The impact of digitalization on economic and financial crime in the context of the Covid-19 pandemic

Iulia Brici[a], Monica Violeta Achim[b], Sorin Nicolae Borlea[c] & Alexandra Ioana Daniela Rus[d]

[a] PhD candidate, Babeş-Bolyai University, Faculty of Economics and Business Administration, Cluj-Napoca, Romania
E-mail: iulia.brici@econ.ubbcluj.ro /Corresponding Author

[b] Professor PhD. Dr. Habil., Babeş-Bolyai University, Faculty of Economics and Business Administration, Department of Finance, Cluj-Napoca, Romania
E-mail: monica.achim@econ.ubbcluj.ro

[c] Professor, PhD. Dr. Habil. 'Vasile Goldis' Western University of Arad, Romania & University of Oradea, Oradea, Romania & Babeş-Bolyai University, Cluj-Napoca, Romania
E-mail: nicolae.borlea@ubbcluj.ro

[d] PhD candidate, Faculty of Economics and Business Administration Babeş-Bolyai University of Cluj-Napoca, Romania
E-mail: alexandra.rus@econ.ubbcluj.ro

DOI: https://doi.org/10.19275/RSEPCONFERENCES155

Abstract

Economic and financial crime became a very captivating topic to study because once technology developed, new methods of committing these types of crimes have made their presence felt. Due to global factors, various sectors of the economy field are more or less affected. One of the most powerful factors was COVID-19 pandemic which restructured all the classical processes into digital ones, mostly because of the conditions imposed by the lockdown.

This research splits economic in financial crime into four main components: corruption, shadow economy, money laundering and cybercrime. The digitalization process was measured using two relevant indicators regarding digitalization of the economy and society and technology adoption.There are also several reasons for the existence of such a high level of economic and financial crime. First of all, the quality of public governance is poor. Secondly, the population is not sufficiently educated in the financial field, but neither in the cyber-protection field. Also, the level of education can significantly affect engagement in such crimes.

The empirical section of the research tests the relationship between every component of economic and financial crime and the digitalization taking also into account the level of economy development, the education and the public governance main forms. The sample incorporates 185 worldwide countries in order to obtain relevant results. Thus, the role of this article is to identify the impact that digitalization has had on economic and financial crime in the context of the COVID-19 pandemic. For this reason, the period of analysis starts in 2015 and end in 2020, in order to cover the period before the pandemic, but also the period in which it manifested its effects. The results show that digitalization determines a decrease of the economic and financial crime under all its four forms, namely: corruption, shadow economy, money laundering and cybercrime, even if the risks are not zero and we have to maintain our concern to prevent and combat them. Our work is addressed firstly to practitioners in the economic and financial domain. It also adds value to the literature of the field, but also helps the general public to be aware of the existing risks and the need to defend against them.

Keywords: economic and financial crime, digitalization, Covid-19 pandemic, cryptocurrency, cybercrime

Jel Codes: G01, O33

1. Introduction

Economic and financial crime became a very captivating topic to study because once technology developed, new methods of committing these types of crimes have made their presence felt. Due to global factors, various sectors of the economy field are more or less affected. If 11-13 years ago we were facing the biggest economic crisis, at the end of 2019 a new phenomenon appeared and destabilized the whole world. Strictly speaking about the economic and financial crime, the COVID-19 pandemic has paved the way for criminals to create new possibilities to engage in crime. Of course, the nucleus was on the online area, because most of the activity was focused in the cyberspace, during the lockdown and beyond it.

In this context, cybercrime has grown significantly. Among the types of crimes that have been committed, can be mentioned fraud involving bank accounts, cryptocurrency fraud, e-commerce fraud or cyber attacks over the platforms of various actors in the economic or financial market. Their purpose was obviously a financial one, done by obtaining confidential data related to users' banking products. The most acute augmentations were found among bank frauds or cryptocurrencies frauds.

There are many attempts in the research literature to measure the impact of digitalization on the level of classical crimes like corruption (Bird & Zolt, 2008; Goel et al., 2012), tax avoidance (Slemrod, 1990; Bird & Zolt, 2008; Immordino and Russo, 2018; Okunogbe and Pouliquen, 2018), shadow economy (Remeikiene et al., 2021; Elgin and Oyvat, 2013), or financial crime index (Achim, Borlea et al., 2021). However, to our knowledge, there is no study to make a comparative analysis of the influences of digitalization on different types of crimes in order to highlight the different movements during the time among these components.

The gap we have identified in the literature is the integration of these forms as a whole concept in order to be able to finally identify how the digitalization process influences the level of economic and financial crime. The role of this article is to identify and synthesize information, both literature and statistics, on the impact that digitalization has had on economic and financial crime in the context of the COVID-19 pandemic. Thus, our research comes to test the relationship between digitalization and every component of economic and financial crime. The database contains information on the two main concepts, digitalization and economic and financial crime. Due to the objective of obtaining the most relevant results, our analysis sample includes 185 countries from all over the world. Also, as control variables are considered education, the amount of GDP and public governance, in all its forms. Our research helps those who work in the economic and financial field to reach some conclusions of some phenomena they have faced in their experience. Also, the contribution made in the academic sphere is certainly an added value. At the same time, our research informs the general public about the risks to which they are exposed, and, of course, helps them to be aware of the need to protect themselves from such events.

The rest of the paper is organized as follows: in section 2 of the paper we present some studies from the existing literature, both conceptually and statistically approaches. Section 3 covers the presentation of the methodology, variables and data sources. Section 4 contains the results of the study, as well as some discussions related to them. The last section of the article consists in the final conclusions of the research.

2. Literature Review

Economic and financial crime is a phenomenon which appeared in literature in the first years of the twentieth century when crime was split into usual and economic crime (Sutherland, 1940). Closer to our days, professor Letia (2014) conducted a study in order to identify the profile of a business criminal. In 2019, professors Achim and Borlea named the concept economic and financial crime. This whole concept includes a list of elements, such as: corruption, shadow economy, money laundering, cybercrime, fraud, tax evasion, intellectual property interactions, illegal e-commerce, bribery, counterfeiting, undeclared employment and so on. In the literature of the field, we can identify many of these forms, but for some of them we can find also some measurement methods. This is the reason why we have chosen to take into account in our study the following ones: corruption, shadow economy, money laundering and cybercrime.

Corruption represents a type of economic crime committed by officials abusing of their role in order to procure a personal gain. Between the most common forms of corruption, we can mention acts of bribery, embezzlement or the abuse of power. The information about the acts of corruption is gathered through surveys. There are several levels at which these surveys are sent for completion, namely: general population, business field, civil servants, following certain methodological standards. One of the most important and useful sources of information in this regard is Transparency International, which has created an index in order to quantify corruption and publishes data annually. In the top of the most corrupt countries in the world, according to the latest available data, we can mention: Iraq, Colombia and Mexico. On the other hand, the least corrupt countries are: New Zealand, Singapore and Northern European countries. The trend is downward , but according to a World Bank article (Anderson, 2020) for a third of the countries for which we have data available, there have been increases in the percentage of corruption in companies. There are, of course, efforts to control corruption, at least at firm-level (Cieślik, 2021), but those targeted to meet these criteria are usually unethical people who act to circumvent the rules, and scandals caused by acts of corruption are still at the forefront of international news.

Shadow economy is another significant component of economic and financial crime. The European Commission defines shadow economy as being "economic activities and the income derived from them that circumvent or avoid government regulations or taxation" (European Commission, 2014). In terms of measuring shadow economy, GDP is a very good method using the income approach (Schneider, 2015). Also, according to Putniņš (2015), shadow economy can be measured as sum of deliberately concealed wages and unreported business profits. Other authors (Elgin & Erturk, 2019) make efforts to improve measurement of informal field size by developing theoretical methods for determinants and effects of informality. Regarding the forecasts, according to the Association of Chartered Certified Accountants (2017), the level of shadow economy is expected to be on a descending trendline, at global level, until 2025, from 23% of global GDP (2011 data) to an estimated 21% in 2025. At the root of this forecast is a mathematical analysis of the factors behing the shadow economy. The descending trendline is not available for all the countries analyzed. For emerging market economies, is expected an increase of the percentage in the global GDP until 2025.

The third important pylon of economic and financial crime that we have taken into account in our study is money laundering. According to OECD (2002, 2009), money laundering is defined as ’the attempt to conceal or disguise the ownership or source of the proceeds of criminal activity and to integrate them into the legitimate financial systems in such a way that they cannot be distinguished from assets acquired by legitimate means’or ’the process of hiding illegally produced sources, through criminal proceedings, in order to give them a seemingly legal origin’.

Money laundering is an extremely serious issue, so it has many implications worldwide. It is also closely linked to other forms of serious and organized crime, as well as to the financing of terrorism. Europol (2021) seeks to provide EU member states with information and forensic assistance to prevent and combat money laundering.

In this regard, the Financial Crimes Information Center (FCIC) has been strengthened. This is a secure web platform that provides information to law enforcement practitioners about money laundering law enforcement. It has about 1200 members and is a portal for the exchange of experience and knowledge, as well as good practices related to financial intelligence. In addition to this role, it also makes a significant contribution to other projects supported by the Europol Financial Intelligence Group.

The Basel Institute on Governance, through the Basel Institute's International Center for Asset Recovery, gathers information on the risk of money laundering and terrorist financing globally. Data are collected from 17 public sources, including World Bank, Transparency International and World Economic Forum.

In terms of another kind of ways of action, according to Mordor Intelligence, the Global Anti-money Laundering market was valued at 2.44 billion dollars in 2020. It is expected to reach 5.28 million dollars until 2026, registering a Compound Annual Growth Rate of 16.71% since 2021 until 2026.

Current statistics (Renolon, 2022) estimate that globally, the amount of money laundering activities reaches 2% to 5% of global GDP. They represent between 800 billion dollars and up to 2 trillion dollars. Most worrying fact is that, according to the same source, 50% of these activities are not identified.

The most recent and common type of economic and financial crime is cybercrime. By definition, it represents a criminal act made with the help of technology, respectively using a device (computer, tablet, smartphone, etc.). In terms of typology, cybercrime takes place at three levels. First level is individual, because it involves distributing malicious or illegal information from one person. Here we can include cyberstalking, trafficking or distributing pornography. That it takes please at property level, when a criminal is illegally possessing data about a person’s identity or banking service. The data can be used to access the owner’s funds or to make phishing or scams acts in order to use a false origin of the problem caused. Then we have cybercrime done at governmental level. Here we talk about a crime made against a country, against a government. These criminals are usually terrorists or enemies of the government because of a certain issue. Examples of such acts, can be hacking government websites, distributing propaganda or terrorism acts.

International Telecommunication Union has developed a way of measuring cybercrime, the Global Cybersecurity Index, in order to try to capture the commitment of countries to cybersecurity at a global level. The reason of developing this index is raising awareness of the importance and different dimensions of cybersecurity.

Cybercrime has registered a massive increase. The incidence of phishing attacks, personal data fraud / identity theft, e-commerce fraud, cryptocurrency fraud, bank fraud (which evolved from card fraud or ATM fraud, attacks on banking applications to increase access to information and funds of the damaged).

Regarding data provided by Insurance Information Institute, in 2020, the reports on identity theft reached 4.8 million dollars, compared to 3.3. millions of dollars as it was in 2019. In an article made by Legal Jobs (2022), it was mentioned that in order to fight and try to prevent the dispersion of the phenomenon, the worldwide spendings on cybersecurity is forecast to reach 133.7 billion dollars this year.

According to a study developed by Forbes (2022), the past two years have gone through a major change in the way of working, from classical to remote and hybrid offices. The statistics show that hackers took only advantage of the vulnerabilities of the security. Also, according to an article developed by Beta News (Barker, 2022), in January

2022, a percentage of 93% had been reached through which companies' networks can be penetrated by cybercriminals and, in this way, they gain access to their local network resources.

In conclusion, we must look for ways to protect ourselves from all these unpleasant situations, which can have serious consequences once they have occurred.

Digitalization is a phenomenon widely met in our times, it has been identified by many to be one of the major trends changing society and business in the future. The concept involves a transformation of data from its analogical state into a digital state. It comprises the integration of digital technologies into everyday life in order to change the way of doing things with the aim of creating value. It implies reorganizing the strategies and methods in order to obtain a benefit from using technology. It can also imply improving communication and interaction for increasing company's performance. Very often, the terms 'digitization', 'digitalization' and 'digital transformation' are confused. Digitization represents the conversion of products to digital format. Digitalization means the innovation of a business model by exploiting digital opportunities. Digital transformation is a system-level restructuring of institutions, economies, society. This process takes place through digital diffusion.

According to Statista, the spendings on digital transformation technologies and services worldwide are on a positive trendline since 2017 (0.96 trillion dollars) until 2025 (forecast predict 2.8 trillion dollars). According to a study of IDC (2020), the premier global provider of market intelligence, advisory services, and events for the information technology, telecommunications, and consumer technology markets, the organizations which suffered a digital transformation are projected to contribute to more than half of the global GDP by 2023. An important role among the factors that boost the level of digitalization in economy is playing by the corporate governance of entities (Sabau (Popa) et al 2021).

The economic digitization has many advantages, but it also generates new channels for the fraudsters to gain illegal benefits when operating in the digital space. There is a vast new promise, but also new perils (Tapscott, 2015).

On the one hand, the digitalization has clear *advantages* on reducing the classical frauds such as tax evasion, corruption, shadow economy etc. The development and spread of ITCs may contribute to the reduction in cash turnover and thus make monitoring of financial transactions much easier, through decreasing shadow economy (Remeikiene et al. 2021; Elgin and Oyvat, 2013), and tax evasion (Immordino and Russo, 2018, Okunogbe and Pouliquen, 2018). Moreover, technology may discourage corruption-engaging activities by reducing the interactions between the taxpayer on the one hand and the representative of the tax authorities on the other hand (Slemrod, 1990; Bird & Zolt, 2008; Goel et al. 2012) that establish internet diffusion to be associated with less corruption. In financial markets, the need of higher investments in regulatory technologies (RegFin) of these is highly required in order to reduce financial markets frauds (Williams, 2013; Joshi, 2020). In banks, regarding anti-fraud technologies, the detection of credit card fraud uses various money laundering techniques, especially those of artificial intelligences while for detecting frauds in financial statements the best performing methods are probabilistic neural networks and genetic algorithms (Sadgali et al., 2019). Similar technologies consisting in computerized data mining programs, machine learning and several tools for risk profiling are used to trace illicit funds for money laundering or terrorist acts (Levi & Wall, 2004; Amoore & de Goede, 2005; de Goede, 2008; Williams, 2013).

On the other hand, there is *the dark side of digitalization* upon economy by facilitating new channels for the fraudsters to gain illegal benefits when operating in digital space under the forms of cybercrime, bank frauds, FinTech frauds, e-commerce frauds etc. In this context, the term "digital shadow economy" has recently emerged in the literature as an expression of the frauds conducted in digital space. In the broad sense, the "digital shadow economy" term is frequently aligned with the terms of "digital underground economy" and "digital black market", respectively meaning profit-driven Internet-based unregistered activities (Herley and Florencio, 2010) and illegal revenues generated as a result of online trade and service provision (Zorz, 2015). Digital shadow economy refers to cybercrime, e-piracy, e-fraud, bank frauds, e-commerce (Remeikien et al. 2021). Considering the illegal nature of digital shadow economy, digital shadow economy is closely related to the concept of cybercrime, which is interpreted as Internet-based crime, conducted remotely to illegally take wealth or resources from others (Smith, 2015; Reimeikiene, 2018). According with the Global Economic Crime and Fraud Survey provided by PwC (2020) a percent of 34% of frauds are conducted under the form of cybercrime, being on the second place after the consumer frauds (with 35%). Romania is among the top four most vulnerable countries in EU at cybercrime attacks after Slovenia, the Czech Republic and Bulgaria (Global Cybersecurity Index, 2020). Regarding bank frauds, the statistics shows an increase of fraud incidents over time. Thus, fraud losses per 100 U.S. dollars of total card sales worldwide have increased by 57 % in 2021 compared to 2010 (from 4.1 in 2010 to an estimate value of 7.1 in 2021) (Nilson, 2020). ATM malware and logical attacks against ATMs were up 269% in the first six months of

2020 compared with the first six months of 2019 (from 35 to 129) and all the reported attacks were Black Box attacks. The financial losses went up from less than €1,000, to just over €1 million (EAST, 2021). In the area of FinTech frauds it's worth mentioning Revolut, one of the world's most popular fintech start-ups, that has been accused of violating basic banking rules and failing to block thousands of potentially suspicious transactions on the platform, favoring money laundering transactions (Finews, September 2020). Also in the FinTech area, it is worth mentioning that cryptocurrency transactions are suspected of hiding cash from the economy, as long as they are made under anonymity conditions (Crawley, 2021). According to the Federal Trade Commission (2021) USA consumers have reported losing more than $80 million to cryptocurrency investment scams, an increase of more than ten-fold year-over-year. People between the ages of 20 and 39 were hit particularly hard, representing about 44% of the reported losses. Fast-Growing E-Commerce attracts many types of frauds such as Chargebacks, Friendly fraud, Gaming and wireless fraud Account Takeover (ATO) (Columbus, 2020). Regarding e-piracy, nearly a quarter of the global Internet bandwidth is used for online piracy. Every year 230,000 to 560,000 jobs are lost in the United States due to online video piracy (Statista, 2017). Despite efforts to curtail piracy, the latest piracy reports indicate that global film piracy increased by 33% during the COVID-19 lockdown (Go-Globe, 2021). Among the dark faces of digital economy we may mention the loss privacy data, i.e. "the destruction of privacy in an unprecedented and irrevocable manner" (Tapscott, 2015). In this view the recent term of "surveillance capitalism" rises up in literature (Zuboff, 2019) and requires higher protection through a more stronger General Data Protection Regulation (GDPR) framework. According to a January 2021 survey of worldwide adults, 66 % of total respondents agreed on feeling that tech companies hold too much control over their personal data (Johnson, May 11, 2021). With more countries introducing modern privacy laws in the same vein as the General Data Protection Regulation (GDPR), the world has reached a threshold where the European baseline for handling personal information (Pettey, 2016) is now the de facto global standard. According to Gartner, Inc. by 2023, 65% of the world's population will have its personal data covered under modern privacy regulations, up from just 10% in 2020 (Gartner,2020).

According to Statista, last year global spending on digital transformation amounted to 1.3 trillion US dollars, an increase of 10.4% year on year. This increase was significant, even though the COVID-19 pandemic caused a global economic recession. The pandemic played a major role in changing the way things were done. Many activities have shifted from the classic to the digital form.

One of the main tools against cybercrime which is found among the priorities of the European Commission is Digital literacy on cybersecurity and training people on how to use internet wisely and safely (Dalli, 2019). Through digital literacy people should be empowered with knowledge on how to respond effectively to cyber attacks (European Agency for Cybersecurity, ENISA, 2021). Another important type of preventive measure of digital fraud consists in the investments in anti-fraud programs / technologies by entities to prevent various types of frauds such as fraudulent insurance claims, identity theft, and money laundering. The market of these programs was estimated to be more than double in 2021 compared with 2017 and the projection for the market in 2023 exceeds 63 billion USD (MarketsandMarkets, 2021). An explanation regarding the high level of digital fraud undertaken in the context of increased IT technologies consists in the pace of technical enforcement ability to deal with these crimes (Gogolin, 2010). Digital skills are perishable unless kept current and thus digital crime investigation is very expensive. To keep the pace, digital crime investigation requires high investments in training and also digital and physical infrastructures (Gogolin, 2010). Based on the presented aspects from the literature of the field, the folowing research hypothesis and research questions are stated:

Hypothesis: *Digitalization has an influence on economic and financial crime (FinCrime).*

3. Methodology, variables and data

We will use in our study qualitative, quantitative analysis, but also graphical and statistical methods.

Variables

Dependent variables - components of economic and financial crime: corruption, shadow economy, money laundering and cybercrime

The first component of economic and financial crime that we consider in our study is corruption. Its quantification method is provided by Transparency International. The index, Corruption Perception Index, shows how corrupt a country's public sector is perceived by experts and business executives. The index, also called CPI, is a composite index, representing a mix of 13 surveys made on corruption, collected by well-known institutions. CPI has a global geographical coverage. The data become available at the end of every year, from 1995 until present day. It takes values between 0 and 100. The 0 level means that the respective country / public sector of the country is very corrupt, meawhile the level of 100 shows a very clean economy or economy field. The original sample contains 180 countries.

For the second component of economic and financial crime, shadow economy, two professors, Friedrich Schneider and Leandro Medina have collected data and developed over time a serie of studies regarding its method of measuring. Their index is called shadow economy and it shows the size of shadow economy calculated as percertage of the official Gross Domestic Product (GDP). The dataset is provided almost annualy, since 1991. The original sample was composed by 158 countries.

The third main part of economic and financial crime, money laundering, is quantified using the Basel Anti-Money Laundering Index. It represents a ranking method which takes into account the risk of money laundering and terrorist financing around the world. It was provided by the Basel Institute on Governance. The data are available since 2012 and the original sample consists in 129 countries.

The other very common and current economic and financial crime form is cybercrime. Is has become more and more mentioned in the literature of the field due to the continous technological development. Its measurement method was provided by the International Telecommunication Union. It measures the level of cybercrime at country level, for a sample of almost 180 countries. The data are available annually and the reports are available only for 2015, 2017, 2018 and 2021.

Independent variable – digitalization

The European Comission developed an index called Digital Economy and Society Index which tracks the evolution of digital competitiveness for the EU state members. This index, also called DESI, is a composite index, comprising five measuring areas: connectivity, human capital, use of internet, integration of digital technology, digital public services. The data are available for 29 countries, from 2015 to 2020.

World Economic Forum developed another measurement method for digitalization, in the form of an index called Technology Adoption (TA) calculated as weighted score of technological readiness (technological adoption and ITC use). It ranges between 1 to 7, from least to most agile company to adopt existing technologies to enhance the productivity of its industry.

Control variables - public governance, standard of living, education

According to the most relevant studies found in the specialized literature, the most significant causes of economic and financial crime are public governance, standard of living or the level of education.

First of all, it is about the low quality of public governance. Specifically, we discuss about the poor perception of the quality of public and civil services and their degree of independence from political pressures, the quality of policy formulation and implementation, and the credibility of the government's commitment to such policies. quality of regulations (excessive bureaucracy, large number of regulations, procedures, etc.).

Then, we refer to the low standard of living. Specialized studies (Achim et al., 2021; Bethencourt, 2022; Nguyen, 2021; Aidt, 2010) show that the level of economic development is a significant factor for engaging in crime. Our studies show that a high standard of living of the population leads to a reduction in the levels of corruption, shadow economy and cybercrime. In addition, we find that an increase in economic and sustainable development is linked to higher levels of money laundering. According to Eurostat, in 2020 Romanian citizens have the highest at-risk-of-poverty rate among EU countries, respectively 35.8%, followed by Bulgaria (33.6%) and Greece (27.5%), given that the EU average is 21.9% (European Comission, 2021). This means that 1 of 3 people in Romania has an income that provides them with a standard of living below the poverty line. In contrast, at the other side of the ranking, the lowest at-risk-of-poverty rates were recorded in Czechia (11.5%), Slovakia (13.8%), Slovenia (14.3%), Netherlands (15.8%) and, in the top of the ranking, we find Finland (15.9%).

Also, the low level of education and, in particular, the low level of financial and cyber-education of the population is an obvious problem. According to (Klapper et al., 2015) Romania has the lowest level of financial education in the European Union. The countries with the highest level of financial education are the countries in the north-west of the EU (Denmark, Sweden, the Netherlands and Germany), and those with the lowest levels are found in south-eastern Europe (Greece, Italy and Portugal, Romania).

A study conducted by the European Union Agency for Fundamental Rights (2020) shows that Romanian citizens are the least concerned about the likelihood of fraudulent information distributed on the Internet. Thus, a percentage of 34% of the respondents of Romanian citizens state that they are not at all concerned about these risks, compared to an average of 55% at EU level. Also, the percentage of the population least worried about the possibility of abusive use of online bank accounts, credit / debit in the next 12 months, is 26% in Romania, compared to an average of 11% in the EU. According to this criterion, Romania ranks third after Cyprus and Lithuania, representing the countries with the least worried citizens about such risks.

Similar results on the existence of an extremely low degree of cyber-education are also provided by the Directorate General for Communication (2020). Thus, according to this study, the citizens of Romania are among the EU citizens who do not know where to report any possible cyber attack. Thus, only 2% are aware of the existence of a website to report such cyber attacks, compared to an EU average of 12%. Also, only 2% of the Romanian citizens interviewed have ever reported a cybercrime or any other illegal online behavior (for example, cyber attack or online harassment), compared to the EU average of 7%. And from this perspective, Romanian citizens prove a low degree of cyber education, along with citizens of Portugal who report a similar percentage of 2%.

Regarding education, Romanians, from their mentality perspective, in any situation, operate on the principle "there must be a cheaper option than the original". So, for example, when it comes to purchasing original licenses for the programs they usually use, they choose cheaper, but totally insecure options. We become vulnerable when we choose to deviate from security principles. Also, unfortunately, the vast majority of the population is easily influenced and believes in almost anything, often without research. Faced with an advantageous offer, the Romanian is in a hurry and does not differentiate between truth and robbery. Many examples of this kind appear in the crimes that take place through the internet, e-mails, social media platforms, etc. Most of those who fall into the trap of this type of cybercrime are those in the older age groups. We have a great need for cyber-education, not at an advanced level, but in such a way that we can distinguish reliable information from one that could endanger us.

Sample

For the descriptive statistics we will use a sample made up only of EU countries for the period 2015-2020. For the empirical study, we will use a larger sample of 185 countries, 2015-2020. We chose to use as much data as possible in order to obtain the most relevant results of the statistical regressions.

A detailed presentation of the variables is made in Table 1 below:

Table 1. Description of variables

Variables	Way of expressing	Calculation	Sources
	Dependent variables		
Corruption	*Corruption perception index (CPI)* which measures the perceived levels of corruption in the public sector for the world countries.	The score ranges from 0 (highly corrupt) to 100 (very clean).	Transparency International
Shadow economy	*Shadow economy* (*SE*) is determined as percentage of GDP, for the world countries.	% of GDP	Medina and Schneider
Money laundering	*Anti-Money Laundering Index (AML)* measures the risk of money laundering.	Ranges between 0 and 10.	Basel Institute on Governance
Cybercrime	*Global Cybersecurity Index (GCI)* is a composite index which monitors the level of cyber-security.	Ranges between 0 and 1.	International Telecommunication Union
	Independent variables		
Digitalization	*Digital Economy and Society Index (DESI)* is a composite index which summarizes indicators on Europe's digital performance and tracks the progress of the European Union's countries.	DESI comprises five dimensions representing main policy areas, each component having a percentage of the final value of the indicator: 1. Connectivity (25%) 2. Human capital (25%) 3. Use of internet services (15%) 4. Integration of digital technologies (20%) 5. Digital public services (15%).	European Commission
Technology adoption	*Technology adoption index (TA) is the weighted score of technological readiness (technological adoption and ITC use).*	Ranges between 1 to 7, from least to most agile company to adopt existing technologies to enhance the productivity of its industry.	World Economic Forum
	Control variables		
Economic development	*Gross Domestic Product per capita (GDP)* is the sum of the gross value achieved by all producers in an economy, plus any other taxes and eliminates discounts that are not included in the value of the products.	Data is expressed in dollars.	World Bank
Education	*Education Index (EI)*	Component of the Human Development Index.	United Nations Development Programme, Human Development Reports
Public governance	*Worldwide Governance Indicators* consist in six dimensions of governance: 1. Voice and Accountability (VA) 2. Political Stability and Absence of Violence (PS) 3. Government Effectiveness (GE) 4. Regulatory Quality (RQ) 5. Rule of Law (RL) 6. Control of Corruption (CC).	Each dimension ranges from –2.5 points (weak) to 2.5 points (strong) in governance performance.	World Bank

Source: own processing

Econometric models

We synthesize the econometric modeling by a multiple linear regression, the model showing thus:

$$\boldsymbol{FinCrime_{it} = \beta_0 + \beta_1 Digitalization_{it} + \beta_2 Controls_{it} + C_i + \varepsilon_{it}}$$

Where,

- **FinCrime**$_{\textbf{it}}$ represents the dependent variable, namely economic and financial crime (we will use an index for each of the four components of FinCrime: Corruption, Money Laundering, Shadow Economy and Cybercrime), for countries i, at the moment t;
- **Digitalization**$_{\textbf{it}}$ represents the independent variable (Digitalization), expressed as Digital Economy and Society Index or Technology Adoption, for the countries i, at the moment t;
- **Controls**$_{\textbf{it}}$ represent the control variables (Public governance, Standard of living, Education) for the countries i, at the moment t;
- $\boldsymbol{\beta_0}$ is the intercept;
- $\boldsymbol{\beta_i}$ represents the regression coefficient which indicates the extent to which the independent variable influences the dependent variable if the coefficient is statistically significant;
- **i** refers to the countries of the panel;
- **t** refers to the analyzed time period (2015-2020);
- $\boldsymbol{\varepsilon_{it}}$ is the residual error.

4. Results and discussions

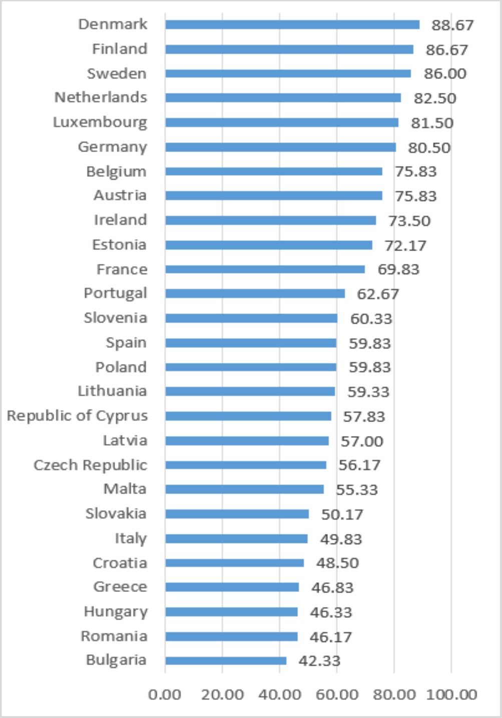
4.1 Descriptive statistics

In the following, we will present some aspects in terms of levels of the components of economic and financial crime. Each of the figures below correspond to the 2015-2020 analysis period. We have made an arithmetic mean of the values in order to see a ranking of the EU member states.

Corruption

According to data provided by Transparency International on the public sector corruption, Bulgaria (42.33), Romania (46.17) and Hungary (46.33) have the highest levels of corruption. In contrast, the countries with the lowest levels are the northern European countries, such as Denmark (88.67), Finland (86.67) and Sweden (86.00) (Figure 1). The index can take values beetween 0 and 100. We can see from Figure 1, that the level of corruption in the EU 27 countries group ranges between 42.33 and 88.67. This reveals a general low to medium level of corruption.

In terms of evolution, in the period 2015-2020, the trend is downward (Figure 2). However, despite the fact that there are many attempts to prevent and combat corruption, it still makes its presence felt in the public sector companies that responded to the survey launched by Transparency International. With the technological development, and especially with the conversion of classical work into digital work, imposed by the COVID-19 pandemic, opportunities such as classic acts of corruption, which involved face-to-face interaction, have diminished. Instead, there are new methods that criminals have developed online, from blackmail to threats using handy technology. Online interaction allows criminals to maintain their anonymous identity, which is why it could even be an incentive to commit these acts.



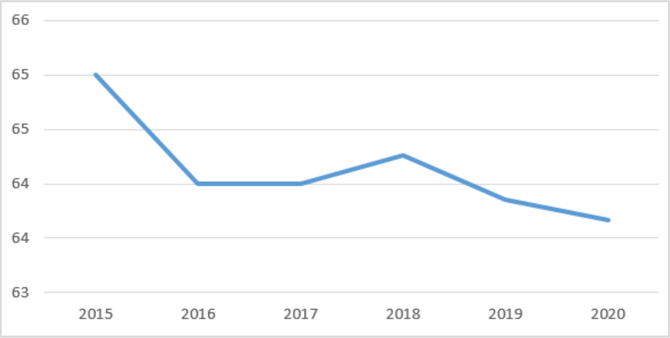


Figure 2. CPI evolution 2015-2020, EU27 evidence
Source: own processing

Figure 1. CPI country average 2015-2020, EU27 evidence
Source: own processing

Shadow economy

If we refer to the shadow economy (Figure 3), taking into account the database developed by Medina and Schneider, it reflects the highest levels of shadow economy as the percentage of GDP in Cyprus (26.17%), Greece (25.17%) and Bulgaria (23.93%). The countries with the lowest percentages of shadow economy are Austria (7.27%), Luxembourg (8.67%) and the Netherlands (8.97%).

For the available data, trends in the shadow economy are declining significantly (Figure 4), which is proving to be an increasing efficiency in the methods of combating these crimes adopted by the bodies involved in the fight against economic and financial crime.

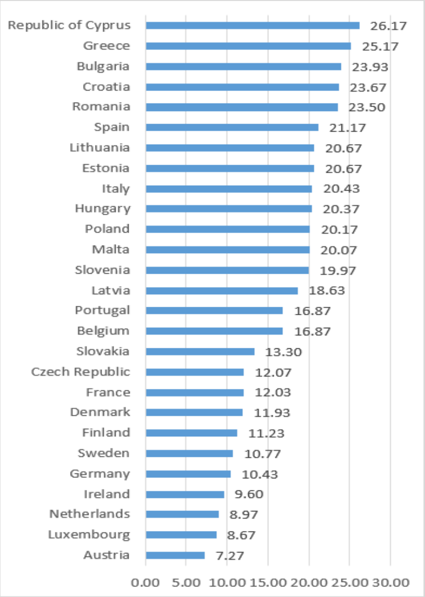


Figure 3. SE country average 2015-2020, EU27 evidence
Source: own processing

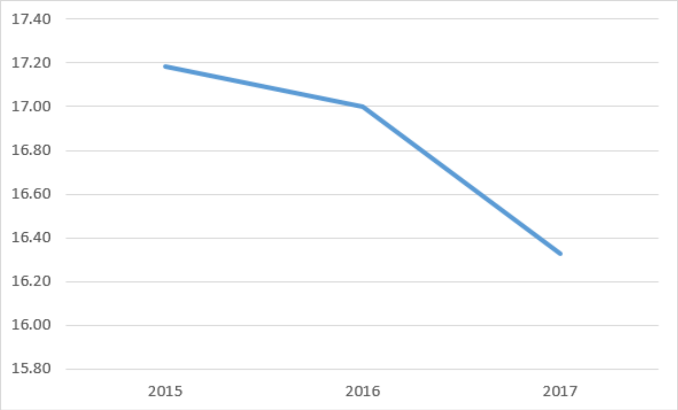
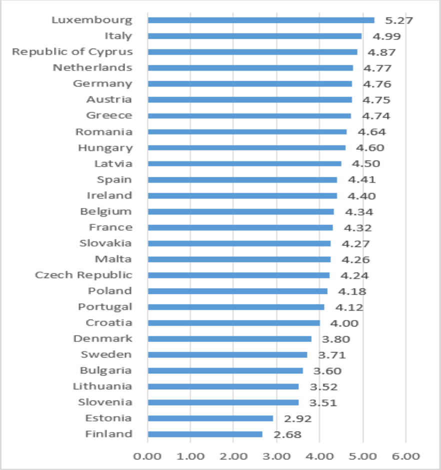


Figure 4. SE evolution 2015-2017, EU27 evidence
Source: own processing

Money Laundering

According to the data on the risk of money laundering, provided by the Basel Anti-Money Laundering score, in the top of the highest values we find Luxembourg (5.27), Italy (4.99) and Cyprus (4.87). In contrast, Finland (2.68), Estonia (2.92) and Slovenia (3.51) have the lowest levels of money laundering risk (Figure 5). Money laundering is a major danger to the economy. The index can take values between 0 and 10, but we notice that all values range between 2.68 and 5.27, which means that the risk is medium to low. From the perspective of the evolution (Figure 6) between 2015 until 2020, in the EU 27 countries group, the trend is a slightly downward, due to the efforts of the authorities to combat this type of economic and financial crime. The decreasing trend, as we can see, matches the period 2019-2020, the same period in which COVID-19 pandemic effects have arrived in the economy. We can conclude that COVID-19 pandemic was a strong factor in decreasing money laundering, due to the digitalization process.



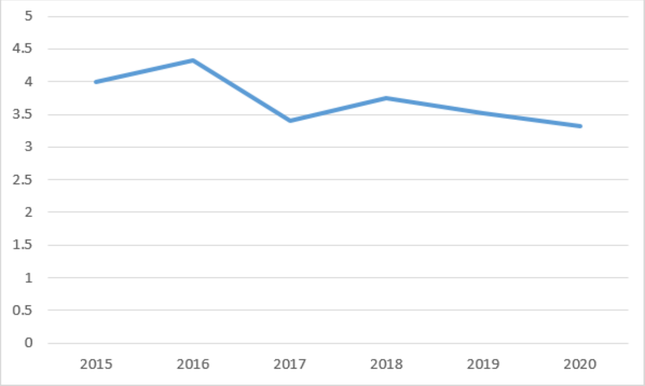


Figure 5. AML country average 2015-2020, E
Source: own processing

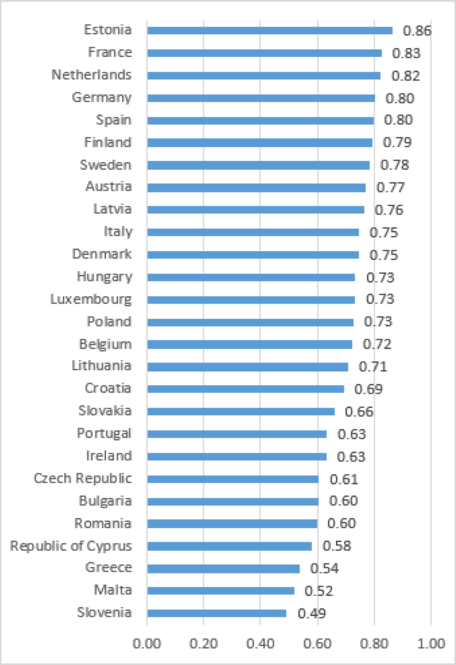
Figure 6. AML evolution 2015-2020, EU27 evidence
Source: own processing

Cybercrime

According to the Global Cybersecurity Index, the countries most exposed to cybercrime are Slovenia (0.49), Malta (0.52) and Greece (0.54). The countries that best apply cybersecurity policies are the Netherlands (0.82), France (0.83) and Estonia (0.86) (Figure 7). Regarding the trend of the EU27 group, in the period 2015-2020, we observe a constant increase in the level of cybercrime (Figure 8) exactly from the beggining of the pandemic. After digitalizing all the economy and society, cybersecurity had to increase, based on the existing of a higher level of cybercrime. This is why, even if cybersecurity increases, it does not necessary mean that cybercrime will decrease, as an immediate effect. It actually means that cybersecurity increases as a response to a higher level of cybercrime, in many situations. Cybercrime makes its presence felt everytime it detects a gap in cybersecurity, but all these deficiencies are corrected as a corrected based on notifications related to them. Thus, additional security filters are added after the detections of some cyber-attacks, strictly in that direction.

Cybercrime is a current problem because the internet has become both a help and a trap. With the development of technology, and with the change produced by the COVID-19 pandemic, cases of cyber attacks, manipulation, fake news, fraud or data theft are becoming more common. Digitalization has led to a dependence on technology induced by the new living conditions. Cybersecurity should have been the starting point for digitalization. Unfortunately, this aspect was neglected, and the awareness of the effects of digitalization came a little later. The high values of cybercrime go hand in hand with a lack of financial education and a minimum of cybersecurity education. In this regard, the European Commission is conducting a campaign to combat organized crime, which is a 5-year strategy to strengthen EU-wide cooperation and make better use of digital investigative tools.

As a general conclusion, the Nordic countries are the ones that adapt best to the new conditions, making efforts to fight any form of economic and financial crime. On the other hand, the countries that occupy the last places and face problems in dealing with the new methods of committing economic and financial crime are countries such as Romania, Bulgaria, Slovenia. Living standards and education level lead us to think of a logical explanation for this ranking, which is why our empirical testing is based on this hypothesis.



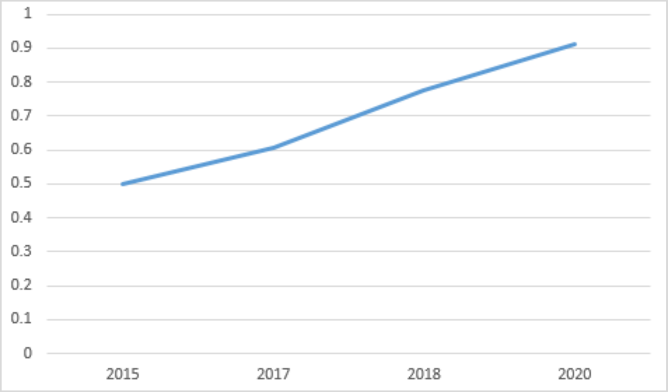


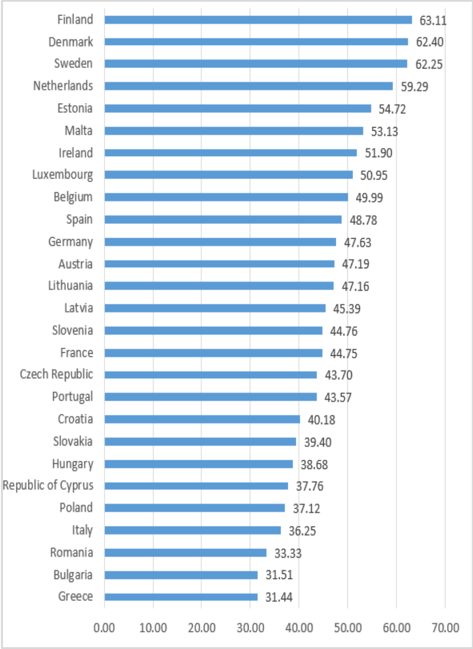
Figure 8. GCI evolution 2015-2020, EU27 evidence
Source: own processing

Figure 7. GCI country average 2015-2020, EU27 evidence
Source: own processing

In order to measure digitalization, we will use two different indicators. The first one takes into account only EU27 countries group (Digital Economy and Society Index). The second one, is available for a sample of 185 counties

(Technology Adoption). To begin with the first index, regarding the degree of digitalization in the 27 countries of the European Union, in the period 2015-2020, we chose to use the index of the digital economy and society developed by the European Commission. Both indicators measure digitalization in terms of technology adoption in companies, respectively in fields of activity and in society as a whole.

Digital Economy and Society Index



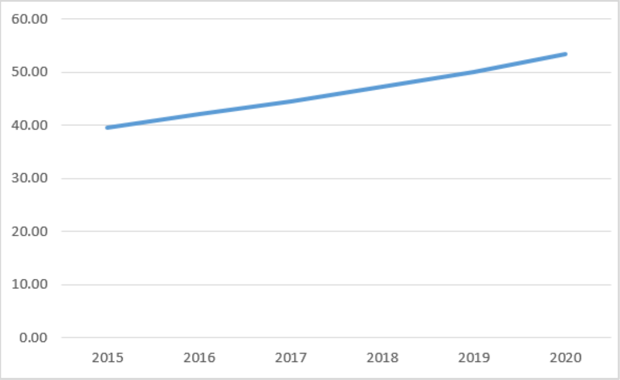


Figure 10. DESI evolution 2015-2020, EU27 evidence
Source: own processing

Figure 9. DESI country average 2015-2020, EU27 evidence
Source: own processing

There are problems on many levels of digitalization. We find from Figure 9, that among the least digitalized countries are also in this case Romania (33.33) and Bulgaria (31.51), along with Greece, which occupies the last place in the ranking (31.44). This score took into account aspects related to connectivity, the use of the Internet by individuals, the integration of digital technologies in enterprises and digital public services. In the countries at the bottom of the rankings, the problems are related to digital skills. The big downside is that in less developed countries, unfortunately, there is no priority to ensure basic digital skills, even if the current working conditions imposed by the COVID-19 pandemic have largely forced online work. The ideal situation would have been at least the knowledge of some basic software by the general population.

At the other end of the list are the Nordic countries, such as Finland (63.11), Denmark (62.40) and Sweden (62.25). However, these percentages are strongly influenced by socio-demographic aspects, given that young people, those with a university degree, students, employees or freelancers have high skills, compared to people aged 55-74, retirees and inactive people in the labor market.

There is also a problem among the number of ICT specialists, so that Romanian companies feel a rather acute shortage compared to other countries in the European Union. The lowest level of use of internet services regarding online transactions is registered in Romania, being followed at a short distance by Bulgaria and Italy. Only 28% of Romanians use the Internet at least once a week, which also puts us at the bottom of the rankings, followed by Bulgarians with 33%, given that 95% of the population of the Nordic countries regularly use Internet services. (at least once a week).

However, overall, from the perspective of the evolution of the DESI index in the period 2015-2020 (Figure 10), the trend is a significant upward one, hoping that with the efforts made to digitize the economy, we will not have such low levels, but only good results make our lives easier and protect us from cyber attacks of any kind. The upward trend of the digitalization of economy and society matches the pre-pandemic and pandemic period. Of course, this aspect was predictable, because the changes imposed by the lockdown have involved technology in every existing process and activity. If the pandemic had not existed, the digitalization of entire systems would have developed much more slowly and perhaps less efficiently. Facing with the accomplished fact, we received technology as a tool that we had to deal with in the shortest possible time.

Technology Adoption

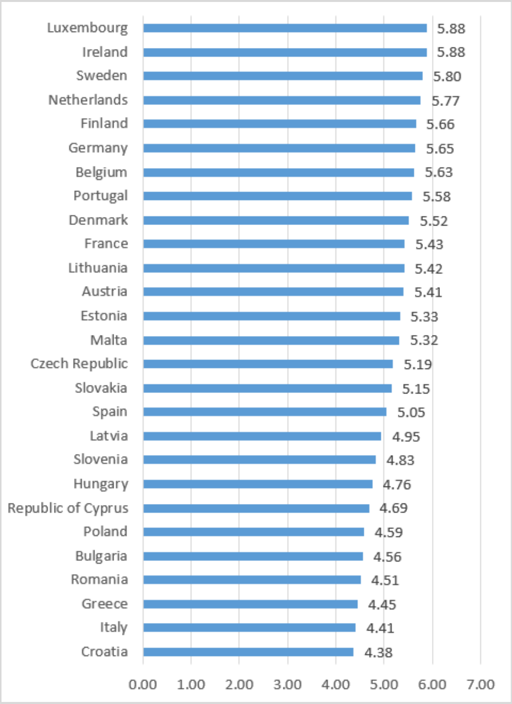


Figure 11. TA country average 2015-2020, EU27 evidence
Source: own processing

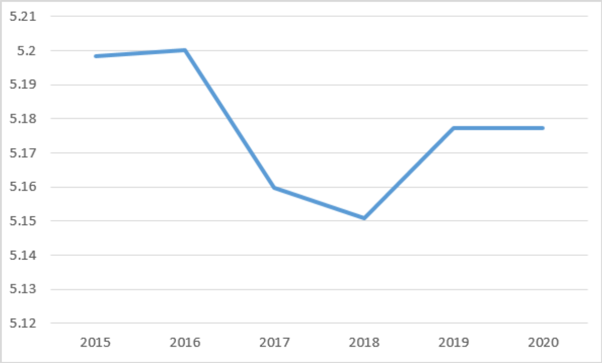


Figure 12. TA evolution 2015-2020, EU27 evidence
Source: own processing

Regarding the Technology Adoption index, the values range between 1 and 7. From Figure 11 we observe that, at the level of EU member states, the registered values are between 4.38 and 5.88. These values reveal an average to good level of technology adoption. Also in this situation, the countries that adopt technology more difficult are Bulgaria (4.56), Romania (4.51), Greece (4.45), along with Italy (4.41) and Croatia (4.38). In the opposite part of the top are the Netherlands (5.77), Sweden (5.80), Ireland (5.88) and, in first place, Luxembourg (5.88).

Regarding the evolution of the index in the period 2015-2020, we observe in Figure 12 that in the period 2015-2016 the degree of adoption of technology was about 5.2-5.3 out of 7. This level is explained by the curiosity to try new devices to facilitate the activity, but later, unfortunately, this level decreased to 5.15, the minimum value in 2018. The good part is that the level has increased in the next period, and the trend is currently stagnant. From the beginning of the pandemic and until now, we faced a lot of changes in our working methods. Technology had to become our closest friend when we had to work from home, but also to give the same efficiency as we did before, in a space dedicated to our activity. Also, not being able to make any kind of purchase of goods and services, we also chose the facilities offered by technology. The process of adapting to all these opportunities has been visibly accelerated by the conjuncture. The pandemic was the key to the rapid adoption of technology in our lives.

We will test the correlation between all the variables included in our model with the help of the correlation matrix. The interpretation of the results of the correlation matrix below (Table 2) will be done taking the components of the economic and financial crime one by one, together with a digitalization index.

For the CPI-DESI index pair we have a value of 0.759048, which means a correlation of 75.91% between the two variables. Having the same mathematical sign, the correlation is positive, which means that the increase in the level of digitalization of the economy and society, will entail an increase in the level of corruption perception.

In the case of the CPI-TA index pair we have a value of 0.813733. Also in this case, the movement of variables is in the same direction, which is why an increase in the level of adaptation to technology will cause an increase in the level of corruption. We can conclude, in this case, that in any way we will try to measure the technological progress or the digitalization, a development in this sense will give way to the appearance of several corruption crimes.

For the SE-DESI indices we observe a value of -0.577506. In this situation, the variables are 57.75% correlated, but the correlation is reversed. From this result, we realize that once the level of digitalization of the economy and society increases, we will also see a decrease in the level of the shadow economy.

In the situation of the SE-TA index pair, the value is -0.783204. Similar to the above situation, the correlation is negative. For this reason, we can conclude that as the level of technology adoption increases, the level of the shadow economy will decrease. As a conclusion of the last two correlations values, the higher the level of digitalization is, the less unpleasant events will be launched by the shadow economy.

In the case of the AML-DESI pair, the value of the correlation coefficient is -0.394133. In this case, the relationship is negative, but weak. If the level of digitalization of the economy and society increases, the risk of money laundering will decrease by 39.41%.

If we look at the relationship between AML-TA, the coefficient also brings to the fore a negative relationship between variables, but much weaker than that between AML-DESI. This time, if the adaptation to technology will go in a positive direction, the risk of money laundering will decrease by 18.57%. Following the two relationships of the money laundering risk measurement index with indices that measure the level of digitalization, we can deduce that these two variables are not so strongly correlated, which can lead to a stagnant trend or a slight decrease in the level of money laundering risk along with the digital progress.

In the case of the GCI-DESI pair, the correlation is strong and positive. If the level of digitalization of the economy and society will increase, the degree of production of digital crimes will also increase, the value of the correlation coefficient being 0.547392.

If digitalization is measured by the degree of adoption of technology, then the correlation between digitalization and cybercrime will still be positive, but not too strong. In this case, the proportion is 18.71%. Summarizing the last two results, overall a higher degree of digitalization will be favorable for the development of new methods of crime using technology as the main tool.

Table 2. Correlation matrix

Correlation/ Probability	CPI	SE	AML	GCI	DESI	TA	GDP	EI	CC	PS	GE	RL	RQ	VA
CPI	1.000000													
SE	-0.749240	1.000000												
AML	-0.242343	0.031400	1.000000											
GCI	0.290334	-0.263220	-0.183672	1.000000										
DESI	0.759048	-0.577506	-0.394133	0.547392	1.000000									
TA	0.813733	-0.783204	-0.185720	0.187157	0.702179	1.000000								
GDP	0.028074	0.172414	-0.260516	0.101612	-0.067188	-0.111383	1.000000							
EI	0.758937	-0.613143	-0.259428	0.220216	0.648916	0.628789	-0.200988	1.000000						
CC	0.988255	-0.754584	-0.246897	0.280171	0.772403	0.820065	0.032562	0.761410	1.000000					
PS	0.422428	-0.513625	-0.282807	0.015841	0.526830	0.533760	-0.254419	0.389891	0.456529	1.000000				
GE	0.926915	-0.772375	-0.205180	0.233866	0.759109	0.845342	-0.007798	0.734515	0.931821	0.522779	1.000000			
RL	0.945953	-0.806842	-0.201664	0.240986	0.774953	0.860110	-0.031569	0.727691	0.948042	0.540037	0.955777	1.000000		
RQ	0.902478	-0.761292	-0.214495	0.292122	0.761239	0.843658	0.000810	0.775029	0.908140	0.489751	0.885730	0.902183	1.000000	
VA	0.915651	-0.731674	-0.130116	0.202514	0.726259	0.822070	-0.088776	0.658287	0.918477	0.466163	0.912975	0.916952	0.863970	1.000000

Source: own calculation

If we look in terms of the correlation between our main variables and the control variables, we can also see some aspects. In the situation of the relation between the perception coefficient of corruption and the control variables, all are positively correlated, being only differences of proportions. The most strongly correlated (98.82%) is the control of corruption, which speaks for itself that once the level of corruption increases, so will the concern in fighting it. The weakest correlation is with GDP, which means that rising levels of corruption also imply a little higher level of economic development.

Regarding the relationship between the shadow economy and the control variables, here all the coefficients are negative, except the one between SE-GDP. In this situation, SE being calculated as a percentage of GDP, we conclude that the fluctuations of the GDP value do not have such a strong connection with the percentage of the shadow economy in its amount (17.2%). The strongest negative correlation is with the rule of law variable. The more the rule of law is implemented, the lower will be the level of the shadow economy (80.06%).

In the case of the link between money laundering risk and control variables, all correlation coefficients are negative, fluctuating between 13.01% (VA) and 26.05% (GDP). The higher the levels of voice and accountability and GDP, the lower will be the risk of money laundering.

Looking from the perspective of the cybercrime link with the control variables, all correlations are positive, with an intensity of up to 29.21%. The most strongly correlated are corruption control and regulatory quality. The correlations being weak, we are not worried that with the increase of the cybercrime, these levels also will register increases.

Finally, we look at the link between digitalization measurement methods and the control variables. GDP registers negative correlations, of low intensity, both with DESI (6.71%) and with TA (1.11%). An upward trend in digitalization is slightly lowering the level of GDP. In the case of DESI, the strongest correlation is with government effectiveness (75.91%). This result reinforces the conclusions of several previous studies and the reality of the practice because the higher the degree of digitalization, the greater the effectiveness of government. In the case of TA, the strongest correlation is with the rule of law (86.01%). An increase in the degree of digitalization will also lead to a greater share of support for equality between all citizens before the law.

In order to prove the existence and the powerfulness of the relationships between the variables above, we will run regressions for each pair of the main variables choosing the control variables that fit best in the models.

4.2. Empirical results

Our results are built with the help of the multiple regression technique. We will test the impact of digitalization (expressed through DESI or TA) on economic and financial crime (expressed through CPI, SE, AML, GCI). These will be our variables of interest, but the other independent variables will be added in order to obtain a Pooled-OLS regression. All the indexes that we have used in our database contain data measured through different methods, this is why we have chosen to rescaled them in order to obtain uniform data.

Table 3 estimates corruption perception as a function of technology adoption and other control variables for the sample of 185 worldwide countries. The coefficient for technology adoption is positive and statistically significant for the OLS model. As the value of technology adoption raises with 1 unit, corruption perception will raise too with 0.81 units.

Table 3. Regression between CPI, Technology Adoption, GDP and Education

CPI	**(1)**	**(2)**	**(3)**
TA	0.8161***	0.8075***	0.6129***
GDP		0.1326***	
EI			0.2722***
Constant	-1,0447	-2.3444	-6.6141
R^2	0.5995	0.5833	0.6391
R-Adj.	0.5991	0.5823	0.6383
Number of observations	882	848	870

Note: *** Statistically significant at 1%

Source: own processing

According the our results, they are significant for 1% level of acceptance. From the perspective of the model goodness-of-fit, the R-squared coefficient is equal to 0.5995 and it indicates that corruption perception (measured through CPI), our dependent variable, depends in proportion of 59.95% from technology adoption, our independent variable. In conclusion, our research hypothesis is accepted, respectively the increasing of Technology Adoption will determine an increasing of Corruption Perception Index (CPI). In other words, an increase in technology adoption increases the degree of cleanliness in terms of corruption practices is higher, thus the level of corruption decreases. In what concern the other control variables, we can conclude that both GDP and education have positive influence on corruption perception at the 1% level of acceptance and in each situation, by taking them one by one in the model, the relationship between corruption perception and technology adoption keeps the same direction. If we take GDP as control variable, for an increase of the technology adoption of 1 unit the corruption perception will increase with 0.8 units. The R-squared, in this situation, has the value 0.5833, which means that corruption perception depends in proportion of 58.33% from technology adoption, being also influenced by an increase of GDP. If we take education as control variable, for an increase with 1 unit of technology adoption, the corruption perception will increase too with 0.61 units. The corresponding R-squared is 0.6391, which means that corruption perception depends in proportion of 63.91% from technology adoption, having also a positive influence of the education.

Table 4 estimates shadow economy (as percentage of GDP) as a function of technology adoption and other control variables for the same sample of 185 worldwide countries. The coefficient for technology adoption is negative and statistically significant for the OLS model. So, as the value of technology adoption will increase with 1 unit, shadow economy will decrease with 0.32 units.

Table 4. Regressions between SE, Technology Adoption, GDP and Education

SE	**(1)**	**(2)**	**(3)**
TA	-0.3263***	-0.3296***	-0.2315***
GDP		-0.0850***	
EI			-0.1244***
Constant	45.8469	47.2968	48.1997
R^2	0.37781	0.3714	0.4074
R-Adj.	0.3770	0.3698	0.4060
Number of observations	840	806	828

Note: *** Statistically significant at 1%

Source: own processing

Based on the obtained results, they are significant for the 1% level of acceptance. From the point of view of goodness-of-fit model, the R-squared coefficient is equal to 0.37781. It indicates that shadow economy depends in proportion of 37.78% from technology adoption. Our research hypothesis is accepted, respectively an increasing of Technology Adoption will determine a decrease of Shadow Economy. Regarding the control variables, both GDP and education have a negative influence on shadow economy at the level of acceptance of 1%. Taking them one by one in the model, the relationship between SE and TA keeps the same direction. If we take GDP as control variable, for an increase of the technology adoption of 1 unit, the shadow economy will decrease with 0.32 units. The R-squared, in this situation, has the value 0.3714, which means that shadow economy depends in proportion of 37.14% from technology adoption, being also influenced by a decrease of GDP. If we take education as control variable, for an increase with 1 unit of technology adoption, the shadow economy will decrease with 0.23 units. The corresponding R-squared is 0.4074, which means that shadow economy depends in proportion of 40.74% from technology adoption, having also a negative influence of the education.

Table 5 estimates anti-money laundering as a function of technology adoption and other control variables for the sample of 185 worldwide countries. The coefficient for technology adoption is negative and statistically significant for the OLS model. At an increase of technology adoption with 1 unit, money laundering risk will decrease with 0.37 units.

Table 5. Regressions between AML, Technology Adoption, GDP and Education

AML	**(1)**	**(2)**	**(3)**
TA	-0.3749***	-0.4062***	-0.1272***
GDP		-0.1641***	
EI			-0.3255***
Constant	87.1921	90.9771	93.6768
R^2	0.3075	0.3533	0.4582
R-Adj.	0.3066	0.3517	0.4569
Number of observations	828	794	810

Note: *** Statistically significant at 1%

Source: own processing

According to the obtained results, they are significant for the 1% level of acceptance. From th perspective of the model goodness-of-fit, the R-squared equals 0.3075 and it indicates that money laundering risk depends in proportion of 30.75% from technology adoption. Our research hypothesis is accepted, which means that an increasing of Technology Adoption will determine a decrease of Money Laundering risk. In what concern our control variables, both GDP and education have a negative influence on money laundering risk at 1% level of acceptance. Taking them one by one in the model, the link between AML and TA keeps the same direction.

If we take GDP as control variable, for an increase of the technology adoption of 1 unit, the money laundering risk will decrease with 0.4 units. The R-squared, in this situation, has the value 0.3533, which means that money laundering risk depends in proportion of 35.33% from technology adoption, being also influenced by a decrease of GDP. If we take education as control variable, for an increase with 1 unit of technology adoption, the money laundering risk will decrease with 0.12 units. The corresponding R-squared is 0.4582, which means that money laundering risk depends in proportion of 45.82% from technology adoption, having also a negative influence of the education.

Table 6 estimates global cybersecurity as a function of technology adoption and other control variables for the same sample of 185 worldwide countries. The coefficient for technology adoption is positive and statistically significant for the OLS model. At an increase of technology adoption with 1 unit, global cybersecurity will increase with 0.75 units.

Table 6. Regressions between GCI, Technology Adoption, GDP and Education

GCI	**(1)**	**(2)**	**(3)**
TA	0.7560***	0.7828***	0.4325***
GDP		0.0656	
EI			0.4290***
Constant	2.6820	0.4121	-5.6940
R^2	0.3524	0.3604	0.4217
R-Adj.	0.3516	0.3589	0.4204
Number of observations	882	852	870

Note: *** Statistically significant at 1%

Source: own processing

According to the obtained results, they are significant for the 1% level of acceptance. From the perspective of the model goodness-of-fit, the R-squared equals 0.3524 and it indicates that cybersecurity depends in proportion of 35.24% from technology adoption. Our research hypothesis is accepted, which means that an increasing of Technology Adoption will determine an increase of Cybersecurity. Regarding our control variables, both GDP and education have a positive influence on cybersecurity at 1% level of acceptance. Taking them one by one in the model, the link between AML and TA keeps the same direction.

If we take GDP as control variable, for an increase of the technology adoption of 1 unit, cybersecurity will increase with 0.78 units. The R-squared, in this situation, has the value 0.3604, which means that cybersecurity depends in proportion of 36.04% from technology adoption, being also influenced by an increase of GDP. If we take education as control variable, for an increase with 1 unit of technology adoption, cybersecurity will increase too with 0.43 units. The corresponding R-squared is 0.4217, which means that cybersecurity level depends in proportion of 42.17% from technology adoption, having also a positive influence of the education.

Table 7 estimates corruption perception as a function of the digitalization of the economy and society (DESI) and other control variables, such as education and four of the total of six public governance dimensions (Government Effectiveness, Political Stability and Absence of Violence, Regulatory Quality, Voice and Accountability). We have used the same sample of 185 worldwide countries that we have used for the previous estimations. For all four OLS models that we have estimated, the coefficient for DESI is positive and statistically significant, meaning that an increase of digitalization measures as DESI conducts to an increase of cleanliness in terms of corruption practices, therefore the level of corruption decreases. Based on the obtained results, they are significant for the 1%, 5% or 10% level of acceptance.

Table 7. Regressions between CPI , DESI, Education and Governance's Dimensions

CPI	**(1)**	**(2)**	**(3)**	**(4)**
DESI	0.0665**	0.3610***	0.1058***	0.0830**
EI	0.2316***	0.8113***	0.1568*	0.4267***
GE	1.2056***			
PS		0.8113***		
RQ			1.2834***	
VA				1.4183***
Constant	-44.4032	-45.1174	-48.2812	-91.6170
R^2	0.8769	0.6494	0.8352	0.8832
R-Adj.	0.8746	0.6427	0.8321	0.8810
Obs. Number	162	162	162	162

Note: *,**,*** Statistically significant at 10%, 5%, 1%

Source: own processing

Firstly, if we estimate CPI, DESI, Education and Government Effectiveness, we observe that if the level of DESI increases with 1 unit, the corruption perception will increase too with 0.06 units. Both control variables have a positive influence on the dependent variable. From the perspective of the model goodness-of-fit, the R-squared equals 0.8769 and it indicates that corruption perception depends in proportion of 87.69% from DESI.

Then, if we estimate CPI, DESI, Education and Political Stability and Absence of Violence, we can see that if the level of DESI increases with 1 unit, the corruption perception will increase too with 0.36 units. Both control variables have a positive influence on the dependent variable. From the perspective of the model goodness-of-fit, the R-squared equals 0.6494 and it indicates that corruption perception depends in proportion of 64.94% from DESI.

If we estimate CPI, DESI, Education and Regulatory Quality, we can see that if the level of DESI increases with 1 unit, the corruption perception will increase too with 0.1 units. Both control variables have a positive influence on the dependent variable. From the point of view of the model goodness-of-fit, the R-squared equals 0.8352 and it indicates that corruption perception depends in proportion of 83.52% from DESI.

If we estimate CPI, DESI, Education and Voice and Accountability, we can see that if the level of DESI increases with 1 unit, the corruption perception will increase too with 0.08 units. Both control variables have a positive influence on the dependent variable. From the point of view of the model goodness-of-fit, the R-squared equals 0.8832 and it indicates that corruption perception depends in proportion of 88.32% from DESI.

Our research hypothesis is accepted, for each situation, which means that an increasing of DESI will determine an increase of Corruption Perception.

Table 8 estimates shadow economy as a function of the digitalization of the economy and society (DESI) and other control variables, such as education and three of the total of six public governance dimensions (Government Effectiveness, Political Stability and Absence of Violence and Rule of Law). We have used the same sample of 185 worldwide countries. For all three OLS models that we have estimated, the coefficient for DESI is negative and statistically significant. Based on the obtained results, they are significant for the 1% or 5% level of acceptance.

Firstly, if we estimate SE, DESI, Education and Government Effectiveness, we observe that if the level of DESI increases with 1 unit, the shadow economy will decrease with 0.006 units. In terms of control variables, education has a positive influence on the dependent variable, but Government effectiveness has a negative influence. From the perspective of the model goodness-of-fit, the R-squared equals 0.1181 and it indicates that shadow economy depends in proportion of 11.81% from DESI.

Table 8. Regressions between SE , DESI, Education and Governance's Dimensions

SE	(1)	(2)	(3)
DESI	-0.0067**	-0.518**	-0.0070**
EI	-0.1193***	-0.2283***	-0.1432***
GE	0.0456***		
PS		-0.3029***	
RL			-0.0854***
Constant	30.9385	63.2006	36.2896
R^2	0.1181	0.4815	0.2000
R-Adj.	0.1013	0.4716	0.1849
Obs. Number	162	162	162

Note: **, *** Statistically significant at 5% and 1%

Source: own processing

Then, if we estimate SE, DESI, Education and Political Stability and Absence of Violence, we can see that if the level of DESI increases with 1 unit, the shadow economy will decrease with 0.51 units. In terms of control variables, both of the, have a positive influence on the dependent variable. From the perspective of the model goodness-of-fit, the R-squared equals 0.4716 and it indicates that shadow economy depends in proportion of 47.16% from DESI.

If we estimate SE, DESI, Education and Rule of Law, we can see that if the level of DESI increases with 1 unit, the shadow economy will decrease with 0.007 units. Both control variables have a negative influence on the dependent variable. From the point of view of the model goodness-of-fit, the R-squared equals 0.2000 and it indicates that shadow economy depends in proportion of 20% from DESI.

Our research hypothesis is accepted, for each situation, which means that an increasing of DESI will determine an increase of Shadow Economy.

Table 9 estimates money laundering risk as a function of the digitalization of the economy and society (DESI) and other control variables, such as education and four of the total of six public governance dimensions (Control of Corruption, Regulatory Quality, Rule of Law and Voice and Accountability). We have used the same sample of 185 worldwide countries. For all four OLS models that we have estimated, the coefficient for DESI is negative and statistically significant. Based on the obtained results, they are significant for the 1% level of acceptance.

Table 9. Regressions between AML, DESI, Education and Governance's Dimensions

AML	(1)	(2)	(3)	(4)	(5)
DESI	-1.1531***	-0.1930***	-0.2003***	-0.2131***	-0.2131***
EI	-0.5131	-0.2997***	-0.3506***	-0.3094***	-0.2728***
CC		0.1904***			
RQ			0.3998***		
RL				0.3028***	
VA					0.4660***
Constant	99.2210	70.6237	58.0005	61.9865	43.3360
R^2	0.7130	0.2012	0.2188	0.2246	0.2498
R-Adj.	0.6525	0.1860	0.2040	0.2098	0.2356
Obs. Number	156	162	162	162	162

Note: *** Statistically significant at 1%

Source: own processing

Firstly, if we estimate AML, DESI and Education, we observe that if the level of DESI increases with 1 unit, the money laundering risk will decrease with 1.15 units. Education also has a negative influence on the dependent variable. From the perspective of the model goodness-of-fit, the R-squared equals 0.7130 and it indicates that money laundering risk depends in proportion of 71.30% from DESI.

Secondly, if we estimate AML, DESI, Education and Control of Corruption, we observe that if the level of DESI increases with 1 unit, the money laundering risk will decrease with 0.19 units. In terms of control variables, education has a negative influence on the dependent variable, but CC has a positive influence. From the perspective of the model goodness-of-fit, the R-squared equals 0.2012 and it indicates that money laundering risk depends in proportion of 20.12% from DESI.

Then, if we estimate AML, DESI, Education and Regulatory Quality, we can see that if the level of DESI increases with 1 unit, the money laundering risk will decrease with 0.2 units. Education has a negative influence on the dependent variable, but RQ has a positive influence. From the perspective of the model goodness-of-fit, the R-squared equals 0.2188 and it indicates that shadow economy depends in proportion of 21.88% from DESI.

If we estimate AML, DESI, Education and Rule of Law, we can see that if the level of DESI increases with 1 unit, the money laundering risk will decrease with 0.21 units. Education has a negative influence on the dependent variable, but RL has a positive one. The R-squared is 0.2246 and it indicates that shadow economy depends in proportion of 22.46% from DESI.

Lastly, if we estimate AML, DESI, Education and Voice and Accountability, we can observe that if the level of DESI increases with 1 unit, the money laundering risk will decrease with 0.21 units. Education has a negative influence on the dependent variable, but VA has a positive one. The R-squared is 0.2498 and it indicates that shadow economy depends in proportion of 24.98% from DESI.

Our research hypothesis is accepted, for each situation, which means that an increasing of DESI will determine an decrease of money laundering risk.

Table 10 estimates global cybersecurity as a function of the digitalization of the economy and society (DESI) and other control variables, such as education and the six public governance dimensions. We have used the same sample of 185 worldwide countries. For all OLS models that we have estimated, the coefficient for DESI is positive and statistically significant. Based on the obtained results, they are significant for the 1% level of acceptance.

Firstly, if we estimate GCI, DESI, Education and Government Effectiveness, we observe that if the level of DESI increases with 1 unit, global cyersecurity will increse too with 0.8 units. Both control variables have a negative influence on the dependent variable. From the perspective of the model goodness-of-fit, the R-squared equals 0.3851 and it indicates that global cyersecurity level depends in proportion of 38.51% from DESI.

Table 10. Regressions between GCI, DESI, Education and Governance's Dimensions

GCI	(1)	(2)	(3)	(4)	(5)	(6)
DESI	0.8005***	1.1480***	0.7895***	1.1037***	1.1530***	1.1252***
EI	-0.2485	-0.5274	-0.6292***	-0.5819*	-0.4395	-0.7386***
GE	-0.6699***					
CC		-0.6057***				
PS			-1.0290***			
RQ				-0.8695***		
RL					-0.9260***	
VA						-1.0386***
Constant	102.7754	104.3053	168.192	135.6727	126.4545	168.8177
R^2	0.3851	0.5692	0.4314	0.5483	0.5870	0.5701
R-Adj.	0.3734	0.56111	0.42067	0.5397	0.5792	0.5619
Obs. Number	162	162	162	162	162	162

Note: *** Statistically significant at 1%

Source: own processing

Secondly, if we estimate GCI, DESI, Education and Control of Corruption, we observe that if the level of DESI increases with 1 unit, global cyersecurity will increse too with 1.14 units. Both control variables have a negative influence on the dependent variable. The R-squared is 0.5692 and it indicates that global cyersecurity level depends in proportion of 56.92% from DESI.

Then, if we estimate GCI, DESI, Education and Political Stability and Absence of Violence, we observe that if the level of DESI increases with 1 unit, global cyersecurity will increse too with 0.78 units. Both control variables have a negative influence on the dependent variable. The R-squared equals 0.4314 and it indicates that global cyersecurity level depends in proportion of 43.14% from DESI.

If we estimate GCI, DESI, Education and Regulatory Quality, we observe that if the level of DESI increases with 1 unit, global cyersecurity will increse too with 1.1 units. Both control variables have a negative influence on the dependent variable. The R-squared has the value 0.5483 and it indicates that global cyersecurity level depends in proportion of 54.83% from DESI.

If we estimate GCI, DESI, Education and Rule of Law, we observe that if the level of DESI increases with 1 unit, global cyersecurity will increse too with 1.15 units. Both control variables have a negative influence on the dependent variable. The R-squared has the value 0.5870 and it indicates that global cyersecurity level depends in proportion of 58.7% from DESI.

Lastly, if we estimate AML, DESI, Education and Voice and Accountability, we can observe that if the level of DESI increases with 1 unit, the money laundering risk will decrease with 1.12 units. Both control variables have a negative influence on the dependent variable. The R-squared has the value 0.5701 and it indicates that global cyersecurity level depends in proportion of 57.01% from DESI.

Our research hypothesis is accepted, for each situation, which means that an increasing of DESI will determine an increase of global cyersecurity level.

In order to conclude our regressions results, no matter what measurement method we will choose for digitalization, its increase will determine a decrease of the economic and financial crime under all its four forms: corruption, shadow economy, money laundering risk and cybercrime.

5. Conclusions

With the help of our research, we have covered a gap in the literature that has never before addressed economic and financial crime as an integrative concept of all its forms common in field studies, namely: corruption, underground economy, money laundering and cybercrime. Each of these shapes has been tested in turn to see how they are affected by the digitization process. The sample consisted of 185 from around the world, so that it was as comprehensive and relevant as possible. As variables of influence were chosen: education, GDP level and the 6 main forms of public governance.

As a general conclusion, digitalization is a phenomenon that manifested much more strongly once the COVID-19 pandemic determined us to restructure all the systems in which we operate, respectively the economy, public and private institutions, but also society as a whole. In this sense, following our study, both related to the existing literature and to the actual contribution of the paper, the digitalization process has a significant effect on the various components of economic and financial crime.

Firstly, by testing the relationship between digitalization and the degree of perception of corruption, we can conclude an increase in awareness of these crimes and a lower rate of their occurrence. Also, trying to determine how the proportion of the shadow economy in GDP fluctuates depending on the digitalization process, we found that it is also registers a regress. Then, testing the relationship that digitalization has with the risk of money laundering, we concluded that as a result of technological development, the risk of money laundering decreases. Finally, in the context of digitalization, the commitment of countries for cybersecurity is growing in order to raise awareness of its importance and different dimensions of the issue.

However, despite these trends, the risks should not be overlooked. From the category of solutions, education, in general, and financial education, in particular, must remain the main lever that will lead to the improvement of all the performances of a nation. In the context of increasing the digitalization of the economy, especially against the background imposed by the COVID-19 pandemic, cybercrime has grown at an alarming rate, so there is a collateral need for cyber-education that will help us to better protect our personal data and our financial resources.

Related to the practical policy implications, our research will be surely interesting for the specialists in the economic and financial field who face such problems along their activity. At the same time, our work informs the general audience about the risks to which they are exposed, and makes them aware of the need to protect themselves from economic and financial crime, especially during the pandemic, in which all activities are transformed into digital forms, and which will surely be transformed for a long time in this way. Also, in what concern the theoretical implications, we reached the gap of the literature of the field that we have stated at the beginning of our research.

The key is to use technology as a friend right next to us in every situation to help, not as an instrument to endanger others. We need to learn to use technology properly, but also to learn to fight against all existing types of economic and financial crime. The final purpose is to prevent and combat, not to commit it.

Regarding the limitations of our research, we used indicators of perception and risk throughout the study. In the future, in our next studies, we aim to cover these limits using values that summarize factual evidence of economic and financial crimes. Also, in order to obtain more consolidated results, in future research papers we will take into consideration more quantification methods for digitalization.

Acknowledgement: This work was supported by a grant from the Romanian Ministry of Education and Research, CNCS-UEFISCDI, project number PN-III-P4-ID-PCE-2020-2174, within PNCDI III.

Conflicts of Interest: The authors declare no conflict of interest.

References

ACCA Global (2017). Emerging from the shadows The shadow economy to 2025. Available at: https://www.accaglobal.com/content/dam/ACCA_Global/Technical/Future/pi-shadow-economy-report.pdf [Accessed on 2nd February 2022].

Achim, M. V., Borlea, N.S. (2020). Economic and Financial Crime: Corruption, Shadow Economy, and Money Laundering, *Studies of Organized Crime, Cham: Springer International Publishing*, Vol. 20.

Achim, M. V., Borlea, S. N., Văidean, V. L. (2021). Does technology matter for combatıng economıc and fınancıal crıme? A panel data study. *Technological and Economic Development of Economy*, Vol. 27, No. 1.

Achim, M. V., Văidean, V. L., Borlea, S. N., Florescu, D. R. (2021). The Impact of the Development of Society on Economic and Financial Crime. Case Study for European Union Member States, *Risks 2021*, 9(5), 97.

Achim, M.V., Borlea, N.S. (2019). Criminalitatea economico-financiară. Corupție, economie subterană și spălarea banilor. Cauze, efecte, soluții. Abordări teoretice și practice. *Ed. Economică, București.*

Aidt, T. S. (2010). Corruption and Sustainable Development. *Cambridge: Faculty of Economics*, No. CWPE 1061. Available at: https://www.repository.cam.ac.uk/bitstream/handle/1810/242086/cwpe1061.pdf;jsessionid533A12327621029A0EF0B6 86DD27C5E5C?sequence51 [Accessed on 7th February 2022].

Amoore, L., De Goede, M. (2005). Governance, risk and dataveillance in the war on terror. *Crime, Law and Social Change*, 43, 149-173.

Anderson, J. (2020), What can we learn from trends in corruption and anticorruption?. WorldBank.

Barker, I. (2022). Cybercriminals can penetrate 93 percent of company networks**.** *Beta News.* Available at: https://betanews.com/2021/12/20/cybercriminals-penetrate-93-percent-of-company-networks/ [Accessed on: 25th January 2022].

Basel AML Index. Assessıng money launderıng rısks around the world. Available at: https://index.baselgovernance.org/ [Accessed on 25th January 2022].

Bethencourt, C. (2022). Crime and social expenditure: A political economic approach, *European Journal of Political Economy*, 102183.

Bird, R. M., Zolt, E. M. (2008). Technology and Taxation in Developing Countries: From Hand to Mouse, *The University of Chicago Press Journals*, Vol. 61, No. 4.2.

Cieślik, A., Goczek, L. (2021). Who suffers and how much from corruption? Evidence from firm-level data. *Eurasian Business Review*. 2147-4281.

Columbus, L. (2020). How E-Commerce's Explosive Growth Is Attracting Fraud. Forbes. Available at: https://www.forbes.com/sites/louiscolumbus/2020/05/18/how-e-commerces-explosive-growth-is-attracting-fraud/?sh=68c94cba6c4b [Accessed on: 25th January 2022].

Dalli, M. (2019). Education as a tool against cybercrime. The European Files. Available at: https://www.europeanfiles.eu/industry/education-as-a-tool-against-cybercrime [Accessed on: 23rd January 2022].

De Goede (2008). *Risk, preemption and exception in the war on terrorist financing*. 1st Edition. Routledge.

Directorate General for Communication Special Eurobarometer 499. (2020). Europeans' attitudes towards cyber security (cybercrime), Available at: https://data.europa.eu/data/datasets/s2249_92_2_499_eng?locale=en [Accessed on 15th January 2022].

EAST (2021). Black box attacks. National & Global Fraud Intelligence sharing – 6th Interim EAST Meeting. Available at: https://www.association-secure-transactions.eu/tag/black-box-attacks/ [Accessed on: 23rd January 2022].

Elgin, C., Erturk, F. (2019). Informal economies around the world: measures, determinants and consequences. Eurasian Economic Review 9, 221-237.

Elgin, C., Oyvat, C. (2013). Lurking in the cities: Urbanization and the informal economy. *Structural Change and Economic Dynamics*, Vol. 27, 36-47.

European Comission (2021). One in five people in the EU at risk of poverty or social exclusion . Available at: https://ec.europa.eu/eurostat/web/products-eurostat-news/-/edn-20211015-1 [Accessed on: 25th January 2022].

European Comission (2022). Digital Economy and Society Index. Available at: https://digital-agenda-data.eu/datasets/desi [Accessed on: 15th January 2022].

European Commission (2014). Shadow Economy. Available at: http://ec.europa.eu/europe2020/pdf/themes/07_shadow_economy.pdf [Accessed on 30th January 2022].

European Union Agency For Cybersecurity (2021). Available at: https://www.enisa.europa.eu/topics/cybersecurity-education?tab=publications [Accessed on: 29th January 2022].

European Union Agency for Fundamental Rights. (2020). Fundamental Rights Report 2020. Available at: https://fra.europa.eu/sites/default/files/fra_uploads/fra-2020-fundamental-rights-report-2020_en.pdf [Accessed on 8th February 2022].

Europol. (2021). Money laundering. Available at: https://www.europol.europa.eu/crime-areas-and-statistics/crime-areas/economic-crime/money-laundering [Accessed on 25th January 2022].

Eurostat. (2020). Living conditions in Europe - poverty and social exclusion. Available at: https://ec.europa.eu/eurostat/statistics-explained/index.php?title=Living_conditions_in_Europe_-_poverty_and_social_exclusion [Accessed on 4th February 2022].

Federal Trade Commission (2021). FTC Data Shows Huge Spike in Cryptocurrency Investment Scams. New data spotlight points to more than ten-fold increase in reported losses in last 12 months. Available at: https://www.ftc.gov/news-events/press-releases/2021/05/ftc-data-shows-huge-spike-cryptocurrency-investment-scams?utm_source=govdelivery [Accessed on: 23rd January 2022].

Finews (2020). Revolut: Blocked Accounts. Available at: https://www.finews.com/news/english-news/42721-revolut-blocked-accounts-money-laundering [Accessed on: 23rd January 2022].

Forbes. (2022). Cybersecurity in 2022 – A Fresh Look at Some Very Alarming Stats. Available at: https://www.forbes.com/sites/chuckbrooks/2022/01/21/cybersecurity-in-2022--a-fresh-look-at-some-very-alarming-stats/?sh=3bb06ca96b61 [Accessed on: 25th January 2022].

Friedrich Schneider (2015). Shadow Work: Measurement. *International Encyclopedia of the Social & Behavioral Sciences (Second Edition),* 862-867.

Gartner (2020). Gartner Says By 2023, 65% of the World's Population Will Have Its Personal Data Covered Under Modern Privacy Regulations. Available at: https://www.gartner.com/en/newsroom/press-releases/2020-09-14-gartner-says-by-2023--65--of-the-world-s-population-w [Accessed on: 29th January 2022].

General Data Protection Regulation. Available at: https://gdpr-info.eu/ [Accessed on: 23rd January 2022].

Goel, R. K., Nelson, M. A. (2012), The internet as an indicator of corruption awareness, *European Journal of Political Economy***,** Vol. 28, Issue 1, 64-75.

Go-Globe (2021). Online Piracy in Numbers – Facts and Statistics [Infographic]. Available at: https://www.go-globe.com/online-piracy/ [Accessed on: 24th January 2022].

Gogolin, G. (2010). *The Digital Crime Tsunami. Digital Investigation*. Vol. 7, Issues 1–2, 3-8.

Herley, C., Florêncio, D. (2010). Nobody Sells Gold for the Price of Silver: Dishonesty, Uncertainty and the Underground Economy. *Economics of Information Security and Privacy*, 33-53.

https://blogs.worldbank.org/governance/what-can-we-learn-trends-corruption-and-anticorruption [Accessed on 10th February 2022].

Immordino, G., Russo, F. F. (2018). Cashless payments and tax evasion, *European Journal of Political Economy***,** Vol. 55, 36-43.

Insurance Information Institute. (2020). Facts + Statistics: Identity theft and cybercrime. Available at: https://www.iii.org/fact-statistic/facts-statistics-identity-theft-and-cybercrime [Accessed on 25th January 2022].

International Telecommunication Union. (2020). Global Cybersecurity Index. Available at: https://www.itu.int/en/ITU-D/Cybersecurity/Pages/global-cybersecurity-index.aspx [Accessed on 25th January 2022].

Johnson, J. (2021). Global consumers opinion on personal data control by tech companies 2021. Statista. Available at: https://www.statista.com/statistics/1233743/global-consumers-opinion-tech-personal-data/ [Accessed on: 23rd January 2022].

Joshi, M. (2020). Definition of Regulatory Technologies, Regtech. Available at: https://www.regtechtimes.com/defination-of-regulatory-technologies/ [Accessed on 7th February 2022].

Klapper, L. (2015). Financial Literacy Around the World, Insıghts from the Standard & Poor's ratıngs servıces global fınancıal lıteracy survey. Available at: https://gflec.org/wp-content/uploads/2015/11/Finlit_paper_16_F2_singles.pdf [Accessed on 8th February 2022].

Legal Jobs. (2022). 39 Worrying Cyber Crime Statistics [Updated for 2022]. Available at: https://legaljobs.io/blog/cyber-crime-statistics/ [Accessed on 26th January 2022].

Leția, A.A. (2014). *Investigarea criminalității în afaceri.* Ed. Universul Juridic, București.

Levi, M., Wall, D. S. (2004). Technologies, Security, and Privacy in the Post-9/11 European Information Society. *Journal of Law and Society*, Vol. 31, Issue 2, 194-220.

Markets and Markets (2021). Fraud Detection and Prevention Market. Available at: https://www.marketsandmarkets.com/Thanks/subscribepurchaseNew.asp?id=1312 [Accessed on: 29th January 2022].

Mordor Intelligence. (2020). Global antı-money launderıng solutıons market - growth, trends, Covıd-19 ımpact, and forecasts (2022 - 2027). Available at: https://www.mordorintelligence.com/industry-reports/anti-money-laundering-solutions-market [Accessed on 24th January 2022].

Nguyen, C. P. (2021). Does economic complexity matter for the shadow economy?. *Economic Analysis and Policy*, 73, 210-227.

Nilson Report (2020). Charts & Graphs Archive. Available at: https://nilsonreport.com/publication_chart_and_graphs_archive.php?1=1&year=2020 [Accessed on 23rd January 2022].

OECD. (2002). Glossary of statistical terms. Available online at: https://stats.oecd.org/glossary/detail.asp?ID=5081 [Accessed on 23rd January 2022].

OECD. (2009). Money Laundering Awareness Handbook for Tax Examiners and Tax Auditors. Available online at: https://www.oecd.org/ctp/crime/money-laundering-awareness-handbook-for-tax-examiners-and-tax-auditors.pdf [Accessed on 23rd January 2022].

Okunogbe, O., Pouliquen, V. (2018). Technology, Taxation, and Corruption : Evidence from the Introduction of Electronic Tax Filing, *World Bank Group, Open Knowledge Repository,* 8452.

Pettey, C. (2016). 5 Reasons Companies Need to Change Their Approach to Personal Data. Gartner. Available at: https://www.gartner.com/smarterwithgartner/5-reasons-companies-need-to-change-their-approach-to-personal-data [Accessed on: 24th January 2022].

Putniņš, T. J., Sauka, A. (2015). Measuring the shadow economy using company managers. *Journal of Comparative Economics*, Vol. 43, Issue 2, 471-490.

PwC (2020). PwC's Global Economic Crime and Fraud Survey 2020. Available at: https://www.pwc.com/gx/en/services/forensics/economic-crime-survey.html [Accessed on: 23rd January 2022].

Remeikiene, R., Gaspareniene, L., Bayar, Y., Ginevičius, R., Ragaišytė, I. M. (2021). ICT development and shadow economy: Empirical evidence from the EU transition economies, *Economic Research-Ekonomska Istraživanja*.

Remeikiene, R., Gaspareniene, L., Schneider, F. G. (2018). The defınıtıon of dıgıtal shadow economy. *Technological and Economic Development of Economy*, Vol. 24, No. 2.

Renolon. (2022). 24+ Alarming Money Laundering Statistics You Need to Know in 2021. Available at: https://www.renolon.com/money-laundering-statistics/ [Accessed on 25th January 2022].

Sabău (Popa), A.I. , Achim M. V., Safta I. L. (2021). Does corporate governance may enhance the digitalization process? A panel data analysis. 23rd RSEP International Economics, Finance & Business Conference Conference Proceedings, 287-302.

Sadgali, I., Sael, N., Benebbou, F. (2019). Performance of machine learning techniques in the detection of financial frauds. *Procedia Computer Science*, Vol. 148, 45-54.

Slemrod, J. (1990). Optimal Taxation and Optimal Tax Systems, American Economic Association. *Journal of Economic Perspectives*, Vol. 4, No. 1, 157-178.

Smith, G. S. (2015). Management models for international cybercrime. *Journal of Financial Crime*, Vol. 22, Issue 1.

Statista (2017). Media piracy in the U.S. and worldwide. Available at: https://www.statista.com/study/42923/media-piracy-worldwide/ [Accessed on: 24th January 2022].

Statista. (2021). Digital transformation. Available online at: https://www.statista.com/topics/6778/digital-transformation/ [Accessed on 2nd February 2022].

Sutherland, E.H. (1940), *White-collar criminality.* Holt, Rinehart & Winston, New York.

Tapscott, D. (2015). *The Digital Economy - Anniversary Edition: Rethinking Promise and Peril in the Age of Networked Intelligence.* McGraw Hill, 2nd Edition.

The World Bank (2022). Gross Domestic Product. Available at: https://data.worldbank.org/indicator/NY.GDP.MKTP.CD [Accessed on: 15th January 2022].

The World Bank (2022). Worldwide Governance Indicators. Available at: https://databank.worldbank.org/source/worldwide-governance-indicators [Accessed on: 15th January 2022].

Transparency International. (2022). Corruption Perception Index. Available at: https://www.transparency.org/en/cpi/2021 [Accessed on: 15th January 2022].

United Nations Development Programme (2022). Human Development Reports. Education Index. Available at: https://hdr.undp.org/en [Accessed on: 15th January 2022].

Williams, J. W. (2013). Regulatory technologies, risky subjects, and financial boundaries: Governing ‘fraud’ in the financial markets. *Accounting, Organizations and Society*, Vol. 38, Issues 6–7, 544-558.

World Economic Forum (2020). Technological adoption. Available at: https://www.weforum.org/reports/the-future-of-jobs-report-2020/in-full/2-1-technological-adoption [Accessed on: 23rd January 2022].

Zorz, M. (2015). Global black markets and the underground economy. Help Net Security. Available at: https://www.helpnetsecurity.com/2015/05/18/global-black-markets-and-the-underground-economy/ [Accessed on: 24th January 2022].

Zuboff, S. (2019). *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*. Profile Books.