotiator*. (6th edn, Pearson 2014)
van Duin Sand Bakhshi N, 'Artificial Intelligence Defined' (2017) *Deloitte*,
<https://www2.deloitte.com/se/sv/pages/technology/articles/part1-artificial-intelligence-defined.html> accessed 19 August 2023.

Goran Georgijevic*

Legal Regime in Mauritius of Consumer Contracts Made through Electronic Communication Means

Abstract: Even though the legal regime of contract has been well established in the Mauritian Civil Code since 1805, the rapid economic development of Mauritius, as from 1980s, generated a new category of contracts, namely consumer contracts, which need some specific rules. In spite of the pivotal place of consumer contracts in the Mauritian economy, it seems that the legal framework of this type of contract still needs to be improved. And this assertion is also applicable, in our view, to consumer contracts made through electronic communication means, such as emails or internet sites, that have emerged at the beginning of the XXIst century. There are currently only few legislations in Mauritius in this field and many important points pertaining to consumer contracts in Mauritius, in general or made via electronic communication means, are still not addressed.

In this paper we will analyze the legal measures that still could be adopted in order to protect a consumer in a consumer contract made through electronic communication means. It will be shown that some of those measures are anterior to the conclusion of an electronic consumer contract and the other ones are applicable to the contract after it has already been made.

Keywords: consumer protection, Mauritius, electronic communications

* Goran Georgijevic is a senior lecturer at the Department of Law, Faculty of Law & Management, University of Mauritius, Mauritius; E-mail: g.georgijevic@uom.ac.mu.

1. Introduction

Mauritian legal system is a hybrid or a mixt one, where the court's organization and the Public Law (Constitutional Law and Administrative Law) are of common law inspiration, whereas the Private Law, and especially Mauritian Civil Law is of French origin.[1] This is explained by Article 8 of the Act of Capitulation of 1810, which ended a war between England and France. According to Article 8, the inhabitants of Mauritius were authorized to preserve their customs, their religion and *their laws*. Mauritius kept, thus, its Civil Code of 1805, modelled on the French *Code Napoléon* of 1804, although during two following centuries the two Codes evolved separately.[2]

In Mauritius, contract is defined in Article 1101 of the Civil Code as an agreement that confers upon one party to it, called *creditor,* the right to ask the other party, called *debtor*, to give him something, to do something or not to do something that normally he is authorized to do.[3] This definition encompasses most of the contracts made in Mauritius, given the fact that they generate most of the time an obligation to transfer the right of

[1] Agostini (2004) 116-117; Agostini (1992) 21-22; Domingue (2002) 62; Law Reform Commission, (2010); Venchard (1982) 31.

[2] Compare Articles 312 through 370-5 of the Mauritian Civil Code with Articles 310-1 through 370-5 of the French Civil Code, Articles 1101 through 1369 of the Mauritian Civil Code with Articles 1101 through 1231-7 of the French Civil Code and Articles 23 through 48 of the Mauritian Civil Code with Articles 311-21 through 311-24-1 of the French Civil Code. - *Vide* also the judgments of the Supreme Court of Mauritius *Jugessur Mrs Shati & ORS v. Bestel Joseph Christian Yann & Anor* 2007 SCJ 106 and *Naikoo v. Société Héritiers Bhogun* 1972 MR 66 1972 compared to the judgments of the French Court of Cassation Cass. Mix. Ch., 27 February 1970 n° of pourvoi: 68–10276 and Cass. Crim. Ch. 17 March 1970 n° of pourvoi: 69–91040.).

[3] Terré, Simler, Lequette, Chénede (2022) 65; Buffelan-Lanore, Larribau-Terneyre (2022-2023) 272; Flour, Aubert, Savaux (2022) 127-128.

property to the creditor[4], or to do something[5], or not to do something that normally the creditor is authorized to do.[6] However, there are also the contracts that have the binding force (*"force obligatoire"*[7]), although they do not generate the abovementioned obligations.[8] For instance, in a debt write-off agreement[9], there are no obligations for the debtor to give or do or not to do something. However, this contract entails legal effects as it erases a part or the whole of a previous contractual debt.

In Mauritian Civil Law, the conditions for the validity of a contract are set out in Article 1108 of the Civil Code. There

---

[4] In a purchase contract (*"contrat de vente"*), the right of property is transferred, in principle, to the creditor at the very moment where the contract has been made (art. 1138 and 1583 of the Mauritian Civil Code). However, the transfer of the right of property may be delayed in some cases such as the case of generic property (*"chose de genre"*), when the right of property passes to the creditor once the object has been individualized and handed over to the creditor, or the case of condition precedent (*"condition suspensive"*) whose fulfilment marks the moment of the transfer of the right of property to the creditor, etc.

[5] The typical example of a contract generating this type of obligation in Mauritian Law is a contract for service (*"contrat d'entreprise"*) where a professional such as a doctor, lawyer, accountant, gardener, etc. has the obligation to act for the benefit of his client.

[6] Such an obligation, limited in the space and time, stems from the contractual clauses known as restrictive covenant. – On this matter see the judgments of the Supreme Court of Mauritius
Hardy Henry and Cie Ltée v. Kaloo 1986 MR 173 and 1986 SCJ 269, *L'Acropole Ltd. v. Gerbe d'or Ltd. and Anor* 1982 MR 153 and SCJ 169, *Lenoir Ducray Ltd v. Ramdhany* B. *& Anor* 2004 SCJ 35 and *Nabridas Ltd v. Coombes M.* 2019 SCJ 142.

[7] This essential characteristic of the contract in Mauritius is provided for by article 1134 of the Mauritian Civil Code.

[8] Ancel (1999) 771-810 ; Terré, Simler, Lequette, Chénedé (2022) 66; Buffelan-Lanore, Larribau-Terneyre (2022-2023) 272; Flour, Aubert, Savaux (2022) 129.

[9] Articles 1282 through 1288 of the Mauritian Civil Code.

must be the capacity for making a contract,[10] which is, in general,[11] acquired at the age of 18,[12] a consent[13] to a contract,[14] a defined, possible and legal object of the contractual obligations,[15] and an existing and legal reason for the contract, whether that reason is defined in an objective[16] or in a rather subjective[17] manner.[18] If some of those conditions is lacking or contains an important defect, the contract can be declared null and void. When the cause of the nullity of a contract goes

[10] Article 1123 of the Mauritian Civil Code.

[11] On one hand, the minors, i. e. the individuals under the age of 18 do not have the full capacity to make contracts in Mauritius, although they may make some less dangerous contracts which are usual in everyday life (Article 390 (1) of the Mauritian Civil Code - Cermolacce (2006) para n° 3; Buffelan-Lanore (2010) para n° 57; Roque (2009) para n° 10). They need to be represented while making contracts by their parents-legal administrators (Articles 390 and subsequent of the Mauritian Civil Code). On the other hand, the adults that do not possess a basic mental capacity need to be place under guardianship ("tutelle") (Articles 395 and subsequent of the Mauritian Civil Code).

[12] Article 388 of the Mauritian Civil Code. – Before Sections 2 and 12 of the *Children's Act* (Act n° 13/2020) formally prohibited child marriage, it was possible, according to articles 476 to 478 of the Mauritian Civil Code, that a minor sixteen years old or more celebrates a marriage and acquire the full capacity to make contracts. It was called emancipation by marriage. However, child marriage became a criminal offence in 2020 and therefore no emancipation by marriage is possible anymore in Mauritius.

[13] Terré, Simler, Lequette, Chénedé (2022) 65 subs.; Buffelan-Lanore, Larribau-Terneyre (2022-2023) 369 subs.; Flour, Aubert, Savaux (2022) 241 subs.

[14] The consent is defined as the acceptance, by a party to a contract, of the legal effects that the contract will generate. It needs to be free and well informed (Articles 1109 through 1117 of the Mauritian Civil Code).

[15] Articles 1126 through 1130 of the Mauritian Civil Code.

[16] *Uteeme J. M. Z. v. Maunick G. & Ors* 2005 SCJ 243; *Sadien D. v. Maurel P.* 1997 MR 248; *Nowbuth v. Bhoyraz* 1991 MR 229; *G. Weg v. K. K. Patel & Anor* 1991 MR 239 and *Rayapen v. Lionnet* 1960 MR 262.

[17] *Y. Pool and Arthur Savy v. Delorié* 1958 MR 266.

[18] Articles 1131 through 1133 of the Mauritian Civil Code. – Terré, Simler, Lequette, Chénedé (2022) 387 subs.; Buffelan-Lanore, Larribau-Terneyre (2022-2023) 421 subs.; Flour, Aubert, Savaux (2022) 563 subs.

against the fundamental values in Mauritius, which are called public order (*"ordre public"*) or good morals (*"bonnes moeurs"*),[19] the nullity of the contract is an absolute one and the contract cannot be corrected or confirmed. Moreover, every interested person, including each party to the contract, may ask a court of justice to declare the nullity of the contract and the action to nullify the contract can be brought before a court of justice during thirty years. If the cause of the nullity of a contract concerns a group of persons that the law wishes to protect, rather than the general interest, the nullity is a relative one then, and the contract can be or confirmed in an explicit or implicit manner. Only the protected person can bring an action for nullity of the contract before a court of justice,[20] and the action can be brought before a court of justice during, in principle, five years.[21] When a valid contract is made, it will produce a binding effect, catered for in Article 1134 of the Mauritian Civil Code. The binding effect of a contract means that each party to the contract needs to fulfil accurately its contractual obligations and that no party to the contract shall take an action that might endanger the execution of the contract.[22] If the contractual obligations are not fulfilled at all, or are fulfilled in an unsatisfactory manner, the contractual liability may be applied.[23] The parties may also insert in their contract a penalty clause that will apply when a contractual

[19] Article 6 of the Mauritian Civil Code.

[20] For instance, pursuant to Article 1117 of the Mauritian Civil Code, a victim of an error or fraud or violence that deforms the consent to the contract may ask that the contract be nullified.

[21] Article 1304 of the Mauritian Civil Code. – Terré, Simler, Lequette, Chénedé (2022) 635 subs.; Buffelan-Lanore, Larribau-Terneyre (2022-2023) 496; Flour, Aubert, Savaux (2022) 749 subs.

[22] Terré, Simler, Lequette, Chénedé (2022) 693-694; Buffelan-Lanore, Larribau-Terneyre (2022-2023) 527 subs.; Flour, Aubert, Savaux (2022) 847 subs.

[23] Articles 1147 and subsequent of the Mauritian Civil Code. – Flour, Aubert, Savaux (2022) 1097 subs.

obligation has not been fulfilled or has been fulfilled in an unsatisfactory manner. The penalty clause is a fixed sum of money, and its amount can be modified by a Judge only in exceptional circumstances when its amount is too low or too high.[24] In case of a breach of contract, the victim of that breach may also ask a court of justice to put an end to the contract that has not been correctly fulfilled.[25]

The above-mentioned general characteristics of the contract are also applicable to consumer contracts in Mauritius.[26] A consumer contract may be defined as a contract made by a professional, acting within the scope of his profession, and an individual that seeks to satisfy his personal or his family needs.[27] This kind of contract allows the consumer to enter into the possession of a desired goods or service.[28] A consumer contract in Mauritius needs to respect the general requirements for the validity of a contract, and will be null and void if those general requirements are not met. On the other hand, if a consumer contract respects the general rules on contracts in Mauritius, it will be vested with the binding force provided for in Article 1134 of the Mauritian Civil Code. However, a consumer contract in general, as well as a consumer contract made through electronic communication means, have their own specificities due to the unequal status of the parties to this contract. The professional is designed as stronger party to the consumer contract and the consumer is weaker party to it.[29]

---

[24] Article 1152 (2) of the Mauritian Civil Code. – Buffelan-Lanore, Larribau-Terneyre (2022-2023) 618 subs.; Flour, Aubert, Savaux (2022) 1179 subs.
[25] Article 1184 of the Mauritian Civil Code. – Comp. with Buffelan-Lanore, Larribau-Terneyre (2022-2023) 610 susb.; Flour, Aubert, Savaux (2022) 1064 subs.
[26] Picod (2018) 160.
[27] Comp. with Law Reform Commission of Mauritius (2010) para n° 102; Pellier (2021) 17-18.
[28] Calais-Auloy (2015) 197.
[29] Picod (2018) 143.

In spite of the pivotal place of consumer contracts in the Mauritian economy, it seems that the legal framework for this type of contract still needs to be improved. And this assertion is also applicable, in our view, to consumer contracts made through electronic communication means, such as emails or internet sites, that have emerged at the beginning of the XXIst century. There are currently only few legislations in Mauritius in this field (Consumer Protection Act,[30] Consumer Protection (Price and Supplies Control) Act,[31] Essential Commodities Act,[32] Hire Purchase and Credit Sale Act[33]) and many important points pertaining to consumer contracts in Mauritius, in general or made *via* electronic communication means, have not been addressed yet.

The Consumer Protection Act addresses the issue of the safety and quality of the goods offered by a professional,[34] but is silent as to the rights and obligations of the consumer in consumer contracts, including those made through electronic communication means. The same silence may be found in the Consumer Protection (Price and Supplies Control) Act which aims at protecting the consumer against abusive trade practices by regulating trade, supply and price of goods. The focus of the Essential Commodities Act is to ensure the continuity of the supply of the essential commodities such as ration rice, sugar, raw and white flour, laundry soap, edible oil, petrol, etc. A non-compliance with the Act is a criminal offence. On the other hand, the Hire Purchase and Credit Sale Act is a rare piece of

[30] Act 11/1991.
[31] Act 12/1998.
[32] Act 8/1991.
[33] Act 6/1964.
[34] Section 3(1) of the Act provides that no person shall supply any goods which suffer from any fault with regard to any prescribed quality, quantity, potency, purity or standard or, in the case of any machinery or motor vehicle, with regard to the quality, nature or manner of its performance.

legislation in Mauritius that ensures the protection of a consumer to a certain extent and confers upon him some rights, but only in two specific consumer contracts, namely the hire purchase contract and credit sale contract. However, for the time being, there is no legal framework in Mauritius as to the general protection of the consumer in consumer contracts, including those made via electronic communication means.

This paper aims, thus, at exploring the possibility to better protect consumers in Mauritius, who conclude contracts with professionals through electronic communication means.
The specificities of consumer contracts, including those made through electronic communication means are such that a consumer, party to a contract in Mauritius, should be better protected before the contract has been made, and also after the contract has been made.[35]

2. The Measures Aiming at Protection of the Consumer Before the Contract Has Been Made

2. 1. The information mandatorily provided to the consumer

Given the fact that the consumer is weaker party to a consumer contract, his consent needs a special protection. The consumer needs a clear information about the contract he is about to make, as well as a certain flexibility as to the decision to be party to the contract or not.[36]

A consumer in Mauritius, including the one making a contract through electronic communication means, needs to be properly informed on the points that are essential to a clear decision to make a contract or not.[37] First of all, the Mauritian law should

[35] Picod (2018) 144.
[36] Picod (2018) 147.
[37] Picod (2018) 169.

stipulate that before a consumer and a professional make a consumer contract, including a contract through electronic communication means, the latter should inform the former, in writing, in a clear manner and before the signature of the contract, on the essential characteristics of the goods or of the service proposed.[38] A professional must also give to a consumer, with whom he is about to enter the contract, a certain amount of information about himself such as name, address, phone number etc. Moreover, the price proposed by the professional for the goods or service on offer must be clearly indicated before the contract is made.[39] The mode of the indication of the price will depend on the nature of the proposed contract,[40] and in consumer contracts made through electronic communication means, the price must be indicated on the internet site of the professional or in the documents sent to the consumer through an email. In consumer contracts for service, in case the price may not be fixed before the contract is made, there must be the objective criteria set out in the contract, that will allow the determination of the price once the execution of the contract begins.[41] This should also apply to consumer contracts made through electronic communication means. The consumer must be made aware of those criteria before the contract is made. When a consumer contract made through electronic communication means is not immediately executed by the parties to the contract, the date of the execution needs to be indicated in the contract,[42] before it is made.[43] However, if the date of execution of the contract is not indicated in a consumer contract, including the one made through electronic means of communication, the professional must execute the

[38] See Article L. 111-1 of the French Consumer Code. - Picod (2018) 171; Pellier (2021) 43-46.
[39] Picod (2018) 172; Pellier (2021) 47-50.
[40] Picod (2018) 178.
[41] Picod (2018) 171.
[42] See Article L. 216-1 of the French Consumer Code.
[43] Picod (2018) 172; Pellier (2021) 51-52.

contract immediately, or at the latest within a reasonable amount of time, which in Mauritian Law might be thirty days.[44]

The question may arise what civil law sanction should be applied if a professional does not respect his obligation to inform a consumer on certain essential points of the contract, before the contract is made. If the lack of information pertains to an essential characteristic of the goods or service offered by the professional, the consumer contract, including the one made through electronic communication means, may be declared null and void[45] by a court of justice,[46] as the essential characteristic of the goods or service offered by the professional determines the consumer's decision to enter into the contract or not. An error of the consumer on those essential characteristics qualifies as error on the substance (*"erreur sur la substance"*) as per Article 1110 of the Mauritian Civil Code. The general regime of this type of error will also apply to consumer contracts made through electronic communication means.[47] In other cases, where the lack of information by the professional does not concern the essential characteristics of the goods and services offered by the professional, it does not entail an error on the substance, the only civil law sanction available to the consumer-victim of the lack of information are damages.[48] Of course, the consumer needs to prove the harm suffered and the lack of information that caused that harm.[49] If a professional does not execute the contract made through electronic means of communication within the deadline provided for in the contract, or within the reasonable deadline of thirty days, the consumer may also put an end to the contract. We are of the view that, by

[44] Picod (2018) 179.
[45] Cass. 3rd ch., 15 January 1971, *Bulletain civil* III, paragraph n° 38 ; Cass. 3rd ch. 3 February 1981, *Dalloz* 1984, 457.
[46] Picod (2018) 176-177; Pellier (2021) 58 subs.
[47] Picod (2018) 176-177.
[48] Comp. with: Pellier (2021) 58-60.
[49] Picod (2018) 176-177.

derogation to Article 1184 of the Mauritian Civil Code and given the unequal strength of the professional and the consumer in a consumer contract, this power to put an end to the contract may be used extrajudicially, i. e. the consumer does not need to bring an action before a court of justice, as per Article 1184 of the Mauritian Civil Code. He simply needs to warn the professional first (*"mettre en demeure"*) and then send to him in writing his decision to put an end to the contract.[50]

2. 2. The impossibility to accept immediately an offer made by a professional

Another measure that protects the consumer in consumer contracts made electronically, before the contract has been made, is the time gap that must exist between an offer has been made by the professional and the acceptance of that offer by the consumer.[51] In some cases, when it seems justified,[52] the Mauritian legislator could impose on the consumer an obligation to reflect on the offer made by the professional before the former accepts the offer of the latter. In such cases, the consumer *may not accept* the offer before the expiry of the period of time provided for by the law, which should range from seven and fourteen days. This legal measure aims at protecting the consumer against his own too rapid decisions to make a contract.[53] This protective measure should be of public order (*"d'ordre public"*), meaning that the period for reflection should not be reduced but can be longer that the minimal period of time provided for by the law.[54]

---

[50] See Article 216-2 of the French Consumer Code.
[51] Picod (2018) 183.
[52] In immovable property related contracts (sale, exchange, etc.), for instance.
[53] See Article L. 313-34 of the French Consumer Code. - Picod (2018) 185.
[54] Picod (2018) 186.

2. 3. The impossibility for a professional to revoke an offer addressed to a consumer

In Mauritian Contract Law, an offer for a contract may be freely revoked by the offeror, which means that he has no legal obligation to maintain it and that he may revoke it before the receiver of the offer accepts it. In that case, the offeror will not be liable in tort. However, there are the exceptional cases when, in Mauritian Contract Law, an offer cannot be freely revoked, and if revoked before the expiry of the time during which it has to be maintained, the offeror will be liable in tort for all the harm suffered by the offeree. The offer is not to be revoked if the offeror has promised to maintain his offer, or has set the period of time during which the offer may be accepted or if the circumstances surrounding the offer justify that it cannot be freely revoked. The solution should be different in consumer contracts, including those made through electronic communication means, in order to protect the weaker party to a consumer contract, i. e. the consumer. In this type of contract, the offer must not be freely revoked, and if revoked by the professional before the expiration of the period of time during which the offer must be maintained, the professional will be liable in tort to the consumer. This measure aims at protecting the consumer by giving him enough time to consider the offer sent to him by the professional and by avoiding him to take a too rapid decision as to the proposed contract.[55]

2. 4. A specific protective rule pertaining to the offers made via internet

A specific rule should exist in Mauritian Consumer Law as to the contracts made specifically by offering the goods *via* internet. This kind of offer should be binding for the offeror as

[55] Picod (2018) 184.

long it is displayed online, even though the professional is out of stock. However, the professional will not be bound by the offer displayed online if the offer is there due to a technical reason which qualifies as *force majeure* or if the offer contains the indication of its period of validity or the indication that it is valid as long as the goods are in stock.[56]

In electronic consumer contracts, made online, a consumer in Mauritius needs to have the opportunity to check the details of the contract he is about to make and this is why his consent to the contract must be given at least twice by clicking on the appropriate button. This rule aims at giving the consumer an opportunity to correct the errors in his online order, before the contract is definitely made.[57] We are of the view that, in order to confer the best possible protection on the Mauritian Consumer, this rule should be of public order (*"d'ordre public"*) and a consumer contract made online could not derogate from it by erasing this protection.

2. 5. Written form of consumer contracts

In Contract Law in Mauritius there is a principle under which a contract may be made verbally and the written form is not a condition for its validity. The need for a special protection of a consumer explains why in Mauritian Law the consumer contracts should be mandatorily be made in a written form, when the value of a contract is 5 000 rupees or more. The idea behind this rule is to inform better the consumer about the contents of the contract before he makes the contract with the professional and to ensure a written proof to the consumer.[58]

[56] Picod (2018) 186.
[57] Article 1127-2 of the French Consumer Code. - Picod (2018) 186.
[58] Picod (2018) 189.

3. The Measures Aiming at Protection of the Consumer Once the Contract Has Been Made

3. 1. The clauses excluding or limiting the contractual liability of the professional

According to Contractual Liability Law in Mauritius, parties to a contract are free to put in their contract a clause pursuant to which a party will not be liable for the harm suffered by the other party, or according to which the former's liability will be limited. However, this type of clause is not valid if a contractual party has committed an intentional fault or a heavy fault,[59] which needs to be proved by the victim. On the other hand, the solution recommended for the Mauritian Consumer Law should be even harder on the professional, who is stronger party to the consumer contract. An efficient protection of the consumer, weaker party to the contract, requires such a mechanism in Mauritius. The clauses excluding or limiting the contractual liability of the professional should be simply prohibited, notwithstanding the gravity of the professional's fault, i.e. intentional or not, heavy or not. In any circumstance a professional could not be exonerated from his contractual liability for the harm caused to the consumer with whom he made a contract.[60]

3. 2. The deadline to reimburse the consumer once the contract has been ended

In order to protect better the consumer, including the contracts made through electronic communication means, the Mauritian Consumer Law should also provide for a period of time, once the contract has been ended, during which the professional needs to pay the money back to the consumer. Fourteen days

[59] Compare with Article 1151 of the Mauritian Civil Code.
[60] See Article R. 212-1 of the French Consumer Code. - Picod (2018) 179.

seem to be a sufficient and reasonable period of time.[61] On the other hand, after fourteen days, if the money is still not reimbursed, the professional will be obliged to pay the interests to the consumer.

3. 3. The possibility for the consumer to revoke unilaterally and arbitrarily the contract

In Contract Law in Mauritius, Article 1134 of the Civil Code provides for the binding force of the contract, which means that no party to a contract may leave the contract unilaterally and arbitrarily, without a good cause provided for in the law and without giving an explanation to the other party. There is a precise framework allowing a party to a contract to put an end to it. For instance, in case of inexecution of contractual obligations one party may bring an action before a court of justice, under article 1184 of the Mauritian Civil Code, and ask the court to put an end to the contract for inexecution of the contract. When a contractual clause called *"clause résolutoire"* is inserted in a contract, a party may put an end to the contract, without the intervention of a court of justice, on the basis of the inexecution of the contractual obligation specified in the *"clause résolutoire"*. The rules set out above are based on the assumption that the parties to the contract are of equal force. This is not the case in consumer contracts, where the consumer is economically weaker party, and this is why the Mauritian Consumer Law should introduce a legal mechanism consisting of the right for the consumer, and only him, to revoke unilaterally a consumer contract, free of charges and without giving the reasons for it during a period of time that may be between seven and fourteen days. This rule is contrary to the basic principles of the Contract Law in Mauritius, *i.e.* the binding force of a contract, but would protect well the consumer

[61] See Article L. 216-3 of the French Consumer Code.

who is weaker party to the contract.[62] This rule should be of public order (*"d'ordre public"*) too, meaning that the period for revocation of the contract provided by the law should not be reduced but can be longer that the minimal period of time provided for by the law.

3. 4. The prohibition of abusive clauses

Currently, in Mauritian Consumer Law there are no the legal rules prohibiting abusive clauses in consumer contracts. However, in some specific cases the laws in Mauritius deal with such clauses and declare it null and void. For instance, under section 6 of the *Hire Purchase and Credit Sale Act* of 1964, a contractual clause that allows the seller or his proxy to enter any premises in order to seize a goods that is in a consumer's possession or to request a payment is null and void. The same legal sanction is applied to a contractual clause that exonerates the professional from all tort liability for the harm caused while he was entering the abovementioned premises. A contractual clause that aims at excluding or limiting the consumer's right to put an end to the consumer contract is also null and void. However, we are of the view that the protection of the consumer in Mauritius will not be complete or satisfactory as long as there is not a general legal rule declaring null and void the abusive clauses in consumer contracts, including those made through electronic communication means. Abusive clauses may be defined in Mauritius as the clauses whose content is aiming at or whose effects create a significant imbalance between contractual obligations and rights of the parties to a consumer contract.[63] This type of clauses should be prohibited in every consumer contract in Mauritius, such as purchase, loan,

[62] Picod (2018) 183-184; Pellier (2021) 184-190.
[63] See Article 212-1 of the French Consumer Code. - Picod (2018) 224; Pellier (2021) 133-137.

insurance contract, etc.[64] The abusive nature of a clause inserted in a consumer contract is evaluated on the basis of the concrete circumstances that surround that particular consumer contract.[65] For instance, a clause in a contract providing that the clauses that are not mentioned in the written agreement between the professional and consumer form part of the contract should be null and void, as this goes against the legal security of the consumers in Mauritius. The same legal sanction should be applied to a clause in a consumer contract that limits or excludes the professional's civil liability for the faults committed by his agent or proxy; to a clause that confers upon the professional the right to modify unilaterally the duration of the consumer contract or the essential characteristics of the goods or the service for which the contract has been made; to a clause that confers upon the professional the right to decide alone, without the consumer, whether the delivered goods or the services carried out are in conformity with the content of the contract made with the consumer; to a clause that excludes or limits the consumer's right to put an end to the contract made with the professional, in case of a breach of contract by the professional, *etc*.

4. Conclusion

In Mauritius, general principles of Contract Law are applicable to consumer contracts, including those made electronically. The Mauritian Civil Code governs, thus, the conditions for the validity of the contract, the nullity of the contract, the binding effect of the contract, etc. However, Mauritian Contract Law is tailored for the parties of equal force, and this is why the protective mechanisms must be added to the Mauritian legislation in order to protect better the consumer who is weaker party to a consumer contract. Some of those measures should

[64] Picod (2018) 225.
[65] Picod, 2018, 229.

precede a consumer contract, for instance the information mandatorily provided to the consumer, the impossibility to accept immediately an offer made by a professional, the impossibility for a professional to revoke an offer addressed to a consumer, etc. On the other hand, some measure aiming at protecting the consumer once the contract has been made, for instance the prohibition of abusive clauses, the right to revoke unilaterally and arbitrarily the contract, etc. should also be included in Mauritian legislation.

Literature

Agostini E, ' Heurs et malheurs du mariage religieux à l'Ile Maurice ' in Gérard Aubin (ed) *Etudes offertes à Pierre Jobert* (Presses universitaires de Bordeaux 1992).

Agostini E, ' Odgovornost za štetu od opasne stvari-primena francuskog prava na Mauricijusu ' (2004) 52 *Anali Pravnog Fakulteta u Beogradu* 116.

Ancel P, ' Force obligatoire et contenu obligationnel du contrat ', (1999) *Revue trimestrielle de droit civil* 771.

Buffelan-Lanore Y *Minorité. - Droits propres de l'enfant*, *Fasc. unique, Jurisclasseur Code civil, art. 388* (LexisNexis 2010).

Buffelan-Lanore YandLarribau-Terneyre V, *Droit civil, les obligations*, (18th ed., Sirey 2022-2023).

Calais-Auloy J, *Droit de la consommation* (9th ed., Paris 2015).

Cermolacce A, ' Les contrats du mineur ', (2015) 6 *Droit de la famille* Study 27.

Domingue P R, ' The Historical Development of the Mixed Legal System of Mauritius during the French and British Colonial Periods ' (2002) 4 *Research Journal*, *Law, Management and Social Sciences*, University of Mauritius 61.

Flour J, Aubert J Land Savaux E, *Droit civil. Les obligations, l'acte juridique* (17th ed., Paris 2022).

Law Reform Commission of Mauritius, Report on *"Review of Aspects of Consumer Protection Law and Proposals for Reform"* (2010) <https://lrc.govmu.org/lrc/?p=2518> accessed 24 May 2023.

Law Reform Commission, *Reform of Codes* (Background Paper, 2010) <https://lrc.govmu.org/lrc/?p=2479>accessed 1 June 2023.

Pellier J D, *Droit de la consommation* (3rd ed., Dalloz 2021).
Picod Y, *Droit de la consommation* (4th ed., Sirey 2018).
Roque J, 'La prémajorité' (2009) 4 *Droit de la famille*, Study 20.
Terré F, Simler Ph, Lequette Yand Chenédé F, *Droit civil, les obligations* (13th ed., Dalloz 2022).
Venchard L-E, ' L'application du droit mixte à l'Ile Maurice ' (1982) 4 *Mauritius Law Review* 31.

Rajendra Parsad Gunputh,[*] Eric Bindah,[*] Joseph Assogbavi,[*] Ambareen Beebeejaun[*]

Computer crime: cryptography and cryptanalysis in the IT sector - where does the Mauritian law stand? -

Abstract: Computer crime encompasses a broad range of potentially illegal activities, such as illegal downloading and distributing protected items (*inter alia*, stealing intellectual property and copyrighted articles, user information (phishing), ID theft, *etc*.). Such activity either targets computer networks or devices directly or they such crimes are facilitated by computer networks or other devices, the primary target of which is independent of the computer network or device, like computer viruses, denial of service attacks, malware, cyber stalking, fraud. Since anyone may be the subject of a cybercrime or attack, there is a huge number of cases related to bank cards (stolen cards, spoofed websites, CNP Txn, ID theft-application, Take-over and account Take-over, skimming and carding using generated numbers, or spamming), coupled with illegal bank transactions through internet. In addition, some individuals might threaten national security by cybercrime, that will be considered as a breach of national security.

[*] Rajendra Parsad Gunputh is a full professor at the Department of Law, Faculty of Law & Management, University of Mauritius, Mauritius; E-mail: rpgunput@uom.ac.mu.

[*] Eric Bindah is a senior lecturer at the Department of Law, Faculty of Law & Management, University of Mauritius, Mauritius; E-mail: e.bindah@uom.ac.mu.

[*] Joseph Assogbavi is a senior lecturer at the Department of Law, Faculty of Law & Management, University of Mauritius, Mauritius; E-mail: kossiassogbavi107@gmail.com.

[*] Ambareen Beebeejaun is a senior lecturer at the Department of Law, Faculty of Law & Management, University of Mauritius, Mauritius; E-mail: a.beebeejaun@uom.ac.mu.

Key words: legislation, crime, cryptography, cybercrime, cyber-attacks

1. Introduction

Cryptography, construed as having a message in disguised form, was developed during World War II, such as rotor machines which famously included the Enigma machine used by the German government and military from the late 20s and during World with many mechanical encryption and decryption devices and were even patented.[1] Cryptography was invented to hide confidential information and to maintain secrecy. However, Julius Caesar used cryptography to communicate with his generals during his military campaigns with a shift to three similar to EXCESS-3 code in Boolean algebra. The earliest form of cryptography was found in the ciphertext on stone in ancient Egypt some 1900 years BC.[2] Cryptography transforms a legible message to an unintelligible form, and then back to its legible form by means of a technique and mathematical formula. In our modern days, linguistic approach allows the use of mathematics and numerology. They include aspects of information theory, computational complexity, statistics, combinatorics, abstract of algebra, number theory and finite mathematics generally. There are code breakers that also allow to pierce the veil of encryption with modern cryptography techniques.[3] Therefore, cryptoanalysis is to find some weakness or insecurity in a cryptography scheme "provided the key material is truly random, never reused, kept secret from all possible attackers, and of equal or greater length than the message".[4] With cryptanalytic attacks, the Council of the OECD adopted Guidelines for Cryptography Policy

[1] Hakim (2007).
[2] Kahn (1967).
[3] Whitfield Diffie and Martin Hellman (1976).
[4] Claude E.Shannon & Warren Weaver (1964).

encouraging its State members to include it in their municipal law. Because of national security, some countries have restricted use of cryptography (France) whilst in some countries, a license is required to use cryptography (China). In some other countries, the use of cryptography is very restricted (Russia, Singapore, Tunisia or Vietnam). And due to its military weapons, the US found it illegal to sell or distribute encryption technology overseas.

The purpose of this empirical study is to test whether academics and students are aware of cryptography and cryptanalysis. A survey was carried out in various sectors like manufacturing, Information Communication Technology (ICT), management, and education. These sectors have embraced the concept of cryptography and cryptanalysis without knowing it as per the outcome of the survey questionnaire that has been carried out and disseminated (*infra*).

After an abstract (*supra*) followed by an Introduction (1), the structure of this empirical paper would be a traditional one with the Problem Statement (2), followed by secondary data in the form of a Literature Review focused on the subject-matter (3), a Research Methodology based on primary data in the form of a survey questionnaire (4), the Facts and Findings of the survey questionnaire (5), and the empirical research will close with a Conclusion and some Recommendations (6) with a list of references (Literature) to enhance further research and development in this emerging field of the law as it is of universal concern to protect the IT sector and its billions of users worldwide.

2. The problem statement

This empirical study is an attempt to assess the cryptanalysis awareness and the danger that it may represent among students

and academics in general. The aim is to determine if the future working generation is knowledgeable, sensitive, and responsible towards cryptography and cryptanalysis. An in-depth quantitative survey was conducted among 70 students, academics and IT Sector users (n=70). The questionnaire consisted of 20 questions specially focusing on the legal issue of cryptography and cryptanalysis. These facts and findings would definitely contribute to the literature review on students' and academics' sustainability awareness and commitment towards this issue. In this empirical paper, the authors will refer to relevant legislations such as, inter alia, the Computer Misuse and Cybercrime Act 2003, though it has been found that previous laws had loopholes or limitations with regards to jurisdiction and extradition at a time where there is a developing social environment, with the development a cyber-city on the island and remedies to violation of confidence (injunctions, damages, account of profit, delivery up), which caters for Alternative Dispute Resolution (ADR), data protection laws (Data Protection Act 2004), e-commerce transaction laws, fair use policies, electronic marketing laws and terms and conditions in website, security and cryptography policies and even child pornography. Therefore, authors of this abstract and paper will focus on security on the website despite the Mauritian legislator has passed an armada of legislation (Copyright and Rights in Database Regulation 1997, Copyright Act 1997, Trade Marks Act 1868, Fair Trading Act 1980) to protect us from cybercrimes, but are they sufficient and to what extent?

3. Literature review

Cryptography is a scientific discipline whose history is as old as that of humanity. It is a method of protecting information and communications by using codes so that only the recipients of

the information can read and process it.[5] Its origin goes back to the Egyptian civilization where writings found on the walls of a sarcophagus contained modified hieroglyphs.

Cryptoanalysis has its origins in cryptography. The need to "break" encrypted messages by analyzing secret messages led to what is known as cryptoanalysis, developed for the first time by the Arab people who understood the mechanisms of cryptography.[6] Cryptography associated with cryptoanalysis gives rise to the grouping of the concept known under the name of cryptology.

Today more than ever, with the constant emergence of information and communication technologies, securing the digital world for optimal protection of computer data is essential. In effect, in an increasingly digitalized world, the use of cryptography must be the cornerstone of data security. The guarantee of data integrity and authenticity depends on it, as does the preservation of its confidentiality and non-repudiation.

Thus, even though the security of a cryptographic protocol is based on a mathematical problem using algorithms,[7] the existence of legal bases that can serve as a regulatory framework should not be overlooked. In France, the outsourcing of digital data, for example, according to cloud computing (so as to make them accessible to other computer terminals), cannot be done without any legal basis or a specific regulatory framework serving as a reference. This provision relating to the control of cryptographic operations is governed by Articles 29 to 36 of Law No. 2004-575 of 21 June 2004, known as the Law for Confidence in the Digital Economy.

[5] Gangadhar (2013).
[6] Talat (2011).
[7] Gagnon (2007).

In Senegal, the adoption of legislation providing a legal framework for cryptology was first reflected in Act No. 2001-15 of 27 December 2001 on the Telecommunications Code. It must be said that articles 37 and 67 of this law give cryptography the legitimacy to be subject to a well-founded legal regulation. However, it is worth noting that it was not until 2008 that Law No. 2008-41 of 20 August 2008, followed by its implementing decree in 2010, defined a much more solid legal and institutional framework to better supervise the institutional framework to better regulate the use of cryptology in Senegal.

In Mauritius, apart from the Data Protection Act presented by the Data Protection Office, axis 4 of the Digital Mauritius 2030 Strategic Plan provided for the establishment of CERT-MU as a legal entity and as a body providing cybersecurity services at the national and international level through partnerships. However, it should be pointed out that the passing of laws governing sanctions in the event of data security offenses deserves to be further emphasized, especially as cyberattacks are multiplying worldwide and can undermine the security of nations.

4. Research methodology

The empirical research was restricted to a survey questionnaire with students of the University of Mauritius where a pilot study was conducted among 70 respondents to gauge their familiarity with the legal framework of cryptography in Mauritius. For this purpose, a Google form was sent to students and academia and the survey was restricted to tertiary student only. The google form consisted of twenty (20) statements to which respondents were asked to answer by either yes or no, and whether they strongly agree to strongly disagree on a scale of 1 to 5. These findings would definitely contribute to the non-existing literature review on students and academics sustainability

awareness and commitments towards cryptography and the need for additional legal protection in addition to some existing legislations (*supra*).

5. Facts and findings

From the pilot test study, it was found that a large majority of the respondents were aware of the meaning of cryptography. When asked if they have heard of the term cryptography, 60% of the respondents reported that they were aware of it. While respondents reported that they were aware of the terms, a large majority however were not familiar with the legal framework encompassing the issue. Most of the respondents were not in the opinion that there exist any laws regulating cryptography in Mauritius. Only a small minority of the respondents believed that there are laws in Mauritius which regulates cryptography (9.9%). While most respondents were perceived to know about the meaning of cryptography, the majority of the respondents were not aware about its utility, particularly when asked if they were aware that cryptography is construed as having a message in disguised form (53.5% of the respondents were not aware of its utility).

When exploring the subject further, respondents were asked if they were aware of OECD Guidelines for Cryptography Policy encouraging its members to include it in their municipal law, the majority of respondents 87.3% were not aware about the OECD guidelines and its use in municipal law. Respondents were also asked about their understanding of the technical aspects of cryptography, whereby cryptography is used to transforms a legible message to an unintelligible form and then back to it's legible by means of a technique and mathematical formula. In this case, a large majority reported that (64.8%) they never sent or received messages. This study also reported that respondents were not aware that code-breakers to pierce the veil

of encryption with modern cryptography techniques were available to use. The majority of respondents reported that it was probable only (59.2%) as opposed to been certain (23.9%).

This study also asked respondents' opinion on whether the measures taken by several countries to restrict the use of cryptography for national security were appropriate. A large majority of respondents were neutral 56.3% on the issue, followed by 26.8% who agreed that it was an appropriate measure. Only 7% of the sample disagreed with the statement. The high percentage of respondent who agreed with the statement could be based on the fact that if the measures are taken by the authority to protect national security interest of the nation, then it could be most likely be appropriate to take such measures by the relevant authorities of the respective countries. Respondents were asked if they found certain restrictions justifiable in certain jurisdictions such as in the U.S., where it is illegal to sell or distribute encryption technology overseas. A majority of respondents, however, felt that it was subjective (62.2%).

In order to ensure respondents' familiarity with the subject, respondents were given some statements to assess their knowledge on the use of cryptography dating back from the past to present before gauging their opinions in the domestic context. Most respondents were not very familiar with the earliest form and use of cryptography. For instance, when asked if they knew that the earliest form of cryptography was found in the ciphertext on stone in ancient Egypt some 1900 years BC, the majority of respondents (67.6%) were not aware of its earliest form. Furthermore, to another statement on whether or not they knew that Julius Caesar used cryptography to communicate with his generals during his military campaigns, the majority of respondents (84.5%) did not know about it.

In the context of Mauritius, and on the issue of the right to privacy, respondents were asked if sending confidential information using cryptography could be considered as a tort. To this extent, the majority of the respondents (63.4%) did not consider it to be a tort. This could be explained by the fact that respondents were not aware that code-breakers, to pierce the veil of encryption with modern cryptography techniques were available to use, and if it is being misused by fraud, it could cause an infringement to privacy and thus considered as tort towards victims. Still within the context of Mauritius, and based upon the sample collected for this study, the majority of respondents believed that cryptography is not a form of cybercrime (45.1%). This could be explained by the fact that most respondents were not really aware as to why cryptography was invented in the first place (47.9%). Nevertheless, when cryptography is being used for cybercrime, most respondents agreed (60.6%) that penalties for people who deal with cryptography as a form of cybercrime should be imposed on offenders of such act. Although respondents agreed to a high extent that misuse of cryptography should be punishable by law in Mauritius, a majority of respondents could not recall or were not aware of any individual who has been arrested and imprisoned for cryptography in Mauritius or elsewhere (63.4%). This could be explained by the fact that such crime may not have received sufficient media coverage or that there has not been many prosecutions by the court on this issue.

Even though a majority of respondents were aware that certain laws on cybercrime exist in Mauritius (66.2% responded positively), when asked if any individual in Mauritius has a right to send any disguised and confidential information, a majority of respondents were indecisive on the issue (50.7%). This could be due to the fact that respondents were uncertain on the parameters of what was considered as legal and/or illegal when sharing disguised or confidential information and their

relative consequences. Because of the incertitude and lack of awareness, respondents also tended to be largely neutral (57.7%) on the question of whether or not their right to freedom of expression could be infringed in case the Mauritian legislator passed a law on cryptography. When exploring the issue of cryptography scheme and cryptoanalysis as a mean to find some weakness or insecurity in a cryptography scheme. The majority of respondents (57.7%) were not familiar with the term 'cryptoanalysis' itself.

Nevertheless, to fulfill certain gaps in the legislations, most of the respondents (64.8%), believe that it could be appropriate to review and adopt certain relevant legislation from the UK that could inspire the Mauritian legislator to implement the same in the Mauritian domestic law.

6. Conclusion and recommendations

Whether cryptography and cryptanalysis are a new form of cybercrime or not is still not well understood, especially in the Mauritian context and as per the survey that has been carried out. Therefore, it is urgent for the Mauritian legislator not to overlook this legal issue and to come forward with relevant legislation, but some countries are suggesting patented algorithms. This research should raise awareness for a more resilient IT sector, but it is still at its burgeoning stage and more in-depth research would be encouraged.

Literature

Claude E.Shannon & Warren Weaver, The Mathematical Theory of Communication, University of Illiniois Press, 1963.
Gagnon Daniel, Cryptographieet Groupesde Tresses; Mémoire présenté comme exigence partielle de la Maîtriseen Mathématiques; Université du Québec à Montréal, 2007.

Hakim J., A History of US: War, Peace and All That Jazz, Oxford University Press. New York, 2007.
Kahn D., The Codebreakers, 1967.
Gangadhar T., Debashis N. and Mandhusudhan M, Cryptography and Cryptanalysis: A Review, International Journal of Engineering Research and Technology (IJERT), Vol. 2 Issue 10, October 2013.
Talat Fatima, Cybercrimes, Eastern Book Company, 2011.
Whitfield Diffie and Martin Hellman, New directions in cryptography, IEEE Transaction on Information theory, Vol. IT, 22-11-1976, 644-54, 1976.

Tea Lalevska*

Digitalization of the cadastral system in the Republic of North Macedonia

Abstract: The subject of research in this paper is the benefits of the digitalization process of the real estate cadastre in the Macedonian legal system. The paper presents the development of cadastral law in the legal system of North Macedonia throughout history until today. Through the analysis of the regulations in the field of cadastral law, the paper shows the functionality of today's system of registration of real estate rights, which is an integral part of the so-called Geodetic-cadastral information system. The creation of this Geodetic-cadastral information system began in 2008 when the first modern Law on real estate cadastre entered into force. The paper shows that the digitalization of the cadaster system in North Macedonia established by the real estate cadaster Laws of 2008 and 2013, brought significant benefits to the legal practice. The digital connection of state authorities, institutions, and other entities with the Agency for Real Estate Cadaster enabled quick and easy access to real estate data which increased the efficiency of public and other services that they offer. The paper also contains an analysis of the digitalization of cadastral systems in comparative law in order to compare the level of development of the Macedonian cadastral law and the EU member states.

Keywords: cadaster, real-estate, data, agency, digitality

1. Introduction

The rapid development of today's modern information technology directly affected the development and digitalization process of the real estate cadaster in the Macedonian legal

* Tea Lalevska is an assistant lecturer at the Iustinianus Primus Faculty of Law, Ss. Cyril and Methodius University, Skopje, Macedonia; E-mail: t.lalevska@pf.ukim.edu.mk.

system. Considering the benefits of digitalization, the Macedonian legislator set up a goal to create a modern and digitalized system for registration of real estate and real estate rights. This modern system was expected to better respond to the needs of the legal practice and the trade relations, especially in the real estate trade.

A reliable system for the registration of real estate and real estate rights was always a primary interest in the Republic of North Macedonia. The creation of such a reliable system was conducted over a certain period of time and in several stages of development. When presenting the creation of a modern and digitalized real estate cadaster system, in this paper we also demonstrate how this system was developed in a historical sense. For this reason, the paper is divided into two parts. The first part of the paper elaborates on the historical development of the real estate cadaster in the Republic of North Macedonia. The second part of the paper analyses on the legal regime of real estate cadaster in the Law on Real Estate Cadaster of 2013, accompanied by a comparative analysis of other existing systems for the registration of real estate and real estate rights.

2. The historical development of real estate cadaster in the Republic of North Macedonia

Every country strives to establish a system for real estate registration for two basic reasons. The first reason is to have full and comprehensive information about real estate and real estate rights for fiscal purposes, and the second reason is to provide legal security in the real estate trade.

In the Republic of North Macedonia, the development of the system of real estate registration has a long history that dates

back to the Ottoman Empire.[8] According to the legal sources, in the Ottoman Empire, a deed system was in place.[9] The use of the deed system in legal practice, among other things, is confirmed by the existence of the Law on issuing deeds of 1931, which was applicable on the Macedonian territory as well. Considering the use of the deed system on Macedonian territory, it is important to emphasize that the deed system was modified in order to correspond to the habits and customs of Macedonian people related to the real estate trade. What was adopted from the Ottoman deed system was its structure. Unlike the Ottoman deed system, which was comprised of deeds only, the deed system in Macedonia also contained intabulation books. This was due to the fact that the Ottoman deed system only registered rights of ownership on real estate and not other property rights (such as servitudes and mortgage). As legal scholars claim, the establishment of intabulation books, as its integral part of the deed system, was a practical solution intended to enable publicity in the registration of other property rights[10], besides the right of ownership. The intabulation books were established after the enforcement of the Serbian Civil Code in 1854, which began to apply on Macedonian territory after 1912.[11] The existence of intabulation books gave to the Macedonian system certain characteristics which were typical for the land registration system[12].

Scholars considered that the deed system was a mere database containing the issued deeds (*tapu*), and as such was used for information purposes. This meant that, according to scholars, the deed system was not a system that could offer reliable and

[8] Групче (1985) 280-286.
[9] Чавдар К., Чавдар Кимо (2009) 25; Stamenković (1989) 7; Gams (1980).
[10] More about the property rights, see: Gavella, Josipović, Gliha, Belaj, Stipković (1998).
[11] Георгиевски (1978) 43.
[12] Георгиевски (1978) 20.

undisputed proof of ownership. Due to this lack of reliability, there was a legal practice that consisted of two steps approach in the process of proving ownership of real estate. The first step was the issuing of the deeds. This was an administrative procedure conducted by the administrative authorities. The second step was the confirmation of the issued deed, which was done by the courts, after running a check on the accuracy of the data contained in the deed. As we can see, the courts played a crucial role in confirming the deeds in the deeds system.[13]

Another reason why the deed system was not considered to provide a definitive proof of ownership, was its facultative nature. The facultative nature meant that landowners were not obligated to acquire a deed, so it was issued only if the owner requested it. Only in exceptional situations issuing of the deed was mandatory.[14] Even though the deed system was used for a long period of time on Macedonian territory, scholars rightfully note that it was not the best solution for land registration. According to scholars, the deed system had many shortcomings, among the most serious were the fragmentation, incoherency, and lack of reliability of this system.

The deed system was also not implemented everywhere on Macedonian territory, which resulted in a relatively small number of real estate being covered by this deed system. As scholars note, providing full coverage of real estate registration by the deed system was expensive and therefore unjustifiable at the time. All these reasons caused the deed system to be slowly abandoned. However, the intabulation books continued to be used.

---

[13] Групче (1985) 283-284.

[14] According to legal sources, issuing deed was mandatory in the following situations: 1. when the acquisition of the land ownership was derivative, 2. when the land was mortgaged and 3. when the land was in social ownership. See: Групче (1985) 281-282.

Due to the noted shortcomings of the deed system, in the period of socialism, the legislator began its replacement with the land cadaster system.[15] Officially, the land cadaster system was implemented when the Law on Land Survey and Cadaster of 1972[16] was enforced. According to legal scholars, the land cadaster system was much more reliable than the deed system, because it contained data about the land (such as geographical position, size, cadastral class, culture, etc.) which was entered into a public record.[17] The presumed reliability of the land cadaster system, according to scholars, was a decisive factor for it to be accepted on Macedonian territory, instead of the land registration system accepted by most of the countries of the Former Yugoslavia.

The Law of 1972 offered a legal base for creating a land cadaster system that contained data about the real estate, acquired by land surveys which was an accurate method for collecting data about real estate.[18] The land cadaster divided the land into land parcels as basic units and presented data for each existing land parcel. The data included numeric identification of the parcel, size of the parcel, cadastral classification, and valuation of the land.[19] According to the Law, the land cadaster was a public record providing information about the physical state of the land, which was considered accurate since they were collected with land surveys. However, the land cadaster was not considered to contain accurate and reliable information about ownership and other property rights over the land parcels. As a result, the data from the land cadaster was issued in the form of

[15] Regarding the historical development and functions of the land cadaster, see: Stojanović (1983) 300.
[16] Official Gazette of SRM number 34/72 и 13/78.
[17] Чавдар Кирил, Чавдар Кимо (2009) 28.
[18] Law on land survey and cadaster, art. 2.
[19] See: Law on land survey and cadaster, art. 28. Also see: Групче (1985) 267-268.

a title deed and not a property sheet. Even though the land cadaster was not a complete record regarding property rights of real estate, it still represented the first major step in creating a real estate cadaster.

The efforts for creating a complete and reliable real estate cadaster continued with the enforcement of the Law on Survey Cadaster and Registration of Rights on Real Estate of 1986.[20] This Law aimed to create a real estate cadaster that would include data about the physical state of real estate (land and structures), and also data about the property rights on that real estate.[21] In order for the data to be complete, the Law mandated registration of the full state of the real estate.[22] The Law also prescribed the issuing of property sheets for each land parcel in the real estate cadaster that contained data about the full state of real estate (its physical state and existing property rights). However, this aim of the Law was not reached in full, because in legal practice the mandatory registration rule was not respected and often the information about real estate was incomplete, meaning, that most property rights were not registered. As a result of incomplete information in the real estate cadaster, the intabulation books were used in parallel with the property sheets.[23] This was an additional burden for people involved in the real estate trade because they had to collect data about the state of the real estate from various sources and still did not have the certainty that the data they collected reflected the actual state of the real estate.

[20] Law on survey, cadaster and registration of rights on real estate, Official Gazette number 27/86, 17/91, 84/05, 109/05 and 70/06.
[21] Law on survey, cadaster and registration of rights on real estate, art. 2 and 3.
[22] Law on survey, cadaster and registration of rights on real estate, art. 10.
[23] Чавдар Кирил, Чавдар Кимо (2009) 27-28.

Since the Law of 1986 did not meet the expectations and did not provide a real estate cadaster system that was complete and reliable, the Macedonian legislator opted for drafting a new Law on Real Estate Cadaster that came into force in 2008.[24] This new Law was drafted following the example of modern real estate cadaster Laws in EU countries.

One of the essential innovations was the creation of a digital system containing all data about real estate.[25] This digital system was called the Geodetic-cadastral information system (GCIS).[26] The graduate creation of GCIS began right after the Law of 2008 came into force. The primary way of collecting data, according to the Law, was the systematic registration of real estate. The systematic registration was funded by the State's budget. This form of registration was intended to include every real estate on Macedonian territory, and it was conducted for the purpose of collecting full data about the state of real estate with land surveys and filling up questionaries about existing real property rights on the land parcels, and also collecting valid legal documents for acquiring ownership and other property rights. All the information collected was digitalized and entered into the GCIS. The process of systematic registration of real estate was finalized in December 2012. By completing the systematic registration of real estate, a complete, reliable, and digital real estate cadaster system was implemented in the Republic of North Macedonia.

[24] Law on real estate cadaster, Official Gazette of the Republic of Macedonia number 40/08, 158/10, 17/11, 51/11 and 74/12.
[25] Живковска (2011) 135.
[26] Law on real estate cadaster, art. 2.

3. The real estate cadaster system in the substantive law in the Republic of North Macedonia

The Law of 2008 contributed significantly to the creation of a modern, complete, and comprehensive real estate cadaster that was also digitalized. However, the issue that was left unresolved by the Law of 2008 was the issue concerning infrastructure. This Law had not planned for incorporation of the infrastructure as part of the real estate cadaster. Considering the issue of infrastructure registration, the Macedonian legislator has decided that infrastructure should be considered as a separate type of real estate, owned independently from the land it is built on. This type of legal regime about infrastructure requires a separate registration, meaning creating a separate cadaster on infrastructure. This major novelty, according to the opinion of the legislator, required a draft of a new Law on real estate cadaster and not amendments to the existing Law of 2008.

All this resulted in the passing and enforcement of the Law on Real Estate Cadaster of 2013.[27] This new Law, which is still in force, adopted many of the legal solutions found in the Law of 2008. This means that the digitalization of the real estate cadaster system continued. At the same time, the process of creating a digital cadaster of infrastructure began.[28]

3.1. The Geodetic-cadastral information system (GCIS)

The creation of the GCIS, as it was underlined, was the first major step in the process of the digitalization of the Macedonian real estate cadaster system. GCIS is a digital system that incorporates different types of data about real estate and the

[27] Law on real estate cadaster, Official Gazette of the Republic of Macedonia number 55/13, 67/13, 41/14, 115/14, 116/15, 153/15, 192/15, 61/16, 172/16, 64/18 and Official Gazette of the Republic of Nort Macedonia number 124/19.
[28] Живковска, Пржеска, Димова, Петрушевска (2013) 12.

rights of real estate. The data collected and entered into the GCIS is divided into several categories that the Law of 2013 describes as parts of GCIS. These parts are 1. Spatial and descriptive data of the real estate cadaster;[29] 2. Basic geodetic works;[30] 3. Geodetic works for special purposes;[31] 4. Real estate survey;[32] 5. State border survey;[33] 6. Real estate value;[34] 7. Topographic maps;[35] 8. Registry of spatial units;[36] 9. Graphic

[29] Spatial data defines the real estate within the single reference system and the State's cartographic projection. Descriptive data from the real estate cadaster refer to the data which describes the features and characteristics of the real estate (such as cadastral culture and class of the land, name of the place, number of the building, data about the separate and common part in the building and data about other structures on the land. See: Law on real estate cadaster, art. 2, par. 2.

[30] Basic geodetic works are defined as works including the State's geodetic data, the cartographic projections and the reference networks, See: Law on real estate cadaster, art. 2, par. 2.

[31] Geodetic works for special purposes refers to the geodetic works related to the spatial planning, production of numerical data on the real estate for realization of the urban plans and urban planning documentation, See: Law on real estate cadaster, art. 2, par. 2.

[32] Real estate survey is defined as a procedure for processing and formulating the spatial and descriptive data in service of the real estate cadaster, See: Law on real estate cadaster, art. 2, par. 2.

[33] The survey of the state border involves the marcation and collecting of spatial and descriptive data of the border points. See: Law on real estate cadaster, art. 2, par. 2. and art. 58.

[34] The calculation of the real estate value which is registered in the real estate cadaster is done on the basis of a mass evaluation model. See: Law on real estate cadaster, art. 2, par. 2 and art. 216, par. 1.

[35] The topographic maps are a type of geographic maps that chart the position of water, vegetation, the topography of the land and administrative borders. See: Law on real estate cadaster, art. 91. Also see: Живковска, Пржеска (2018) 160.

[36] The spatial unit is defined as limited part of area that is established for registering and processing statical and other type of data in interest to the country. See: Law on real estate cadaster, art. 2, par. 2.

registry of streets and house numbers;[37] 10. Registry of prices and rents[38] and 11. Graphic registry of construction land.[39] As we can notice from the content of GCIS, it includes the digital real estate cadaster as its comprising component. This is very important for the cohesion of the entire system because it enables all the data to be interlaced compared, analyzed, and evaluated as a whole.[40]

This type of systematic approach in collecting and evaluating the data enabled the Agency for Real Estate Cadaster (in the following: the Agency) to offer complete and accurate information about the state of the real estate. It needs to be noted, that the collection and digitalization of the data, now entered in the GCIS, has relevance both for the public interest, and the interest of private individuals. The data concerning the State's border, topographic maps, spatial units, and other spatial data concerning the real estate are matters of public interest. Their digitalization enables State authorities to have precise information about the terrain which is very useful for urban planning and development purposes, and also for the State's security system. The data contained in the Graphic registry for streets and house numbers was especially important for municipalities and other local authorities because it provides accurate digital data that makes the location of the streets and house addresses to be easily identified. Regarding the

[37] The Graphic registry contains spatial and descriptive data for streets and house numbers, as well as the spatial data that enables the affiliation of the house number with the street. See: Law on real estate cadaster, art. 227.
[38] The Registry of prices and rents records the sale prices of the real estate collected from the sales contract and the value of the real estate determined as a base for calculating of the sales tax. See: Law on real estate cadaster, art. 221.
[39] The Graphic registry for construction land consists of spatial and descriptive data for the construction land overlapped with the data obtained from zoning plans and other urban planning acts. See: Law on real estate cadaster, art. 232.
[40] Живковска, Пржеска (2018) 268-269.

importance of the Graphic registry for construction land, we note that the digital data it contains is very helpful for municipalities and other authorities tasked to prepare and pass zoning plans and other urban planning acts. This Registry is helpful because enables the creators of the zoning plans to plan urban parcels that coincide with the shape and size of the land parcels. As a result, the enforcement of the passed zoning plans is easier for the landowners and other investors. Considering this, we can conclude that the Graphic registry for construction land is useful for private individuals as well, who are looking to exercise their right to build. As for the Registry for prices and rents, it is created to provide data in a digital form that enables interested parties to collect information about the value of the real estate in a certain area and also about the prices of rents in that area. This data could potentially impact the real estate market and affect the sales and rent prices. The data from the Registry for prices and rents is also used for fiscal purposes when determining the base value for calculating taxes. The fact that this data is collected in a digital form makes it very easy for it to be distributed and evaluated by the interested parties. Of all the data collected and entered into the GCIS in a digital form, the most important is the data found in the real estate cadaster as part of the GCIS. The real estate cadaster is created as a result of processing and presenting the processed data in the form of comprehensive information about the physical state of the real estate and also about the rights of the real estate. This information is issued to the interested parties by the Agency in the form of a property sheet, pre-registration sheet, information sheet, and as a certificate for changes made in the real estate registration for a particular land parcel. The property sheet contains information about the land, structures, and rights on a certain land parcel.[41] This sheet is crucial for legal traffic, because it is considered to be a valid proof of ownership and

[41] Law on real estate cadaster, art. 156.

other property rights on real estate. The pre-registration sheet contains information about structures, under construction, information about the land parcel where the construction is conducted, and the pre-emption contracts and mortgage contracts related to the structure under construction.[42] This sheet resulted from the need for publicity concerning the trade with structures under construction in the real estate market. The information sheet contains information about illegal structures[43] found on the land parcels.[44] From this sheet, we can gather information about the land parcel where the illegal structure is found, a description of the structure, and information about the person in possession of the structure. It is important to note that the information sheet is not considered to be proof of ownership for the illegal structure. The certificate contains information about all the consecutive changes in the registration of a certain land parcel and the rights on that land parcel, starting from the moment when that land parcel was entered into the real estate cadaster.[45] This information, provided by the certificate, is used as proof in property disputes and for other purposes by

[42] Law on real estate cadaster, art. 158.

[43] According to Law on construction, all structures built without a building permit or contrary to the issued building permit are considered to be illegal structures. See: Law on construction of 2009, Official Gazette of the Republic of Macedonia number 130/09, 124/10, 18/11, 18/11, 36/11, 49/11, 54/11, 13/12, 144/12, 25/13, 79/13, 137/13, 163/13, 27/14, 28/14, 42/14, 115/14, 149/14, 187/14, 44/15, 129/15, 129/15, 217/15, 226/15, 30/16, 31/16, 39/16, 71/16, 103/16, 132/16, 35/18, 64/18, 168/18 and Official Gazette of the Republic of North Macedonia number 244/19, 18/20, 279/20, 96/21 and 227/22, art. 57 and art. 134.

[44] The reason why illegal structures are registered in separate parts of the real estate cadaster and not in property sheets, is because Macedonian law does not recognize ownership rights over illegal structures. The information sheet only contains data about the factual state of real estate without registering any type of property rights. The data in the information sheet for illegal structures exists until an illegal structure is found on the real estate. If the illegal structures are later legalized or demolished the information in the information sheet will be deleted. See: Law on real estate cadaster, art. 159.

[45] Law on real estate cadaster, art. 161.

individuals looking to prove, reaffirm, or exercise their rights over a particular land parcel.

Digitalization also enabled the process of collecting and evaluating the data about real estate to be much faster as opposed to collecting the data in an analog form. In order to secure the safety of the data stored in the GCIS database, the legislator prescribes an obligation for the data to be stored in a manner that provides a maximum degree of protection from unauthorized access and intervention of the stored data. Providing the safety of the data directly contributes to their reliability.[46] The legal obligation for providing data safety falls on the Agency according to the Law of 2013. As the Law states, the Agency is to undertake legal and technological measures and procedures for the protection of data preventing any illegal collection, processing, use, or transfer, as well as any modification, destruction, or disclosure of the data to unauthorized persons inside or outside the Agency.[47] In compliance with its obligations, the Agency permits strictly controlled access to the GCIS by its employees. The controlled access also means limited access, so that each employee can only modify the data he is assigned to work with.[48] Any access and modification of the data in the GCIS by its employees is also recorded in the system, which means that the system provides insight into who and how used, altered, and issued the data from GCIS to third parties.

Another step in the process of digitalization of the real estate cadaster system was also the transformation of the analog data, previously collected, into a digital form. This primarily included the cadastral plans drawn on paper and also included the digitalization of documents and other relevant information

[46] Law on real estate cadaster, art. 28.
[47] Law on real estate cadaster, art. 32.
[48] Law on real estate cadaster, art. 30.

collected and stored on paper. The process of digitalization of the analog data did encounter some problems. The problems mainly resulted from the different methodologies used at that time of the collection of the analog data as opposed to the methodologies used during the digitalization process. As a result, the data entered in the digital form did not completely overlap with the data collected in the analog form. For example, it often occurred for the same real estate parcel to have different descriptive data concerning its size. The analog data showed that a parcel was 500 m^2, while the digital data showed that the parcel was 487 m^2. Real estate owners were affected by these discrepancies to a point that they sued the Agency before the Administrative Court, for entering the digital data incorrectly, to their opinion. Since these discrepancies in most cases could not be avoided, the Administrative Court was flooded with these types of lawsuits.[49]

One of the most important novelties, as it was mentioned, is the implementation of cadaster on infrastructure.[50] This type of cadaster exists within real estate cadaster as its separate component. The cadaster of infrastructure contains spatial and descriptive data about infrastructure. According to provisions of the Law of 2013, the term "infrastructural objects" includes traffic infrastructure underground and aboveground installation and electronic communication networks with all its components.[51] All the infrastructures defined in the Law of 2013, are considered as a separate type of real estate independent of the land they are found on. Due to this legal treatment, infrastructure is registered in a separate cadaster and owners of infrastructure get separate property sheets for

[49] More about this, see: Živkovska, Prževska (2015) 487-503.
[50] Живковска, Пржеска, Димова, Петрушевска (2013) 319.
[51] Law on real estate cadaster, art. 2, par. 1.

infrastructure as proof of their right to ownership.[52] As for the content of the property sheets for infrastructure, it is very similar to the content for the property sheet and includes data about the owner, data about the land where the infrastructure is found (starting point and ending point), and descriptive data about the type, shape, size, etc. of the infrastructure and data about the other property rights over the infrastructures.

Since the implementation of the cadaster of infrastructure was a novelty of the Law of 2013, there needs to be a process of initial registration of the infrastructure by entering all the necessary data in a digital form. This was done at the request of the owner of the infrastructure who is obligated to provide evidence about his ownership of the infrastructure, and documentation about the conducted survey of the infrastructure contained in a project for infrastructure.[53] If the owner provides proof of ownership and submits a project for infrastructure, then his right to ownership and all data concerning the infrastructure is entered in a property sheet in the cadaster of infrastructure. In cases when the person was not able to provide proof of ownership and only submitted a project for infrastructure, the Agency proceeds to enter the data from the project of infrastructure in an information sheet.[54] This means that the infrastructure is considered an illegal structure until such time that proof of ownership can be provided or legalization is conducted.

Considering that, there are no provisions of the Law of 2013 for a mass registration of infrastructure, the implementation of the

[52] See: Law on real estate cadaster, art. 157, par. 1 and par. 2. Also see: Живковска, Пржеска, Димова, Петрушевска (2013) 259-262.
[53] See: Law on real estate cadaster, art. 178, par. 1, par. 2 and par. 3. Also see: Живковска, Пржеска, Димова, Петрушевска (2013) 320.
[54] See: Law on real estate cadaster, art. 184 par. 1 and art. 185, par. 1. Also see: Живковска, Пржеска, Димова, Петрушевска (2013) 325.

cadaster of infrastructure is an ongoing process that continues on until the present day. Nevertheless, the fact that infrastructure is gradually been registered in a digital cadaster of infrastructure is a significant step towards creating a complete real estate cadaster system that can provide 3D data about all structures above and below ground. This is very helpful for public authorities and private individuals as well because knowing exactly where infrastructure is located, makes it easier to plan for its protection when needed and to prevent any damages to it that can be both costly and dangerous. For owners and other property rights holders of infrastructure, the digital cadaster of infrastructure provides security in guaranteeing their rights.

The digitalization of the real estate cadaster system enabled the establishment of a digital connection between the Agency, the public authorities, notary publics, and private surveyors.[55] This digital connection that was established enabled the connected outside parties to directly access the data collected in GCIS.[56] The outside parties, that were connected, can only view the data and use it for their work related to real estate, but without the possibility to make any alteration to that data.[57] This was very beneficial for the outside parties because they had easy access to the data at any time without delays, which in return increased the effectiveness of the services they provided for the public.

Taking into account all the novelties and overall benefits of the digitalization of the real estate cadaster system in the legal system of the Republic of North Macedonia, we can draw several conclusions:

[55] See: Живковска, Пржеска, Димова, Петрушевска (2013) 80. Also see: Law on real estate cadaster, art. 34.
[56] Law on real estate cadaster, art. 31.
[57] Law on real estate cadaster, art. 33.

First: the digitalization process of the real estate cadaster system brings significant benefits for the legal practice providing quick and easy access to detailed data about the state of real estate and rights on that real estate.
Second: the fact that the data about the real estate is kept in a digital form, makes it easy to be processed and distributed for different aims and purposes.
Third: the fact that the registration of data in real estate cadaster is mandatory, provides legal security for all concerned parties, guaranteeing that all entered data is complete and trustworthy.
Fourth: the documentation issued by the Agency for Real Estate Cadaster in the form of property sheets, pre-registration sheets, information sheets, and certificates, are used as proof for existing rights on real estate (property sheet) and other facts related to the real estate and/or to the rights on real estate.
Fifth: considering that the real estate cadaster is a public record, its existence provides publicity of the entered data which in return provides legal security for all concerned parties.
Sixth: the digitalization of the real estate cadaster system also enables the creation of a digital network where all the officially acting parties in the areas of real estate trade, urban planning and development, and protection of rights on real estate can cooperate, extracting the information they need from this digital network.

4. The digitalization of cadastral systems in comparative law

By analyzing the existing real estate registration systems, we note that there are four basic real estate registration systems: integral cadaster system, land registration system (cadaster and land books), Torrens system, and the system of transcription and inscription.[58]

[58] More about this, see: Kovačević Kuštrimović, Lazić (2004) 391; Бабић (2021) 525; F. Čulinović (1931); Krstić (1971); L. Marković (1928) 387; Станковић, Орлић (1999) 318; Gams (1980); Георгиевски (1984) 10-11;

The integral cadaster system is characterized by the integration of all real estate data (state of real estate and rights on real estate) in one all-inclusive system that in modern times goes from being analog to being part analog part digital or completely digital. This type of system is accepted for real estate registration in the Macedonian legal system and in the legal system of Montenegro.[59]

The land registration system, also known as the Austrian-German system, differs from the integrated real estate cadaster because it is comprised of two elements: cadaster and land books.[60] The cadaster contains data about the state of the land. The land books contain data about the rights of real estate.[61] These books are comprised of several parts such as a main book and a collection of documents.[62] According to this system, the entry in the land book is a presumption for the acquisition of real estate rights based on legal acts.[63] This system, according to scholars, was initially created in the German legal system and later on was adopted by other countries such as Poland, the Czech Republic, Croatia, Serbia, Slovakia, Hungary, Slovenia and other countries.[64]

Regarding the Torrens system[65], the scholars note that this system is based on the direct registration of real estate rights in

---

Орлић (2000) 434; Simonović (1998) 777; Stamenković (1989) 167; Josipović (2001) 9; Групче (1985) 264; Карамарковиђ (2003) 100-120.

[59] Rašović (2005) 565.

[60] Гостовић (2000) 246-272; Kovačević-Kuštrimović, Lazić (2004) 403. About the historical review of land books, see: W. Raiser (1957) 81-85.

[61] Гамс (1949) 256-257.

[62] Kovačević-Kuštrimović, Lazić (2004) 404.

[63] F. Čulinović (1931) 1.

[64] Бабиђ (2021) 527.

[65] More about Torrens system and its characteristics, see: Групче (1985) 265; Станковић, Орлић (1999) 316.

the land registry. This system for the first time was created in Australia in 1958 with the enforcement of the Law of ownership of real estate. According to legal scholars, the Torrens system is a very simple system characterized by entering data about land in a book[66]. This system is considered suitable for countries where land holdings represent a large area. This system is accepted by several states in the USA and parts of Great Britain.[67]

The system of transcription and inscription is also known as the French system.[68] The legal scholars considered that this system was built gradually over a long period of time.[69] According to this system, the property rights on real estate are acquired by submitting an application form in the public registration book. In other words, the right of ownership is transferred with the contract, and the transfer is publicized with the registration in a public book in order to inform third parties about the property transfer. This system was accepted by several EU countries such as Italy, Belgium, Spain, Portugal, and others.[70]

As scholars note, each country accepts some type of real estate registration system that is considered to be the most appropriate, due to the traditions, history, habits, and modern needs for real estate trade and legal security.[71] It is important to keep in mind that the classifications of the real estate registration systems are mainly theoretical. In practice, each country has developed, modified, and adjusted the accepted system to its specific needs. This is why there is no pure form of land registration system that completely coincides with the theoretical classifications.

---

[66] Групче (1985) 265.
[67] Станковић, Орлић (1999) 317.
[68] Групче (1985) 264; Орлић (2003) 33.
[69] P. J. Chenu (1960) 15.
[70] Бабић (2021) 526.
[71] Krstić (1972) 1-30.

5. Conclusion

The paper analyzes the digitalization of the cadastral system in the Republic of North Macedonia focusing on its benefits. As the paper demonstrates, in the Republic of North Macedonia, the development of the system of real estate registration has a long history that dates back to the Ottoman Empire when a deed system was in place. Taking into account the use of the deed system on Macedonian territory, the paper points out that the deed system was modified in order to correspond to the habits and customs of the Macedonian people related to the real estate trade. As a result, the deed system in Macedonia, unlike the Ottoman deed system, also contained intabulation books where other property rights were also registered.

By analyzing the shortcomings of the deed system and the need for its reformation, the paper demonstrates that in the period of socialism, the legislator began replacing it with the land cadaster system. The land cadaster system was officially implemented with the Law on Land Survey and Cadaster of 1972. As the paper shows, the land cadaster system turned out to be more reliable than the deed system. The higher degree of reliability of the land cadaster system was a result of the fact that it contained data about the land (such as geographical position, size, cadastral class culture, etc.). A closer analysis of the land cadaster system implemented in Macedonian law has also shown some shortcomings as well. This was due to the lack of accuracy of the information about land ownership and other property rights on the real estate. Since the data lacked reliability, the information pertaining to the real estate was issued in the form of a title deed, and not a property sheet. Even with its shortcomings, the land cadaster system still represented the first major step in creating a real estate cadaster.

As the paper shows, the creation of a complete and reliable real estate cadaster system continued with the enforcement of the Law on Survey Cadaster and Registration of Rights on Real Estate of 1986. This Law aimed to create a real estate cadaster that would include data about the physical state of real estate, and also data about the property rights on that real estate. This aim of the Law was not reached in full, because in legal practice the mandatory registration rule was not respected and often the information about real estate was incomplete, meaning that most property rights were not registered. Additionally, the paper emphasizes that the process of collecting data about the state of real estate at that time was complicated because data collection was done using various sources, and at the end, did not result in demonstrating the actual state of the real estate. In conclusion, the Law of 1986 did not provide a real estate cadaster system that was complete and reliable.

The Law of 2008 was the first contemporary Law on real estate registration which was drafted following the example of modern real estate laws in EU countries. The paper concludes that one of the essential innovations of this Law was the creation of a digital system (GCIS) that provided digital registration of the state of the real estate and of the rights of the real estate. As the paper underlines, the Law of 2008 provided a modern real estate cadaster system. However, it did not include registration on infrastructure.

The need for further development of the real estate cadaster system in the Republic of North Macedonia resulted in the enforcement of the new Law on Real Estate Cadaster of 2013, which is in force today as substantive law. As the paper shows, the Law of 2013 offers a regulation intended to provide an upgrade to the existing real cadaster system created on the basis of the Law of 2008. The most important novelty of the Law of 2013 is the implementation of the cadaster on infrastructure.

This novelty provided a complete registration of all types of real estate in the Macedonian legal system. As a result, a modern, digital, and complete real estate cadaster system was in place. The creation of this cadaster system, as the paper shows, provided many positive effects on real estate trade, and the protection of real estate rights, it augmented the performance of public institutions, the court system, the administration, and other entities involved in protecting the property rights of all individuals.

Literature

Бабић И, *Увод у грађанско право и стварно право* (девето измењено и допуњено издање, Службен гласник, Београд 2021).
Gams A, *Osnovi stvarnog prava* (Naučna knjiga, Beograd, 1980).
Gavella N, Josipović T, Gliha I, Belaj V i and Stipković Z, *Stvarno pravo* (Informator, Zagreb 1998).
Гамс, *Стварно право* (Београд 1949).
Групче А, *Имотно (граѓанско) право, втор дел, Стварно право* (Култура, Скопје 1985).
Георгиевски С, *Таписки систем во Југославија,* (Правен факултет "Јустинијан Први", Скопје 1978).
Георгиевски С, "Evidencija nepokretnosti" (Naša zakonitost 1984).
Гостовић М, "Системи јавних регистара земљишта у Европи" (Земљишне књиге и јединствена евиденција, Зборник регерата и законски текстови, Анали, Правног Факултета у Београду 2000).
Živkovska R, and Prževska T, "Problemi povodom sudske zaštite upisa u katastar nepokretnosti" (Pravni život, Časopis za pravnu teoriju i praksu, Broj 10/15, Godina LXIV/ Knigja 576, Beograd 2015).
Живковска Р, and Пржеска Т, *Стварно право, Практикум* (Европа 92, Скопје 2018).
Живковска Р, Пржеска Т, Димова С, and Петрушевска Н, *Коментар на Законот за катастар на недвижности* (Правен факултет "Јустинијан Први" Европа 92, Скопје 2013).
Живковска Р, *Стварно право* (Европа 92, Скопје 2005).
Живковска Р, "Катастарот на недвижности во правниот систем на Република Македонија" (Зборник на Правниот факултет "Јустинијан Први", Скопје 2011).

Josipović T, *Zemljišno knjižno pravo* (Zagreb 2001).
Kovačević Kuštrimović R, and Lazić M, *Stvarno pravo* (GIP PUNTA, Niš 2004).
Krstić Đ, *Evidencija prava na nepokretnostima* (uporedni prikaz, Beograd 1972).
Карамарковиђ Л, "Систем земљишних књига и јединствене евиденције" (Земљишне книге и јединствена евиденција, Зборник регерата и законски текстови, Анали, Правног Факултета у Београду 2000).
Marković L, *Građansko pravo – Opšti deo i stvarno pravo* (Beograd 1928).
Rašović Z, *Stvarno pravo* (drugo izdanje, Beograd 2005).
Pierre J C, *De la transcription a la publicite fonciere* (Bordeaux 1960).
Simonović D, *Reafirmacija zemljišnih knjiga* (Pravni život 1998).
Stojanović D, *Stvarno pravo* (šesto izmenjeno i dopunjeno izdanje, Beograd 1983).
Stamenković D, *Priručnik za upise nepokretnosti* (Savremena administracija, Beograd 1989).
Станковић О, and Орлић М, *Стварно право* (десето издање, Номос, Београд 1999).
Орлић М, "Увођење и обнављање земљишних књига" (Земљишне книге и јединствена евиденција, Зборник регерата и законски текстови, Анали, Правног Факултета у Београду 2003).
Чавдар К, Чавдар Кимо, "Правнозаштитна функција на запишувањата на правата во катастарот на недвижности", (стручно списание Правник 204, Здружение на правници на РМ, Скопје 2009).
Čulinović F, *Zemljišne knjige i njihovo osnivanje* (Beograd 1931).
Wolf R, *Sachenrecht,* (Tübingen 1957).
Law on land survey and cadaster (1972), Official Gazette number 34/72 и 13/78.
Law on survey, cadaster and registration of rights on real estate (1986), Official Gazette number 27/86, 17/91, 84/05, 109/05 and 70/06.
Law on real estate cadaster (2008), Official Gazette of the Republic of Macedonia number 40/08, 158/10, 17/11, 51/11 and 74/12.
Law on real estate cadaster (2013), Official Gazette of the Republic of Macedonia number 55/13, 67/13, 41/14, 115/14, 116/15, 153/15, 192/15, 61/16, 172/16, 64/18 and Official Gazette of the Republic of North Macedonia number 124/19.

Law on State's survey and real estate cadaster (Montenegro), Official Gazette RCG, br. 29/07, 32/11, 40/11, 43/15, 37/17, 17/18.

Bhavna Mahadew*

The digitalisation of law: how prepared are we to welcome legal practice and education which are artificially intelligent?

Abstract: The global epidemic of 2020 has increased the importance of distant work and team collaboration. Teams are looking into and making use of the remote work platforms required to replace the stand-up meetings that are regularly held in agile organizations. Online solutions are necessary to provide insight into project status and the accountability needed to ensure that tasks are completed in a timely manner and within budget. In order to provide corporate transparency and predictive insights into the working process, contemporary AI projects aim to digitally convert organizational data. The relationship between artificial intelligence, the law, and the pervasive digital revolution is examined in this essay. This essay explores the connections between artificial intelligence, the law, and the widespread digital change. The extent to which numerous emergent problems with modern technologies conflict with human rights and wellbeing is a cause for legitimate worry. However, attorneys will be crucial to the enforcement and protection of these rights. Lawyers will be a vital source of information and direction for the creation of "ethical" AI in a proactive not just a reactive way, if not even more so.

Keywords: artificial intelligence, legal profession, legal education, effects, digitalization of law

1. Introduction

We live in a world where knowledge may be shared instantly and as needed. 2020's global epidemic has made remote work and team communication more important than ever. Teams are

* Bhavna Mahadew is a lecturer at the School of Business, Management and Finance, University of Technology, Mauritius; bhavna.mahadew@utm.ac.mu.

investigating and exploiting the remote work platforms necessary to take the place of stand-up meetings frequently seen in agile workplaces. Online solutions are required to give project status visibility and the accountability required to guarantee that activities are done on time and within budget. The goal of current AI projects is to digitally convert organizational data in order to deliver corporate transparency and predictive insights into the working process. This essay explores the connections between artificial intelligence, the law, and the widespread digital change. The extent to which numerous emergent problems with modern technologies conflict with human rights and wellbeing is a cause for legitimate worry. However, attorneys will be crucial to the enforcement and protection of these rights. Lawyers will be a vital source of information and direction for the creation of "ethical" AI in a proactive not just a reactive way, if not even more so.

Legal professionals were compelled to swiftly embrace the tools and strategies of online sharing of information and virtual interaction as the face-to-face, on-site world of work transitioned into a time of working from home, virtual meetings, and sophisticated analytics of data. The remote work environment received less attention from the courts. After the pandemic began, access to justice through legal remedy almost completely disappeared. Courts shut down and only progressively started using technology for virtual meetings to carry out certain aspects of their business. Due to lengthy delays in jury trials, the cornerstone of American justice, there will be a significant backlog of cases in American courts through the rest of 2020.[1] Justice administered through the courts is inertia-bound in its practices, despite the voices of hope being heard.[2]

[1] Timms, M. (2021).
[2] Suuskind, R. (2020).

Legal instructors were forced to implement remote learning procedures or cease operations entirely. The second choice was not an option. Prior to March 2020, academics who were inexperienced with Zoom discovered that it was their newly established classroom. Professors of law and their students found the conversion of on the spot legal education to remote learning to be less than satisfying. Remote employment 'Zooming' in 2020 happened quickly. Business as usual in almost all areas of the economy was drastically altered by the global pandemic. As the spread of infection threatens even the standard physical examination in healthcare, telehealth services multiplied. In the United States, the number of remote medical consultations rose by 4,347% between March 2019 and March 2020.[3] Depending on the country or region, non-essential services were discontinued, and face-to-face interactions were considered potentially fatal.

Almost overnight, the majority of office employment switched to a work-from-home arrangement. Up to 85% of staff at some companies reportedly only work from home.[4] The shift to a virtual employment, economy, and even social environment will continue after the pandemic. Up to 20% of the workforce, and no less than 50% of the workers whose jobs permit it, is anticipated to work from home continuously and exclusively.[5] The exponential rise in everyday digital data production brought on by the growth of remote workers' reliance on cloud-hosted technology resources has been an unforeseen effect of the 2020 worldwide pandemic.[6] The legal industry is comparable to all other industries in this regard.

[3] Gelburd, R. (2020).
[4] Ekholm, B. & Kutcher, E. (2020).
[5] Thompson, D. (2020).
[6] Zacks Equity Research (2020).

The evolution of most industrial sectors, namely the practice of law and the training of attorneys, will change as a result of the digital revolution. Technology advancements will change the essence of justice and instruction and how they are given, although not being without substantial problems.[7] The expansion of digital data stimulates the creation of cutting-edge AI technology that can transform vast quantities of binary digits into useful information. Digital data has been referred to be "the new oil" since it is buried deep and difficult to obtain.[8] This resource's hidden gems need to be refined and given to the consumer. An important use case for AI applications that will significantly alter current legal procedures and the function of legal professionals is the intricate intersection of international laws.[9]

Can technological advancements also promote justice and prevent civic unrest? Can AI-powered resolution of disputes effectively handle conflicts while also addressing the more fundamental requirements of justice in a culture that values technology? For the legal community, especially those who instruct and educate lawyers, these are crucial inquiries. Swift action is necessary to protect legal frameworks without sacrificing the moral high ground of ethical making of rules, norm setting, and practical application. To convince those they represent (clients, students, and anyone turning to them for direction) that AI will help to protect human legal rights, obligations, and solutions, legal practitioners and legal scholars must band together to offer one voice.

[7] Sternlight, J. (2020).
[8] Rob, S. (2020).
[9] Deeks, A. (2020).

2. An environment of collaboration enabled by technology

The company's in-house legal department, the main source of clients for attorneys, was activated by the pandemic of 2020. Over 80 worldwide in-house compliance and legal officials used the terms "digital transformation," "technology strategy," and "automation" to characterize their top operational objective in the economy following the pandemic.[10] By reducing the amount of time spent on low-value tasks and focusing squads on high-value-add assignments, simplifying the natural productivity of a growing remote staff, boosting organizational efficiency and productivity, and permitting more effectively risk evaluation and reduction by means of IT/data analytics, these corporate legal leaders particularly hope to accomplish higher-value work and improved productivity through digital change.

Compared to outside counsel, in-house legal departments place a much greater emphasis on teamwork and the technological tools that support it.[11] Compared to outside counsel, in-house counsel had a 305% COVID-19 spike. Client expectations are crucial in a buyers' market. To optimize their contribution to the environment of legal services, LPM practitioners would be well advised to take into account the corporate clients' digital transformation ambitions. An annual detailed study of technological trends and how they might affect the sectors they service is provided by the Gartner Hype Cycle. Legal technologies are examined in terms of how they now affect the legal sector. When it comes to consumer usefulness, enthusiasm frequently precedes practicality in emerging technology applications.[12] Despite the fact that many legal-related software applications have yet to live up to their potential, Gartner

[10] Dance, E. & Pedersen, J (2020).
[11] In-house Counsel Go Collaboration Crazy (2020).
[12] Van der Meulen, R. (2020).

identified four developing trends that, by 2020, will start to meet the needs of the legal business. These trends may be observed on the "slope of enlightenment" and the "plateau of productivity."[13] Enterprise legal administration is one of them, as are subject rights requests, forecasting and AI applications which employ business information to foresee risks and opportunities, and process automation (control dashboards for which scripts can be composed to automate routine, repetitive, rule-driven, predictable tasks). These applications are all incorporated and selected tactically to meet the requirements of the business.[14] It would be absurd for the legal profession and legal education to remain outside of the digital revolution.

3. The role of AI in legal education and profession

The methods used in legal research are changing as a result of AI-powered technologies. In order to deliver pertinent information and analysis, AI algorithms can quickly sift through enormous amounts of legal data, including cases, statutes, rules, and legal opinions.[15] These resources can assist researchers and law students save time, spot trends, and access extensive legal databases, thereby improving the caliber and effectiveness of their work. AI tools are being created to help lawyers, law students, and legal professionals draft briefs, contracts, and other legal documents. These tools can evaluate linguistic patterns, make edit suggestions, verify for consistency, and offer advice on the best practices for legal writing.[16] AI-powered writing aides can assist law students in developing their writing abilities and minimizing errors in legal documents. AI-based virtual learning environments can provide individualized learning opportunities catered to the

[13] Van der Meulen, R. (2020).
[14] Van der Meulen, R. (2020).
[15] Donahue, L. (2018).
[16] Sobowale, J., (2016) 1.

requirements of specific law students. These platforms can evaluate the performance of learners, point out areas for development, and offer specialized study guides and tests. AI can improve adaptive learning, improving the effectiveness, efficiency, and involvement of legal education.

The time-consuming task of document inspection can be automated using AI technologies, particularly machine learning and natural language processing. Large amounts of legal papers, contracts, and emails can be analyzed and categorized by AI-powered software, requiring less manual work from legal practitioners. This reduces the chance of human error while simultaneously improving accuracy and saving time. Legal practitioners can use AI to help them forecast case outcomes, evaluate risks, and make well-informed judgments. AI algorithms can shed light on the likely outcome of a case by examining prior legal data and patterns. This information can be used by lawyers to plan their approaches and control client expectations. Predictive analytics can also help in calculating the costs of litigation and predicting the outcome of settlement negotiations.[17]

Automating typical legal processes and providing quick answers to frequently requested queries are both possible with the help of AI-powered chatbots and virtual assistants. These AI tools can help customers set up appointments, obtain basic legal information, and do preliminary legal analyses. Legal chatbots can increase access to justice by offering round-the-clock support, particularly for those who cannot afford conventional legal services. Legal practitioners can benefit from AI technologies by guaranteeing ethical compliance and completing thorough study on laws and regulations. Legal documents can be examined by AI algorithms for potential

[17] Sil, R. & Roy, A. (2021) 6.

moral dilemmas, conflicts of interest, and legal compliance. Additionally, AI can speed up the legal research process, enabling lawyers to more quickly obtain pertinent cases, statutes, and legal opinions.

By examining a massive amount of legal material, such as case law, statutes, and legal opinions, AI-powered systems can help in legal research. These resources can offer accurate and thorough information, assisting attorneys and judges in their decision-making procedures and reducing the time and effort required for manual research. Artificial intelligence (AI) systems can examine past data and patterns to forecast case outcomes and offer insights into the prospects for resolving legal conflicts. By encouraging settlement negotiations, this can help attorneys create effective tactics, manage client expectations, and possibly lighten the load on the courts. Due diligence and examination of documents, which take a lot of time in litigation, can be automated with the help of artificial intelligence (AI) technology. In order to increase productivity, accuracy, and reduce errors, AI-powered software can evaluate and classify legal documents, contracts, and evidence.

For those who cannot afford traditional legal services, AI-powered chatbots and virtual assistants can fill the gap in legal support. The public now has easier access to legal materials thanks to these tools, which can also offer basic legal advice, direction, and assistance. By automating administrative procedures, keeping track of deadlines, and monitoring court records, AI technologies help streamline case administration. This can facilitate improved efficiency, lessen paperwork, and better handle legal proceedings.[18]

[18] Moses, L. (2017) 561.

4. AI and its effect on the legal field

A more thorough comprehension of and involvement in the worldwide discussion of "ethical AI" is crucial in order to assess the readiness of academics and legal professionals to support the maintenance of a balanced view and deployment of AI. People must become more actively involved in everything linked to AI as it becomes the pervasive ecology of human existence in the future. In terms of AI and the law, legal professionals and academics could have distinct expectations and experiences. They both continue to be important players in the push for the creation of ethical and revolutionary AI.

It is hardly unexpected that the legal profession is already being impacted by the digital shift that businesses are adopting. A "one two punch to the profession" has been delivered by the epidemic and the development of emerging technologies, which "will inevitably transform and reshape it in ways that would not have been thought possible years ago."[19] The epidemic has boosted the use of technology in the legal sector, but this has also raised new ethical questions. Artificial intelligence (AI) and its effects on the legal industry present ethical questions that need for lawyer knowledge, use, and advice to adhere to Codes of Professional Responsibility. In particular, note 8 to Rule 1.1, introduced in 2012, elaborates on the idea of competent representation in light of developments in legal technology. Comment 8 states a lawyer must stay current with changes in the law and how it is practiced, as well as the advantages and dangers of relevant technology, engage in ongoing study and education, and adhere to all continuing legal education requirements that apply to them in order to maintain the necessary knowledge and skills.[20]

[19] Suarez, C. (2020).
[20] Yamane, N. (2020) 883.

Globally, and in the United States no less, access to justice is dwindling rather than growing. According to the United Nations, access to justice is "a basic principle of the rule of law." The United Nations goes on to say that "people are unable to have their voice heard, exercise their rights, challenge discrimination, or hold decision-makers accountable" in the lack of access to justice.[21] However, there is no inherent conflict between the field of legal aid and developments in AI applications. The growing application of AI in the legal industry can help to improve adherence to Ethical Rule 1.1 and address the problems identified in the Legal Services Corporation's 2017 report. In particular, AI applications in legal practice can 1) increase people's use of self-help tools like online dispute resolution and legal robots that walk people through the legal system, and 2) "by permitting lawyers to operate with greater effectiveness, enabling them to serve more customers" in less time and at a lower cost. Lawyers cannot accept AI legal conceptions without oversight and confirmation, which is the ethical paradox in the use of AI in legal services. AI also cannot take the place of human legal advice and discretion. Both outcomes could theoretically be considered the illegal practice of law or the failure of a lawyer to appropriately supervise legal services given under their official responsibility.

Not all observers on the state of the legal industry in the face of technological upheaval are doomsayers. Observers are discovering a growing number of reasons for practitioners to increase the value of their services as legal consultants. Instead than living in terror of a machine's autonomous takeover, lawyers who control this shift will profit from it. Lawyers must work to be current and digitally savvy in today's tech-driven society. Lawyers can relate to their clients by having a basic understanding of computers and cellphones. The ability to

[21] Yamane, N. (2020) 885.

respond to a client's legal difficulties intelligently and with a detailed understanding of how their troubles occurred is made possible by this information, which is more significant. Lawyers must acknowledge that in today's high-tech environment, conventional legal remedies might not be sufficient to meet their duty to clients.[22] Where will students learn to live in the world that has been revolutionized by technology given the obvious practical, ethical, and economic challenges assumed by the expansion of AI in the field of law? If legal academics can get over their disrespect for practical education, they can advance to the next level of instruction and study. By connecting the actual and theoretical work of practitioners and academics, their contributions will be more relevant to the profession they wish to grow and will result in much-needed income improvements for their institutions.

Legal universities take a while to adjust to the evolving technology, even if AI has the potential to advance the legal profession. It goes without saying that the prospects of the profession of law is centered on education. There is demand to give law students a training that will enable them to compete in the legal market. The growing use of AI research tools in the legal profession requires law schools to accept this trend and modify their curricula accordingly. Although legal educators are aware of how AI is changing the legal industry, most of the required coursework for students is still in its infancy.[23]

For a long time, the law school culture has been hampered by the demand for "practice-ready" attorneys. The volume of it will only rise as the digital transition transforms law, society, and business in unforeseen and unprecedented ways. Law schools must offer instruction on the particular software and technologies that support the practice of law, such as programs

[22] Moore, T. (2019) 28.
[23] Connell, W. (2019) 6.

that introduce students to the fundamentals of artificial intelligence. What distinguishes generic AI from domain-specific AI? How can AI systems act, think, and behave? How does artificial intelligence interact with people, and how does AI develop over time when more and fresh data sets are added? What is a robo-advisor, a virtual assistant, and an algorithm?[24]

Beyond the effects of AI applications on the legal profession, attorneys will be essential in evaluating, guarding against, and setting up the limits of AI's ability to harm people. Lawyers need to be familiar with the language and fundamental functional components of AI development in order to minimize bias in algorithms or the effect of biased data. Students should be taught to examine the data generated by an AI program and avoid relying too heavily on technology, much as how to evaluate the motivations and testimony of a criminal informant. Unfortunately, AI technology has drawbacks. Attorney biases may be reinforced by algorithmic biases linked with such technology (e.g., robots are programmed by imperfect humans). When using such systems, students need to learn to challenge the information they are given and view it with a slightly cynical/skeptical eye. Inaccuracies can also be caused by giving AI computers duties that are too broad. Such procedures require analysis and extensive human supervision. Law students must understand their responsibilities as managers and overseers of such initiatives as well as their results.[25]

Arguably the most important function the law school can play right now is this one. Law practitioners and students will need to undergo extensive retraining, and the law school experience will need to be redesigned, in order to be prepared to play a critical part in the development of "Ethical AI" rules and regulations.

[24] Reid, M. (2019) 484.
[25] Reid, M. (2019) 484.

5. Challenges and Considerations

Although the use of AI into the Indian legal system shows potential, there are several difficulties and moral dilemmas to be aware of. Incomplete or biased data can produce skewed or unfair results since AI algorithms rely on data for training. In order to reduce prejudice and maintain fairness in AI applications, it is essential to ensure high-quality and diverse data. The use of AI in decision-making poses moral and legal concerns, especially with regards to responsibility, openness, and the possibility that AI could take the role of human judgment. To overcome these issues, precise rules and regulations must be set.

Technology Infrastructure and Implementation: To facilitate the integration of AI in the legal system, a sufficient technology infrastructure, including data storage, processing power, and security systems, must be in place. Additionally, for implementation to be successful, legal practitioners must receive the appropriate training and instruction. Even though AI can help with a range of legal activities, human monitoring and interpretation are still essential. Human judges should make the final determinations and judgements to ensure that ethical issues, contextual variables, and subjective concerns are properly taken into account. In conclusion, applying AI to the legal system has the potential to increase effectiveness, expand access to justice, and aid in decision-making. To establish a balanced analysis, though, attention must be taken to take data quality, moral implications, infrastructure, and the role of human judgment into account.

Recent developments in AI technology have raised questions about whether or not they could eventually replace lawyers. Even though AI can automate some activities and offer

insightful data, it cannot fully take the position of a lawyer. Lawyers contribute a special set of abilities and knowledge that surpass what AI can now provide. They have the critical thinking, discernment, and inventiveness necessary for the practice of law. Lawyers interpret the law, negotiate complicated legal systems, and offer contextualized advice unique to each situation. These abilities need a thorough knowledge of legal rules, moral concerns, and the capacity to apply legal logic to particular circumstances.

While AI can help with legal research, document review, and even case results to some level, it is unable to fully understand the subtleties of interpersonal relationships, emotions, and the ethical intricacies of legal situations. Additionally, the practice of law requires negotiation, advocacy, and strategic thinking, all of which are best handled by qualified human experts. AI can help lawyers by automating repetitive processes, increasing the effectiveness of their research, and providing data-driven insights. The use of this technology can increase a lawyer's effectiveness and productivity by enabling them to concentrate on more challenging and valuable areas of their work. Although AI is a potent tool that can supplement and improve a lawyer's abilities, it cannot take the place of the distinctive abilities, knowledge, and discretion that human lawyers offer to the legal profession. The legal industry needs a mutually beneficial connection between technology and human legal practitioners for AI to be successfully integrated.

Humans can concentrate on more difficult and creative areas of their work by using AI to automate routine and repetitive chores. By handling repetitive and time-consuming tasks, AI can enhance productivity by freeing up human resources for more important work. AI can support human decision-making processes by providing data-driven insights and analysis. AI systems can support human decision-making by analyzing

massive amounts of data quickly and seeing patterns, which improves outcomes. AI can be used to supplement human knowledge and talents. For instance, AI can help professionals in industries like health and law access and analyze large amounts of information, assisting in diagnosis and legal research, as well as increasing general efficiency in these professions. Virtual assistants and chatbots powered by AI can offer people individualized support and help, facilitating information access and task completion. This can include contacts with customers and targeted educational opportunities.

People frequently need training and must go through a learning curve to adopt AI technologies. Up until people become skilled, learning new skills and adjusting to new systems can reduce efficiency. The changeover process can be difficult and drawn out. Overuse of AI technologies can lead to dependency and a decline in human skills and decision-making capacity. Without crucial human oversight, relying only on AI might lead to mistakes or lost opportunities that an AI system might not be able to handle. Biases in the data can be seen in the AI's outputs since AI systems are only as accurate as the data they were taught on. This can affect efficiency and fairness in a variety of areas, including recruiting procedures, criminal justice, and approvals for loans. It may also result in biased decision-making or unfavorable outcomes. Certain work roles could be replaced by AI technology, raising concerns about job loss and economic relocation. This could necessitate retraining or a move into other roles for those who are affected, both of which can be quite difficult for some people.

6. The way forward

Academics are working to inform the general public about the advantages and disadvantages of AI. The majority of academics studying "Ethical AI" are often professors of engineering or

public policy. However, these alliances might be more successful as they become more multidisciplinary. The widespread effects of digital transformation demand a more widely conceived strategy to solve these problems. Expertise in a variety of fields, including medicine, law, pharmacology, architecture, engineering, literary works, philosophical psychology, and neuroscience is required to develop joint projects to address the extensive effects of AI on all individuals and organizations around the world. The Institute of Electrical and Electronic Engineers (IEEE), for instance, has devoted a significant portion of its resources to creating a framework for formulating guidelines for ethical AI. A global initiative on the ethics of autonomous and intelligent systems was created by the IEEE. The organization's goal is to "[t]o ensure that all parties associated with the development and creation of autonomous and artificially intelligent systems is well-informed, educated and equipped to give prominence to ethical issues so that these developments evolve for the betterment of humanity."[26]

It is recommended that legal instruction shift from a retrospective approach to a prospective and projective philosophical perspective, integrating knowledge from technological disciplines and quantitative techniques without sacrificing conventional normative skills, communicative abilities, and narrative principles that law specialists highly value, and emphasizing the need to encourage student creativity. Additionally, it is advised that university curricula incorporate coding and foster students' creativity and communication skills; however, a rule should be developed to handle the ethical concerns associated with employing AI in the classroom. Last but not least, it is clear that the legal professions are not currently in danger of being replaced by AI, but institutions must warn students that some positions may be

[26] IEEE (2023).

replaced by AI tools to assist them focus on responsibilities that cannot be replaced.

When confusion may emerge, AI deployers should let people know that they are engaging with an AI system, and people should be given the option to decline when doing so could impinge on their sense of dignity. Sustainable development and usage of AI systems are essential, and employers and developers of AI should take all necessary precautions to limit any physical or psychological harm to people, society, and the environment. People should have the ability to effectively question and reject judgments influenced by or made by an AI system, as well as the freedom to choose to be excluded from manipulation, personalization, and forecasts using AI. In order to successfully combat the possible discriminatory effects of AI systems deployed by both the public and private sectors, as well as to safeguard persons from their unfavorable effects, Member States should implement standards. Every time an AI system produces legal effects or has other similar effects on people's lives, people should have the right to a meaningful explanation of how the system works, what optimization logic it adheres to, what kinds of data it uses, and how it affects one's interests. The explanation needs to be appropriate for the situation at hand and delivered in a way that is clear to the person receiving it.

Literature

Dance E and Pedersen J, 'In-House Leaders Prepare Midyear to Advance on Digital and Operational Goals' (CORP. COUNS., 9 July 2020)
<https://static1.squarespace.com/static/5a5533fa49fc2bc6f15468b4/t/5f0e0efae796e91ca62573d4/1594756860028/Corp+Counsel+-+9+July+20+-+InHouse+Leaders+Advance+on+Digital+Operational+Goals+-+E+L+Dance+%2B+J+Pedersen.pdf > accessed 25 August 2023.

Deeks A, ‘High-Tech International Law’ (2020) 88 GEO. WASH. L. REV. 574.
Donahue L, 2018. A primer on using artificial intelligence in the legal profession. *Jolt Digest*.
Ekholm B and Kutcher E, 'Critical Communications Infrastructure and COVID-19: An Interview with Ericsson’s CEO' (MCKINSEY & CO., 20 Aug. 2020) <https://www.mckinsey.com/industries/technology-media-and-telecommunications/our-insights/critical-communications-infrastructure-and-covid-19-an-interview-with-ericssons-ceo> accessed 26 August 2023.
Gelburd R, 'The Coronavirus Pandemic and the Transformation of Telehealth (US NEWS & WORLD REPORT, 02 June 2020) <https://www.usnews.com/news/healthiest-communities/articles/2020-06-02/covid-19-and-the-transformation-of-telehealth> accessed 26 August 2023.
In-house Counsel Go Collaboration Crazy, (CORP. COUNS. BUS. J. BLOG, 09 Oct. 2020) <https://ccbjournal.com/blog/in-house-counsel-go-collaboration-crazy> accessed 25 August 2023.
Reid M, 'A Call to Arms: Why and How Lawyers and Law Schools Should EmbraceArtificial Intelligence', (2019) 50 U. TOL. L. REV. 477.
Moses L B, 'Artificial intelligence in the courts, legal academia and legal practice' (2017) 91 AUSTRALIAN LJ561.
Rob S, ‘High Scrutiny of Hi-tech Data Practices’ (LEGAL WEEK , 31 Jan. 2020) <https://www.law.com/> accessed 25 August 2023.
Sil R, Alpana and Roy A, 'A review on applications of artificial intelligence over Indian legal system' (2021) IETE Journal of Research1.
Sobowale J, 'How artificial intelligence is transforming the legal profession' (2016) ABA J, 11.
Sternlight, J., ‘Justice in A Brave New World?’ (2020) 52 CONN. L. REV. 213.
Suarez C, ‘Disruptive Legal Technology, Covid-19, and Resilience in theProfession’ (2020) 72 S.C. L. REV. 393.
Susskind R, 'The Future of Courts, Remote Courts' (6, HARV. CENT. LEGAL PROF., July 2020) <https://thepractice.law.harvard.edu/article/the-future-of-courts/> accessed 25 August 2023.

'The IEEE Global Initiative on Ethics of Autonomous and Intelligent Systems;(IEEE SA STANDARD ASSOC. year)https://standards.ieee.org/industry-connections/ec/autonomous-systems.html [https://perma.cc/2Z5X-N4K4] accessed 26 August 2023.
Thomas A M, 'The Upgraded Lawyer: Modern Technology and its Impact on the Legal Profession' (2019) 21 UDC/DCSL L. REV. 27.
Thompson D, 'The Workforce Is About to Change Dramatically', (ATLANTIC ONLINE, 06 Aug. 2020) <https://www.theatlantic.com/ideas/archive/2020/08/just-small-shift-remote-work-could-change-everything/614980/> accessed 26 August 2023.
Timms M, 'Jury Trials in Davidson County Pushed Back Again, Some to 2021 as COVID-19 Cases Continue' (THE TENNESSEAN 13 Aug. 2020) <https://www.tennessean.com/story/news/local/2020/08/13/davidson-county-no-jury-trials-nashville-until-2021/3365611001/> accessed 25 August 2023.
Van der Meulen R, '4 Key Trends in the Gartner Hype Cycle for Legal and Compliance Technologies' (SMARTER WITH GARTNER NEWSL., 21 Sept. 2020) <https://www.gartner.com/smarterwithgartner/4-key-trends-in-the-gartner-hype-cycle-for-legal-and-compliance-technologies-2020/> accessed 27 August 2023.
William J C, 'Artificial Intelligence and Legal Education' (2019) 67 R.I. B. J. 5.
Yamane N, ‘Current Developments 2019-2020: Artificial Intelligence in the Legal Field and the Indispensable Human Element Legal Ethics Demands’, (2020) 33 GEO. J. LEGAL ETHICS 877.
Zach Equity Research, 'Microsoft (MSFT) Keen on Building Subsea Data Center Network' (NASDAQ, 15 Sept. 2020,) <https://www.nasdaq.com/articles/microsoft-msft-keen-on-building-subsea-data-center-network-2020-09-15> accessed 25 August 2023.

Aleksandar Matkovic,* Ivana Novakov*

Decoding the changing (id)entity of cybercriminals: from human perpetrators to AI

Abstract: This paper aims to explore the changing trajectories of identities of cybercrime perpetrators. The problem of this study revolves around the question of what we know so far about the psychological profile of traditionally defined cyber offenders, and what it means for the legislative system if artificial, non-human entities may also become cybercriminal subjects on their own. After the introductory chapter, in which the problem of this paper is discussed, the results of previous empirical research regarding the psychological profile and personality traits of human individuals as perpetrators of cybercrime are presented. Furthermore, based on previous studies, we tended to demarcate some popular stereotypes attributed to the personality of cybercriminals by the media and popular culture, from verified scientific findings, as well as to make an overview comparison of personality traits of cyber offenders with offline offenders and the general population. Within the third part, the criminal law aspects of the participation of artificial intelligence (AI) in the execution of cybercrimes are discussed. In this regard, special attention was given to the determination of the legal status of AI, that is, to the analysis according to the following two perspectives: "crimes with AI" and "crimes by AI". Among other things, it was stated that, correspondingly to the aforementioned division of criminal acts related to AI, we can make a similar classification of the perpetrators of such criminal acts. Thus, we can distinguish between 1) human cybercriminals (understood as perpetrators who use AI as a means of committing a crime); 2) AI as a cybercriminal, *i.e.,* as an independent entity that autonomously commits criminal acts without human

* Aleksandar Matkovic is a senior lecturer at the Faculty of Law and Business Studies Dr Lazar Vrkatić, Novi Sad, Serbia; E-mail: al.matkovic@gmail.com.
* Ivana Novakov is a senior lecturer at the Faculty of Sport and Psychology, Novi Sad, Educons University, Sremska Kamenica, Serbia.

guidance. Also, the possibility of overlapping these two categories was pointed out, *i.e.,* the possibility of the existence of cases in which AI is "somewhere between" a tool that is completely directed by a person and a subject that acts completely independently. Although the second category (AI as a cybercriminal) still represents a scenario that is closer to science fiction than reality, the dizzying development of information technologies reminds us and warns us that such possibilities must also be taken into account when making serious, comprehensive, and far-reaching security strategies. In any case, as the best available way to legally prevent the harmful consequences of the use of AI, it is recommended to precisely regulate its use, as well as to limit the exploitation of its maximum capacities (which scientific and technological development enables) until the possible harmful consequences that may occur due to such exploitation are scientifically explored in detail.

Keywords: artificial intelligence, AI, cybercrime, cybercriminals, cyber offenders, cyberspace

1. Introduction

A few decades ago, crime was limited only to the physical world, where offenders had to operate in real space and time. Their criminal maneuvers and strategies depended on limitations imposed by the physical world. With the advent of the Internet, however, everything changed. Criminal activities have expanded into the domain of virtual space – a space that doesn't comply with the laws and boundaries of the real world. What's more, the rapid development of information technology has led to the rise of a phenomenon such as machine learning and artificial intelligence, which still perhaps seem to us more like scenarios from science fiction literature and movies, than as a phenomenon that could become a regular part of our everyday lives. In recent years and especially months, we have witnessed a so-called expansion in the development of different artificial intelligence software that can be trained with the help of reinforcement learning based on human feedback, so that

they can perform different tasks. There are also large language models (LLM) based on neural networks and self-supervised/semi-supervised learning strategies, which have found their purpose in performing various activities. We already have software that can create realistic images, write music, answer different kinds of questions, and solve complex intellectual tasks, among other things. Many AI performances might certainly be used for the good of humanity. According to some predictions, in relatively near future AI could revolutionize our education, healthcare system, medical diagnostic and therapeutic procedures, or even help solve energy and ecology crisis. However, various controversies about these systems also arise, drawing attention to the numerous dangers that can lurk behind the usefulness of modern technologies associated with artificial intelligence. There are growing calls for caution, in order to establish restrictions on the development of AI, to prevent possible harmful consequences in various areas of human functioning. Thus, we arrive at a completely new possibility that only a few years earlier might have sounded like a science fiction scenario - that the immediate perpetrator of a cybercrime no longer necessarily has to be a human being, but a derivative of artificial intelligence. This possibility brings a series of questions, dilemmas, and the need to define legal strategies and preventive regulatory guidelines. Therefore, our paper aimed to explore the changing trajectories of identities of cybercriminals – what do we know so far about the so-called psychological profile of traditional human cyber offenders, and what it means in the legislative context, if artificial, non-human subjects may also become cyber offenders.

2. Decoding the identity of traditional cybercriminal and a sketch for the "behavioural profile" of AI cybercriminal

Who is a cybercriminal? What do we know so far about the psychological profile of online offenders? Are they really awkward, socially withdrawn, quiet loners, and technology fanatics, as many stereotypical representations from popular culture made us believe? Cybercrime takes place in a specific context, in which little is known about the offender, where criminals use the anonymity of the Internet to hide their identities and illegal activities. Covered in a veil of the invisible and the unknown, they violate the rules and norms of software systems, causing minor or large and serious damages to other subjects. Yet, a great number of professionals are interested in constructing psychological profiles of hackers and other cybercriminals. Antisocial personality disorder has been widely studied in the context of traditional crime.[1] However, traditional and cybercrime differ significantly in various ways. For example, cyberspace requires no physical contact, allows anonymity and requires a specific set of highly sophisticated technological skills. Therefore, the question arises – are cybercriminals fundamentally different from traditional ones, according to some of their individual and personal characteristics? It seems that cybercriminals are less likely to be prone to addiction, low self-control, and drug use, unlike traditional offenders.[2] Some authors emphasize that anonymity is one of the main factors that invokes antisocial behaviour in different situations,[3] and some studies have shown that anonymity may be correlated with cybercrime.[4] This might be related to the so-called online disinhibition effect,[5] according to

[1] Fridell *et al.* (2008).
[2] Rokven *et al.* (2018).
[3] Baggily & Rogers (2009).
[4] Rogers *et al.* (2006).
[5] Suler (2004).

which individuals have a higher probability of breaking ethical rules online than in the real world. Even though, it is still difficult to distinguish between empirically explored and validated facts that describe the psychological profile of cybercriminals and the numerous stereotypes often presented in the media. There are many stereotypes about what a cybercriminal might be like.[6] Some of the traits that are attributed to these individuals are social awkwardness, a tendency towards social isolation, and technology addiction.[7] However, it is still unclear if the results of empirical findings are consistent with this stereotypical public image of cyber offenders. Surprisingly, research on the personality traits of cybercriminals is largely scarce.[8] Nevertheless, here we will try to sumarize some of the main results obtained in previous literature.

Known characteristics of the hackers and cybercriminals are still mainly of a demographic nature, as there is a lack of psycho-social insight into the minds of online criminal offenders.[9] For instance, it has been found that online sex offenders were more likely to be Caucasian and younger, compared to offline sex offenders; they were also more likely to be Caucasian, younger, single, and unemployed relative to members of general population.[10] Additionally, there are also indicies that online sex offenders, unlike offline ones, could have greater sense of self-control, and inhibitions when it comes to acting on behalf of their deviances.[11] As for the psycho-social aspects, some earlier authors stated that hackers, virus writers, and monetary cyber offenders might be attracted to cybercrime

[6] Seigfried-Spellar & Villacís-Vukadinović (2017).
[7] Seigfried-Spellar & Villacís-Vukadinović (2017).
[8] Weulen Kranenbarg *et al.* (2023).
[9] Bada & Nurse (2021).
[10] Babchishin et al. (2011).
[11] Babchishin et al. (2011).

activities due to financial reasons, intellectual challenges, drawing the attention of the world (while at the same time staying anonymous) and enhancing self-esteem.[12] Woo[13] suggested that hackers might also have some narcissistic traits. More recent observations by other authors are in line with this notion; for example, Van Der Wagen[14] suggests that some highly skilled hackers have a strong sense of self-importance, based on the belief that they can do the things that they believe other people are not capable of. Furthermore, Rogers and colleagues[15] emphasize that cyber offenders tend to have flexible ethical boundaries, without internalized ethical norms, which helps them to break rules. Few other studies go in line with this notion, suggesting that the morality of cyber offenders might be lacking.[16] Furthermore, some studies indicate that traits related to low extraversion are more common among highly technically skilled cyber offenders.[17] However, it is important to note that there are also studies that yielded mixed and inconsistent results regarding the question of introversion/extraversion.[18] Finally, one of the assumptions could be that cyber offenders might be creative, as many of them are motivated by the challenge of mastering computer systems,[19] which suggests that cybercriminals may score relatively high on openness to experience. However, there is still insufficient empirical data about the personality traits of cyber offenders.

[12] Turvey (2002).
[13] Woo (2003).
[14] Van Der Wagen (2018).
[15] Rogers *et al.* (2006).
[16] Seigfried-Spellar & Treadway (2014); Young *et al.* (2007).
[17] Aiken et al. (2016); Harvey *et al.* (2016); Payne *et al.* (2019).
[18] Ledingham & Mills (2015); Seigfried-Spellar *et al.* (2015).
[19] Steinmetz (2015); Van Der Wagen (2018).

Weulen Kranenbarg and colleagues[20] tried to address this lack of empirical findings by conducting very significant research in which they compared a group of participants who were suspects of cybercrime, with a group of suspects of offline crime, and a control group, which consisted of community participants, on the HEXACO personality domains and their facets. The findings of this study indicated that potential cyber offenders were more likely to have significantly lower scores on extraversion and higher scores on conscientiousness and openness to experience when compared to suspects of offline crime. Another interesting finding of this study is that cyber offenders turned out to be more similar to the community participants on main personality domains; cyber offenders and the participants from the community sample shared higher scores on conscientiousness and openness to experience. However, when underlying facets were observed, potential cybercriminals were more similar to potential offline offenders on lower levels of modesty, fearfulness, and flexibility – traits that may be in charge of performing criminal activities and violating social and ethical norms. On the other hand, suspects of cybercrime showed more similarity to the community sample on traits such as heightened levels of patience, perfectionism, and prudence – traits that might play an important role in choosing the digital domain (and not the real world) as a space for criminal activities. Potential cyber offenders seem to be specific in their elevated level of diligence, which is a facet of conscientiousness. Compared to offline offenders, cyber offenders seemed more similar to those individuals from a community sample, and there is an impression that cyber offenders are somewhere in between offline offenders and the community sample on honesty-humility.[21]

[20] Weulen Kranenbarg *et al.* (2023).
[21] Weulen Kranenbarg *et al.* (2023).

Although it is difficult to talk about the "individual characteristics" of AI as a cybercriminal independent entity, for the sake of insight into this aspect of cybercriminal activity, we can offer several orientation guidelines that can help during future, more extensive analyses. Generally speaking, the following might be singled out as the main factors that influence the individual determinants of AI: the reasons for which a specific AI was created, the purpose it is intended for, the tasks it is set to perform, etc. Also, as relevant factors, we can recognize those individual and behavioral performances that its creator consciously encoded into it, but also their personal features that they unconsciously incorporated into the AI during the process of its creation. Finally, it is necessary to take into account those features that AI could independently develop during its "development", "learning" and "adaptation" – whether the acquisition of such features is part of a pre-planned process or falls into unforeseen activities.

3. AI, cybercrime and cybercriminals: Criminal law aspects

There is an abundance of literature on the criminal law and criminological aspects of cybercrime perpetrators, created over a long period of time, since cybercrime became a subject of scientific interest.[22] On the other hand, the issue of AI being understood as a potential cybercriminal entity came into the focus of scientific attention much later, and there are still a number of questions that require scientific answers. Bearing in mind the above, in the further text we will focus exclusively on cybercrime which implies the participation of AI in the process of committing a criminal act.

[22] Among other relevant works, see: Brenner (2012); Clough (2015); Gordon & Ford (2006); Holt & Bossler (2015); Marcum & Higgins, (2019); McQuade (2006); Shinder & Cross (2008); Wall (2007).

As in many other spheres of social life, the general issue of AI causes plenty of questions and dilemmas in the field of law as well. Limiting our attention to the criminal law sphere, we will try to trace some of the questions that may arise about the criminal law regulation of the field of AI. In this regard, the first item to be considered is the question of possible forms of relationship between AI and criminality.[23] According to Hayward and Maas,[24] it is possible to distinguish three modalities of interaction: 1) "crimes with AI", 2) "crimes against AI", and 3) "crimes by AI". Adopting this division, according to the topic of our analysis, our primary focus will be on the first and third categories (crimes committed with the use of AI by humans, as well as crimes committed by AI as an independent entity).

The next question that arises in connection with the criminal law regulation of AI is the problem of the subject of the criminal act, that is, the bearer of criminal responsibility. Reducing the problem to its basic elements, it can be presented (for now, hypothetically) as follows: 1) criminal liability of man; 2) criminal liability of AI;[25] 3) criminal responsibility of man and AI. This kind of division, for now, must remain hypothetical, as evidenced by the positive legal solutions in the legislation of a number of countries. For the sake of illustration, according to the legislation of the Republic of Serbia, the subject of a criminal offence is a person, i.e. a natural person who undertakes the act of execution (perpetrator) or the act of

[23] For earlier works regarding criminal law aspects of AI, see *e.g*: Hallevy, (2010, 2013); Lodder, Oskamp, & Duker (1998); Pagallo (2011). Among the newest works, *e.g*: Barabas (2020); Begishev et al. (2023); Custers (2022); Khan (2021); King *et al.* (2020); Lagioia & Sartor (2020); Ligeti (2019); Quattrocolo (2018).

[24] Hayward & Maas (2021).

[25] Regarding the possibility of criminal liability of AI, *see e.g*: Dobrinoiu (2019); Dremliuga & Prisekina (2020); Kirpichnikov et al. (2020); Lima (2018); Radutniy (2017).

complicity (accomplice).[26] However, this circumstance does not exclude the possibility of expanding the boundaries of the subjects of the criminal offence at some future point, by analogy with the similar expansions that have already taken place in the past (for example, stipulating that legal entities, in addition to natural persons, can also be subjects of criminal acts).[27]

Analyzing further the notion of human criminal liability, the question can be raised as to which subject (i.e. which human) will be responsible, considering that in the process from the creation of AI to the execution of a criminal offence with the participation of AI, a number of persons appear: the inventors of AI as a phenomenon, the inventor of specific AI that was used during the execution of the given criminal act, AI manufacturers, distributors, end users, etc. Considering the general rules that apply when determining the subject of criminal liability, it seems that in most cases, the burden of criminal liability would be on the end user who used AI in the commission of a criminal offence. However, this does not exclude the possibility of liability for other persons as well (for example, the person who constructed the AI whose primary function is to perform a certain legally prohibited action, the seller or reseller of such AI, etc.).

In connection with the above, the mutual relationship between humans and AI should be considered in more detail in the light of criminal law and criminal liability. Thus, we can distinguish between several hypothetical modalities: 1) exclusive criminal responsibility of man; 2) treating AI as an object/tool used by a

[26] Cf. Criminal Code of the Republic of Serbia, *Službeni glasnik RS*, no. 85/2005, 88/2005 - corrected, 107/2005 - corrected, 72/2009, 111/2009, 121/2012, 104/2013, 108/2014, 94/2016 and 35/2019.

[27] For an insight into the evolution of the domestic theoretical thought about the subject of the criminal act, see inter alia: Mihajlovski (1986); Šuput (2009); Vrhovšek (2011).

person during the commission of a criminal act; 3) treating AI by analogy with the abuse of other living beings 4) treating AI as an equal subject of the execution of a criminal act.

If AI is not characterized as the subject of a criminal act, the situation, at first glance, may seem somewhat simpler. However, the situation is not so simple even then, we can illustrate through several examples that can occur in practice. First of all, there is the question of the legal status of AI, in terms of determining its position in relation to the overall process of committing a criminal offence. As a dilemma, the question arises as to how to treat AI: as an object, as an intangible legal asset, as a living being, as an entity *sui generis*, etc. If the legislator resorts to defining AI as an object, that is, as a part of inanimate nature, the problem may be caused by the circumstance that AI, undeniably, possesses a certain autonomy of action, which, at least in that aspect, makes it closer to living beings than inanimate objects. On the contrary, focusing on the possibility of legal characterization of AI as a living being, one of the options appears to be the legal treatment of AI analogous to the legal status of an animal that a person used to commit a criminal act. However, if one approaches the point of view (or at least the legal fiction) that in the case of AI, it is about a living being, a new question arises: according to what criteria is AI legally treated as an animal and not as a human? Finally, we should look at the possibility of the existence of the so-called "crimes without guilt", i.e. illegal actions that cannot be blamed on any subject due to the absence of some of the components necessary to establish criminal responsibility. Applying an analogy with other examples from theory and practice, this situation would exist when, in addition to the impossibility of invoking the legal responsibility of AI, it would not be possible to determine the responsibility of any human being either. All the possibilities listed certainly represent challenges that require a more detailed analysis in the future.

On the other hand, if AI is characterized as the subject of a criminal offence on an equal footing with human perpetrators of the same criminal offences, then an even greater number of legal dilemmas arise that require answers. We will list some of them in the following paragraphs.

The first question that must be considered in connection with the above concerns the *ratio legis* for the introduction of AI as the subject of a criminal offence and criminal liability in the legal system. Undoubtedly, there is considerable room for a challenging and productive debate on the ethical and philosophical aspects of the mentioned issue. However, since, in accordance with its social function, legislation is traditionally oriented towards pragmatic goals, i.e. towards meeting real social needs, it is precisely in that sphere that it is necessary to look for reasons that can lead the legislator to introduce AI as a subject of criminal liability. In other words, the primary reason for opting for the option according to which AI will be legally treated as eligible to be the subject of a criminal offence would have to be justified by real social needs about which traditional legal solutions (i.e. exclusively humans as the subject of responsibility for cybercrime) proved to be inadequate.[28]

An extremely important problem related to prescribing the possibility of AI being a legally responsible entity concerns the following ethical and legal dilemma: Does predicting the liability of AI absolve the human behind that AI from liability? The answer to this question is twofold. If it were a situation in which a human directed or instructed an AI to commit a certain criminal act, shifting the responsibility from a human to an AI would really represent a legal and moral violation of justice.[29] At the same time, such a possibility would open up space for

[28] For criminal liability of AI, cf. Hallevy (2013).
[29] Similar in: Uljanov & Kočović (2023) 373.

numerous legal abuses. On the other hand, if AI would hypothetically reach an appropriate level of independence, which does not involve receiving direct instructions from a human to perform a certain illegal act, but rather such an illegal act occurs through the autonomous action of AI, it seems that there are no logical obstacles to foresee the legal liability of AI to such an act at some point in the future and with the fulfilment of the appropriate conditions.

One of the circumstances that are important to consider in connection with analyzing AI as a potential subject of the execution of a criminal offence concerns the possibility of applying the institution of coercion. Focusing on the domain of the use of physical force for coercion, the following logical question arises: Can we objectively talk about physical coercion in virtual space? Bearing in mind that, in today's world, manipulation of AI is carried out with the use of computers or other related technological devices (mobile phones, various gadgets), physical coercion would have to be indirect in nature, that is, it would have to be mediated by the use of computers or other appropriate devices (for example, issuing a computer command to an AI to act in a certain way even though it is against its "will"). Likewise, the issue of legal property whose endangerment would be achieved by applying physical coercion to AI is also problematic. Being aware that we are dealing with AI as an immaterial entity mediated by material devices, one can logically come to the conclusion that the object of physical coercion could be twofold: 1) immediate (e.g.: in the case of a violent, physical command through a suitable device, whereby the intention of the person exercising coercion is exhausted precisely in such an act of issuing a mechanical command; physical destruction or damage to the device that articulates the AI, with the intention of physically coercing the AI in this way); 2) indirect (in the event that the coercion is carried out through a computer, but the goal of the person performing the coercion

is to achieve such coercion on the immaterial plane of the AI itself).

On the other hand, the consideration of psychological coercion appears as equally problematic. Namely, in that case, the question that requires an answer would be: Is it possible to talk about psychological coercion in relation to AI as an entity that, on the manifest level, really shows numerous similarities with the psychological characteristics of humans, but, for understandable reasons, (at least for now) certainly cannot be identified with man. Also, as a supplement, the question of possible mechanisms of psychological coercion could be raised, which could, hypothetically, be applied to AI. Analogous to the examples we have given for physical coercion, in the case of psychological coercion, it could primarily be certain manipulative actions associated with endangering the integrity, functioning or even the very survival of a given AI (e.g. the threat that the AI will be destroyed, shut down, deprogrammed, reprogrammed, directed towards other goals, etc.). In any case, the basic dilemma boils down to the question of whether – at the present moment, or in the foreseeable future – it is at all conceivable the stage of AI development at which the threat could be a method of coercion suitable to make the AI act in a certain way? To this, as well as to other disputed questions, the best answers, in all likelihood, will be provided by the future itself.

As a very intriguing situation, one can imagine the possibility of complicity between humans and AI. As in other previously discussed situations, the basic assumption for considering this possibility concerns the decision for AI as a full-fledged subject of the execution of a criminal offence. Otherwise, it would be one of two alternative possibilities: 1) AI as a means of committing a criminal act; 2) AI as an entity used by man to commit a criminal act. However, if the legislator decided to

accept the possibility of complicity between man and AI, it would raise a series of additional questions to which it is not at all easy to provide satisfactory answers. For example, in the case of co-perpetration, the question arises as to how an agreement for the execution of a criminal offence between a human and an AI will be defined, what such an agreement could entail, how conceivable the realization of this concept in practice, etc. In the case of assistance as a form of complicity, a number of dilemmas also arise regarding the type of assistance that AI can provide to a human perpetrator of a criminal offence (but also vice versa), ways of implementing such assistance, etc. Finally, the possibility of incitement in the AI-human relationship (and vice versa) also represents an extremely controversial issue, since it opens up a series of legal, technical-technological, logical, ethical and other dilemmas, but also because it leaves a wide space for legal abuses.

Speaking of sanity, it's only fair to ask: How could we even imagine assessing the sanity of an entity like AI? The basic obstacle is the impossibility of determining the sanity criteria by analogy with the criteria applied to people, as so far, the only imaginable individual perpetrators of criminal acts. As a programmed entity that is based on algorithms and mathematical, linguistic or other models, AI cannot have a mental status – only some kind of simulation of it. For that reason, a different term should be invented in order to distinguish the phenomenon of "artificial simulation of mental status" from human experience. However, as it is impossible to predict the totality and the tempo of the future technological progress, we cannot categorically rule out the possibility for development of some real "mental features" regarding AI. Relying on logic, it seems that such a possibility should be sought first in the field of interaction between a human being and AI or even more broadly, a human being and a "machine" in general. As a discreet, initial traces of such possibilities, we

can mention, for example, some pioneering biomedical researches that include merging off human cells with the nanorobotic entities. In any case, leaving space for a future more detailed debate, we can only state that, even in the hypothetical case of requiring AI's sanity as a necessary presumption of its guilt, a number of issues ranging from general medical and psychological criteria for classifying AI's mental status, all the way to technical aspects of conducting expert examinations, would have to be regulated beforehand, as a necessary prerequisite for the action of judicial authorities. On the other hand, if AI's legal responsibility were to be based solely on analogy with the responsibility of a legal entity, the situation would be much simpler since then, understandably, it would be neither possible nor necessary to consider the question of sanity.[30]

Another interesting question that arises is the possibility of applying the institute of necessary defense to the operation of AI. More specifically, the dilemma is: Could the action of an AI that seeks to protect itself by attacking an individual who tries to threaten its existence in self-defense be treated as a form of necessary defense?[31] To solve this problem more creatively, we can use the basic laws of robotics formulated by Isaac Asimov. According to the mentioned author, the basic laws of robotics are as follows: 1) A robot must not injure a human being or, through its inactivity, allow a human being to be injured; 2) The robot must obey the orders of human beings unless those orders conflict with the First Law; 3) The robot must protect its own existence unless it conflicts with the First and Second Laws.[32] According to these laws, applied to the field of AI, it could be concluded that the injury of a human by an AI (understood as an entity in the service of a human) could not be recognized as

[30] About sanity/insanity concerning AI, cf. Hallevy (2013).
[31] Cf. Hallevy (2013).
[32] Asimov (1950) 40.

a form of necessary defense. However, if AI were to be treated as a phenomenon that is not in the service of man, but which has a separate legal subjectivity, the dilemma arises as to whether the aforementioned laws of robotics are still applicable, or whether AI, analogously to man, acquires the right to the necessary defense?

Apart from the ones listed, it is possible to see a number of other controversial issues relevant to the field of (criminal) law. Limiting ourselves to the individual characteristics of AI as a perpetrator, let us list only some of the possible points of contention: the issue of gender structure, marital status, age and educational structure, labor law status, etc. As can be seen at first glance, these are highly debatable issues, the resolution of which causes a series of dilemmas and contradictions. Some of such dilemmas are, among others: whether the mentioned AI features are the fictional constructs (made, for example, just for entertainment purposes), or are they their real features which are inseparable from the very essence of concrete individual artificial intelligence; whether such features are relevant to the legal matter, or their determination is not important; whether they are static categories or fluid categories; in the case of their fluidity, is it necessary to make an analogy with human individuals in whom such changes are incomparably slower and more complicated (for example, changing gender in humans is an extremely complex and long-term procedure, while the same change in AI can follow only one click of the computer pad).

As a general circumstance, we can generally state that if the legislator were to adopt the point of view on AI as a subject of criminal responsibility, then in principle there should be no formal obstacles to the application of many of the existing criminal law institutes. However, this certainly does not mean that all obstacles would be removed since it is quite realistic to expect that even then various factual obstacles would continue

to exist on the way to the implementation of the mentioned institutes in practice.

Despite all the mentioned factors that can be interpreted as hypothetically leaving the possibility for predicting the legal possibility of AI being the subject of a criminal act and the bearer of criminal responsibility, it is necessary to point out a very significant fence concerning the will component. Namely, it is about the problem of the absence of autonomy of the will in the sense of the conditions that the legislation foresees in order to be able to talk about the existence of a criminal offence and guilt on the part of the perpetrator. As stated by Uljanov and Kočović, "Algorithms, as mathematical patterns for solving given problems, cannot be factors of autonomous will and consciousness of some software, regardless of whether it is developed and perfected, that is, whether its capacity for quickly solving a large the number of tasks evolves over time."[33] On the contrary, several authors believe that all the essential conditions have already been met so that AI could be considered a subject of criminal responsibility.[34] Leaving aside, for the moment, a categorical answer to this question, we can only note that as long as in the case of the acts of AI one cannot speak of the existence of its autonomy of will, the mentioned remarks deserve to be taken into account; however, bearing in mind the unpredictable development of information technologies, it does not seem correct to categorically write off the possibility of technological progress that would enable a certain "independence" of AI regarding even the matter of will. In any case, if the analogies with a legal entity as a subject of a criminal offence are applied, it means that at this moment there are no logical or legal obstacles to the introduction of AI into the status of a subject of a criminal offence if such a legislative

[33] Uljanov & Kočović (2023) 373.
[34] *See e.g.* Hallevy (2010); Kirpichnikov (2020). See also: Dobrinoiu (2019); Dremliuga & Prisekina (2020); Lima (2018); Radutniy (2017).

procedure would be beneficial to the functioning of the criminal justice system, judiciary and the social system in general.

Of course, it is important to clearly emphasize once again that most of the enumerated dilemmas are still fiction that is not realizable at the current historical moment, and therefore do not cause legal problems in practice. However, taking into account the dizzying development of technology related to AI, it seems extremely important to consider such possibilities already now – regardless of how hard they are still imaginable or unrealistic today – so that tomorrow does not welcome us unprepared for such challenges.

From all that has been presented, it can be easily concluded that the issues we considered, apart from being relevant from the position of (criminal) law, are certainly significant from the point of view of other disciplines, in an extremely wide range from IT and technical sciences to philosophy and ethics. As a result of the above, in order to limit the problem to the domain of legal theory and practice, it can be stated that, for now, the best legal way of preventing the harmful consequences of the use of AI lies in the precise legal regulation of its use. In addition to generalized regulations, such regulation should also include the adoption of a series of specialized provisions that would regulate in detail the subject of AI and the conditions of its application in the most diverse circumstances. Additionally, an extremely important factor in the prevention of the side effects of the use of AI concerns the limitation of the exploitation of all its capacities that scientific and technological development enables, until the possible harmful consequences that may occur due to such exploitation are examined in detail. Seen from a legal point of view, such limitation would have to imply the coordinated application of all legal protection mechanisms available to a particular society, state or supranational community. However, one should keep in mind

the limitations that the legal approach to the identified problem must necessarily encounter, since a number of important issues directly depend on wider socio-political aspects and socio-political strategies (both at the national and supranational level), while legal mechanisms in such a context usually have a coordinating, "service" function, not a leadership and decision-making function. As various authors have warned decades ago, regarding technology in general, society should limit the use of technological opportunities according to its capacities for sustainable development and ultimately for its survival.[35] Accepting these statements and applying them to the sphere of information technology, and especially to the phenomenon of AI, we can state that a responsible, cautious and thoughtful approach when approving the use of certain forms of AI and their placement in the public space is of primary importance for avoiding and mitigating the negative consequences of rapid development of AI.

4. Conclusion and recommendations

In the modern information society, we are witnessing an increasing equalization of reality and virtual reality, where the development of AI is one of the key generators of that process. The emergence and accelerated expansion of the AI phenomenon causes very diverse viewpoints both among experts and the general public, with opinions varying between extremes of complete optimism and catastrophic pessimism. Avoiding both extremes, and opting for a moderate approach, we can generally state that the phenomenon of AI undoubtedly brings numerous challenges, but also represents a great opportunity for the further progress of humanity and the entire ecosystem. Limiting the discussion on the field of crime prevention and suppression, it is enough to recall a series of

[35] *Cf.* Gorz (1982); Grul (1985); Meadows *et al.* (1974); Rifkin (1986).

modern technological and software inventions that contribute to the work of the police, prosecutor's office and courts in various ways, both on a preventive and repressive level.

Focusing on the legal aspects of regulating AI, and staying in the domain of criminal law and the issue of AI participation in the process of committing criminal acts, one of the most important issues is determining the legal status of AI. In this sense, the key step is deciding on one of the following two positions: a) AI as the subject of the execution of the criminal act; b) AI as a means of committing a crime. At the same time, it is possible to distinguish several transitional or related options that build on these two basic possibilities.

At this historical moment and against the currently available technical and technological possibilities, the issue of (mis)use of AI during the commission of criminal acts still mostly falls under the sphere of human legal responsibility – that is, a human being who in a certain form and in a legally relevant way contributed to the commission of a criminal offence with the use of AI or contributed to the creation of malicious AI. As a transitional category that is already present today, and which, in all probability, will be more and more present in the future, one can see a kind of category "crime without guilt", i.e. those situations in which AI caused certain illegal damage that is foreseen in the regulations as a criminal act, but without the interaction of a person who could be held responsible on that basis. Finally, the third (and for now hypothetical) scenario would be a situation in which AI acts independently as a perpetrator of a criminal act and as such is recognized as a legal entity capable of bearing responsibility for the committed act.

Speaking about cybercrime and its potential perpetrators, in accordance with what has been stated so far, we can distinguish between 1) human cybercriminals (understood as perpetrators

who use AI as a means of committing a crime); 2) AI as a cybercriminal, i.e. as an independent entity that autonomously commits criminal acts without human guidance. Also, we can point out the possibility of overlapping these two categories, i.e. the possibility of the existence of cases in which AI is "somewhere between" a tool that is completely directed by a person and a subject that acts completely independently. At the present moment, the second category (AI as an independent cybercriminal) still represents a scenario that is closer to science fiction than reality. However, the dizzying development of information technologies, together with the rapid development of various aspects of society in general (especially in the domain of human rights, rights of other living beings etc.), reminds us and warns us that such possibilities must also be taken into account when making serious, comprehensive, and far-reaching security strategies. In any case, as the best available way to legally prevent the harmful consequences of the use of AI, it is recommended to precisely regulate its use, as well as to limit the exploitation of its maximum capacities (which scientific and technological development enables) until the possible harmful consequences that may occur due to such exploitation are scientifically explored in detail.

Literature

Aiken, M., Davidson, J., & Amann, P., *Youth pathways into cybercrime* (Europol 2016).
Asimov, I., *I, Robot* (Doubleday 1950).
Babchishin, K. M., Hanson, R. K., & Hermann, C. A., 'The characteristics of online sex offenders: a meta-analysis' (2011) *23*(1) Sexual abuse: A journal of research and treatment 92.
Bada M., & Nurse, J. R. C., 'Profiling the Cybercriminal: A Systematic Review of Research' (2021 International Conference on Cyber Situational Awareness, Data Analytics and Assessment (CyberSA*)* Dublin, Ireland, 14-18 June 2021).

Baggily, I. & Rogers, M., 'Self-reported cybercrime: An analysis of the effects of anonymity and preemployment integrity' (2009) *3*(2) International Journal of Cyber Criminology, 550.
Barabas, C., 'Beyond Bias: Re-Imagining the Terms of "Ethical AI" in Criminal Law' (2020) Georgetown journal of law & modern critical race perspectives *12*.
Begishev, I. R., Kirillov, M. A., Bersei, D. D., Nechaeva, E. V., Perepelkin, V. I., Serkova, T. V., ... & Narimanova, N. R., 'Robotics, artificial intelligence and criminal law: An overview of contemporary studies' (AIP Conference Proceedings, *2701*(1), 9. Mar 2023).
Brenner, S. W., *Cybercrime and the law: Challenges, issues, and outcomes*. (UPNE 2012).
Clough, J., *Principles of cybercrime* (Cambridge University Press 2015).
Custers, B., 'AI in Criminal Law: An overview of AI applications in substantive and procedural Criminal Law' (2022) Law and Artificial Intelligence: Regulating AI and Applying AI in Legal Practice 205.
Dobrinoiu, M., 'The influence of artificial intelligence on criminal liability' (2019) *26*(1) LESIJ-Lex ET Scientia International Journal 140.
Dremliuga, R., & Prisekina, N., 'The Concept of Culpability in Criminal Law and AI Systems' (2020) *13*(3) *Journal of Politics and Law* .
Fridell, M., Hesse, M., Jaeger, M. M., & Kühlhorn, E., 'Antisocial personality disorder as a predictor of criminal behaviour in a longitudinal study of a cohort of abusers of several classes of drugs: relation to type of substance and type of crime' (2008) *33*(6) Addictive Behaviors 799.
Gordon, S., & Ford, R., 'On the definition and classification of cybercrime' (2006) 2 *Journal in computer virology*, 13.
Gorz, A., *Ekologija i politika* (Prosveta 1982).
Grul, H., *Jedna planeta je opljačkana* (Prosveta 1985).
Hallevy, G., 'I, Robot-I, criminal: When science fiction becomes reality: Legal liability of AI robots committing criminal offenses' (2010) *22*(1) Syracuse Science & Technology Law Reporter
Hallevy, G., *When robots kill: Artificial intelligence under criminal law* (UPNE 2013).
Harvey, I., Bolgan, S., Mosca, D., McLean, C., & Rusconi, E., 'Systemizers are better code-breakers: Self-reported systemizing

predicts code-breaking performance in expert hackers and naïve participants' (2016) Frontiers in Human Neuroscience 10.
Hayward, K. J., & Maas, M. M. Artificial intelligence and crime: A primer for criminologists (2021) *17*(2) Crime, Media, Culture, 209.
Holt, T., & Bossler, A., *Cybercrime in progress: Theory and prevention of technology-enabled offenses* (Routledge 2015).
Khan, K. F., Ali, A., Khan, Z. F., & Siddiqua, H., 'Artificial Intelligence and Criminal Culpability' (2021 International Conference on Innovative Computing (ICIC), 9-10 Nov. 2021).
King, T. C., Aggarwal, N., Taddeo, M., & Floridi, L., 'Artificial intelligence crime: An interdisciplinary analysis of foreseeable threats and solutions' (2020) 26 Science and engineering ethics89.
Kirpichnikov, D., Pavlyuk, A., Grebneva, Y., & Okagbue, H, 'Criminal liability of the artificial intelligence' (In *E3S Web of Conferences*, Vol. 159). EDP Sciences.
Kranenbarg, M. W., Van Gelder, J. L., Barends, A. J., & de Vries, R. E., 'Is there a cybercriminal personality? Comparing cyber offenders and offline offenders on HEXACO personality domains and their underlying facets' (2023) Computers in human behavior 140.
Lagioia, F., & Sartor, G., 'Ai systems under criminal law: a legal analysis and a regulatory perspective' (2020) *33*(3) Philosophy & Technology 433.
Ledingham, R., & Mills, R., 'A preliminary study of autism and cybercrime in the context of international law enforcement' (2015) *1*(1) Advances in Autism 2.
Ligeti, K., 'Artificial Intelligence and Criminal Justice' (2019) AIDP-IAPL International Congress of Penal Law.
Lima, D., 'Could AI agents be held criminally liable: artificial intelligence and the challenges for criminal law' (2018) *69*(3) South Carolina Law Review .
Lodder, A. R., Oskamp, A., & Duker, M. J., 'AI & Criminal Law: Past, Present & Future' (1998) Proceedings of JURIX.
Marcum, C. D., & Higgins, G. E., 'Cybercrime' in M Krohn and others (eds), *Handbook on Crime and Deviance* (Springer International Publishing 2019).
McQuade, S. C., *Understanding and managing cybercrime* (Pearson/Allyn and Bacon 2006).
Meadows, D. H., Meadows, D. L., Randers, J. & Behrens, W. W. III, *Granice rasta* (Stvarnost 1974).

Mihajlovski, A., 'Subjekt krivičnog dela' (1986) *34*(6) Anali Pravnog fakulteta u Beogradu634.
Pagallo, U., 'The adventures of Picciotto Roboto: AI and ethics in criminal law' in A Bissett and others (eds), *The Social Impact of Social Computing* (ETHICOMP 2011).
Quattrocolo, S., 'The impact of AI on criminal law a, and its twofold procedures' in W Barfield and U Pagallo (eds), *Research Handbook on the Law of Artificial Intelligence* (Edgar Elgar 2018).
Radutniy, O. E., 'Criminal liability of the artificial intelligence' (2017) 138 Проблеми законності 132.
Rifkin, J., *Posustajanje budućnosti* (Naprijed 1986).
Rogers M., Seigfried K., & Tidke K., 'Self-reported computer criminal behavior: A psychological analysis' (2006) 3 *Digital Investigation* 116.
Rogers, M., Smoak, N. D., & Liu, J., 'Self-reported deviant computer behavior: A big-5, moral choice, and manipulative exploitive behavior analysis' (2006) *27*(3) Deviant behavior245.
Rokven, J. J., Weijters, G., Beerthuizen, M. G., & van der Laan, A. M., 'Juvenile Delinquency in the Virtual World: Similarities and Differences between Cyber-Enabled, Cyber-Dependent and Offline Delinquents in the Netherlands' (2018) *12*(1) International Journal of Cyber Criminology27.
Seigfried-Spellar, K. C., O'Quinn, C. L., & Treadway, K. N., 'Assessing the relationship between autistic traits and cyberdeviancy in a sample of college students' (2015) *34*(5) Behaviour & Information Technology533.
Seigfried-Spellar, K. C., & Treadway, K. N., 'Differentiating hackers, identity thieves, cyberbullies, and virus writers by college major and individual differences' (2014) *35*(10) Deviant behavior782.
Seigfried-Spellar, K.C., Villacís-Vukadinović, N., & Lynam, D. R., 'Computer criminal behavior is related to psychopathy and other antisocial behaviour' (2017) 51 Journal of Criminal Justice 67.
Shinder, D. L., & Cross, M., *Scene of the Cybercrime* (Elsevier 2008).
Suler, J. 'The online disinhibition effect' (2004) 7(3) Cyberpsychology & behavior321.
Šuput, J., 'Odgovornost pravnog lica za krivična dela' (2009) 1 Strani pravni život 169.
Turvey B., *Criminal Profiling* (Academic Press 2002).

Uljanov, S., & Kočović, P., 'Kriminalna eksploatacija veštačke inteligencije' in N Krasulja and others (eds), *Pravo, ekonomija i menadžment u savremenim uslovima-Veštačka inteligencija (AI)-LEMiMA 2023* (Fakultet za poslovne studije i pravo, Beograd, Srbija 2023).
Vrhovšek, M., 'Koja pravna i odgovorna lica mogu biti odgovorna za krivična dela' (2011) 28(7-9) Pravo-teorija i praksa22.
Wagen, W. van der, 'The Cyborgian Deviant: An Assessment of the Hacker through Actor-Network Theory' (2018) *6*(2) Journal of Qualitative Criminal Justice and Criminology157.
Wall, D., *Cybercrime: The transformation of crime in the information age* (Polity 2007).
Woo, H. J., 'The hacker mentality: Exploring the relationship between psychological variables and hacking activities' (Doctoral dissertation, University of Georgia 2003).
Young, R., Zhang, L., & Prybutok, V. R., 'Hacking into the minds of hackers' (2007) 24(4) Information systems management281.
Criminal Code of the Republic of Serbia, *Službeni glasnik RS*, no. 85/2005, 88/2005 - corrected, 107/2005 - corrected, 72/2009, 111/2009, 121/2012, 104/2013, 108/2014, 94/2016 and 35/2019.
Vrhovšek, M., 'Koja pravna i odgovorna lica mogu biti odgovorna za krivična dela' (2011) *Pravo-teorija i praksa, 28*(7-9), 22-53.
Wagen, W. van der, 'The Cyborgian Deviant: An Assessment of the Hacker through Actor-Network Theory' (2018) *Journal of Qualitative Criminal Justice and Criminology, 6*(2), 157-178.
Wall, D., *Cybercrime: The transformation of crime in the information age* (Polity 2007).
Woo, H. J., 'The hacker mentality: Exploring the relationship between psychological variables and hacking activities' (Doctoral dissertation, University of Georgia 2003).
Young, R., Zhang, L., & Prybutok, V. R., 'Hacking into the minds of hackers' (2007). *Information systems management, 24*(4), 281-287.
Criminal Code of the Republic of Serbia, *Službeni glasnik RS*, no. 85/2005, 88/2005 - corrected, 107/2005 - corrected, 72/2009, 111/2009, 121/2012, 104/2013, 108/2014, 94/2016 and 35/2019.

Tea Micevska*

The written form of the civil proceedings in the digital era: an evolution in the digital work environment

Abstract: For the last decades, the world has been witnessing rapid digitalization of the judicial systems which influenced the functionality of the global distribution of justice. The new era of industrial revolution, *i.e.* the digital era, allowed litigation to lean towards a process of digital transformation. It is certain that a digitalized civil procedure is a prerequisite for a modern justice system in which the traditional legal principles are constantly evolving. However, the use of the information technologies should not undermine the fundamental principles of civil procedure, including the written form of the proceedings regarded as a guarantee for an effective legal protection. Therefore, the question arises: how to enable the transition of judicial processes from paper to digital while enhancing trust in such electronic transactions? Based on the aspiration of elaborating on different aspects of the evolution of the written form of civil proceedings in the period of digital rhetoric, this paper offers insights of the European Union's *acquis communautaire* and its integration into the legal order of North Macedonia. The author emphasizes the manners in which the traditional principle of the written form of civil proceedings evolves with the introduction of the information technology in the digitalizing judicial systems.

Keywords: civil procedure, digitalization, written form, evolution, electronic documents

* Tea Micevska is an assistant lecturer at the Department of Civil Procedural Law, Iustinianus Primus Faculty of Law, Ss. Cyril and Methodius University, Skopje, Macedonia; E-mail: t.micevska@pf.ukim.edu.mk.

1. Introduction

The principles of civil litigation are foundational pillars of each proceeding which ensure integrity, fairness and equality in the administration of justice. In the pursuit of justice, judges tend to ascribe great weight on the concept of "truth", which is often considered to be key value in the hierarchy of procedural values.[1] However, even in a philosophical sense, the concept of absolute truth is elusive, therefore, much less can it be expected to be reached in a court proceeding.[2] In that regard, due to the fact that achieving a justice system which always reflects the actual truth is highly unattainable, each country's aim should be to guarantee its citizens fair and equal treatment of all parties in public civil proceedings.[3]

Historically, oral proceedings were associated with publicity, just as written proceedings were associated with secrecy and confidentiality.[4] However, the public character does not necessarily arise from the oral nature of the proceedings.[5] Through the years, the principle of the written form of the proceedings has gained strength, in order to make the proceedings easier, more efficient and less costly.[6] This serves as another confirmation that the way in which the Romans adapted the procedure to the needs of life, is a proven historical experiment, applicable even in today's conditions.[7] Thus, it provides evidence that the principles of civil procedure, *inter alia*, the principle of written proceedings, are constantly evolving over time.

---

[1] Uzelac (2010) xxiii.
[2] Georgievski (1995) 65.
[3] Habscheid (1978) 15, 30.
[4] Habscheid (1978) 30.
[5] Habscheid (1978) 30.
[6] Zoroska-Kamilovska (2004), 465.
[7] Zoroska-Kamilovska (2004), 465.

The written form of the proceedings, deeply rooted in the traditional principles of civil procedure, is under a continuous process of evolution as a result of the challenges that each distinct period imposes, thereby adjusting to the needs of the progressive legal field. Given the fact that digitalization has confronted the world with whole new, previously unencountered challenges, it is inevitable to notice that its intrusive nature has impacted civil procedure as well. It is evident that the governments have made investments in digitalizing justice in the past years, however, the degree of digitalization differs throughout the member states of the European Union. The question of how information technologies can support improving the problems of delay has grown significantly in recent times.[8] Therefore, with the aim of providing a comprehensive framework for improving the use of digital technology in the judicial process, while securing the fundamental values of civil procedure, the European Union has been developing different instruments which offer a framework and safeguards to member states.[9]

The main intention of this paper is to examine how the modern dynamic of the digital work environment incorporates into the traditional foundation of the written form of the civil proceedings, especially in regard to the treatment of the electronic documents. Through an analysis of the main instruments adopted by the European Union, designed for implementing and pursuing digitalization of the courts, primarily, the paper will provide an overview of the framework established within the European *acquis communautaire*, with focus on the electronic documents submitted as evidence. Afterwards, by conducting a detailed observation of the Macedonian legislation and the relevant practice, the paper will present perspectives regarding the harmonization of the

[8] Reiling (2009) 17.
[9] CEPEJ(2021)15, 1.

Macedonian legal system with the European legislation, the application of the provisions by the courts and the challenges with which relevant stakeholders, such as judges, practitioners and legal scholars are dealing. Nonetheless, the attention will gravitate around one core element – the electronic document, which is pivotal for the introduction of the electronic and information technology into the civil proceedings.

2. European framework

The electronic document flow is becoming an integral part of the modern society, and the activity of the courts is not an exception. The indiscreet invasion of information technology into the judicial systems on global scale called upon the European Union's institutions to set authoritative standards governing the comprehensive treatment of the electronic documents, along with their place in the legislations of the countries. The main issues surrounding electronic documents - submission, e-filing, secure e-platforms, probative value, storage etc. will be examined in the following text through the viewpoint of the most relevant documents of the European *acquis communautaire*.

2.1. ELI-UNIDROIT Model European Rules of Civil Procedure (MERCP)[10]

The joint project of the European Law Institute (ELI) and the International Institute for the Unification of Private Law (*Institut international pour l'unification du droit privé*, UNIDROIT) launched in 2014 resulted with adopting the Model European Rules of Civil Procedure which were formally approved in 2020 and published in 2021. The MERCP were built upon an instrument produced jointly by the American Law

[10] MERCP (2021).

Institute (ALI) and UNIDROIT, the Principles of Transnational Civil Procedure of 2004,[11] by adapting those principles to the European context in the light of: (*i*) the European Convention on Human Rights (ECHR)[12] and the Charter of Fundamental Rights of the European Union;[13] (*ii*) secondary EU legislation; (*iii*) common traditions in the European countries; (*iv*) the Storme Commission's work;[14] and (*v*) other pertinent European sources.[15] The aim of the MECRP is to devise a set of best practice rules for the future development of European civil procedure through different countries.[16]

As a general rule, in so far as appropriate, Rule 18(4) supports the use of information and communication technologies.[17] Many other rules complement and expand this general rule,[18] however, according to the paper's subject, the main focus will revolve around Rule 111 which contains provision for documentary and electronic evidence, their production and

[11] Principles of Transnational Civil Procedure (2005).
[12] ECHR (1950).
[13] CFREU (2016).
[14] Storme (1994).
[15] Haukeland Fredriksen, Strandbeg (2022).
[16] MERCP (2021), Preamble, 3.
[17] MERCP (2021), Rule 18(4): "In so far as appropriate, proceedings may be conducted using any available means of information and communication technology."
[18] See for example: Rule 17(3) in connection with Rule 18(4) on electronic publication of judgments; Rule 61(2) on the use of electronic means of communication for case management hearings (e.g., video or audio transmission); Rule 74(1)(b) and (1)(c) on service by electronic means that guarantees receipt; Rule 79 on the mandatory provision of an electronic address for service by lawyers; Rule 97(2) on mandatory video recording of hearings where evidence is taken; Rule 97(3) on evidence-taking by video-conferencing or similar distance communication technologies; Rule 115(2) on the oral examination of witnesses by video-conferencing or similar technology; and, Rule 220 on the use of a secure electronic platform ensuring efficient management for collective proceedings.

storage and Rule 112 which prescribes the probative force of electronically recorded authentic instruments.[19]

Namely, Rule 111 equates the paper and electronic form of the document, stating that documents could be understood as anything which contains the embodiment of information recorded in "*writing, pictures, drawings, programmes, voice messages, or electronic data, including e-mail, social media, text or instant messages, metadata, or other technological means*."[20] With this, the MERCP introduce and confirm the use of electronic documents in civil proceedings, which serve the same function as documents in tangible physical form by permanently storing information and displaying it authentically.[21] It is noticeable that this Rule may be applied in procedural systems that have implemented digital proceedings or that enable electronic submission of documents, including statements of case.[22]

One extremely important factor because of which Rule 111 should be regarded in conjunction with Rule 112 is the authenticity of the electronic documents. Although the MERCP do not address specific types of tests for determining the authenticity of the documents, Rule 112 primarily outlines the notion of authentic instruments.[23] Additionally, and probably most importantly regarding the electronic documents, Rule 112 provides that "*electronically recorded authentic instruments have the same probative force as those recorded on paper*."[24] However, since the formal requirements for establishing the

[19] MERCP (2021), 54.
[20] MERCP (2021), Rule 18(2).
[21] MERCP (2021) 158.
[22] MERCP (2021) 159.
[23] MERCP (2021) Rule 112(1): "An authentic instrument is a document, which has either been formally drawn up or the authenticity of which has been certified by a public authority."
[24] MERCP (2021) Rule 112(2).

authenticity of the documents may vary in different jurisdictions, the MERCP do not enter into further elaboration of the procedure. Nonetheless, it is of paramount importance that according to Rule 112, the (authentic) electronic documents have the same probative value as the (authentic) paper based documents. The procedure and requirements for confirming the authenticity depend on the disposition of different countries.

2.2. Guidelines of the Committee of Ministers to member States on electronic evidence in civil and administrative proceedings

With the aim of providing a common framework and achieving greater unity between different member States, the Council of Europe adopted the Guidelines of the Committee of Ministers to member States on electronic evidence in civil and administrative proceedings[25] which provide practical guidance for the handling of electronic evidence in civil and administrative proceedings to courts and other competent authorities.[26] Taking into consideration the diversity of the different legal systems, the Guidelines are not established to serve as binding legal rules, but rather as a tool for accommodating the differences in the legal systems of the member States whose diversity is fully acknowledged.[27]

Primarily, the Guidelines define the notion of electronic evidence[28] and acknowledge its use in court proceedings by stating that it should not be denied or refused "*only because it*

[25] Guidelines and explanatory memorandum (2019).
[26] Guidelines and explanatory memorandum (2019) 5, 6.
[27] Guidelines and explanatory memorandum (2019) 13, 14.
[28] Guidelines and explanatory memorandum (2019) ""Electronic evidence" means any evidence derived from data contained in or produced by any device, the functioning of which depends on a software program or data stored on or transmitted over a computer system or network.".

is collected and/or submitted in an electronic form".[29] Thus, they emphasize the use of the electronic signature in the sense of the Regulation (EU) No 910/2014,[30] however, they state that the electronic documents should not be rejected due to the lack of an advanced, qualified or similarly secured electronic signature.[31] Having in regard the easily alterable nature of electronic documents, the Guidelines highlight that the electronic documents "*should be collected in an appropriate and secure manner, and submitted to the courts using reliable services*."[32] In order to improve the efficiency in the court proceedings, Guideline 15 for example, encourages the transmission of electronic evidence by electronic means, but only if the systems and devices used for such transmission are capable of maintaining its integrity.[33] The implementation of these particular Guidelines is highly dependable on the digital advancement of the legal system of the State. Regarding the concept of integrity, the relevance and reliability of electronic documents are important elements in its preservation. In that regard, the Guidelines call upon the importance of a competent technical expertise, such as expert opinion, in order to sustain the documents' relevance and to avoid introduction of unnecessary electronic evidence.[34] As regards reliability, the courts should take into consideration the source of the electronic documents as well as its authenticity.[35] The Guidelines widely leave this question to the discretion of the judge, as well as to the regulation of the different national legal systems.[36] Furthermore, the storage, preservation and archiving should

[29] Guidelines and explanatory memorandum (2019) 8.
[30] Regulation (EU) No 910/2014, Articles 25-34.
[31] Guidelines and explanatory memorandum (2019), Guideline 7.
[32] Guidelines and explanatory memorandum (2019), Guideline 10.
[33] Guidelines and explanatory memorandum (2019), Guidelines 15 and 16.
[34] Guidelines and explanatory memorandum (2019) 22, 23, Guidelines 17 and 18.
[35] Guidelines and explanatory memorandum (2019) Guideline 19.
[36] Guidelines and explanatory memorandum (2019) 23, 24.

meet all safety requirements and guarantee the integrity, authenticity, confidentiality and privacy of the data, taking into account the evolution of the information technology in the specific State.[37]

In sum, the Guidelines imply that electronic documents regarded as evidence should not be discriminated against or favored over other types of evidence. In this sense, the courts should apply a technology-neutral approach while assessing the electronic evidence, as long as its admissibility, authenticity, accuracy, and integrity are preserved.[38] Even though the use of electronic documents as evidence in civil proceedings has already been introduced in the legal systems of some member States of the European Union,[39] the Guidelines serve as a tool for encouraging and giving direction to the countries for maximizing the use of information technologies in their legal systems in accordance with their digital capacities.

2.3. Guidelines on electronic court filing (e-filing) and digitalisation of courts

With the purpose of improving the efficiency and the quality of justice by enhancing the use of information and communication technologies, the Council of Europe made an effort in developing tools which offer a framework and safeguards to member states and justice professionals.[40] As a result, the Guidelines on electronic court filing (e-filing) and digitalization of courts (CEPEJ(2021)15) were adopted, which provide a set

[37] See: Guidelines and explanatory memorandum (2019), Guidelines 25-30.
[38] Oręziak, Świerczyński (2019) 272.
[39] For example: Austria, Slovenia, the Netherlands, Germany, France. See also: Nunner-Krautgasser, Anzenberger (2015) 21, 22; Ivanc (2015) 41-45; van Rhee (2015) 17; Wolf, Zeibig (2015) 36; Oudin (2015) 27, 28.
[40] CEPEJ (2021)15 3.

of key measures necessary for a functioning e-filing system.[41] The main goal of CEPEJ(2021)15 is to enable each party to start a judicial proceeding by issuing electronic documents, exchange documents with other parties, judges or prosecutors, send and receive notifications and summons electronically, pay court fees online, access a secure repository of all procedural documents and provide an efficient and effective treatment of data for all the users that are involved.[42] In other words, such e-filing systems should be able to provide the complete set of functionalities needed to establish digital workflows, promote cooperation with relevant parties (court users, citizens, lawyers) and to enable the transition of judicial processes from paper to digital.[43]

Since the electronic documents are the essence of the e-filing system and the overall digital workflow, CEPEJ(2021)15 has covered all the aspects of the entire lifecycle of an electronic document.[44] Therefore, the underlying key requirements for a successful digitalization are: adding links to legislation and/or case law, the use of qualified e-signatures (or equivalent services) to ensure the integrity and authenticity, transmission and quality checks of metadata to automatically update the case management system, inclusion of multimedia and large files (i.e., wiretaps, video files, etc.), possibility to personalize templates for documents for internal users, measures to guarantee secure platforms for handling and exchanging of e-evidence with other authorities and cross-border.[45]

---

[41] CEPEJ (2021)15 4: "electronic court filing (or e-filing) refers to technological solutions facilitating access to justice by establishing a digital channel that enables the interaction and exchange of data and e-documents between courts and court users".
[42] CEPEJ (2021)15 4.
[43] Contini, Reiling (2022) 657.
[44] Giuliana Civinini (2021).
[45] CEPEJ (2021)15 Points 55-65.

CEPEJ(2021)15 enshrines the core judicial values embodied in the fundamental legal principles of civil proceedings, such as: rule of law; independence of the judiciary; guarantees to a fair trial; non-discriminatory implementation of the proceedings; access to an effective judicial remedy shall be granted in case any user's basic rights are negatively impacted or harmed and data protection principles.[46] However, in addition to these principles, essential elements of any e-governance strategy are: the "digital by default" principle;[47] inclusiveness and accessibility; openness and transparency; performance, security, and integrity of information – data protection by design and by default; data management and preservation of information; interoperability and measures for better allocation of resources and monitoring of management processes.[48] These principles serve as a foundation for enabling a digital working environment with information technology tools that people will prefer to use.

The introduction of digital technologies is often seen as a way to modernize justice on a small or large scale, with more or less important financial implications.[49] Nonetheless, the implementation of the various digital tools into the judicial systems without altering the already existing fundamental values is a burdensome process. The all-round digitalization may appear unprecedented, therefore, the guidelines from CEPEJ(2021)15 require change that involves not only utilizing

[46] CEPEJ(2021)15 5 Points A-F.
[47] CEPEJ(2021)15 5: "Digital by default" is a principle with both organisational and technical dimensions and strategic importance and should be implemented as such. In general, it refers to providing public services by digital means as the preferred option for people to use them, i.e., digital services that are so straightforward and convenient that all those who can use them will choose to do so whilst those who cannot or are not willing to are not excluded."
[48] CEPEJ(2021)15 5 Points G-M.
[49] CEPEJ(2016)13 5.

modern technologies to support the judicial system, but also considering the legal, organizational and socio-cultural considerations which influence the functioning of the judicial bodies.[50] While much has been learned by simply doing during the peak of the pandemic, it can still be seen that the member States are increasingly deploying information technologies to support judicial activity which is also reflected in the greater percentage of courts' budget which is allocated to information technologies.[51]

2.4. Regulation (EU) 2020/1784 on the service of documents[52]

The purpose of the Regulation (EU) 2020/1784 is to expedite and simplify the transmission of judicial and extrajudicial documents in civil or commercial matters between the Member States while increasing the efficiency and expeditiousness of judicial procedure.[53] It outlines several amendments to Regulation (EC) 1393/2007,[54] which establishes expedited channels and uniform processes for sending documents between Member States, primarily for the purpose of delivering them within the receiving state.[55]

[50] CEPEJ (2021)15 3.
[51] CEPEJ Evaluation Report 2022 122.
[52] Regulation (EU) 2020/1784 of the European Parliament and of the Council of 25 November 2020 on the service in the Member States of judicial and extrajudicial documents in civil or commercial matters (service of documents) (recast) (Regulation (EU) 2020/1784).
[53] Maciejewski (2021) 5.
[54] Regulation (EC) No 1393/2007 of the European Parliament and of the Council of 13 November 2007 on the service in the Member States of judicial and extrajudicial documents in civil or commercial matters (service of documents).
[55] European Sources Online Regulation (EU) 2020/1784 (2020).

Firstly, what sets the Regulation (EU) 2020/1784 apart from the previous one is the inclusion of electronic service as a recognized method, thereby enhancing the role of digitalization in legal proceedings.[56] It is logical to assume that the guiding principle set forth by the European Union Court of Justice, which asserts the equal standing of various service methods,[57] will continue to apply in the implementation of this new Regulation.[58] Secondly, a major change in the new regulation involves requiring the agencies and bodies chosen by Member States to use a reliable decentralized IT system[59] called e-Codex[60] for sending legal documents, ensuring secure and efficient transmission.[61] This system comprises national IT systems that are interconnected and technically interoperable.[62] Thus, a Commission Implementing Regulation (EU) 2022/423[63] was adopted in order to lay down the technical specifications, measures and other requirements for the

[56] See: Regulation (EU) 2020/1784, Article 19.
[57] Plumex v Young Sports NV (2006) 22.
[58] Rose Vincze, Kàrolyi, Olga Kiss (2022) 10.
[59] Regulation (EU) 2020/1784, Article 2(2): ''decentralised IT system' means a network of national IT systems and interoperable access points, operating under the individual responsibility and management of each Member State, that enables the secure and reliable cross-border exchange of information between the national IT systems.'
[60] Also, a brand-new Regulation on e-CODEX has entered into force this year: Regulation (EU) 2022/850 of the European Parliament and of the Council of 30 May 2022 on a computerized system for the cross-border electronic exchange of data in the area of judicial cooperation in civil and criminal matters (e-CODEX system), and amending Regulation (EU) 2018/1726 (Text with EEA relevance).
[61] See: Regulation (EU) 2020/1784, Article 5 'Means of communication to be used by transmitting agencies, receiving agencies and central bodies'.
[62] Adoption of (EU) Regulation No. 2020/1784 on the service of documents (2020).
[63] Commission Implementing Regulation (EU) 2022/423 of 14 March 2022 laying down the technical specifications, measures and other requirements for the implementation of the decentralised IT system referred to in Regulation (EU) 2020/1784 of the European Parliament and of the Council.

implementation of the decentralized IT system.[64] Thirdly, where the documents to be served, requests, confirmations, receipts, certificates, and other communications referred to in Article 5(1) of the regulation require or feature a seal or handwritten signature, qualified electronic seals or qualified electronic signatures as defined in Regulation (EU) No 910/2014 may be used instead.[65] Fourthly, in cases where the recipient's address in another Member State is unknown, the Regulation (EU) 2020/1874 provides methods for determining the address.[66] This represents a significant leap forward in obtaining recipient details. Previously, locating the recipient's address in the Member State of service was sometimes impossible. Article 7 of the new regulation is designed to eventually verify the recipient's legal domicile, thus reducing the necessity for delivering documents when the recipient resides at a specific location with an undisclosed address.[67]

The Regulation (EU) 2020/1784 aims to expedite cross-border legal proceedings by taking advantage of digitalization and modern technology, promoting fair access to justice. It allows electronic document service to individuals in other Member States with prior consent, utilizing registered electronic delivery or, with certain conditions, email.

---

[64] Celis (2022).

[65] Adoption of (EU) Regulation No. 2020/1784 on the service of documents (2020). *See*: Article 5(3).

[66] Regulation (EU) 2020/1784, Article 7: '(a) providing for designated authorities to which transmitting agencies may address requests on the determination of the address of the person to be served; (b) allowing persons from other Member States to submit requests, including electronically, for information about addresses of persons to be served directly to domicile registries or other publicly accessible databases by means of a standard form available on the European e-Justice Portal; or (c) providing detailed information, through the European e-Justice Portal, on how to find the addresses of persons to be served.'

[67] Adoption of (EU) Regulation No. 2020/1784 on the service of documents (2020).

2.5. Regulation (EU) 2020/1783 on taking of evidence

Similarly to the Regulation (EU) 2020/1784, the main intention of the Regulation (EU) 2020/1783 on taking of evidence[68] is to replace the traditional paper-based process of transmitting requests, and by that, to expedite the proceedings.[69] Both the Regulation (EU) 2020/1784 and Regulation (EU) 2020/1783 deal with the similar questions: communication methods used by transmitting agencies, receiving agencies, courts and central bodies through a secure and reliable decentralized IT system.[70]

However, the Regulation (EU) 2020/1784 rules in details the use of modern communications technology to improve the speedy transmission of requests between Member States in taking of evidence.[71] It seeks to enhance the effectiveness of judicial proceedings by simplifying the cross-border evidence cooperation mechanisms, while reducing delays and costs, providing legal certainty and digitalized procedures, thereby encouraging individuals and businesses to engage in cross-border transactions to boost trade and the internal market.[72] It sets out a number of amendments to Regulation (EC) No 1206/2001,[73] which establishes a system for the transmission of requests for the taking and execution of evidence between courts.[74]

---

[68] Regulation (EU) 2020/1783 of the European Parliament and of the Council of 25 November 2020 on cooperation between the courts of the Member States in the taking on evidence in civil or commercial matters (taking of evidence) (recast) (Regulation (EU) 2020/1783).
[69] Celis (2022).
[70] Celis (2022).
See: Regulation (EU) 2020/1783, Article 7(4).
[71] Anh Tran (2022).
[72] Regulation (EU) 2020/1783 (3).
[73] Council Regulation (EC) No 1206/2001 of 28 May 2001 on cooperation between the courts of the Member States in the taking of evidence in civil or commercial matters.
[74] European Sources Online Regulation (EU) 2020/1783 (2020).

Regarding one of the main key points - the decentralized IT system, the Regulation (EU) 2020/1783 gives the Member States an extended deadline with specific requirements for developing the system.[75] A guarantee for application of said regulation is Article 8 according to which: "*Documents that are transmitted through the decentralized IT system shall not be denied legal effect or considered inadmissible as evidence in the proceedings solely on the grounds that they are in electronic form*." The Regulation (EU) 2020/1783 extends the use of technology by introducing the notion of direct taking the evidence by videoconferencing.[76] It is of great importance that both the Regulation (EU) 2020/1783 and the Commission Implementing Regulation (EU) 2022/422[77] safeguards the procedural rights of the litigants by stating that the overall process of taking evidence should ensure that the procedural rights, as well as the privacy, integrity and confidentiality of the data should be ensured.[78]

Undoubtedly, the Regulation (EU) 2020/1783 aims to normalize the use of technology and maximize its application from a legal, technical and institutional point of view.[79] It is up to the Member States, depending on how technologically advanced they are, to implement the Regulation (EU) 2020/1783 as soon as possible, including all the necessary details.

---

[75] Regulation (EU) 2020/1783, Article 35(3).
[76] Regulation (EU) 2020/1783, Article 20.
[77] Commission Implementing Regulation (EU) 2022/422 of 14 March 2022 laying down the technical specifications, measures and other requirements for the implementation of the decentralised IT system referred to in Regulation (EU) 2020/1783 of the European Parliament and of the Council.
[78] Regulation (EU) 2020/1783, Recital (30) - (21).
[79] Onţanu (2022).

The European legal framework is going through substantial transformation influenced by the process of digitalization and the adoption of modern technologies. These legislative and guideline initiatives, such as the ELI-UNIDROIT Model European Rules of Civil Procedure, the Guidelines on Electronic Evidence, and the Regulations on Service of Documents and Taking of Evidence, collectively aim to simplify the legal processes, to improve efficiency, and to ensure the secure handling of electronic documents. In addition to opening a path for the normalization of technology in the legal field, they also give the Member States the authorities to adopt these instruments in accordance to their technological advancement. As these initiatives continue to evolve, they have potential to harmonize the legal systems of the countries in Europe, with the ultimate goal to promote access to justice in the context of the inevitable digital future.

3. Reflection of the European framework into the Macedonian legislation

In the process of continuous evolution, North Macedonia introduced electronic documents in civil procedure and extended the legislation with provisions that facilitate more efficient legal processes, including several legal acts that regulate the legal system. The position of the electronic documents in North Macedonia's judicial system is mainly determined by the Law on Civil Procedure (LCP),[80] the Law on electronic documents, electronic identification and confidential services (LEDEICS),[81] the Rulebook for the mandatory

[80] Law on Civil Procedure, Official Gazette of RM, No.79/2005, 110/2008, 83/2009, 116/2010 and 124/2015 (LCP).
[81] Law on electronic documents, electronic identification and confidential services, Official Gazette of RM, No. 101/2019.

elements of the electronic documents (the Rulebook),[82] the Rules of Court,[83] thus, the official Judicial Portal of the Republic of North Macedonia[84] provides instructions for using the System for electronic delivery and receipt of acts in the courts of North Macedonia.[85]

In 2015, the LCP introduced a novelty according to which "*a document is a written record, image, drawing, data or information of any kind stored on paper or recorded in electronic, audio, visual or other form*."[86] With this, the electronic form of the documents was incorporated into the Macedonian legal system. Appearing as *lex specialis*, the LEDEICS achieves compliance with Regulation (EU) no. 910/2014 and defines electronic documents as "*any content stored in electronic form, especially textual or sound, visual or audio-visual records.*"[87] The fact that the LCP now prescribes both 'document' ('исправа')[88] and 'document' ('документ) as

[82] Rulebook for the mandatory elements of the electronic documents, Official Gazette of RNM, No. 47/2020.
[83] Rules of Court, Official Gazette of RNM, No. 47/2020.
[84] Judicial Portal of the Republic of North Macedonia, <http://sud.mk/wps/portal/central/sud/!ut/p/z1/hZDRCoJAEEW_KGZKXe1xwVyxRAnXdF5CQkrILUT7_oyeVsudt4Fz7lwGCAogVb2aa9U3D1Xdx70kdmbCttHb4yHBwEMeRyzO0Lbw6MBJB0Qq3RHwMcy20Ua4DGjZz4GALkPX1aqHsu-Geho5dz6R-Gc4Tn0vZGvkO9_JEyksHlimSl9_4YDRJ1NF0jN-VNSB-VtDhMjEPFvZrqQssElvb5No_Zk!/dz/d5/L2dJQSEvUUt3QS80TmxFL1o2XzZHNDQwOEswTEdQVTcwQU1EMEhUOUoyRzc2/>.
[85] System for electronic delivery and receipt of acts in the courts of the Republic of Macedonia <https://edostava.sud.mk/>.
[86] LCP, Article 215-a.
[87] LEDEICS, Article 3 (1)(3).
[88] LCP, Article 215(1): "A document issued in a prescribed form by a state authority or an authority of the state administration within the limits of its competence, as well as a document issued in such a form by an organization or other institution when exercising a public authority entrusted to it by law or by a decision of an authority of the municipality based on law (public document), proves the truth of what is confirmed or determined in it."

means of evidence led to confusion among the legal scholars and practitioners. However, the key point to be highlighted in this paper is that electronic documents are now recognized as valid means of evidence, alongside the traditional paper-based, physical document ('исправа').

Considering that the relevant documents from the European *acquis communautaire* focus on the categorization and the evidentiary value of the electronic documents, it is of great importance to examine the position of the Macedonian legislator on this matter. In that regard, according to the LCP, electronic documents fall within the category of the traditional means of evidence: inspection, documents, witnesses, expertise and hearing of the parties.[89] In practice, they are treated as documents or items for inspection. However, the LCP doesn't provide further details about the use of electronic documents. It simply prescribes Article 215-a, which integrates the use of electronic documents into the legal system and equalizes them with the other means of evidence. On the other hand, the LEDEICS enters into further regulation of the electronic documents, including aspects such as their legal effect, creation, digitalization, verification,[90] which are crucial factors for determining their legal regime. Regarding the legal effect and evidentiary value of the electronic documents, the LEDEICS prescribes explicit provisions according to which "*the electronic document has the same legal and evidentiary force as the written form of the document, in accordance with the law. An electronic document cannot be challenged as evidence in an administrative or judicial procedure solely because it has been created in electronic form. When the law establishes a written form for documents or acts, the electronic document is considered a document or act in written form*."[91] By that,

[89] See: LCP, Articles 212-256.
[90] LEDEICS, Articles 6-10.
[91] LEDEICS, Article 6.

LEDEICS put the evidentiary value between the electronic and paper-based documents on equal basis, just as MERCP[92] and the Guidelines of the Committee of Ministers to member States on electronic evidence in civil and administrative proceedings[93] provide.

Nonetheless, in order to be admissible in the court proceedings, the document has to be authentic and reliable. An electronic document is considered authentic when it goes through a process of 'electronic authentication'. This process enables electronic identification of either a natural or legal person and ensures that the origin and integrity of the data presented in electronic form is verified.[94] Thus, the LEDEICS prescribes conditions and standards for said identification.[95] Regarding the reliability of the electronic documents, the '*courts should be aware of the value of trust services in establishing the reliability of electronic evidence*.'[96] In this context, LEDEICS lays out rules for verifying electronic signatures, seals, timestamps, and certificates, even those verifying website authenticity, provided by confidential service providers. The law also sets out criteria for both systems for electronic identification[97] and service providers.[98] In order for the parties to ensure the authenticity and reliability of the electronic documents before submitting them to the Court, a specific format and technical instructions have to be followed. Namely, the Rulebook states that any electronic document issued by a public or a private authority should have three parts: a header with the issuer's logo, a body with legally required elements, and footer with an electronic signature or seal and a QR code for document verification. The

[92] MERCP, Rule 112.
[93] Guidelines and explanatory memorandum (2019) 8.
[94] LEDEICS, Article 3(7).
[95] LEDEICS, Articles 11-20.
[96] Guidelines and explanatory memorandum (2019) 10.
[97] LEDEICS, Article 11.
[98] LEDEICS, Article 24.

visual representation of the electronic seal is constituted of four components: logo, visual representation of the timestamp, verification location and QR code and circular message from the issuer of the electronic document about the validity of the electronic document.[99]

The fact that none of the above-mentioned legal sources explicitly clarify whether the evidentiary value for (paper-based) public documents applies to electronic documents raises an intriguing legal question. It can be concluded that, by analogy, if the electronic document is issued by a public legal authority, it will have the same evidentiary value as a document issued by a public authority in written form. Thus, the Law on Electronic Governance and Electronic Services (LEGES)[100] which, *inter alia*, regulates the functioning of the courts and other legal entities entrusted by law to exercise public powers, prescribes that '*the electronic documents issued by the competent authorities through the National Portal for electronic services are issued based on the prescribed standards*' of LEDEICS.[101]

One of the provisions that probably stand out as the best example of the evolution of written to electronic form of the documents is Article 9 from LEDEICS, which prescribes rules for digitalization of the documents. Understood as "*the process of converting a document whose form is not originally electronic into a digital document*",[102] the effects of the digitalization are threefold:
(1) It confirms the incorporation of the electronic documents into the legal system,

[99] The Rulebook, Article 9.
[100] Law on Electronic Governance and Electronic Services, Official Gazette 98/2019 from 21.05.2019.
[101] LEGES, Article 20(2).
[102] LEDEICS, Article 3 point 43.

(2) It introduces a digital workflow and a new way of processing the documents by court clerks, and
(3) It enables electronic storage of the documents.

According to LEDEICS, a digitalized document will have the same legal and evidentiary value as the original document if certain conditions are met, including supervision by an authorized individual and confirmation of the identity of the digitalized document through qualified electronic seal or a qualified electronic signature of the authorized individuals.[103] The digitalization is important due to the fact that it enables preparation of the digitalized documents for electronic storage, even if the original document was not created in an electronic form.[104] The aim of the preparation is to prepare documents for secure electronic storage, to ensure that all essential original document elements are transferred, to preserve usability of the original document, to maintain content integrity by using electronic signatures, seals and timestamps, conduct quality control, and maintain proper records of all related activities by using appropriate procedures and technological solutions.[105] Nonetheless, the LCP prescribes that the documents can be delivered "*by post, electronically, through a court official, directly in court, through a notary, executor or other person determined by law*".[106] Therefore, it can be seen that direct electronic submission is prescribed as well. In that regard, the Rules of Court further provide that if the parties submit the documents electronically, they have to send their submissions using a specialized web portal, provided that they have registered on the portal and can identify themselves with an electronic certificate.[107] After the registration, the party should

[103] LEDEICS, Article 9.
[104] LEDEICS, Article 57.
[105] LEDEICS, Article 58, 59.
[106] LCP, Articles 98(1), 125(1).
[107] Rules of Court, Article 159.

send the submission with all accompanying documents in electronic format through the court's electronic mailbox to the reception department of the competent court which is afterwards sent to the opposing party.[108] Regardless whether the documents are submitted electronically or not, the court clerk scans them in order to form an electronic court case, processes them in the automated computer system for managing court cases (ACCMIS), adds them to the case in chronological order, and delivers them to the judge handling the case for further proceedings.[109] In regard to the archiving, the Rules of court do not provide special procedures for archiving electronic documents by stating that the material "*created in courts in paper and electronic form previously deposited in the passive archive, is carried out in accordance with these rules of procedure and related regulations of the archival material.*"[110]

In the Macedonian court practice, a tendency towards acceptance of electronic documents can be observed, by regarding the e-mail communications,[111] Viber messages[112] and video recordings[113] as admissible evidence. It can be seen that the Regulation (EU) no. 910/2014 is quite literally incorporated into the Macedonian legal system through the LEDEICS. The other legal sources supplement the framework of the electronic documents in line with the European *acquis communautaire*, however, the main problem arises in regard to the implementation of those rules in practice. Most of the courts are not technologically equipped to properly implement electronic

[108] LEDEICS, Article 159.
[109] Rules of Court, Articles 164, 169.
[110] Rules of Court, Article 374.
[111] Decision of the Basic Court of Skopje, No. RO-1790/13 of 17.03.2017; Decision of the Supreme Court of the Republic of North Macedonia. Rev3. No. 58/2018 of 17.04.2019.
[112] Decision of the Basic Court in Veles MALVPL1-TS-43/19; Decision of the Basic Court of Veles, No. PL1-TS26/18 of 01.04.2020.
[113] ROŽ -331/21; GŽ-201/21.

document management. Therefore, instead of coming to life, most of the rules on electronic document management remain dead letters on paper. While it is correct that the European framework requires improvement of the national legislations to the extent that technological advancement in each state allows, it is evident that North Macedonia should adopt a more progressive approach to digital document management. Additionally, the absence of provisions regulating the possible alteration of the electronic documents, video-conferencing and cross-border services highlight the need for further development of the Macedonian legislation in accordance with the European standards.

4. Conclusion

The legal changes and software development go hand in hand. It is inevitable to accept that the information technologies are no longer a tool, but rather a digital work environment. The global digitalization of the justice system paved its way towards digital transformation in civil procedure as well. In this process, even the traditional legal principles have to adapt to the technology-driven world. Regarded as a pillar, the evolution in the principle of written form of the proceedings imposes the need of a seamless transition from paper-based to digital documents while instilling trust into the electronic workflow. The under-resourced courts, the fragile and easily alterable nature of the electronic documents, the lack of organizational change and management strategy and the resistance to change are one of the main challenges imposed to the countries in Europe, including North Macedonia.

In conclusion, the digitalization of the civil proceedings offers a dynamic evolution in the pursuit of justice. It is a path which requires constant dedication in order to make sure that the legal systems uphold their fundamental core principles while

maximizing the information technology's revolutionary potential.

Literature

Anh Tran Q, *Electronic Evidence in Civil and Commercial Dispute Resolution, A Comparative Perspective of UNCITRAL, the European Union, Germany and Vietnam* (Springer, European Yearbook of International Economic Law, 2022).

C.H. van Rhee, and Uzelac A, 'The pursuit of truth in contemporary civil procedure. Revival of accuracy or a new balance in favour of effectiveness?' (2012) Truth and Efficiency in Civil Litigation Fundamental Aspects of Fact-finding and Evidence-taking in a Comparative Context, xxiii.

Celis, M., 'A few developments on the modernisation of the service of judicial and extrajudicial documents and the taking of evidence in the European Union' (Conflictoflaws. net 2022) < https://conflictoflaws.net/2022/a-few-developments-on-the-modernisation-of-the-service-of-judicial-and-extrajudicial-documents-and-the-taking-of-evidence-in-the-european-union/ > accessed 8 September 2023.

Charter of Fundamental Rights of the European Union (OJ C 202, 2016).

Wolf Ch, and Zeibig N, *Evidence in Civil Law - Germany* (Maribor: Institute for Local Self-Government and Public Procurement, 2015).

Commission Implementing Regulation (EU) 2022/422 of 14 March 2022 laying down the technical specifications, measures and other requirements for the implementation of the decentralised IT system referred to in Regulation (EU) 2020/1783 of the European Parliament and of the Council (European Commission, 2022).

Commission Implementing Regulation (EU) 2022/423 of 14 March 2022 laying down the technical specifications, measures and other requirements for the implementation of the decentralised IT system referred to in Regulation (EU) 2020/1784 of the European Parliament and of the Council (European Commission, 2022).

Contini, F., and Reiling, D., 'Double normalization: When procedural law is made digital' Norm, Normal and Disruption: The role of Law, Knowledge and Technologies in Normal Social Life' (2022) 12(3) Oñati Socio-Legal Series 654.

Convention for the Protection of Human Rights and Fundamental Freedoms (Council of Europe Treaty Series 005, 1950).
Council Regulation (EC) No 1206/2001 of 28 May 2001 on cooperation between the courts of the Member States in the taking of evidence in civil or commercial matters (Council of the European Union, 2001).
Court of Justice of the European Union, Plumex v Young Sports NV, Case C-473/04, 09.02.2006 Case C-473/04 Plumex v Young Sports NV. [2006] *European Court Reports 2006 I-01417*.
Decision of the Basic Court in Veles MALVPL1-TS-43/19.
Decision of the Basic Court of Skopje, No. RO-1790/13 of 17.03.2017.
Decision of the Basic Court of Veles, No. PL1-TS26/18 of 01.04.2020.
Decision of the Supreme Court of the Republic of North Macedonia, No. Rev3. No. 58/2018 of 17.04.2019.
European Commission for the Efficiency of Justice, Guidelines on electronic court filing (e-filing) and digitalisation of courts (Council of Europe, 2021).
European judicial systems CEPEJ Evaluation Report 2022 Evaluation cycle (2020 data) (Council of Europe, 2022).
European Sources Online, 'Regulation (EU) 2020/1783 on cooperation between the courts of the Member States in the taking of evidence in civil or commercial matters (taking of evidence)' *Official Journal of the European Union* (2020) < https://www.europeansources.info/record/proposal-for-a-regulation-amending-regulation-ec-no-1206-2001-on-cooperation-between-the-courts-of-the-member-states-in-the-taking-of-evidence-in-civil-or-commercial-matters/> accessed 9 September 2023.
European Sources Online, 'Regulation (EU) 2020/1784 on the service in the Member States of judicial and extrajudicial documents in civil or commercial matters (service of documents)', *Official Journal of the European Union* (2020) <https://www.europeansources.info/record/proposal-for-a-regulation-amending-regulation-ec-no-1393-2007-on-the-service-in-the-member-states-of-judicial-and-extrajudicial-documents-in-civil-or-commercial-matters-service-of-documents/> accessed 8 September 2023.

Georgievski, S., *The basic principles of the civil procedural law of the Republic of Macedonia* (University of Ss Cyril and Methodius in Skopje 1995).
Civinini M, 'Introduction into CEPEJ instruments ENCJ Digital Justice Forum Seminar #4 The way forward' (Webinar, 2021)
Guidelines of the Committee of Ministers to member States on electronic evidence in civil and administrative proceedings (Council of Europe, 2019).
Guidelines on electronic court filing (e-filing) and digitalisation of courts (European Commission for the Efficiency of Justice, 2021)
Guidelines on how to drive change towards cyberjustice - Stock-taking of tools deployed and summary of good practices (European Commission for the Efficiency of Justice, 2017).
Habscheid WJ, 'The Fundamental Principles of the Law of Civil Procedure' (1984) 17(1) The Comparative and International Law Journal of Southern Africa 1 <http://www.jstor.org/stable/23246919> accessed 8 September 2023.
Fredriksen H, and Strandbeg, M., 'Impact of the ELI/UNIDROIT European Model Rules for Civil Procedure on national law – the case of Norway' (2022) 13(3) Civil Procedure Review 143.
International Union of International Officers, 'Adoption of (EU) Regulation No. 2020/1784 on the service of documents', < https://www.uihj.com/2020/12/07/adoption-of-eu-regulation-no-2020-1784-on-the-service-of-documents/ > accessed 8 September 2023.
Ivanc, T., *Evidence in Civil Law - Slovenia* (Maribor: Institute for Local Self-Government and Public Procurement 2015).
Judicial Portal of the Republic of North Macedonia, <http://sud.mk/wps/portal/central/sud/!ut/p/z1/hZDRCoJAEEW_KGZKXe1xwVyxRAnXdF5CQkrILUT7_oyeVsudt4Fz7lwGCAogVb2aa9U3D1Xdx70kdmbCttHb4yHBwEMeRyzO0Lbw6MBJB0Qq3RHwMcy20Ua4DGjZz4GALkPX1aqHsu-Geho5dz6R-Gc4Tn0vZGvkO9_JEyksHlimSl9_4YDRJ1NF0jN-VNSB-VtDhMjEPFvZrqQssElvb5No_Zk!/dz/d5/L2dJQSEvUUt3QS80TmxFL1o2XzZHNDQwOEswTEdQVTcwQU1EMEhUOUoyRzc2/> accessed 11 September 2023.
Law on Civil Procedure, Official Gazette of RM, No.79/2005, 110/2008, 83/2009, 116/2010 and 124/2015.

Law on electronic documents, electronic identification and confidential services, Official Gazette of RM, No. 101/2019.
Law on Electronic Governance and Electronic Services, Official Gazette 98/2019 from 21.05.2019.
Maciejewski, U., *Judicial cooperation in civil matters - legal basis objectives* (European Asylum Support Office 2021).
Model European Rules of Civil Procedure (ELI/UNDROIT, Oxford University Press 2021).
Nunner-Krautgasser B, and Anzenberger Ph, *Evidence in Civil law - Austria* (Maribor: Institute for Local Self-Government and Public Procurement, 2015).
Onţanu, E. A., 'Normalising the use of electronic evidence: Bringing technology use into a familiar normative path in civil procedure' (2022)12(3) Oñati Socio-Legal Series582, <https://opo.iisj.net/index.php/osls/article/view/1370> accessed 10 September 2023.
Oręziak B, and Świerczyński M, 'Electronic evidence in the light of the Council of Europe's new Guidelines' (2019) 25 Comparative Law Review 257.
Oudin, M., *Evidence in Civil Law - France* (Maribor: Institute for Local Self-Government and Public Procurement, 2015).
Principles of Transnational Civil Procedure (ALI/UNDROIT, Cambridge University Press, 2005).
Regulation (EU) 2020/1783 of the European Parliament and of the Council of 25 November 2020 on cooperation between the courts of the Member States in the taking on evidence in civil or commercial matters (taking of evidence) (recast) (2020).
Regulation (EU) 2020/1784 of the European Parliament and of the Council of 25 November 2020 on the service in the Member States of judicial and extrajudicial documents in civil or commercial matters (service of documents) (recast) (2020).
Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC.
Reiling, D., *Technology for Justice How Information Technology Can Support Judicial Reform* (Leiden University Press 2009).
Vincze F, Kàrolyi K, and Kis L, *The end of courts? Revamping the access to justice in cross-border cases* (Themis 2022).

Rulebook for the mandatory elements of the electronic documents, Official Gazette of RNM, No. 47/2020.
Rules of Court, Official Gazette of RNM, No. 47/2020.
Storme M, 'Approximation of Judiciary Law in the European Union' (1994) 19 Martinus Nijhoff Publishers
System for electronic delivery and receipt of acts in the courts of the Republic of Macedonia < https://edostava.sud.mk/ > accessed on 11 September 2023.
Van Rhee, C.H., *Evidence in Civil Law - the Netherlands* (Maribor: Institute for Local Self-Government and Public Procurement, 2015)
Zoroska-Kamilovska, T, 'The Roman civil procedure and its influence on modern civil procedure' (2004) 2 Contemporary law, legal science and the Iustinian's codification 453.

Marija Mijatovic,* Tamara Gajinov*

Corporate strategy of planned obsolescence - a reflection of the reality of technological development

Abstract: Planned obsolescence is a corporate policy phenomenon of creating (electronic) products with artificially limited useful lives or deliberately weak designs. The term includes all strategies that increase the rate of product replacement by shortening its life before the optimal term, both in a technical and psychological sense, or by discouraging their repair. This kind of manufacturer's behavior causes multiple harmful consequences. Firstly, the rights of consumers are being played out by not fulfilling their expectations and due to the need for premature replacement purchases. Secondly, the strategy of planned obsolescence has an extremely negative effect on the preservation of the environment, primarily through the creation of the so-called e-waste. However, defining planned obsolescence is a challenge for science, given that the manifestations of the strategy are multiple, legal regulation is just starting to emerge, and multidisciplinary approach to the problem is required before establishing clearer standards. The beginning of the fight against planned obsolescence was recorded through the class lawsuits in the USA, which served as an inspiration for the wave of current proceedings in the European Union. Therefore, the authors observe the existing judicial practice, the pioneering legislative example of the French Consumer Code, which sanctioned planned obsolescence for the first time, and the existing initiatives and the perspective of the regulation of this issue in the European Union, which for now has the form of non-binding soft law instruments.

* Marija Mijatovic is an assistant professor at the Faculty of Law and Business Studies Dr Lazar Vrkatić, Novi Sad, Serbia; E-mail: mrksicmarija@gmail.com.

* Tamara Gajinov is an associate professor at the Faculty of Law and Business Studies Dr Lazar Vrkatić, Novi Sad, Serbia; E-mail: tamara.gajinov@gmail.com.

Keywords: planned obsolescence, right to repair, corporate responsibility, technological development, EU law, consumer law

1. Introduction

Contemporary consumer society is marked by the need for constant innovation of products offered on the market, with special emphasis in this context on electronic devices. Consequently, there is an inherent triad of assumptions aimed at the growth of consumption: purchase - use - rejection of the product. Such a construction, which is very profitable from the producer's point of view, arouses from three instruments: 1) marketing - a means of creating a psychological need for the product on the part of the customer, 2) loan - a means of bridging the impossibility of immediate payment through binding to financial institutions, and 3) planned obsolescence[1] - the phenomenon of corporate strategy, which is the focus of this paper.

The authors point out the difficulty of defining planned obsolescence phenomenon, its types, the consequences for the consumer and the environment, and they also stress the conflicting attitudes referring to the categorical sanctioning of this concept in light of the constant need for innovation. The term is observed from the multidisciplinary perspective of economics, ecology, criminology and finally, law. The authors also analyze class action jurisprudence in the US, and also the jurisprudence inspired by it and developing in the European Union. A comparative legal presentation follows: 1) the pioneering French Consumer Law which for the first time sanctioned planned obsolescence, 2) indirect regulation of this issue in certain EU countries through, above all, the protection of consumer rights, and 3) legislative initiatives related to

[1] Mijatović & Gajinov (2023).

planned obsolescence at the EU level, for now formulated through soft, unsanctioned regulations – the soft law.

2. Planned obsolescence – terminology and phenomenon development

The term "planned obsolescence" was used for the first time in 1932 by an American real estate agent, Bernard London, in his essay named “Ending the Depression Through Planned Obsolescence.” In fact, London proposed that the authorities use the planned obsolescence approach regarding products for personal use that would be considered "legally dead" after a certain period of time, *i.e.* obsolete legally, although not factually. Two kinds of results would be achieved that way. Firstly, the primary desired result in the form of increased demand for new products would cause the volume of production increase, and consequently it would make the employment rate grow. One more goal that would be achieved as a secondary option would represent a certain "punishment" for consumers. Namely, those who would not be involved in the trend of higher consumption would be additionally taxed for the use of the product after the end of the foreseen period. From this initial, and it should be mentioned, only partially conceptually accepted but unrealized idea, the phenomenon has developed as a corporate ecosystem tool that requires constant growth[2], and as a policy of planning or designing products with a limited life span so that they become obsolete, *i.e.* old-fashioned or dysfunctional after a certain period of time.[3] Historically, planned obsolescence has even been promoted as part of the ‘Throw-Away Society’ campaign, championed most prominently in the United States, but with an impact across

[2] Bisschop *et al.* (2022).
[3] Bulow (1986).

Europe, which has enabled businesses to preserve a high volume of sales.[4]

Planned obsolescence symbolizes "instilling in the customer the desire to own something a little newer, a little better, a little earlier than necessary" as stated by the American industrial designer Brooks in speech at a marketing conference in Minneapolis in 1954, after which the term became popular.[5] The term planned obsolescence, but also equally indicative terms in use, such as built-in obsolescence, premature obsolescence or dynamic obsolescence[6] are used to name the corporate policy of producing goods with an artificially limited useful life, or deliberately weak design, which involves all practices that shorten the life of a product before it is optimally achieved, and induce its replacement. The lifespan here refers to the ability of a product to function at the anticipated performance level over a given period (*i.e.* the number of cycles; hours in use) under the expected conditions of use and pursuant to foreseeable actions.[7] Nevertheless, this term can be understood as the decline in the value of a product before its natural onset of obsolescence as a result of the technology development, consumer behavior changes, fashion dictates and the like.

As one of the first examples of such a corporate strategy we may mention the case from 1924, when the world's largest manufacturers of light bulbs (Philips, General Electric, Osram and Compagnie des Lampes) reached a treaty on limiting their products lifespan. This way the market standard from 2,500 was shortened to 1,000 burning hours by 1940 - well below the incandescent light bulbs predicted life expectancy that was

[4] Malinauskaite & Erdem (2021) 720.
[5] Brooks according to Adamson (2003) 4-5.
[6] Grattan (2016).
[7] Princen (2010).

several decades.[8] As an indicator of different corporate strategies before applying the planned obsolescence concept, we give an example of the so-called The Centennial Light - hand-crafted light bulbs that were installed in a California fire station in 1901 and still shine today, while the three cameras that observe it around the clock as a kind of attraction have broken down within couple of years. Another example is the strategy employed by DuPont to produce fast-wearing nylon stockings, which were easily torn or stretched, leading to a high number of sales throughout the 1950s and beyond.[9] More up-to-date examples of this practice are related to the Apple company and their product Airpods - wireless headphones that are designed to function for only 18 to 36 months of everyday use before turning into longevous and toxic e-waste.[10] Similarly, slowing down of older iPhone models (6, 6 Plus, 6S and 6S Plus) through a software update (and undisclosed to consumers) is considered a planned obsolescence tactic.

3. Planned obsolescence through the prism of different sciences and planned obsolescence types

The institute of planned obsolescence is not easy to define, but there is a multitude of examples. Therefore, the consequences from the point of view of consumers and harm to the environment are rather clear, and that gives possibility for framing the concept with clear boundaries. Furthermore, there is a multidisciplinary approach to the phenomenon of planned obsolescence - from the economic, ecological, criminological, and legal points of view.

Thus, from the point of view of economics, planned obsolescence is viewed as a business strategy in the context of

[8] Bisschop *et al.* (2022).
[9] Rivera & Lallmahomed (2016) 119.
[10] Taffel (2023) 433.

corporate ethics and circular economy. From the ecological point of view, the effects of this practice on the environment and the ideas of eco-design are being studied.[11] From the criminological aspect, there is constructive observation of planned obsolescence as a subtype of corporate crime. In this sense, it is considered to be a typical white-collar crime - an illegal and harmful practice in elite circles carried out in order to generate the profit for the company within the framework of legitimate professional activities.[12] On the other hand, from the legal aspect, there are important challenges in terms of the analysis of planned obsolescence since there is no parent branch that studies it. It is rather observed through the judicial practice's prism (mainly class actions in the USA and in the EU, recently) and fragmented regulations within consumer rights, competition, corporate responsibility and environmental protection. Consequently, it is not possible to obtain protection before the court by referring exclusively to planned obsolescence as a criminal offense (except in France), but within the framework of the violation of other institutes of consumer rights, and through opposition to unfair business practices, etc. For instance, in the US, there are no specific federal laws against planned obsolescence, but there is a series of cases filed alleging deceptive or unfair business practices violating consumers' rights.

Given that planned obsolescence manifests itself in several ways, it is classified according to different criteria. Thus, for instance, there is legal obsolescence. For example, governments wanting to increase electric vehicle ownership could increase the replacement rate of cars by subsidizing them. Several cities such as London, Berlin, Paris, Antwerp and Brussels have introduced low-emission zones banning older diesel cars. Such practice, founded on a legal basis, directly led to the need to

[11] Rivera & Lallmahomed (2015).
[12] Friedrichs according to Bisschop *et al.* (2022).

purchase new cars. However, the basic manifestations of planned obsolescence are technical and psychological obsolescence. Hence, they will be considered here with a special emphasis on the technical type.

Technical obsolescence exists when manufacturers deliberately design products with a shorter physical lifespan than the industry is capable of producing under existing technological and cost conditions.[13] So, this obsolescence type is related to the objective criterion of material defects that lead to the substitution of the product before the consumers' expectations. The reasons for this can be various - software obsolescence, insufficient possibilities for repairing the product (limited repair), or because the component required for repair is unobtainable, or it is simply not practical or worth repairing the product, or repair can only be done in authorized service center, and so on. Here, product design plays a crucial role in terms of the product's lifespan, which is reinforced by advertising, incompatibility (for instance, in the scenarios where software no longer works once an operating system is updated; this is also known as incompatibility obsolescence) and poor aftersales services.[14]

On the other hand, there is also psychological or perceived obsolescence, *i.e.* "obsolescence of desirability" caused by subjective motives for product replacement, which may refer to the changed perception of product attractiveness from the consumer's point of view. That strategy is particularly characteristic for the fashion industry. It relates to scenarios where manufacturers or sellers induce consumers to replace goods even though they still retain substantial physical usefulness. This is connected to marketing campaigns and is based on the consumer's perception, rather than the product

[13] Aladeojebi (2013).
[14] Malinauskaite & Erdem (2021) 720.

itself. This is mainly because of different 'fashion trends', different colors, changed styles or the addition of an extra function to a model, which makes the appearance of previous models 'old' and undesirable. Still, technological obsolescence can overlap with psychological obsolescence: producers that release technically updated products might persuade consumers who are vulnerable to 'status' to buy the technically newer or better product, whereas the 'old' product still functions properly.[15]

Still, despite increasingly obvious manifestations of the consequences of the planned obsolescence corporate concept and strategy, and the rising scientific interest for that phenomenon, there is no universally accepted definition of it. The reasons for this lie in the previously mentioned heterogeneous manifestations, and also, in the absence of legal regulation of this issue, or only indirect regulation for it. For the purposes of this work paper, the authors analyze planned obsolescence as a determined business strategy of limiting products life that has far-reaching ecological and social consequences, and that may be observed from the perspective of corporate responsibility towards the consumer and the environment.

4. Condemnatory attitudes regarding effects of planned obsolescence

The consequences of the implementation of corporate policy of planned obsolescence may be divided into negative ones, with a dominant 'involvement' in the overall effects, and on the other hand, positive effects that are related to innovations and real upgrading of products through constant improvements. The negative connotation relating to this phenomenon relates to

[15] Malinauskaite & Erdem (2021) 724.

causing material damage to consumers by violating their rights, and to the impact that the insatiable production policy makes on the environment. Actually, the strategy behind planned obsolescence artificially limits products lifespan at the expense of the consumer in order to increase profits, but also to the detriment of environmental sustainability, because the product becomes obsolete prematurely and is rejected.[16] This practice is oftentimes related to electronic devices and contributes to the accumulation of so-called e-waste from thrown refrigerators, washing machines, television sets, computers, mobile phones, *etc*. In accordance with that, the concept of planned obsolescence and e-waste is connected to the phenomenon of the so-called waste or toxic colonialism.[17][18]

In a sense of material damage to the consumer, these intentional producers' actions and the following products' characteristics are reflected in some of the many possible appearance forms. For example, after the expiration of a predetermined time period, the product stops functioning properly, and the possibility of its repair is reduced or discouraged (access to repair services becomes difficult or they are available only in particular services). Sometimes, repair is impossible because the product cannot be dismantled without causing damage on it.

---

[16] Wrbka & DiMateo (2018).

[17] Nigam (2023).

[18] The term waste colonialism was coined by activist in the late 1980s to describe the practice of developed nations dumping toxic wastes in developing and low-income countries, even though these countries had no technological or regulatory means to deal with the waste. Today, the toxic waste trade has been replaced by large volumes of post-consumer plastic, paper and e-waste trade. Countries like Japan, United States of America, and the United Kingdom have become world leaders of plastic waste export. As an example, we emphasise and question India's capacity, as one of the leading countries when it comes to waste import, to safely recycle imported waste, since about 40 per cent of domestic waste goes uncollected due to poorly implemented laws. Of this, 56 per cent of recyclable wastes generated, and only 5 per cent of India's total e-waste gets recycled (Sridhar, Lekha & Kumar, Parul (2019)).

For example, Apple's iPhone 11 batteries are almost impossible to replace without causing significant damage to the product and without the necessary expertise.[19] Furthermore, repairing the product may be unprofitable (replacement parts are disproportionately expensive in comparison to a new product price) or impossible (spare parts are only available for a limited period of time), or the product is sure to become obsolete in such a way that it will be considered "out of date" within the specified period and less desirable from the consumers point of view, as previously mentioned.

As a consequence for the environment, planned obsolescence causes the excessive waste of natural resources in production processes, while e-waste is one of the most rapidly growing categories of waste in terms of size and toxicity. In 2022 alone, around 60 million tons of e-waste was generated worldwide.[20] When carelessly disposed of or dismantled (and there are over 347 million tons of unrecycled e-waste on Earth at the moment), toxic substances (such as cadmium) can contaminate surrounding water, air, and soil. In turn, it causes pollution of ecosystems, crops and drinking water, jeopardizing human health and the environment.[21]

5. Innovation as an obstacle for legislative limitation of planned obsolescence

Besides the obvious negative consequences of the corporate concept of planned obsolescence, the authors draw attention to the fact that this strategy also has consequences that cast another light on this concept. Namely, it is unquestionable that constant, even minor products improvements lead to innovations for consumers benefits. Therefore, its "blank" sanctioning would

[19] Suovanen (2019).
[20] Global Transboundary E-waste Flows Monitor 2022.
[21] Bisschop *et al.* (2022).

also mean slowing down the progress and competition development on the free market. On the other hand, deliberate resort to the fragmentation of innovations, that is their intentional gradual introduction may contribute to the fraudulent aspect of planned obsolescence. Companies may intentionally exclude certain attributes of current product models, reserving them for future ones that will be launched at the planned moment - when parts of the older model begin to break down, and to ensure maximum attraction of consumers.[22] Corporations may take advantage of the rapid technological and scientific developments in product manufacturing to increase their sales and profits by using various strategies, including the planned obsolescence,[23] but also mentioned fragmented innovation.

Anyhow, companies can defend themselves with the argument that it is not illegal to make improvements to a product, and that it is in the consumers' best interest to have continuous access to modernized versions of the product. In this manner the tension occurs between innovation, on the one hand, and product sustainability, on the other, as two ends of the spectrum that manufacturers and legislators are guided by. Also, it is difficult to define the cases in which the plan to change product should be regarded as justified (on the clear standards basis), as well as distinguishing them from unfair business practices. Therefore, the consequences of the planned obsolescence need to be objectively observed from both angles - condemnatory and affirmative, in order to find a way towards acceptable common denominators for the regulatory basis.

[22] Bisschop *et al.* (2022).
[23] Malinauskaite & Erdem (2021) 720.

6. Stand out class actions in the USA regarding planned obsolescence

As famous examples of class actions in the USA related to planned obsolescence, which became the starting point for the fight against this phenomenon on European soil, we accentuate those connected to printer producers. A 2006 lawsuit against Epson resulted in a settlement related to printers that were suspended even when the cartridges were not yet empty, *i.e.* had a significant amount of ink remaining inside.[24] In 2010, as many as three unfair business practice class actions were filed against Hewlett Packard (HP) since a "smart chip" in the printer indicated that the cartridges needed to be replaced long before they were empty. This way, printers became unusable, even for functions that did not require ink.[25] One more class action lawsuit was filed against the same company in 2018, related to false error messages on their printers, and it resulted in a $1.5 million settlement.[26] The historic success of the US jurisdiction in this matter (that was used as a template for initiating court proceedings on the same basis in EU member states) was achieved after the class action against Apple. Namely, Apple has agreed to pay up to $500 million for settlement for the lawsuit in which the company was accused of covertly slowing down older iPhone models, in parallel with the promotion of newer models, with the goal to lead owners to buy substitute phones or batteries.[27] Furthermore, a class-action lawsuit has been filed against Tesla, requesting compensation for the owners of the Model S and Model Ks. In fact, many Tesla car owners have noticed a reduction in the distance they could travel prior to recharging the battery. The lawsuit argued that

[24] Epson Ink Cartridge Class Action Lawsuit Settlement.
[25] Ciolino v. Hewlett-Packard Co; Rich v. Hewlett-Packard Co; Blennis v. Hewlett-Packard.
[26] The HP Ink Cartridge Monopoly Class Action Lawsuit.
[27] Apple Inc Device Performance Litigation.

Tesla intentionally reduced battery capacity using a software update, and the company agreed to pay each owner $625 as a settlement.

7. Legal (non)regulation of planned obsolescence and related court practice in the EU

The prevailing practice relating to the problem of planned obsolescence is still not legally defined but is approached through various regulatory initiatives with the intention of improving the position of consumers,[28] and within the scope of expanding the range of what is meant by the so-called right to repair. Considering the fact that the right to repair is enforceable up to the expiry of the warranty is of relevance in cases of planned obsolescence, as one can claim that businesses manipulate their products' lifespan to coincide with the end of the warranty period, by designing their goods in such a way that they malfunction shortly after the warranty period lapses.[29] That is why there is a need to broaden the scope of what is considered as the right to repair.

European countries, using various legislative approaches, encourage the fight against the concept of planned obsolescence, often and indirectly within the framework of environmental protection programs. For example, Sweden makes it easier to repair and recycle products by reducing the VAT rate, and with more aggressive taxes for products that are difficult for recycling. Italy administratively sanctions business practices that are unfair, while the Netherlands, Austria and Finland have taken measures to improve consumer rights related to warranty.[30] In 2022, Austria started a project of granting vouchers to its citizens for mobile phones repairing in

[28] Malinauskaite & Erdem (2021).
[29] Wrbka & DiMatteo (2019).
[30] Wrbka & DiMatteo (2018).

order to reduce e-waste, and within a year more than 560,000 vouchers were issued.

The EU has also put efforts in managing the problem of planned obsolescence - although initially implicitly by regulating policy regarding waste, natural resource use, consumer information and the circular economy.[31] Furthermore, a circular economy is the EU's main strategy for replacing linear 'take– make–use–waste' models with more circular ones, where resources are used and kept for longer to reduce and avoid waste as much as possible. Planned obsolescence directly contradicts the concept of a circular economy due to its promotion of a culture of wastefulness by perpetuating a 'buy new and buy often' mentality.[32] Presently, in the EU, this and related matters are regulated directly and indirectly through soft law - non-sanctioned sources of law whose application is only recommended but not binding (recommendations, opinions, resolutions, declarations, action plans, white papers, green papers, guides, guidelines, *etc.*). In that sense, these resolutions or action plans are just the first step towards classic, sanctioned hard law regulation (*e.g.* EU directives).[33] Back in 2013, the European Economic and Social Committee raised the issue of a complete ban on planned obsolescence, and in 2015 adopted the Action Plan for the Circular Economy and also, among other things, with the aim of making consumer goods more durable and easier to repair.[34] Thus, measures covering the whole cycle were embraced, from production and consumption to waste management and the market for secondary raw materials, thus contributing to 'closing the loop' of product life cycles through greater recycling and reuse, and bringing benefits for both the

[31] La Rosa (2020).
[32] Malinauskaite & Erdem (2021) 719-720.
[33] Mijatović (2018).
[34] Malinauskaite & Erdem (2021).

environment and the economy.[35] In 2017, the European Parliament made the Resolution which encouraged the Commission to focus on solving the planned obsolescence problem through harmonization, and in the Action Plan for the Circular Economy from 2020 the Commission expresses its indignation to this practice. In resolutions from 2020 and 2021, the European Parliament required the Commission to consider specific measures for protecting consumers from planned obsolescence. Finally, in 2022, it presented a proposal for the adopting regulations that would establish rules for all products in the internal market, with the aim to make them more durable, reusable, repairable, suitable for recycling, and generally less harmful to the environment. This would also make changes in the existing regulations on eco-design by involving rules on the passport of digital products and banning the destruction of unsold goods.[36]

It can be concluded that the concept of planned obsolescence is being given increasing, yet insufficient regulatory attention at the EU level. Theoretical positions on the matter, which we consider to be justified, distinguish that the current EU measures are not sufficient to deal with the planned obsolescence issues, and that there is therefore an urgent need to have strict measures at the EU level banning planned obsolescence. The EU action is justified as it relates directly to the internal market, especially as it is supported by the circular economy concept. Furthermore, the EU-driven strategy towards a circular economy is superfluous where the durability of products is curtailed by unregulated planned obsolescence.[37] It is also strongly suggested that a three-tier approach to legislation with options inspired by the waste hierarchy could be introduced, where the most preferred option would be

[35] Malinauskaite & Erdem (2021) 719.
[36] European Parliament, Briefing EU, 2022.
[37] Malinauskaite & Erdem (2021) 721.

prevention (due to durable products), followed by boosting reparability and upgradability, with a further suggestion to promote trade-in options in order to influence recycling.[38]

8. The French example and influence

As a pioneering venture in terms of regulating planned obsolescence we may highlight the provisions of the French Consumers Law from 2015 (*Code de la Consommation*).[39] This regulation made France the first country in the world to provide the legal definition of planned obsolescence (and to amend it in 2022), banning and sanctioning such a practice. Planned obsolescence is defined by this regulation as "a group of techniques through which a manufacturer or a marketer seeks to deliberately reduce the lifecycle of a product in order to increase its replacement rate".[40]

Aforementioned techniques may involve the intentional introduction of an error or weakness into the product, a technical limitation, incompatibility, and other obstacles to repairing the product. Such regulation is combined with the guarantee of the consumer's right to know how long the spare parts of the product will be available, and with the obligation to deliver them within two months from the date of the request. Also, since 2016, device manufacturers are obliged to repair or replace a faulty product within two years of purchase and free of charge. That, in fact introduced a mandatory two-year warranty and elaborated the so-called right to repair. If the responsible persons are found guilty of performing this practice, they face fines of up to €300,000 (or up to 5% of the average annual turnover for the last 3 years), with the possibility of two

[38] Malinauskaite & Erdem (2021) 749.
[39] Code de la Consommation, 2015.
[40] L. 441-2 Code de la Consommation.

year imprisonment.[41] Certainly, it remains disputable whether the planned obsolescence in the sense of this regulation also implies manufacturers' omissions, and how to prove in court that reduction of the product's lifespan with the aim of increasing the replacement rate was intentional. In France, the legislative regulation of this and related issues continued through the circular economy regulation and the imposition of the obligation to make public the so-called repairability index of electrical and electronic products. Also, it is prohibited to prevent the product from being repaired by any technique, including software. Finally, it is planned to make a commitment for manufacturers to inform consumers about how long software updates, provided at the time of purchase, will remain compatible with regular use of the device.

In France, additionally to the revolutionary legislative initiative, the activity of the consumer rights group called Stop Planned Obsolescence (*Halte a l'Obsolescence Programée* - HOP) has great significance for setting the practice and standards regarding this matter. Namely, in 2017, HOP filed a lawsuit against Apple since the company failed to inform consumers that an operating software update for the iPhone 6, 6S, SE and 7 could slow down these older models, and that was highlighted as a criminal offense of deception in the economy by inaction and the case of planned obsolescence which is subject to sanctions. In 2020, the French Consumer Protection Agency fined Apple €25 million, and HOP described this outcome as a "historic first victory" against the outrageous practices of creating "ready to toss" products. However, there is dissatisfaction because the charge of planned obsolescence has been dismissed, and there will be no public trial that would shed additional light on a topic about which there is not enough awareness. HOP also filed criminal charges in 2017 against

[41] L454-6 Code de la Consommation.

several computer printer manufacturers (Epson, HP and Canon) for selling products allegedly designed with planned obsolescence (*e.g.* the printer shows "empty" cartridges, however, they sometimes still contain 20-40% ink; consumer may be forced to change all cartridges in order to continue to use other functions of the printer, *e.g.* scanner; printer locks up with ink pad end of life *etc.*). The process has not been concluded even six years later, and in 2020 the HOP supported the complaints of the *UFC-Que Choisir* consumer association against Nintendo for planning the obsolescence of console controllers.[42] Also, spurred on by such initiatives, the European Commission, the Cooperation Network for Consumer Protection and the European Consumer Organisation reacted in a coordinated manner towards this company and regarding numerous complaints about the operation of the joystick. Therefore, in 2023, Nintendo agreed to repair Nintendo Switch joysticks for free, and even beyond the legal warranty period, after numerous complaints from consumers and warnings from the afore-mentioned organizations. Also, at the end of 2022, the HOP association filed a complaint against Apple for planned obsolescence and obstacles to repair, and the investigation by the Public Prosecutor is now under way. HOP calls on the smartphone maker to guarantee the right to repair of its devices, and to stay away from the practice known as voluntary irreparability. In particular, HOP alerts the courts to the damage of an increasingly widespread practice: serialization or "pairing". This consists of associating the serial numbers of spare parts with that of a smartphone, in particular via microchips, giving the manufacturer the possibility of restricting repairs for non-approved repairers. The association considers that Apple could organize many brakes on repairs, contrary to what its communication suggests, in particular on the "Self Service Repair" program which turns out to be

[42] Halte a l'Obsolescence Programmée.

"expensive and absurd" (for example, a consumer needs to order two 35 kg tool cases to repair a battery).[43]

In Italy, too, the giants Samsung and Apple were fined €5 million each by the antitrust body in 2018 (in connection with the afore-mentioned slowing down of device update software), with the obligation to display a notice of this decision on their Italian websites. Apple was also fined an additional €5 million because it did not provide customers with clear information about the essential characteristics of lithium batteries. Furthermore, this initiative was also followed by the Euroconsumers association, based on US judicial practice and the whistleblower activities of the Repair Association, using as an argument the compensation that American consumers obtained from Apple.[44] Namely, a wave of lawsuits was launched against this company due to the planned obsolescence, starting from Belgium and Spain in 2020,[45] through Italy and Portugal in 2021. It is estimated that if these disputes are lost, the damage to Apple could reach 180 million euros. However, the most serious consequences for this company can result from

[43] Halte a l'Obsolescence Programmée.

[44] Millions of people were affected when the models of iPhone 6 and 7 and SE were slowed down in 2016 in a case dubbed Batterygate. At the time, Apple declined to comment, however, it had previously said the phones were slowed to preserve ageing battery life. Thirty-three US states claimed that Apple had done this to drive users into buying new devices. A case was settled in 2020, when Apple agreed to pay $113m to settle allegations that it slowed down older iPhones.

[45] Euroconsumers' Spanish member OCU started its fight against Apple for deceptive business practices in court on behalf of 400,000 consumers with claim that under Spanish law, the way this 'planned obsolescence' happened amounted to unfair, deceptive and aggressive commercial practice in direct violation of the country's Unfair Competition Law and General Law for the Defence of Consumers and Users. Furthermore, it is claimed, Apple has profited from deliberately encouraging people to renew their iPhones earlier than they needed to - leaving Spanish consumers with an economic loss of between 40 and 80 million euros (Euroconsumers).

the procedure initiated in the United Kingdom by the British Consumers Association in connection with the so-called *Batterygate*. Namely, British consumer association accused Apple of having "hid faulty batteries in millions of iPhones by throttling them with software updates". The claim, which has been filed with the Competition Appeal Tribunal, alleges Apple slowed down the performance of older iPhones, in order to avoid expensive recalls or repairs. If the accusation is proven correct for up to 25 million affected UK iPhone users, then Apple would have to pay a $2 billion fine.

9. Conclusion

Planned obsolescence is a strategy of manufacturers, which, in order to increase the replacement rate, limits the life of the product in various ways. This strategy has far-reaching environmental and social consequences, which can be viewed from the perspective of corporate responsibility to the consumer and the environment. However, due to the lack of a unique position on what the concept of planned obsolescence exactly involves as a practice, and due to the aim of product innovation in the interest of consumers, that manufacturers can refer to, the normative regulation of this issue is proving to be a great challenge. Therefore, in general, this phenomenon is not specifically regulated, rather it is regulated indirectly and sporadically through institutes of various branches of law, primarily through consumer law. Class actions in the USA have great significance for shaping standards and creating awareness of the harmfulness of this practice, and also provide an inspiration for actions on the European Union soil, which are initiated against large corporations.

The most decisive legislative step forward in this matter, *i.e.,* the pioneering regulatory determination and sanctioning of planned obsolescence, both with a fine and a prison sentence of

up to two years, was carried out by France in the 2015 Consumer Law. Also of particular importance are the initiatives and lawsuits of consumer protection organizations that act in anticipation of the European Union taking more concrete steps in relation to the current practice of regulating this issue, through non-binding, just "recommending" soft law sources - action plans, resolutions and the like. The prospect of sanctioning this practice through binding source of law, which will make it more feasible to discipline corporate "players" based on clear criteria and can serve as a model - regulation for numerous legal systems, certainly seems significant.

Literature

Adamson G, *Industrial strength design: how Brooks Stevens shaped your world* (MIT Press 2003).

Aladeojebi, T. 'Planned Obsolescence' (2013) 4 International Journal of Scientific and Engineering Research 1504.

Apple Inc Device Performance Litigation, US District Court, Northern District of California, No 18-md-02827.

Apple Inc Device Performance Litigation, US District Court No 18-md-02827.

Bisschop, L., Hendlin, Y., Jaspers, J. 'Designed to break: planned obsolescence as corporate environmental crime' (2022) 78 Crime, Law and Social Change 271.

Blennis v. Hewlett-Packard Co., Case No. 5:07-cv-00333-JF.

Bulow, J. 'An Economic Theory of Planned Obsolescence' (1986) Quarterly Journal of Economics 729.

Ciolino v. Hewlett-Packard Co., Case No. 5:05-cv-03580-JF.

Code de la Consommation. https://www.legifrance.gouv.fr/codes/texte_lc/LEGITEXT000006069565/2023-03-18 accessed 27 May 2023

Epson Ink Cartridge Class Action Lawsuit Settlement (*EpsonSettlement.com,* 2006) <https://www.epsonsettlement.com/ >accessed 27 April 2023

Apple Class Action Lawsuits (*Euroconsumers*, 2020) <https://www.euroconsumers.org/activities/apple-class-action-lawsuits> accessed 20 May 2023.
European Parliament, Briefing EU - Legislation in Progress. https://www.europarl.europa.eu/RegData/etudes/BRIE/2022/733524/EPRS_BRI(2022)733524_EN.pdf accessed 15 May 2023
Grattan, L, 'Populism's Power: Radical Grassroots Democracy in America' (Oxford University Press 2016).
Baldé C.P, D'Angelo E, Luda V, Deubzer O, and Kuehr R, 'Global Transboundary E-waste Flows Monitor 2022' (*UNITAR,* 2020) <https://ewastemonitor.info/wp-content/uploads/2022/06/Global-TBM_webversion_june_2_pages.pdf >accessed 23 May 2023
Halte a l'Obsolescence Programmee. <https://www.halteobsolescence.org/apple-condamne-suite-a-la-plainte-deposee-par-hop/ >accessed 20 May 2023
La Rosa E, 'Planned obsolescence and criminal law: A problematic relationship' (2020) Sustainability and Law 221.
London B, 'Ending the depression through planned obsolescence' (1932)
https://web.archive.org/web/20120819154515/http://upload.wikimedia.org/wikipedia/commons/2/27/London_%281932%29_Ending_the_depression_through_planned_obsolescence.pdf >accessed 22 May 2023
Malinauskaite J, and Erdem F B, 'Planned obsolescence in the context of a holistic legal sphere and the circular economy' (2021) 41 Oxford Journal of Legal Studies 719.
Mijatović, M. 'Agencije za formulisanje – metodi rada i saradnja savremenih subjekata harmonizacije međunarodnog trgovinskog prava' (2018) 2 Strani pravni život 169.
Mijatovićand Gajinov, 'Planirana dotrajalost kao korporativna strategija proizvođača: pojmovno određenje, posledice primene i pravna regulacija' (2023) 30 Ecologica 173.
Nigam A, 'Climate Crisis, Productivism and Waste' (2023, <https://link.springer.com/chapter/10.1007/978-3-031-22895-7_4> accessed 28 April 2023.
Princen T, 'Treading Softly: Paths to Ecological Order' (MIT Press 2010).
Rich v. Hewlett-Packard Co., Case No. 5:06-cv-03361-JF.

Rivera J, and Lallmahomed A, 'Environmental implications of planned obsolescence and product lifetime: a literature review' (2016) 9 International Journal of Sustainable Engineering 119.
Sridhar L,and Kumar P, 'The New Face of Waste Colonialism: A Review of Legal Regulations Governing the Import of Waste into India' (2019) 15 Socio-Legal Review 101. <https://repository.nls.ac.in/slr/vol15/iss2/1> accessed 21 May 2023.
Suovanen J, 'IPhone 11 Battery Replacement' (IFixit, 2019) <https://www.ifxit.com/Guide/iPhone+11+Battery+Replacement/127450> accessed 21 May 2023.
Taffel S, 'AirPods and the earth: Digital technologies, planned obsolescence and the Capitalocene' (2023) 6 Environment and Planning E: Nature and Space 433<https://doi.org/10.1177/25148486221076136> accessed 19 May 2023.
The HP Ink Cartridge Monopoly Class Action Lawsuit, Case No. 5:16-cv-05820-EJD.
Wrbka S,and DiMatteo L A, 'Comparative warranty law: Case of planned obsolescence' (2018) 21 *University of Pennsylvania Journal of Business Law* 907.

Bengi Sargin*

Determination of *"lex loci protectionis"* in the digital environment

Abstract: With globalization and the spread of liberalism in the world, borders between states have become more permeable than before. This situation has led to both the acceleration of international trade and increased competition in international trade. Intellectual property is considered one of the most affected areas. The need to protect intellectual property rights has also come to the fore over time. Although copyright protection has been provided at a minimum level by international agreements and its general framework has been outlined, the provision of protection has been left to the legislation of the nation states due to the principle of territoriality. Despite all these debates, the application of *lex loci protectionis* as the applicable law has been accepted in both international and national legislation. The development of technology has significantly affected the use and infringement of intellectual property rights. Because the Internet intellectual works have spread all over the world very quickly and it has become very easy for people to access them. Thus, the application of the territoriality principle and protection under the *lex loci protectionis* has become more difficult. In this paper, the applicable law to intellectual property rights with foreign element will be examined, and following this, the connecting factors in terms of applicable law will be evaluated. Afterwards, it will be examined how to determine *lex loci protectionis* in intellectual property disputes arising in the Internet environment. Last but not least evaluations and suggestions will be given.

Keywords: *lex loci protectionis*, digital environment, applicable law, intellectual property rights.

* Bengi Sargin is a research assistant at the Department of Private International Law, Faculty of Law, Yozgat Bozok University, Yozgat, Turkey; and PhD candidate at the Institute of Social Sciences, Ankara Yıldırım Beyazıt University, Ankara, Turkey; E-mail: bengi.sargin@gmail.com.

1. Introduction

Intellectual property rights have been an indispensable element of international trade since their emergence. Especially along with liberalism, both the use of intellectual property rights and related infringements have increased significantly. Therefore, the need for protection has emerged.

In 1886, the Berne Convention for the Protection of Literary and Artistic Works was signed and came into force in 5th of December 1887.[1] With the Berne Convention, the first step towards the international protection of intellectual and artistic works was taken. There were several amendments made in Berne Convention.[2] The aim of the Convention is to provide uniform and effective protection of the rights of authors.[3] Protected works are described briefly in article 2 of the Berne Convention.[4] The purpose of such a broad enumeration is to enable the contracting states to establish comprehensive intellectual property legislation in their own countries.[5] Besides, works describe mainly fall in four categories such as: literary works, artistic works, dramatic works and music works.[6] The types of works included in these four main categories are listed

[1] Sheinblatt (1998) 536.
[2] Bozbel (2012) 7; Kılıçoğlu (2013) 33. These amendments can be seen as follows: 1896 in Paris, 1908 in Berlin, 1914 in Stockholm, 1928 in Rome, 1948 in Brussels, 1967 in Stockholm, 1071 and 1979 in Paris. For more information see Goldstein (2001) 21-28.
[3] Sargın (2020) 83.
[4] Article 2 of the Convention *"(1) The expression "literary and artistic works" shall include every production in the literary, scientific and artistic domain, whatever may be the mode or form of its expression, such as books, pamphlets and other writings; lectures, addresses, sermons and other works of the same nature; dramatic or dramaticomusical works; choreographic works and entertainments in dumb show; musical compositions with or …"*
[5] Tekinalp (2012) 271.
[6] Sargın (2020) 84.

as examples.[7] The main protection provided by the Berne Convention is mentioned in Article 5. According to this article, the protection provided by the contract cannot be claimed in the country of origin of the work.[8]

Today, the Convention has a significant function in international copyright law.[9] There are two main reasons for the continuing influence of the Convention. The first of these reasons is the accessibility of the Convention.[10] The desire to have as many states as possible as parties to the Convention and the making of regulations in this direction are the main indicators of accessibility. The other reason is the amendments made to the Convention in accordance with the requirements of the time.[11]

Over time, the World Intellectual Property Organization (WIPO) was established with the unification of the unions (for instance Berne Union) established under the roof of the United Nations.[12] WIPO is based on the Paris Convention for the Protection of Industrial Property of 1883 and the Berne Convention for the Protection of Literary and Artistic Works of 1886.[13]

Article 2 of the WIPO Copyright Treaty states that *"Copyright protection extends to expressions and not to ideas, procedures, methods of operation or mathematical concepts as such."*.

---

[7] Because the phrase "such as" is used in several times in the Convention. Goldstein (2001) 24.
[8] Dardağan (2001) 29.
[9] Abelman and Berkowitz (1977) 626.
[10] Abelman and Berkowitz (1977) 626.
[11] Abelman and Berkowitz (1977) 627.
[12] Sheinblatt (1998) 536; Kılıçoğlu (2012) 33; Goldstein (2001) 32; Okutan (1999), 246; Çalışkan (2008) 43.
[13] Sheinblatt (1998) 536; Kılıçoğlu (2012) 33; Çalışkan (2008) 43.

Article 3 of the WIPO Copyright Treaty regulates the protection issue. It states that *"Contracting Parties shall apply mutatis mutandis the provisions of Articles 2 to 6 of the Berne Convention in respect of the protection provided for in this Treaty."*. Therefore, it would not be wrong to say that the type of protection agreed in the Berne Convention is applied. According to article 14 of the WIPO Copyright Treaty contracting parties undertake to adopt, in accordance with their legal systems, the measures necessary to ensure the application of the Treaty.

Another international agreement for the protection of intellectual property rights is TRIPS. Adopted as an annex to the founding agreement of the World Trade Organization during the Uruguay rounds between 1986 and 1994, TRIPS was signed in 1994. Rather than introducing a new system, the purpose of the Agreement is to expand the scope of the Berne Convention by making additions to the Berne Convention.[14] According to article 2 of the Agreement, contracting states shall follow the rules of the Berne Convention.[15] Same protection approach is also chosen in the Agreement.

Regarding conflict of law rules in this field in the European Union Rome II Regulation is an important source.[16] Article 8 of the Regulation titled "infringement of intellectual property rights" states that *"The law applicable to a non-contractual obligation arising from an infringement of an intellectual property right shall be the law of the country for which protection is claimed."*.

[14] Dardağan (2001) 43; Okutan (1999) 247.
[15] *"In respect of Parts II, III and IV of this Agreement, Members shall comply with Articles 1 through 12, and Article 19, of the Paris Convention (1967)."*.
[16] Intergovernmental Copyright Committee (2005) 3.

Considering all the above-mentioned international agreements, minimum protection has been tried to be provided by *lex loci protectionis*, but the actual protection has been left to the legislation of the nation states themselves. When the legislation of nation states is examined, it is seen that, in line with international agreements, applicable law is determined based on the *lex loci protectionis* principle.

In the following, I explain briefly the applicable law and suggested connecting factors to intellectual property rights with foreign element, and following this, examine the determination of *lex loci protectionis* in the digital environment[17].

2. Applicable law to intellectual property rights with foreign element

The need for the protection of intellectual property both by national legal orders and international law is unquestionably accepted in doctrine and practice.[18] Although copyright protection has been provided at a minimum level by international agreements and its general framework has been outlined, the provision of protection has been left to the legislation of the nation states because of the principle of territoriality and lack of comprehensive international agreements.[19] The most important feature of intellectual property rights is that they are territorial.[20] The principle of territoriality refers to the natural link between these rights and the country in which they are located.[21] On the basis of the principle of territoriality, within the framework of the

[17] In order not to broaden the scope of this study, international jurisdiction, recognition and enforcement issues are left out of examination.
[18] Doğan (2019) 391.
[19] Çelikel and Erdem (2017) 359; Erdem (2005) 175; Doğan (2019) 395.
[20] Çelikel and Erdem (2017) 359; Nomer (2017) 312; Tekinalp (2012) 265.
[21] Çelikel and Erdem (2017) 359; Erdem (2005) 173.

independence of laws, intellectual property rights are not considered to exist outside the country of origin, but are interpreted as part of the law within the country, which is in line with the purpose of copyright.[22]

Since the rights in the work subject to intellectual property protection are neither fully property rights nor fully personal rights, there are some difficulties in terms of the application of classical attachment points.[23] Besides, the adoption of either the principle of territoriality or universality plays an important role in determining the law applicable to intellectual property rights. For this reason, it is useful to examine the proposed anchor points in determining the law applicable to copyright.[24]

In private international law, the suggested connecting factors for the protection of intellectual property rights are the law of the country of origin (*lex loci originis*), national law (*lex fori*), the law of the place where the intellectual property right is infringed (*lex loci delicti*), and the law of the state of protection (*lex loci protectionis*).[25] In addition, there are also opinions advocating the application of the law of the country of origin by adopting the criterion of the law of the state of protection, but only in cases where it is deemed necessary to ensure the private international law justice and according to the characteristics of the concrete case.[26]

[22] Dardağan (2001) 145-146.
[23] Doğan (2019) 392.
[24] Sargın (2020) 109.
[25] Çelikel and Erdem (2017) 361; Doğan (2019) 392.
[26] Tekinalp and Uyanık (2016) 265.

a. Lex loci originis

The law of the country of origin (*lex loci originis*) in copyright is the law of the place where the work was first published.[27] It is accepted that intellectual rights, which have the ability to circulate freely between countries due to their nature, have a connection with a certain country.[28] According to the criterion of the law of the country of origin, which provides a close/intensive connection with the country, it is important to determine the place of origin.[29] This is because the country of origin fixes the state to which the intellectual right and the work or the author are bound.[30]

International treaties take into account the nationality of the author or the country where the work was first published or first made available to the public in determining the place of origin.[31] Where these two elements are the same, there is no problem regarding the applicable law.[32] The nationality of the author is considered as personal statute for the author, and the place of publication is considered as a personal statute for the work.[33]

There are mainly two criteria determining the place of origin:

One is the nationality of the author: According to this criterion, the country of nationality of the author is the country of origin of the work and should enjoy the protection of that country.[34] The main justification for the view that the nationality of the

[27] Erdem (2005) 176; Okutan (1999) 214.
[28] Dardağan (2001) 110.
[29] Doğan (2019) 392; Dardağan (2001) 110.
[30] Öztürk (2019) 111.
[31] Doğan (2019) 392-393; Dardağan (2001) 110; Öztürk (2019) 111; Henn (1953) 44; Intergovernmental Copyright Committee (2005) 2.
[32] Sargın (2020) 110.
[33] Dardağan (2001) 110; Henn (1953) 44.
[34] Sargın (2020) 111.

author should be taken into account, is that the work is a reflection of the author's personality and has no independent existence.[35]

The other is the place of publication of the work: The criterion of place of publication essentially separates the work from the personality of the author and is based on the subject matter of the right itself.[36] According to this criterion, the intellectual right should benefit from the protection of the law of the place where it is embodied and made available to the public.[37]

Article 3 of the Berne Convention defines the country of origin as the country of nationality of the author for works first published in a Contracting State, and the country of nationality of the author for unpublished works or works first published in a non-Contracting State.

Subordination to the law of the country of origin ensures that intellectual property rights acquired under the law of that country are internationally recognized and that disputes concerning such rights are resolved in accordance with the law of that country, whichever country they arise.[38] Therefore, the law of origin criterion bears the impression of the universalist theory and constitutes the opposite of the principle of territoriality.[39] The law of origin criterion has not been accepted because it is incompatible with the territoriality of intellectual property rights and the state does not want to give up its sovereignty over intellectual property rights.[40]

[35] Doğan (2019) 393; Dardağan (2001) 111; Okutan (1999) 216.
[36] Doğan (2019) 393; Dardağan (2001) 111.
[37] Sargın (2020) 111.
[38] Dardağan (2001) 128.
[39] Sargın (2020) 111-112.
[40] Erdem (2005) 176.

b. Lex fori

The main justification for the view that intellectual property rights should benefit from the protection of the *lex fori*, is that the judge hearing the case knows and applies his/her own law better than foreign laws, and that intellectual property cases are subject to both civil and criminal proceedings due to their nature.[41] In the vast majority of copyright infringements, a lawsuit is filed and protection is sought in the place where the infringement occurs.[42] In other words, in many disputes, *lex loci delicti comissi* and *lex fori* are intertwined.[43]

One of the main criticisms of this connecting factor are the problem encountered in cases that are not related to the *lex fori.*[44] Namely, if the *lex fori* prevails, the frequent recourse to the law of a country that has no relation with the intellectual property right in dispute, but has ruled on the existence of infringement in accordance with its own laws, may bring up problems such as forum shopping.[45] In the event that the law of the court hearing the case and the law of the country where the infringement occurred are different, it is possible that the principle of legal security may be damaged if the dispute is resolved by using the *lex fori* binding rule.[46]

c. Lex loci delicti

According to this connecting factor, the law of the country in which the intellectual property right is infringed should be

[41] Doğan (2019) 394; Dardağan (2001) 132; Intergovernmental Copyright Committee (2005) 3.
[42] Doğan (2019) 394.
[43] Dardağan (2001) 132.
[44] Erdem (2005) 176.
[45] Doğan (2019) 394; Dardağan (2001) 133.
[46] Dardağan (2001) 132-133.

applied.[47] The infringement of an intellectual property right may occur by wrongful act or wrongful exploitation.[48] In the event that this connecting factor is taken as a basis, the judge must first determine in which country the infringement has occurred.[49]

Lex loci delicti comissi is considered to be a connecting factor suitable for the cases of infringement of intellectual property rights, while *lex loci protectionis* is considered to be a connecting factor suitable for the problems regarding the essence of intellectual property rights.[50]

Among the criticisms of this connecting factor are the evaluation of only the issues after the infringement of the intellectual right, the inadequacy of this criterion in cases of infringements that do not qualify as tortious acts, and its inadequacy in explaining issues such as the birth and content of the intellectual right.[51]

d. Lex loci protectionis

Lex loci protectionis is a connecting factor that is generally accepted in the legal systems of all states, that best responds to the economic and political interests of the states, and that best suits the nature of intellectual property rights and the principle of territoriality.[52] Unlike the law of origin connecting factor, *lex loci protectionis* is based on the application of the law of the state where the protection is sought for the protection of the right.[53] The justifications for the application of *lex loci*

[47] Doğan (2019) 394.
[48] Sargın (2020) 113.
[49] Doğan (2019) 394.
[50] Dardağan Kibar (2016) 446.
[51] Erdem (2005) 176; Doğan (2019) 394-395.
[52] Çelikel and Erdem (2017) 361; Erdem (2005) 177; Okutan (1999) 217.
[53] Doğan (2019) 394; Öztürk (20199 116.

protectionis are that it is in line with the historical reality of intellectual property rights and that it is the manifestation of the territoriality principle in the conflict of laws.[54]

Lex loci protectionis is the law that determines whether there is an intellectual right worthy of protection in foreign intellectual property disputes, and if so, who is the owner of that right, and after determining the owner, whether the alleged infringement has occurred.[55] In other words, intellectual property rights are subject to the law of the country where the question of protection arises.[56] Unlike the law of the country of origin, the protection of intellectual property rights under *lex loci protectionis* exists for each state where protection is sought and in each of these states independently of each other. In this case, the law of the country from which protection is sought will apply.[57]

The territoriality principle is less clear with respect to copyright.[58] This is because, for the recognition of copyright, it is sufficient that the work has been created. As a rule, registration or other formalities are not required.[59] Therefore, a distinction must be made between copyrights and other rights in determining the content of the law of the country of protection.[60] For intellectual rights subject to registration, since the intellectual right is created by an official act, the country that grants the right is the same as the country where protection is

[54] Erdem (2005) 177.
[55] Çelikel and Erdem (2017) 361; Şanlı, Esen and Ataman-Figanmeşe (2018) 241-242; Öztürk (2019) 116-117; Intergovernmental Copyright Committee (2005) 4.
[56] Dardağan (2001) 133.
[57] Dardağan (2001) 131; Öztürk (2019) 116-117.
[58] Sargın (2020) 114.
[59] Dinwoodie (2009) 729.
[60] Dardağan Kibar (2016) 442.

provided on the intellectual right.[61] In other words, for intellectual property rights subject to registration, the *lex loci protectionis* and the place of registration overlap.

In the case of intellectual rights, the determination of ownership differs in terms of the existence, emergence and termination of these rights.[62] Considering the characteristics of the intellectual right, the existence, emergence, elements and termination of intellectual rights are exclusively determined according to the law of the place where the intellectual rights are infringed, or in other words, the law of the country where the protection of the intellectual right is claimed (*lex loci protectionis*).[63] This point of reference is a reflection of the territoriality principle.[64]

Despite all these debates, it would not be so wrong to say, that the application of *lex loci protectionis* as the applicable law to intellectual property disputes with foreign element has been accepted in both international and national legislation.[65]

The *lex loci protectionis* rule is present in international conventions, notably the Berne Convention.[66] Article 5(2) of the Berne Convention is a general rule of conflict of laws that authorizes the law of the State of protection. Pursuant to this article, the exercise and enjoyment of the rights provided for in the Convention shall not be subject to any formalities, shall be independent of the country of origin of the work, and the scope of protection of these rights shall be governed by the law of the country where the protection is sought.

---

[61] Schack (2009) 138-139.
[62] Sargın (2020) 114.
[63] Çelikel and Erdem (2017) 359; Erdem (2005) 173; Nomer (2017) 312.
[64] Sargın (2020) 115.
[65] Dardağan (2001) 134; Okutan (1999) 218; Xalabarder (2002) 80.
[66] Intergovernmental Copyright Committee (2005) 4.

In Article 8 of the Rome II Regulation applicable to non-contractual debt relations, a special binding rule has been adopted on the law applicable to non-contractual debt relations arising from the infringement of intellectual property rights. According to this article, the law of the state from which the protection is sought shall apply to the non-contractual debt relationship arising from the infringement of intellectual property rights. In line with other international and national regulations, the principle of territoriality is also accepted in the Regulation.

3. Determination of *lex loci protectionis* in the digital environment

The development of technology has significantly affected the use and infringement of intellectual property rights.[67] Because, through the Internet, intellectual works have spread all over the world very quickly and it has become very easy for people to access these works.

In legal circles, the Internet is proving to be quite a challenge: its global dimensions, which transcend territorial boundaries, create significant legal problems.[68] Copyright law possesses no exception.[69] Thus, the problem occurs as follows: Which law will apply to online intellectual property disputes with a foreign element and which court will have jurisdiction in this case?[70]

The existence of the right and the act of infringement have gone beyond the borders of the country in violations committed through the Internet. In other words, since markets have turned "global" significantly, while copyright law and private

[67] Kaya Ülken (2023) 113.
[68] Xalabarder (2002) 79; Lundin (2016) 4.
[69] Xalabarder (2002) 79.
[70] To see the explanations related to international jurisdiction please see *supra*.

international law rules are still “territorial”.[71]This situation is referred to as "ubiquitous breach/ mosaic system" in the doctrine.[72]

The mosaic system is the application of the strict territoriality principle, whereby protection is sought from each State in which the right has been violated and the person concerned can bring an action in each State.[73] Adhering to the mosaic system is very burdensome for the beneficiary.[74] However, accepting the other situation – the idea of applying the law of a single state valid all around the world - would lead to extraterritorial application.[75]

Thus, the acceptance of the territoriality principle and protection under the *lex loci protectionis* has become more difficult.[76] Because, as regards to Internet, the strict enforcement of the *lex loci protectionis*, as stated in article 5 of the Berne Convention[77], results in the application of many national laws as there are counties in which the work can be uploaded/distributed *etc*.[78] This difficulty is more serious for intellectual property rights that are not subject to registration.[79] For such rights, a truly global copyright protection would arise for the right holder under the provisions of the law of the country where protection is sought in each country.

---

[71] Xalabarder (2002) 80; Lundin (2016) 5.
[72] Kaya Ülken (2023) 114.
[73] Metzger (2010) 173.
[74] Kaya Ülken (2023) 114.
[75] Metzger (2010) 174.
[76] Geller (1996) 572-573.
[77] It should not be forgotten that this Provision was written at the time that copyrighted work were understood only in tangible medium not by means of intangible medium through the Internet. Xalabarder (2002) 83.
[78] Xalabarder (2002) 83.
[79] Kaya Ülken (2023) 113.

The state in which the person whose rights have been violated will seek to enforce his or her rights and which law will apply to the dispute, is an important question to be resolved.[80] According to Metzger, this problem, *inter alia* worldwide infringement actions, would be effectively solved by identifying the most important market for forcing the infringer to shut down its Internet service, bringing the action there, and applying the law of that market as *lex loci protectionis*[81].

According to Ginsburg, since downloading/uploading takes place easily on the Internet, the plaintiff can choose the law of any state and no conflict of laws rule can provide fully satisfactory protection unless there is a minimum worldwide standard of protection.[82]

There is no specific conflict of laws rule in the Rome II Regulation or in the legal regulations regarding this issue[83]. Besides, this issue is debated in the doctrine.[84] In doctrine, 4 main solution proposals are given:[85]

a. Law of the place of performance

Possible solution is to apply the law of the country where the initial act took place (communication to the public).[86] In the case of the Internet, this would be the country where the server hosting the allegedly infringing content is located.[87] Even

[80] Lundin (2016) 15.
[81] Metzger (2010) 174.
[82] Ginsburg (1995) 323.
[83] Akipek and Dardağan (2001) 135-136.
[84] Kayal Ülken (2923) 114.
[85] Akipek and Dardağan (2001) 135-136.
[86] Xalabander (2002) 85.
[87] This was precisely the approach taken in the EU Directive on satellite broadcasting and cable retransmission to determine the applicable law for the protection of works transmitted by satellite. Xalabander (2002) 85. As for text

though this approach helps to the judge to solve the dispute by reducing the number of applicable laws, it may not be useful because there are too many servers connected to the Internet worldwide.[88]

b. Law of the place of result

The core element of the digital environment, such as Internet, is the recipient on the other side.[89] Since Internet users who make use of uploading in the online world download, it was deemed more appropriate to provide spatial binding with "result place".[90]

When considering the Internet and its nature, the law of the place of result can be anywhere. In other words, determination of the place of result is a bit problematic.[91] Because, in the digital environment, especially on Internet, all these acts, such as viewing, downloading, reproducing, printing the unauthorized uploaded content, are different consequences of the same act of infringement (uploading).[92] For instance, we would like to send an e-mail to someone. The place of the clicking "send" button refers to place of action, whereas possible locations where this e-mail can be read refer to the place of damage.[93] However, since there will be more than one place of result, this acceptance raises the question of the law of which of these will be applied.[94] Therefore, another proposal given below was suggested.

<https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:31993L0083> accessed: 24.07.2023.
[88] Xalabander (2002) 86.
[89] Kaya Ülken (2023) 115.
[90] Akipek and Dardağan (2001) 126.
[91] Kaya Ülken (2923) 116.
[92] Akipek and Dardağan (2001) 126-127.
[93] Özel (2004) 613.
[94] Kaya Ülken (2023) 116.

c. Law of habitual residence/place of business of the author

This solution proposal is a type of *lex loci delicti* because the damage occurs in that country, regardless of where the harmful act took place.[95] From the traditional point of view; applicable law should be *lex loci delicti*.[96] In this case, the act must take place at the place of the installation on the infringer's computer or at the place of the damage.

In determining the applicable law in intellectual property disputes via the Internet, another view advocates the application of the law applicable to intellectual property disputes via satellite broadcasts by analogy.[97] There are two main approaches accepted within this view:

The place of origin theory: According to this theory, for the place of origin should be considered the country where the work was first uploaded to the network/first stored in the computer's memory, that is to say, this will be the country of infringement.[98]

The theory of the place where the broadcast was received (Bogsch theory), according to which the law of all countries from which the broadcast was received can be considered as applicable law.[99]

This approach becomes worthless when the copyrighted work has several authors residing in different countries.[100] On the

[95] Xalabander (2002) 85.
[96] Intergovernmental Copyright Committee (2005) 10; Xalabarder (2003) 84.
[97] Kaplan (2004) 190.
[98] Dardağan (2001) 193.
[99] Özel (2004) 614; Kaya Ülken (2023) 115.
[100] Xalabander (2002) 85.

other hand, this proposal has not found many supporters since it is in close contact with the economic policy of the state where the protection of the intellectual property rights is requested.[101]

d. Law of habitual residence/place of business of the infringer

This approach was also criticized due to the closest relation between economic policy of state and requested protection of the intellectual property rights.[102]

4. Evaluations and conclusion

Intellectual property rights are considered one of the essential elements of international trade. Due to the economic power provided by intellectual property rights, every state has wanted to protect and benefit from these rights within its own structure. Therefore, both competition and disputes have increased over time. Copyright protection is provided at a minimum level by international agreements, and due to the principle of territoriality, protection is left to the legislation of nation states. When the legal legislation of nation states is examined, it is seen that the *lex loci protectionis* is generally adopted.

The development of technology has not only affected the way in which intellectual property rights are used, but has also caused infringements to occur in different dimensions. With the invention of the Internet and its unpredictable spread around the world, copyrighted works have spread very quickly and it has become possible for everyone to access these works.

We have seen that the significant factor in intellectual property infringement via the Internet is the recipient on the other side.

[101] Akipek and Dardağan (2001) 128-129.
[102] Akipek and Dardağan (2001) 130.

A spatial link is provided with the place of result, rather than the place of action. The question of how to determine the place of result will come to the agenda this time. Because the places of result in the Internet environment are all different from each other. The places where all these actions - such as viewing, downloading, reproducing, printing - happened of the unauthorizedly uploaded content are considered as the place of result.

One of the important studies on this subject in the US law is the principles of the American Law Institute. The ALI principles provide a comprehensive set of rules on international jurisdiction, applicable law and recognition of foreign judgments in intellectual property disputes.[103] There is also significant work in this area at the EU Law level. The Max Planck Institute in Munich initiated a project in 2004 to publish draft principles on jurisdiction in intellectual and industrial property rights, and this academic initiative later evolved into a project called "CLIP".[104]

According to ALI and CLIP, the law most closely connected to the dispute (the most closely related law) should be applied, not the *lex loci protectionis*.[105] In making the determination, the judge should take into account the domicile of the injured and

[103] Kaya Ülken (2023) 98.
[104] Kaya Ülken (2023) 98.
[105] CLIP, Article 3:603: Ubiquitous infringement *"In disputes concerned with infringement carried out through ubiquitous media such as the Internet, the court may apply the law of the State having the closest connection with the infringement, if the infringement arguably takes place in every State in which the signals can be received. This rule also applies to existence, duration, limitations and scope to the extent that these questions arise as incidental question in infringement proceedings."*. <https://www.ip.mpg.de/fileadmin/ipmpg/content/clip/the_draft-clip-principles-25-03-20117.pdf> accessed: 21.08.2023. § 321 ALI Principles is used as a blueprint by CLIP. Meztger (2005) 21.

the infringing party, all damages caused by the infringement in the market, and the main markets, if any, in which the parties carry out their professional activities. Unlike CLIP, the ALI provides, that this law also applies to the existence, validity, duration, and nature of the infringed IP right. However, it should not be forgotten that the principle of territoriality, which is at the core of intellectual property rights, will be eliminated by adopting this view.

In my opinion, a regulation should be made in order to uniformize the binding rules indicating the applicable law in this regard. Although it would mean the elimination of the principle of territoriality, the most appropriate solution is to determine the most closely related law as the applicable law.[106] This is because *lex loci protectionis* does not solve the problem, on the contrary, it further complicates it. In other words, applying such a strict territoriality principle to the widespread infringements made possible by the Internet is likely to adjudicate a multi-territorial infringement claim quite complicated itself.[107] Therefore it's important to interpret *lex loci protectionis* with a different meaning.[108]

Literature

Abelman L.E and Berkowitz L.L., 'International Copyright Law' (1977) 22(3) New York School Law Review 619.

Agreement on Trade-Related Aspects of Intellectual Property Rights, December 2005, <https://www.wto.org/english/docs_e/legal_e/trips_e.htm#art1> accessed 13.07.2023.

Akipek, Ş. and Dardağan, E. 'Sanal Ortamda Gerçekleşen Telif Hakkı İhlâllerine Uygulanacak Hukuk' (2001) 50 Ankara Üniversitesi Hukuk Fakültesi Dergisi 115.

[106] Dardağan Kibar (2016) 446.
[107] Ginsburg (1998) 36.
[108] Ginsburg (1998) 36.

Berne Convention for the Protection of Literary and Artistic Works, September 1979, <https://www.wipo.int/wipolex/en/text/283693 > accessed 11.07.2023.
Bozbel, S., *Fikir ve Sanat Eserleri Hukuku* (1st edn, On İki Levha 2012).
Çalışkan, Y., *Uluslararası Fikrî Mülkiyet Hukukunda Uyuşmazlık Çözüm Mekanizmaları: WIPO Tahkimi ve Dünya Ticaret Örgütü* (1st edn, Siyasal 2008).
Çelikel, A. and Erdem B.B., *Milletlerarası Özel Hukuk* (15th edn, Beta 2017).
European Max Planck Group, 'Principles for Conflict of Laws in Intellectual Property' (Draft, 2011)
<https://www.ip.mpg.de/fileadmin/ipmpg/content/clip/the_draft-clip-principles-25-03-20117.pdf> accessed 21.08.2023.
Dardağan Kibar, E., *Fikrî Haklar Alanında Uygulanacak Hukuk Sorunu- Milletlerarası Özel Hukukta Güncel Konular Sempozyumu* (1st edn, Yetkin 2016).
Dardağan, E., *Fikir ve Sanat Eserleri Üzerindeki Haklardan Doğan Kanunlar İhtilâfı* (1st edn, Betik 2001).
Dinwoodie, G. B., 'Developing a Private Intellectual Property Law: The Demise of Territoriality?' (2009) 51 William and Mary Law Review 711.
Doğan, V., *Milletlerarası Özel Hukuk* (5th edn, Savaş 2019).
Erdem, B.B., *Fikrî Hakların Korunmasına Uygulanacak Hukuk- 1. İstanbul Fikrî Mülkiyet Hukuku Sempozyumu* (1st edn, İstanbul Ticaret Üniversitesi 2005).
EU Directive on satellite broadcasting and cable retransmission to determine the applicable law for the protection of works transmitted by satellite, <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:31993L0083> accessed: 24.07.2023.
Geller, P. E., 'Conflict of Laws in Cyberspace: Rethinking International Copyright in a Digitally Networked World' (1996) 20(4) 571.
Ginsburg, J., 'Global Use/Territorial Rights: Private International Law Questions of the Global Information Infastructure Part I' (1995) 42(4) Journal of the Copyright Society of the USA 318.
Ginsburg, J., 'Group of Consultants on the Private International Law Aspects of the Protection of Works and Objects of Related Rights

Transmitted through Global Digital Network' (1998) GCPIC/2 WIPO 3.
Goldstein, P., *International Copyright: Principles, Law nad Practice* (1st edn, Oxford University Press 2001).
Henn, H. G., 'The Quest for International Copyright Protection' (1953) 39 Cornell Law Quarterly 43.
Intergovernmental Copyrigt Committee, 'Law Applicable to Copyright Infringement in the Digital Environment' (April 2005) 1.
Kaplan, Y., *İnternet Ortamında Fikri Hakların Korunmasına Uygulanacak Hukuk* (1st edn, Seçkin 2004).
Kaya Ülken, C., *Milletlerarası Özel Hukukta Televizyon Programları ve Sinema Yapımlarından Doğan Uyuşmazlıklara Uygulanacak Hukuk*, PhD Dissertation, Eskişehir Anadolu Üniversitesi Sosyal Bilimler Enstitüsü (2023).
Kılıçoğlu, A., *Sınaî Haklarla Karşılaştırmalı Fikrî Haklar* (2nd edn, Turhan 2013).
Lundin, E., *The Conflict of Laws and Jurisdiction- An Essay on the Connection between Private International Law and Copyright in Enforcing Online Copyright Infringements* (Lund University 2016).
Metzger, A., 'Applicable Law under the CLIP Principles: A Pragmatic Revaluation of Territoriality' in Jürgen Basedow, Toshiyuki Kono and Axel Metzger (eds). *Intellectual Property in the Global Arena* (Mohr Siebeck 2010).
Metzger, A., *Applicable Law under the CLIP Principles: A Pragmatic Revaluation of Territoriality- Intellectual Property Mohr Siebeck in the Global Arena* (Mohr Siebeck 2010).
Nomer, E., *Devletler Hususî Hukuku* (22th edn, Beta 2017).
Okutan, G., *Türk Milletlerarası Özel Hukukunda Fikir ve Sanat Eserleri, Prof. Dr. Nihal Uluocak'a Armağan* (1st edn, İstanbul Üniversitesi Hukuk Fakültesi Yayınları 1999).
Özel, S., 'İnternet Yoluyla Kişilik Hakkı İhlâllerinde Uygulanacak Hukuk Meselesi' (2004) 24(1-2) İstanbul Üniversitesi Hukuk Fakültesi Mecmuası 609.
Öztürk, A., *Türk Hukukunda ve Karşılaştırmalı Hukukta Telif Haklarına İlişkin Sözleşmelere Uygulanacak Hukuk* (1st edn, On İki Levha 2019).
Şanlı, C., Esen, E. and Ataman-Figanmeşe, İ., *Milletlerarası Özel Hukuk* (4th edn, Vedat 2018).

Sargın, B., *Yabancı Unsurlu Televizyon Program Formatlarının Korunması* (1st edn, Yetkin 2020).
Schack, H., 'The Law Applicable to unregistered IP Rights After Rome II' (2009) 20 Ritsumerikan Law Review 129-144.
Sheinblatt, J., 'The WIPO Copyright Treaty' (1998) 13(1) Berkeley Technology Law Journal 535.
Tekinalp G. and Uyanık, A., *Milletlerarası Özel Hukuk- Bağlama Kuralları* (12nd edn, Vedat 2016).
Tekinalp, Ü., *Fikrî Mülkiyet Hukuku* (5th edn, Vedat 2012).
WIPO Copyright Treaty, December 1996, <https://www.wipo.int/wipolex/en/text/295157> accessed 13.07.2023.
Xahalabarder, R., 'Copyright: Choice of Law and Jurisdiction in the Digital Age' (2002) 8 (1) Annual Survey of International& Comparative Law 79.

Marie Valerie Uppiah*

Assessing the regulation of maritime cybersecurity at the level of the African continent

Abstract: With the digitization of the shipping industry worldwide, many ports and shipping companies are becoming the victims of maritime cyberattacks. The purpose of these attacks is to get access to information which can be intercepted or manipulated in order to smuggle drugs in a country or to obtain ransoms. This paper examines the concept of maritime cybersecurity and analyses the legal actions ought to be taken by the African Union and the Southern African Development Community to address potential cases of maritime cyberattacks.

Keywords: maritime cybersecurity, maritime cyberattacks, African Union, SADC

1. Introduction

Maritime security is a concept which has gained much attention recently. With different threats such as: piracy; illegal, unregulated and unreported (IUU) fishing; drugs and human trafficking at sea and marine pollution, States are adopting security measures to combat these threats. Even though there is no universally accepted definition of maritime security, the concept involves the adoption, by States, of measures which protect them from dangers and threats which affect their maritime territory and industry.[1] An example of such a

* Marie Valerie Uppiah is a senior lecturer at the Department of Law, Faculty of Law & Management, University of Mauritius, Mauritius.

[1] Christian Bueger, 'What is Maritime Security?' (2015) 53 Marine Policy accessed 06 July 2023.

preventive measure is the implementation of maritime cybersecurity mechanisms and regulations.

The maritime industry worldwide is changing at a rapid pace. With the constant conception of new technologies, the maritime industry has to adapt and embark on the digitization of its services. Although Artificial Intelligence and the digitization of the maritime sector have been welcomed by its stakeholders, for the past decades the maritime industry has been the victim of several cyberattacks. Examples of cyberattacks include: hacking a shipping company's wi-fi network to gain access to databases, pirating ships' tracking systems to know their exact geolocations and infecting shipping companies with ransomware viruses.[2]

With the increasing number of maritime cyberattacks, the regulation of maritime cybersecurity becomes crucial. Maritime cybersecurity can be defined as the creation of policies, tools and technologies that aim at countering maritime cyberattacks.[3] The International Maritime Organisation (IMO), through its 2022 Guidelines on Maritime Cyber Risk Management, sets out actions to be taken by its members to combat maritime cyber threats and attacks.[4]

---

[2] P.H. Meland and others, 'A Retrospective Analysis of Maritime Cybersecurity Incidents (2021) 15(3) International Journal of Marine Navigation and Safety of Sea Transportation accessed 06 July 2023.

[3] Mission Secure <https://www.missionsecure.com/maritime-security-perspectives-for-a-comprehensive-approach#:~:text=Maritime%20cybersecurity%20is%20the%20collection,vessels%2C%20and%20their%20cyber%20environment> accessed 08 July 2023.

[4] International Maritime Organisation <https://wwwcdn.imo.org/localresources/en/OurWork/Security/Documents/MSC-FAL.1-Circ.3-Rev.2%20-%20Guidelines%20On%20Maritime%20Cyber%20Risk%20Management%20(Secretariat)%20(1).pdf> accessed 08 July 2023.

At the level of the African continent, many ports and shipping companies are digitalizing their operation processes and services. This is making many African ports and shipping companies vulnerable to maritime cyberattacks. Hence, the development and regulation of maritime cybersecurity become significant for African states.

The purpose of this paper is to examine the regulation of maritime cybersecurity at the level of the African continent. This research examines the legal actions taken by the African Union and the South African Development Community (SADC) in regulating maritime cybersecurity in the region. The methodology used to conduct the research is qualitative. The analysis consists of a review of the existing literature on maritime cybersecurity worldwide and in Africa. Cases are used to illustrate the different forms of maritime cyberattacks. Finally, a black letter analysis of the different legislations on cybersecurity in the African context is done.

This paper is made up of three parts. The first elaborates on the concept of maritime cybersecurity and examines cases of maritime cyberattacks and the response thereon. The second part assesses the regulation of maritime cybersecurity at the level of the African Union and the SADC. And the last part consists of the recommendations and conclusions.

2. Maritime Cybersecurity

The shipping world has changed drastically over the past decades. For years, navigation and other shipping related activities were done manually or through analogue systems, today the shipping industry is becoming increasingly digitized. Modern ships' Information Technology (IT) systems and Operational Technology (OT) systems have improved radically. Ships are no longer relying on analogue displays and buttons,

manual rudders or high number of crew members to operate. Nowadays, as an integral part of their OT system, ships are equipped with: Electronic Charts Displays and Information System (ECDIS), Global Positioning Systems (GPS), radars and satellite systems which keep them constantly connected to the land and with other ships.[5] Through their IT systems, there is high volume of data sharing between ships and ports. Due to this digital evolution in the shipping industry, the regulation of maritime cybersecurity has become significant.

Local, regional and international trade rely heavily on the shipping industry for the carriage of goods and passengers. More than 80% of goods traded worldwide is carried by sea. According to the UNCTAD Review of Maritime Transport 2022, there has been a 3.2% increase in the shipment of goods following the COVID-19.[6] Concerning shipping cruise, this sector is growing at an exponential rate. There has been an estimated 6.6% annual growth in the cruise industry worldwide from 1990 to 2019.[7]

With shipping activities being constantly on the rise and the need to have up-to-date and accurate information, many shipping companies felt the need to move from the manual and analogue ways of operating and opted for the digitalization of their services and processes. This resulted in several advantages for the shipping companies. According to *Tijan et al*, shipping

---

[5] O. Jacq and others, 'Detecting and Hunting Cyberthreats in a Maritime Environment: Specification and Experimentation of a Maritime Cybersecurity Operations Centre' (2nd Cyber Security In Networking Conference, Paris, October 2018) <10.1109/CSNET.2018.8602669> accessed 10 July 2023.

[6] UNCTAD, 'Review of Maritime Transport 2022' (UNCTAD, 2022) <https://unctad.org/rmt2022#:~:text=UNCTAD%20projects%20global%20maritime%20trade,during%20the%20past%20three%20decades> accessed 10 July 2023.

[7] Cruise Watch Market <https://cruisemarketwatch.com/growth/> accessed 10 July 2023.

companies are now adopting Blockchain Technology, Artificial Intelligence, Internet of Things and Big Data to modernize their operations and accelerate information processing and sharing.[8] By digitalizing their services and processes, shipping companies stay competitive and meet the demand of their market in a prompt way. For instance, importers and exporters rely on rapid services for the carriage and delivery of their goods. Hence, shipping companies are expected to meet this requirement without delay. The manual and analogue ways of managing shipping activities were time consuming and sometimes prone to mistakes. By moving towards the digitalization of shipping services and processes, this reduced the amount of time spent on administrative procedures and allowed the storage and retrieval of large amount of information rapidly. Digitalization of shipping administrative procedures allowed for transparency and consistency in the services offered.

In addition to this, the digitalization of the shipping industry ensures cost efficiency and increases the volume of goods being transported. Through electronic documentation and real-time tracking of goods, importers and exporters do not have to use extra financial resources for planning and coordinating shipping operations. This promotes productivity and efficiency in the shipping world.

With regards to operation and maintenance of ships, the digitalization process ensures a degree of safety and security of the ship at sea. For example, as the Operational Technology of ships becomes more digitalized, this has a proactive role in ensuring the safety of the ship. If any component or equipment of the ship needs maintenance or be replaced, the OT system of

[8] Edvard Tijan and others, 'Digital Transformation in the maritime transport sector' (2021) 170 Technological Forecasting & Social Change <https://doi.org/10.1016/j.techfore.2021.120879> accessed 11 July 2023.

the ship shall highlight same so that the necessary action can be taken.[9]

Furthermore, with enhanced IT systems, ships can stay connected with neighboring countries and other ships. Advanced IT systems on board of ships allow for information sharing and offshore-onshore communication on a regular basis. With ships being connected to satellites, their geolocation is permanent. Hence, in cases of distress at sea, national and international agencies can track the vessel and provide assistance when needed.

Despite the advantages that the digitalization process of the shipping industry has, there are various cyber risks associated with it.

According to Park *et al*, a maritime cyber risk can be defined as the extent to which maritime IT and OT systems are threatened by events or circumstances which can cause them to be digitally corrupted, damaged or lost.[10] Thus resulting in shipping activities being disrupted or cancelled. As ships and shipping companies today have wider digital IT and OT systems surfaces, they have to stay connected to different forms of networks, whether secure or unsecure, on a regular basis. This makes them vulnerable to cyberattacks. Examples of such attacks are: insertion of ransomware viruses into the IT system, remote manipulation of ships' positioning information and data

---

[9] Dock Master <https://www.dockmaster.com/blog/key-benefits-of-digitalization-in-the-maritime-industry/#:~:text=Ships%20can%20save%20fuel%20and,fuel%20required%20to%20maintain%20speed> accessed 11 July 2023.

[10] C Park and others, 'Cybersecurity in the maritime industry: a literature review' (International Association of Maritime Universities Conference, November 2019) <http://researchonline.ljmu.ac.uk/id/eprint/11929/1/IAMU%202019%20Park%20et%20al.pdf> accessed 14 July 2023.

theft, among others. These attacks are usually geared towards ships, shipping companies or cargoes.[11]

In their article, Meland *et al* provides for the following examples of cyberattacks against ships, shipping companies and cargoes.[12] In 2019, a ship heading to New York was hacked with a malware through its onboard control system network which affected the ship's functionality. This could have potentially put the life of people on board of the ship at risk. Another example of a maritime cyberattack on board of a ship was in 2018 when, through GPS spoofing, the geolocation system onboard of the ship showed that the ship was on land while it was actually sailing.

Examples of cyberattacks against shipping companies are: the 2017 cyberattack against Maersk's shipping company and 2019-2020 cyberattack against Carnival Corporation & plc cruise operator. In 2017, the NotPetya ransomware was used to infect several software used by Maersk's shipping company. This disrupted Maersk's shipping operations worldwide and resulted in an economic loss of USD 300 million for the company. Carnival Corporation & plc were the victims of a ransomware virus whereby personal information of the company's employees and clients were stolen.

Cargo tracking systems are also hacked in order to smuggle drugs or other illicit products. From 2011-2013, in the Port of Antwerp in Belgium, the cargo tracking system was hacked and this allowed drugs to be smuggled in the country. In 2014 in Australia, the cargo handling system was hacked, and this allowed the hackers to check whether some of the products

[11] K Jones, 'Threats and Impacts in Maritime Cyber Security' (2016) Engineering and Technology Reference <doi:10.1049/etr.2015.0123> accessed 14 July 2023

[12] See *supra*.

getting in the country were categorized as 'suspicious'. Products falling in this category were not collected. These attacks are usually orchestrated by cyber-criminals who can be state or non-state actors. Their main motivation is either money or smuggling illicit products in a country.[13]

The shipping industry is vulnerable to these types of cyberattacks for several reasons. First, there is a lack of trained personnel in the shipping industry as well as on board of ships who have the relevant technical skill and knowledge to deal with cyberattacks.[14] Errors such as opening infected emails or pdfs, as well as clicking on fake websites can cause malware infection of a maritime network system.[15] The second vulnerability is the use of outdated IT and OT systems. Many vessels operate with software that have not been updated or which are not appropriate to combat the different types of cyber threats that exist.[16] Hence, this makes them vulnerable to cyberattacks. Based on all these challenges and cyber risks that ships and shipping companies face, the regulation of maritime cybersecurity becomes significant.

Van Schaik *et al* define cybersecurity as the protection of individuals, organizations and assets that function within a cyberspace and the protection of the cyberspace itself from cyberattacks.[17] Using this definition in the context of maritime

---

[13] European Union Agency For Cybersecurity, 'ENISA Threat Landscape Report 2018' (ETL, 2018) <https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2018> accessed 14 July 2023.

[14] Afenyo Mawuli and Ceasar D. Livingstone, 'Maritime cybersecurity threats: Gaps and directions for future research' (2023) 236 Ocean and Coastal Management <https://doi.org/10.1016/j.ocecoaman.2023.106493> accessed 15 July 2023.

[15] See *supra.*

[16] See *supra.*

[17] Paul Van Schaik and others, 'Risk perceptions of cyber-security and precautionary behaviour' (2017) 75 *Computers in Human Behavior*, 547-559.

cybersecurity, it refers to the protection of, *inter alia*, shipping stakeholders, ships and their digital infrastructures as well as cargoes from being cyberattacked. Maritime cybersecurity measures are being developed in order to address the vulnerabilities that the shipping industry faces. Appropriate software updates, system maintenance and proactive measures are implemented to secure the maritime network. For example, after the COSCO terminal in the Port of Long Beach, US, was infected with a ransomware in 2018, the response of COSCO was to create different network servers for its company. If one server is infected, operations could be shifted to other functioning servers.[18] Additionally, staff working on board of ships as well as in the overall shipping industry are being trained to face cases of cyberattacks and how to avoid them.

The shipping industry worldwide is vulnerable to cyberattacks. Governments as well as the stakeholders of the shipping industry have to be proactive in combatting cyberattacks in the maritime domain. From a regulatory perspective, at the international level, the IMO has enacted the 2022 Guidelines on Maritime Cyber Risk Management. The Guidelines provides for the measures to be implemented to avoid and manage cyber risk.

As part of its maritime cybersecurity regulatory framework, the IMO, in Section 3.5 of the 2022 Guidelines, provides for a maritime cyber risk management strategy. The strategy involves the following five steps: (1) The identification of any vulnerable system that can be prone to a cyberattack, (2) Implementing measures to protect the vulnerable systems from being threatened or attacked, (3) Detecting cyberattacks in a timely manner, (4) Being proactive and resilient in responding to attacks, and (5) Restore the affected system in a timely

[18] See *supra.*

manner in order to ensure a smooth shipping operation. Even though the Guidelines provides for these proactive measures to be taken, maritime cyber risks and attacks are still on the rise and affecting the shipping industry worldwide.

At the level of the African continent, the shipping sector plays an active role in facilitating trade across the continent and across the global. With high volume of products being transported and high amount of information being shared by ships, the African shipping industry is also under the threat of cyberattacks. Hence, the regulation of maritime cybersecurity is important for African states.

3. Regulation of Maritime Cybersecurity at the African Level

The African continent consists of 55 countries among which 36 are coastal and island states. For centuries, the sea has significantly contributed to the socio-economic and cultural development of the continent. Many coastal communities across Africa have relied, and today still depend, on fishing and other maritime related employment activities for their livelihood.

Recognizing the importance of the sea for African States, and in order to promote and regulate maritime trade at an intra-African level, the African Union in 2019 enacted the Africa Blue Economy Strategy. The strategy sets out the guidelines and actions to be taken by African States to boost the development of the blue economy at a national level.[19] Blue Economy can be defined as the sustainable use of marine

[19] African Union – Inter-African Bureau for Animal Resources, 'Africa Blue Economy Strategy' (2019) <https://www.au-ibar.org/sites/default/files/2020-10/sd_20200313_africa_blue_economy_strategy_en.pdf> accessed 01 August 2023.

resources for the economic growth and development of a country while ensuring the protection of the marine ecosystem health.[20]

The Africa Blue Economy Strategy identifies five sectors which African States can focus on to boost the development of their blue economy. These sectors are:

i. Fisheries, aquaculture and ecosystem conservation
ii. Shipping, transportation and trade
iii. Sustainable energy, extractive minerals, gas, innovative industries
iv. Environmental Sustainability, climate change and coastal infrastructure
v. Governance, Institutions and social actions.

The shipping and maritime transportation industry in Africa is one of the least dynamic and economically viable industry of the continent. In their 2021 Review of Maritime Transport, the UNCTAD examined the performance of shipping activities and maritime trade in Africa. It was highlighted that Africa's global containerized trade flow was relatively low compared to other regions of the world. For instance, Africa had 3.9% of global container port traffic, compared to 14.9% for Europe and 65% for Asia.[21] Furthermore, concerning shipping infrastructure and shipping lines, Africa has among the oldest bulkers, ports, container ship and oil tanker fleet in the world.[22] Hence, this

---

[20] World Bank <https://www.worldbank.org/en/news/infographic/2017/06/06/blue-economy> accessed 01 August 2023.

[21] UNCTAD <https://unctad.org/news/afcfta-could-boost-maritime-trade-africa> accessed 01 August 2023.

[22] UNCTAD, UNCTAD's Review of Maritime Transport 2022: Facts and Figures on Africa (2022) <https://unctad.org/press-material/unctads-review-maritime-transport-2022-facts-and-figures-africa#:~:text=Africa%20is%20the%20region%20with,mostly%20on%20foreign%2Downed%20vessels> accessed 01 August 2023.

leads to a lack of competitiveness for Africa's shipping industry worldwide.

Based on these shortcomings, many African States have taken the steps to modernize and digitize their maritime and shipping activities in order to become competitive. For instance, in Ghana, the Terminal Operating System (TOS) was introduced in 2015 at the Tema Port. The purpose of the TOS is to replace face-to-face meetings with a digital system to maximize cargo clearing time. The Port of Durban in South-Africa has been using drones and track-and-trace technology. The purpose of these equipment is to: collect information about port traffic, inspect ports and ships infrastructure and collect port performance management data. A third example is the Tangier Med Port in Morocco which partnered with a Finnish firm to create a new Port Management Information System (PMIS). This new PMIS uses Artificial Intelligence and other digital tools. The advantages of this new PMIS are: its ability to reduce anchorage time and congestion at port, reduce human errors when dealing with administrative matters and improve efficiency of port activities.[23]

With the digitization of shipping activities across the continent, the risk of cyberattacks is omnipresent. In 2021 for instance, activities in the Port of Durban (South-Africa) were disrupted because the port operator, Transnet, was the victim of a cyberattack. This caused several financial losses, disruption of the supply chain and delays.[24] Hence cybersecurity, particularly in the maritime context, becomes a subject of concern for

[23] Mandira Bagwandeen, 'Development of smart ports in Africa An opportunity for Singapore to step in' (2022) <https://www.ntu.edu.sg/cas/news-events/news/details/development-of-smart-ports-in-africa> accessed 03 August 2023.

[24] UNCTAD <https://resilientmaritimelogistics.unctad.org/guidebook/case-study-17-port-durban-south-africa> accessed 03 August 2023.

Africa. The African Union as well as the SADC are taking action to address and regulate cybersecurity at the level of the continent. The African Union Convention on Cyber Security and Personal Data Protection (Malabo Convention) 2014 is the first regional legal framework that establishes the regulation of cybersecurity at the African level. The purpose of the Convention is to protect personal data, prevent cybercrimes and harmonize cybersecurity legislation across the continent.[25]

Various cybercrimes such as hacking, identity theft and cyber fraud are criminalized under the Convention. Section 29 of the Convention provides for the criminal offences committed via information and communication technologies.[26] States parties have the liberty to determine the applicable sanctions in cases of breach. Furthermore, the Convention promotes cooperation among Member States of the African Union to address issues related to cyber security. The Malabo Convention was adopted by 15 countries, and it came into effect on 08 June 2023 after being ratified by Mauritania.

With regards to maritime cybersecurity, the Convention does not specifically address this concern. The general premise of the Convention allows it to be used by Members States in the maritime context. The Convention can be applicable either to prevent maritime cyberattack or take the necessary measures in cases of attacks. In the absence of a specific regulation on maritime cybersecurity in Africa, the Malabo Convention

[25] Brigid Gesami and Gregory Kasembeli, 'Combating Cyber Security Threats in the African Maritime Domain' (2022) <https://ssrn.com/abstract=4086504> accessed 10 August 2023.

[26] African Union Convention on Cyber Security and Personal Data Protection (Malabo Convention) 2014 <https://au.int/sites/default/files/treaties/29560-treaty-0048_-_african_union_convention_on_cyber_security_and_personal_data_protection_e.pdf> accessed 10 August 2023.

serves as a legal safety net for Member States of the African Union in regulating maritime cybersecurity.

The African Union has also adopted the African Integrated Maritime Strategy (AIMS) 2050, as well as the African Peace and Security Architecture Roadmap which elaborate on the measures to be adopted by States to protect the African maritime domain. These measures include, *inter alia*, regional collaboration among African states to ensure safety and security at sea and reduce maritime pollution. However, one aspect which needs further consideration at the level of the African Union is the regulation of maritime cybersecurity. As mentioned above, as the maritime sector across the continent is being digitized, the risk of maritime cyberattacks is high. Hence, the AU must proactively take steps to address this concern.

Alike the African Union, the South African Development Community (SADC) does not have a specific set of regulations concerning maritime cybersecurity. The SADC consists of 16 countries of the southern African region. As a Regional Economic Community (REC), the SADC aims at promoting trade among its Member States and enhance regional partnership and collaboration. The shipping and maritime industry is vibrant among the Member States of the SADC. The Port of Port-Louis in Mauritius, Port of Durban (South Africa) and the Port of Dar-es-Salam in Tanzania are among the most active ports in the region. It has been estimated that by 2027 the volume of traffic across the ports in the SADC region will reach 500 million tons.[27] The majority of the ports in the SADC regions are taking the steps to digitalize their activities and services. By doing so, they become vulnerable to cyber-attacks.

[27] Southern African Development Community <https://www.sadc.int/pillars/maritime-ports-inland-waterways> accessed 10 August 2023.

The regulation which addresses cybersecurity at the level of the SADC is the SADC Model Law on Computer Crime and Cybercrime 2012. The Model Law lists the cybercrimes which should be addressed and regulated. These crimes are: illegal access of data, interception and espionage among others.[28] Furthermore, it lists the regulations that States can adopt in order to combat cybercrimes at national level. The Model aims at harmonizing the regulation pertaining to computer crimes and cybercrimes in the southern African region.[29]

Concerning maritime cybersecurity, this concept has not been dealt with specifically by the SADC. In case of maritime cyberattacks, Member States must take the necessary action at a national level to address the issue. This was the case for South Africa when the server at the Port of Durban was cyberattacked. Hence, at the level of the SADC, maritime cybersecurity has not been properly addressed by the community. Therefore, it is time that proactive measures be taken at this regional level to avoid further attacks in the future.

4. Recommendations and conclusions

With the number of maritime cyberattacks on the rise worldwide, countries and regional blocks must take the necessary actions to combat them. At the level of the African continent, maritime cybersecurity is not yet a subject of intense focus and concern. However, the African shipping and maritime industry is already the object of cyberattacks and cyber threats.

---

[28] International Telecommunication Union <https://www.itu.int/en/ITU-D/Cybersecurity/Documents/SADC%20Model%20Law%20Cybercrime.pdf > accessed 11 August 2023.

[29] MISA- Zimbabwe <https://data.misa.org/api/files/1634498575242w6kap89lsf8.pdf> accessed 11 August 2023.

Hence, it is important that measures be taken at a national, as well as regional level to enhance the regulation of maritime cybersecurity in Africa.

The following recommendations are made to promote the regulation of maritime cybersecurity at a national and regional level in Africa.

The governments in many African states may not have the technical capacity and resources to deal with the various technical and infrastructural aspects of maritime cybersecurity. Hence, it is recommended that governments work in close collaboration with the private sector which may have the resources needed to address maritime cyber threats and security concerns.

The office of an ombudsperson for maritime cybersecurity should be created at a national level. As African shipping and maritime industry is being digitized, the risk of cyberattacks is high. Hence, in a proactive move to take the necessary measures to avoid the attacks or address them in an efficient way whenever they happen, the office of the ombudsperson for maritime cybersecurity would be responsible for that. The office would coordinate actions to be taken and ensure a smooth implementation of the relevant procedures.

At the regional level, in the present absence of a legal framework which specifically addressed maritime cybersecurity in Africa, all Member States of the African Union ought to sign and ratify the Malabo Convention. The rationale behind is that as a common legal framework applicable in all African States, it will allow for a coordination of action among the States, and this will ensure a harmonization in the implementation of the rules pertaining to maritime cybersecurity.

Additionally, at the African level, further research and investment should be done on maritime cybersecurity. With the digitization of the shipping and maritime industry, more research on maritime cybersecurity in Africa should be done in order to better protect the industry from a legal and technical perspective.

The current regulation of maritime cybersecurity in Africa is at an elementary stage. The main conventions that deal with cybersecurity in the continent are general in nature and do not specifically focus on maritime cybersecurity. Using this current loophole as an advantage, the African Union as well as its Member States, can proactively take the legal, technical and infrastructural steps to devise a sound maritime cybersecurity structure that will shield its shipping and maritime industry from cyberattacks.

Literature

African Union – Inter-African Bureau for Animal Resources, 'Africa Blue Economy Strategy' (2019) <https://www.au-ibar.org/sites/default/files/2020-10/sd_20200313_africa_blue_economy_strategy_en.pdf> accessed 01 August 2023.

African Union Convention on Cyber Security and Personal Data Protection (Malabo Convention) 2014 <https://au.int/sites/default/files/treaties/29560-treaty-0048_-_african_union_convention_on_cyber_security_and_personal_data_protection_e.pdf> accessed 10 August 2023.

Bagwandeen M, 'Development of smart ports in Africa An opportunity for Singapore to step in' (2022) <https://www.ntu.edu.sg/cas/news-events/news/details/development-of-smart-ports-in-africa> accessed 03 August 2023.

Bueger C, 'What is Maritime Security?' (2015) 53 Marine Policy 159 <http://dx.doi.org/10.1016/j.marpol.2014.12.005> accessed 06 July 2023.

'Growth of the Ocean Cruise Line Industry' (*Cruise Watch Market*) <https://cruisemarketwatch.com/growth/> accessed 10 July 2023.
'Key Benefits Of Digitalization In the Maritime Industry' (*Dock Master*, 11 May 2023) <https://www.dockmaster.com/blog/key-benefits-of-digitalization-in-the-maritime-industry/#:~:text=Ships%20can%20save%20fuel%20and,fuel%20required%20to%20maintain%20speed> accessed 11 July 2023.
European Union Agency For Cybersecurity, 'ENISA Threat Landscape Report 2018' (*ETL*, 2018) <https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2018> accessed 14 July 2023.
Gesami, B and Kasembeli, G, 'Combating Cyber Security Threats in the African Maritime Domain' (2022) <https://ssrn.com/abstract=4086504> accessed 10 August 2023.
'Guidelines On Maritime Cyber Risk Management' (*International Maritime Organisation*, 07 June 2022) <https://wwwcdn.imo.org/localresources/en/OurWork/Security/Documents/MSC-FAL.1-Circ.3-Rev.2%20-%20Guidelines%20On%20Maritime%20Cyber%20Risk%20Management%20(Secretariat)%20(1).pdf> accessed 08 July 2023.
International Telecommunication Union <https://www.itu.int/en/ITU-D/Cybersecurity/Documents/SADC%20Model%20Law%20Cybercrime.pdf> accessed 11 August 2023.
Jacq O and others, 'Detecting and Hunting Cyberthreats in a Maritime Environment: Specification and Experimentation of a Maritime Cybersecurity Operations Centre' (2nd Cyber Security In Networking Conference, Paris, October 2018) <10.1109/CSNET.2018.8602669> accessed 10 July 2023.
Jones K, 'Threats and Impacts in Maritime Cyber Security' (2016) Engineering and Technology Reference <doi: 10.1049/etr.2015.0123> accessed 14 July 2023.
Mawuli, A and Livingstone, D.C, 'Maritime cybersecurity threats: Gaps and directions for future research' (2023) 236 Ocean and Coastal Management <https://doi.org/10.1016/j.ocecoaman.2023.106493> accessed 15 July 2023.
Meland P.H and others, 'A Retrospective Analysis of Maritime Cybersecurity Incidents (2021) 15(3) International Journal of Marine

Navigation and Safety of Sea Transportation <DOI: 10.12716/1001.15.03.04> accessed 06 July 2023.
MISA- Zimbabwe <https://data.misa.org/api/files/1634498575242w6kap89lsf8.pdf> accessed 11 August 2023.
Mission Secure <https://www.missionsecure.com/maritime-security-perspectives-for-a-comprehensive-approach#:~:text=Maritime%20cybersecurity%20is%20the%20collection,vessels%2C%20and%20their%20cyber%20environment> accessed 08 July 2023.
Park C. and others, 'Cybersecurity in the maritime industry: a literature review' (International Association of Maritime Universities Conference, November 2019) <http://researchonline.ljmu.ac.uk/id/eprint/11929/1/IAMU%202019%20Park%20et%20al.pdf> accessed 14 July 2023.
Southern African Development Community <https://www.sadc.int/pillars/maritime-ports-inland-waterways> accessed 10 August 2023.
Tijan, E and others, 'Digital Transformation in the maritime transport sector' (2021) 170 Technological Forecasting & Social Change <https://doi.org/10.1016/j.techfore.2021.120879> accessed 11 July 2023.
UNCTAD, 'Review of Maritime Transport 2022' (UNCTAD, 2022) <https://unctad.org/rmt2022#:~:text=UNCTAD%20projects%20global%20maritime%20trade,during%20the%20past%20three%20decades> accessed 10 July 2023.
UNCTAD <https://unctad.org/news/afcfta-could-boost-maritime-trade-africa> accessed 01 August 2023.
UNCTAD <https://resilientmaritimelogistics.unctad.org/guidebook/case-study-17-port-durban-south-africa> accessed 03 August 2023.
UNCTAD, UNCTAD's Review of Maritime Transport 2022: Facts and Figures on Africa (2022) <https://unctad.org/press-material/unctads-review-maritime-transport-2022-facts-and-figures-africa#:~:text=Africa%20is%20the%20region%20with,mostly%20on%20foreign%2Downed%20vessels> accessed 01 August 2023.
Van Schaik, P and others, 'Risk perceptions of cyber-security and precautionary behaviour' (2017) 75 *Computers in Human Behavior*, 547.

World Bank <https://www.worldbank.org/en/news/infographic/2017/06/06/blue-economy> accessed 01 August 2023.