Contributions to Finance and Accounting

Monica Violeta Achim *Editor*

Economic and Financial Crime, Sustainability and Good Governance

Springer

Contributions to Finance and Accounting

The book series ‘Contributions to Finance and Accounting’ features the latest research from research areas like financial management, investment, capital markets, financial institutions, FinTech and financial innovation, accounting methods and standards, reporting, and corporate governance, among others. Books published in this series are primarily monographs and edited volumes that present new research results, both theoretical and empirical, on a clearly defined topic. All books are published in print and digital formats and disseminated globally.

Monica Violeta Achim
Editor

Economic and Financial Crime, Sustainability and Good Governance

Springer

Editor
Monica Violeta Achim
Faculty of Economics and Business
Administration
Babeș-Bolyai University
Cluj-Napoca, Romania

ISSN 2730-6038 ISSN 2730-6046 (electronic)
Contributions to Finance and Accounting
ISBN 978-3-031-34081-9 ISBN 978-3-031-34082-6 (eBook)
https://doi.org/10.1007/978-3-031-34082-6

This Springer imprint is published by the registered company Springer Nature Switzerland AG
The registered company address is: Gewerbestrasse 11, 6330 Cham, Switzerland

Acknowledgement

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

About the Book

The book titled "Economic and Financial Crime, Sustainability and Good Governance" deals with the financial crime issues regarding its most spread forms of our days, respectively corporate frauds, corruption, tax fraud, shadow economy, informal entrepreneurship, money laundering, international informal capital flows, cybercrimes, cryptocurrency scams. In the context of a high increase of digitalization, especially due to the Covid-19 pandemic context, the financial crime has recognized a huge increase especially in the form of cybercrime, affecting the financial security of people. Governances issues are essential drivers of the sustainable economy while one cannot be about sustainability without accounting on strong measures to fight against financial crime.

The aim of this book is to stress to connectivity between the financial crimes and good governance, in order to achieve the most suitable sustainable development of the society. This work describes the evolution of various types of financial crime regarding its most spread forms of our days, respectively corporate frauds, corruption, tax fraud, shadow economy, informal entrepreneurship, money laundering, international informal capital flows, cybercrimes, cryptocurrency scams. Then, its effects on sustainable development are highlighted on reducing volume of state budget, volume and quality of public services, the degree of business development and performance, reducing the soundness of financial-banking institutions, and eventually reducing the level of poverty and social inequality. In order for the measures to combat financial crime to be effectively applied, knowing the profile of the fraudster is extremely important. The types of countermeasures that should be adopted by a good public and corporate governance are presented in detail, as well. The role of preventive measures in the form of investments in anti-fraud programs and investments in education is underlined, as well.

The book contains 15 chapters divided into four main parts, presented in short as follows:

Part I "Financial Crimes Around the World: The Landscape Around the World Countries" includes three chapters that provides a general screen of the level of economic and financial crime around the world countries, enhancing the level of tax

compliance, tax morale, corruption, money laundering, frauds in banking system or the relationship between illegal logging and corruption in different world countries.

Part II "Economic and Political Determinants of Financial Crime" consists in two chapters that highlights that agriculture, cash in labour, trust morale, trust in tax and social security authorities, economic development, urbanization are important determinants of the level of informal entrepreneurship. In addition, it is reflected that the tax wedge represents another important factor with a positive influence on the shadow economy.

Part III "The Effects of Economic and Financial Crimes on the Society" includes five chapters reflecting the impact of corruption on human well-being, the impact of cybercrimes on the business environment in the digital era, the effects of economic and financial crime on the government budget and the quality of public services, effects on the economic and sustainable development and on the poverty and social inequality or the negative effects on soundness of financial-banking institutions and on the business development

Part IV " Fighting Financial Crimes Strengthens the Sustainable Economy" includes five chapters referring to policy and regulatory framework on fighting financial crime for developing sustainable economy models, strengthening the EU fight against money laundering to promote sustainable economic models, an overview of forensic accounting and its effectiveness in the detection and prevention of fraud, cyber-attacks, cryptoccurency, and cybersecurity, cyber-risk insurance framework considerations.

The present book is useful for managers and policy makers to provide important avenues that may help in reaching the 2030 Agenda for Sustainable Development, adopted by all United Nations Member States in 2015, by eradication of all the types of economic and financial crimes in order to achieve the most suitable sustainable development of the society.

Contents

Part I
Financial Crimes Around the World: The Landscape Around the World Countries

Chapter 1
Comparative Case Study on Economic and Financial Crime in Germany and Romania

Sandra Clement and Monica Violeta Achim

Abstract With the scientific work, a contribution is made to the investigation of the perception of economic and financial crime in Germany and Romania. With a survey in 2022 in the respective country with 1742 answers from Germany and 1856 answers from Romania, a statistically relevant database could be created. Using the chi-square model and intensity scoring in conjunction with the survey, the results show that there are some similarities in terms of the influence of education and age. Occupation exerts only a partial influence. Gender, in turn, does not show a specific pattern of behavior. The results also show different levels of tax honesty and tax morality, which can be explained by the fact that the Romanian government provides incentives for earlier payment of taxes. It also became clear that the level of corruption in Romania is almost twice as high as in Germany. These comparative analyses reflect the importance of the role that education plays in building high tax morale and tax compliance. Improving the educational system and the general education of citizens through various information campaigns and presenting the negative consequences of economic and financial crimes can be an important way to reduce the prevalence of illegal activities.

Keywords Germany · Romania · Corruption · Money laundering · Tax evasion · Education

JEL Classification D73 · G18 · H26 · H75

S. Clement · M. V. Achim (✉)
Faculty of Economics and Business Administration, Babeș-Bolyai University, Cluj-Napoca, Romania
e-mail: monica.achim@econ.ubbcluj.ro

M. V. Achim (ed.), *Economic and Financial Crime, Sustainability and Good Governance*, Contributions to Finance and Accounting,
https://doi.org/10.1007/978-3-031-34082-6_1

1 Introduction

Germany is a country that has the lowest perception of occurrences within the shadow economy (fifth place within the EU (Medina & Schneider, 2022)), and Romania belongs to the lower stratum (third last country in the EU (Medina & Schneider, 2022)). This statistic raises the interest to conduct a comparative survey between Germany and Romania, investigating the perception of economic and financial crime. Based on various scholarly articles examining economic crime in Germany and Romania (Medina & Schneider, 2022; Achim & McGee 2023; Entorf & Spengler, 2002), it can be assumed that different behavioral patterns are observed in Germany than in Romania. In addition to the behavioral patterns, the perception of the different economic and financial crimes may also be of different nature. This finding, which has been discussed in public, will now be investigated with the survey. The results may shed light on whether the values of Medina & Schneider (2022) are reflected in people's perceptions and whether country-specific measures need to be taken to combat economic and financial crime or whether a global campaign is possible. In addition, the comparison represents a contribution to the adaptation of possible successful approaches of countries. Thus, it is possible that Romania can learn from a possible policy of the Germans or vice versa.

2 Delimitation of the Behavior Patterns of Germany and Romania

At the beginning of the chapter, the differences between Germany and Romania in terms of geographical, economic, and political factors are described, which underline the need to analyze the different behavioral patterns regarding economic and financial crime.

2.1 Geographical Delimitation

Germany is located in the center of Europe surrounded by nine countries (Denmark, the Netherlands, Belgium, Luxembourg, France, Switzerland, Austria, Czech Republic, and Poland). No other country in Europe has more neighboring countries. In addition, Germany has access to the sea with North Sea and the Baltic Sea Germany covers 357,592 square kilometers (Federal Statistical Office, 2023), making it the fourth largest country in the EU. Romania, on the other hand, is located in southeastern Europe and has countries such as Bulgaria, Serbia, Hungary, Ukraine, and Moldova as neighbors. The country is also bordered by the sea, namely the Black Sea. Romania covers an area of 238,390 square kilometers (European Union, 2023).

With the findings, much can be said about the conditions of a country. Germany is located in the center of Europe, which is an advantageous position in trade with the EU. Likewise, Germany is surrounded by many states, which invites cooperation and alliances, creating trade advantages and political stability and security. Considering the countries that surround it, Germany is also in a much more comfortable situation than Romania. The richest countries in terms of GDP are Germany, France, Italy, Spain, and the Netherlands. These countries already account for 68% of the total GDP in the EU. All economically strong countries border Germany. Romania, on the other hand, has neighboring countries that account for about 1% of the total GDP of the EU (Statista, 2023).

2.2 Economic Delimitation

The economic situation in Romania is considered rather difficult. The country's transformation into a market economy system is seen as sluggish compared to other Eastern European countries. The country has to contend with many setbacks, such as corruption, a lack of legal security, bureaucratic arbitrariness, and other hurdles. Although it is evident that Romania has made significant progress in the economy, statistics show that Romania is still the second poorest country in the EU. The statistics on the unemployment rate of 5.7% (2016) underline the difficult situation once again. However, it can also be seen that the country is making great efforts through economic reforms such as tax cuts and measures to combat financial and economic crime. This should create a better investment climate and enable jobs (National Agency for Civic Education). Germany is a highly developed country and has been one of the most developed countries since joining the EU. Germany is a country with a very high gross domestic product (Germany: 38.982 per inhabitant; Romania 24.043 per inhabitant) in 2022 (Statista, 2022). The unemployment rate of 3.14% also suggests that there is a high level of economic utilization. If the exported goods of Germany are considered here approx. 1,700,000 million euros (20.36 million euros per 1000 inhabitants) are turned over, while in Romania it is 100,000 million euros (5.12 million euros per 1000 inhabitants). In terms of imported goods, in Germany it is 1,500,000 million euros (18.04 million euros per 1000 inhabitants), while in Romania it is 110,000 million euros (5.84 million euros per 1000 inhabitants) (Country Data, 2023).

In terms of economic differences, Germany is a strong import and export country, with a high GDP and a low unemployment rate due to its economic strength. In Romania, on the other hand, there are major obstacles such as corruption and a clear deficiency in the economic situation, which is associated with high unemployment and expandable imports and exports.

2.3 Political Delimitation

The political reform of Gorbatschow initiated in the 1980s was not supported by the political leadership, which had the result that the attitude within the country underwent a change. The people distanced themselves more and more from the Soviet Union and discontent grew. Only after Ceausescu's fall in 1989 was the country able to embark on the path of democracy. After the Ceausescu overthrew the government, there was a constant change of parties and party leaders (National Agency for Civic Education, 2023). This strong fluctuation makes it difficult to conduct a constant policy in which consistent and targeted measures can be implemented. In Germany, on the other hand, the country was divided for the first time into West and East with two independent developments and all spheres of life. It was not until 1989 that the country was reunified and a unification of the country could be sought. After the Second World War, four parties were in power with similar orientations, which made it possible to implement a stringent strategy and stick to measures and political reforms that had been started (Federal Government of Germany, 2023).

In addition to the form of government, the political orientation of education is also an essential building block for a country. Basically, it is clear that education is the key to a country's success and the foundation of all science and progress (Schleicher, 2006; Khasanova, 2021; Madani, 2019). With the collapse of Germany in 1945, one of the first concerns was to drastically reform the nation's education system. The past made it clear that Nazi policy's lack of enlightenment resulted in grievances in all areas. Thus, it became clear that a complete transformation had to be carried out in the social, political, and economic spheres in order to prepare the country for the future. When looking at the development of Romanian education, one of the most dramatic statements made by Tascu et al. (2002) is that 80% of Romanian students aspire to study but cannot afford to do so (Tascu et al. (2002)).

3 Methodology and Data

The methodology of the survey was chosen following the publication of Achim and McGee (2023). Their work is based on a survey in Romania, which achieved 1856 responses. The survey is based on qualitative and ordinal scaled variables dealing with the different forms of economic and financial crime. Following the work of Achim and McGee (2023) for Romania, in this chapter we replicated a similar survey for the case of Germany. Based on these results, we intend to find the main differences between financial crime community pulse in Germany compared with Romania.

3.1 Hypotheses Research

Therefore, in this chapter the following hypotheses research are stated:

1. Referring to Tax Compliance

Hypothesis 1.1: What is the dependency between tax compliance/tax morale and age in a comparison between Romania and Germany?
Hypothesis 1.2: What is the dependency between tax compliance/tax morale and gender in a comparison between Romania and Germany?
Hypothesis 1.3: What is the dependency between tax compliance/tax morale and education in a comparison between Romania and Germany?
Hypothesis 1.4: What is the dependency between tax compliance/tax morale and professional status in a comparison between Romania and Germany?

2. Referring to Perception Level of Corruption

Hypothesis 2.1: What is the dependency between perception level of corruption and age in a comparison between Romania and Germany?
Hypothesis 2.2: What is the dependency between perception level of corruption and gender in a comparison between Romania and Germany?
Hypothesis 2.3: What is the dependency between perception level of corruption and education in a comparison between Romania and Germany?
Hypothesis 2.4: What is the dependency between perception level of corruption and professional status in a comparison between Romania and Germany?

3. Referring to Money Laundering Risk

Hypothesis 3.1: What is the dependency between money laundering risk and age in a comparison between Romania and Germany?
Hypothesis 3.2: What is the dependency between money laundering risk and gender in a comparison between Romania and Germany?
Hypothesis 3.3: What is the dependency between money laundering risk and education in a comparison between Romania and Germany?
Hypothesis 3.4: What is the dependency between money laundering risk and professional status in a comparison between Romania and Germany?

3.2 Sample and Method

The German survey is an online survey, which should reach a broad mass of participants. Thus, the survey was placed on various platforms, such as LinkedIn, Xing, Instagram, and Facebook, personal networks (relatives, friends, sports group, mother–child groups, and former study colleagues), three different banking institutions, eight different companies (work colleagues, suppliers, and customers), and four different universities. With the mailing of the surveys to the different groups of

people, we asked at the same time to forward them to their contacts, which resulted in a quick multiplication. The survey was active from October 19, 2022, to November 09, 2022. Thus, within 22 days the answers were collected. The selection of the group of participants is intended to ensure both a heterogeneous group in terms of interests, residence, and age and different employment statuses, thus covering a broad range of bands.

The Germany survey refers to nine questions, as they are presented in the Appendix.

The first five questions are referring to the investigation of different patterns of economic and financial crime, while the last four questions refer to investigation of the biological and social patterns of respondent such as age, gender, level of education, and professional status.

The first question covers tax compliance in the form of meeting the tax payment deadline. More exactly, question 1 was formulated as follows: "Which of the following behavior patterns applies to you when it comes to paying taxes?". Three answer choices were possible: (1) pay taxes long before the deadline, (2) pay taxes at a time very close to the deadline, and (3) are generally late in paying taxes. Multiple selection is not possible.

The second question asks about tax morale, ranking behavior, and what attitude a person has toward tax fraud. The specific second question asks, "What behavior applies when visiting a restaurant, hairdresser, hotels, or similar?". Answer choices are as follows: (1) You will always receive a receipt, (2) you always ask for a receipt, (3) you receive a receipt but do not take it with you, and (4) you do not mind if you do not receive a receipt. In this case, multiple choice is possible.

The third area in the shadow economy represents the perception level of corruption, which was formulated as follows: "How would you rate the level of corruption in German public institutions (schools, old people's homes, sports grounds, cemeteries, theaters...) on a scale of 1 (very low) to 5 (very high)?" Five answer options are possible as below: (1) very low level of corruption, (2) low level of corruption, (3) medium level of corruption, (4) high level of corruption, and (5) very high level of corruption. Multiple choices are not possible.

The following two questions, which include questions 4 and 5, are about money laundering. The fourth question refers to the detection of money laundering activities by means of questioning on the part of bank employees. Specifically, question 4 is as follows: "In terms of money laundering risk, do you think people are capable of detecting a suspicious transaction in business?". The following response options can be selected: (1) high ability, (2) medium ability, (3) low ability, and (4) very low ability. Multiple selections are not possible.

The last and fifth question refers to the customer's willingness to cooperate in providing information to bank employees about the origin of the money. The question is as follows: "When you or people close to you make a bank transaction (deposit/withdrawal) and the bank employee asks you to provide some information about the origin of the money or the whereabouts of the amount. How do you respond?". The answer choices are as follows: (1) you provide the requested information because you know that bank employees are just doing their job,

(2) you are upset about the requested information, but provide information, and (3) you refuse to provide information.

Questions 6 to 9 ask about age, gender, level of education, and professional status.

3.3 Variables and Data

Several dependent variables were used in the survey. In the superordinate form, the dependent variable represents economic and financial crime under the form of tax compliance, tax morale, corruption, and money laundering. Then, the independent variables are expressed by age, gender, level of education, and professional status.

In addition to the description, analysis, and identification of correlations of achieved results, several scores are also calculated, for each category of financial crime. The mentioned scores serve as average frequencies and contribute to simplified comparability. The scores are formed in the context of the independent variables (age, gender, education, and professional status). The scores for the individual patterns of economic and financial crime are calculated according to Achim and McGee (2023) as follows:

$$\text{Q1 : Tax compliance score} = (1 \times \text{N1} + 2 \times \text{N2} + 3 \times \text{N3})\,\text{i} \tag{1.1}$$

The numbers 1–3 represent the answer choices related to the question of the behavior when paying the tax burden:

1. Pay taxes long before the deadline
2. Pay taxes at a time very close to the deadline
3. Are generally late in paying taxes

N1–N3 refer to the relative frequency in percent of responses 1–3, within the different determinants "i" (age, gender, education, and professional status). The score ranges from 1 (best tax compliance attitude) to 3 (worst tax compliance attitude).

The second score includes tax morale. The following formula was used:

$$\text{Q2 : Tax morale score} = (1 \times \text{N1} + 2 \times \text{N2} + 3 \times \text{N3} + 4 \times \text{N4})\,\text{i} \tag{1.2}$$

Variables 1–4 refer to the answers describing the behavior when visiting a restaurant, hairdresser, or hotels regarding the receipt of a bill.

1. You will always receive a receipt
2. You always ask for a receipt
3. You receive a receipt but you do not take it with you
4. You do not mind if you do not receive a receipt

Variables N1–N4 include the frequency of responses distribution of options 1–4, within category "i" (age, gender, education, and professional status). Again, the score covers the range of 1 (high tax morale)–4 (low tax morale).

The corruption perception score can be determined using the third question. The score is determined using the following formula:

$$\begin{aligned} &\text{Q3 : Corruption perception score} \\ &\quad = (1 \times \text{N1} + 2 \times \text{N2} + 3 \times \text{N3} + 4 \times \text{N4} + 5 \times \text{N5})\ \text{i} \end{aligned} \tag{1.3}$$

Variables 1–5 represent the response options, which are intended to express the level of corruption perception.

1. Very low level of corruption
2. Low level of corruption
3. Medium level of corruption
4. High level of corruption
5. Very high level of corruption

The values N1–N5 represent the relative frequency of the answers 1–5 and are expressed in percent, in the category "i" (age, gender, education, and professional status). The calculated score ranges from 1 (very low perception of corruption) to 5 (very high perception of corruption).

The next function represents the estimated ability to detect money laundering transactions by bank employees and is asked in question 4.

$$\begin{aligned} &\text{Q4 : Anti} - \text{money laundering skills} \\ &\quad = (1 \times \text{N1} + 2 \times \text{N2} + 3 \times \text{N3} + 4 \times \text{N4})\ \text{i} \end{aligned} \tag{1.4}$$

Numbers 1–4 represent the response options in terms of money laundering level.

1. High ability
2. Medium ability
3. Low ability
4. Very low ability

The variables N1–N4 represent the relative frequency of the answer options 1–4 in the context of the category "i" (age, gender, occupational status, and level of education). The score behaves within the range between 1 (very low ability to detect money laundering) and 4 (high ability to detect money laundering).

The last equation refers to the last question, which refers to the willingness to cooperate in the form of KYC processes in connection with questions from bank employees about the origin of the money.

$$\text{Q5 : Cooperation money laundering} = (1 \times \text{N1} + 2 \times \text{N2} + 3 \times \text{N3})\ \text{i} \qquad (1.5)$$

Numbers 1–3 refer to the answer options.

1. You provide the requested information because you know that bank employees are just doing their job
2. You are upset about the requested information, but provide information
3. You refuse to provide information

The values N1–N3 represent the relative frequency of the answers 1–3 and are expressed in percent, in the category "i" (age, gender, education, and professional status). The score ranges from 1 (very high willingness to cooperate) to 3 (low willingness to cooperate).

Differing from the Romanian survey, the score for tax compliance was recalculated by me. The reason for this is that in Romania there is the possibility to pay the tax early in order to get a 10% discount. This possibility does not exist in Germany. In the Romanian survey, there are four choices for question 1: "Regarding paying your tax duties, which one of the following behavior is common for you and people around you," which include 1-long before the deadline, no matter discounts, and 2-long before the deadline to benefit of discounts. These choices could not be made in Germany, so the Romanian score had to be recalculated to ensure comparability. In addition to the descriptive description of the results and the determined score, the values are examined for correlation and compared using the statistical methods of the chi-Square model and the intensity assessment.

4 Results

4.1 Comparison Based on Correlation Model

In both the German and Romanian surveys, the chi-square test states that there is no relationship between two categorical variables. Thus, for both surveys, it can be inferred that the variables are not independent of each other and there is a statistically significant relationship between the perception of economic and financial crime. Now, it is interesting to know how strongly the factors are related to the different manifestations in comparison between Germany (DEU) and Romania (RO) (Tables 1.1 and 1.2).

A closer look at the intensity of the German and Romanian results shows that all Romanian contingency coefficients are below 0.3, indicating low intensity. The German results range from a very low intensity of 0.09 (Q5: gender) to a strong intensity of 0.5 (Q2: age, Q2: education, Q2: occupational status). Here, a clear difference in the correlation intensity of the Romanian and German survey becomes apparent.

Table 1.1 Chi-square test comparison in Germany/Romania

Variables	Age		Gender		Education		Professional status	
Country	DEU	RO	DEU	RO	DEU	RO	DEU	RO
Q1—Tax compliance	301.63	48.2	10.24	9.14	123.85	28.98	76.94	34.99
	(0.000)	(0.000)	(0.006)	(0.028)	(0.000)	(0.004)	(0.000)	(0.000)
Q2—Tax morale	638.91	59.47	254.05	2.94	650.54	21.8	629.49	51.23
	(0.000)	(0.000)	(0.000)	(0.568)	(0.000)	(0.150)	(0.000)	(0.000)
Q3—Perception of corruption	512.66	37.64	149.05	9.3	405.21	46.84	159.90	15.99
	(0.000)	(0.010)	(0.000)	(0.054)	(0.000)	(0.000)	(0.000)	(0.453)
Q4—AML skills	125.45	121.05	21.04	7.66	230.06	49.4	331.57	72.22
	(0.000)	(0.000)	(0.000)	(0.105)	(0.000)	(0.000)	(0.000)	(0.000)
Q5—Attitude toward KYC procedures	308.70	59.91	14.66	8.00	59.49	27.62	289.58	38.16
	(0.000)	(0.000)	(0.0007)	(0.018)	(0.000)	(0.001)	(0.000)	(0.000)

Source: German values: own calculation; Romanian values: Achim and McGee (2023)

Table 1.2 Intensity assessment comparison in Germany/Romania

Variables	Age		Gender		Education		Professional status	
Country	DEU	ROU	DEU	ROU	DEU	ROU	DEU	ROU
Q1—Tax compliance	0.076	0.159	0.258	0.07	0.258	0.124	0.206	0.136
Q2—Tax morale	0.518	0.176	0.357	0.04	0.521	0.108	0.515	0.164
Q3—Perception of corruption	0.316	0.141	0.281	0.071	0.434	0.157	0.290	0.092
Q4—AML skills	0.259	0.247	0.109	0.064	0.342	0.161	0.400	0.194
Q5–Attitude toward KYC procedures	0.388	0.172	0.091	0.066	0.182	0.121	0.378	0.142

Source: German values: own calculation; Romanian values: Achim and McGee (2023)

A closer analysis of age (Fig. 1.1) and the associated factors influencing economic and financial crime reveals that the highest score (0.259) in the Romanian survey was obtained for AML skills (Q4). In Germany, on the other hand, the highest intensity was found between age and tax morale (Q2). The intensity of tax compliance (Q1) and AML skills (Q4) find convergence in the Romanian and German values. For the other intensity values (Q2, Q3, and Q5), there is almost an opposite development. When considering gender, an almost mirrored development can also be observed for tax compliance, tax morale, and perception of corruption. For money laundering issues (Q4, Q5), there is a convergence and the intensity strength is very similar.

In terms of education (Fig. 1.2), it is clear that there is a high intensity in Germany, especially in the first four categories (Q1-Q4). Education in Germany plays an important role in combating financial and economic crime compared with Romania. This difference is the most significant in the case of tax morale. Moreover,

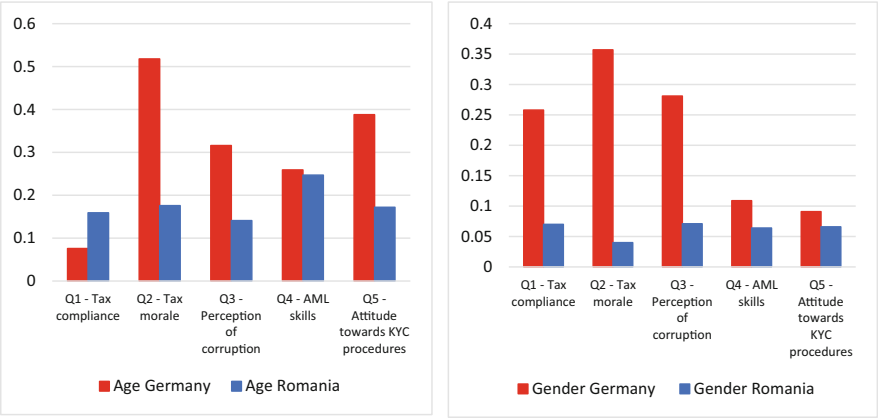


Fig. 1.1 Intensity assessment economy and financial crime and age/gender. Source: Own composition, Romanian values based on Achim and McGee (2023)

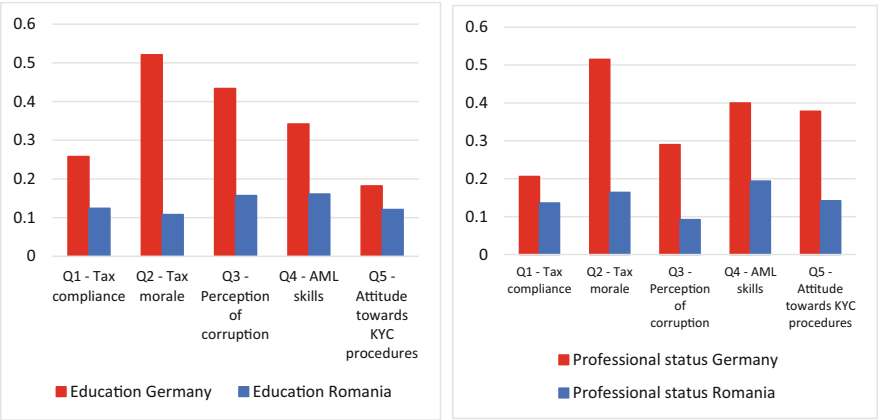


Fig. 1.2 Intensity assessment economy and financial crime and education/professional status. Source: Own composition, Romanian values based on Achim and McGee (2023)

we have to consider the fact that tax morale is a characteristic formed in centuries, so for this reason the level of education in Germany is so important and the German people are more compliant. Various scholars can confirm the link between the shadow economy and education. Some scholars found that there is a negative correlation, confirming the results of the survey, the higher the level of education, the lower the economic crime (Dabla-Norris et al., 2008; Saha et al., 2021; Melgar et al., 2010; Mocan, 2008). The course is particularly contrasting for the tax morale. In the German survey, the peak rises to 0.5. The Romanian survey finds its low point here (0.1). The categories are as follows: Q1: tax compliance, Q4: AML skills, and Q5: attitude toward KYC procedure converge. When looking at the professional

relationship, an almost identical trend is evident at different intensity levels. The values are most similar for tax compliance (Q1), while tax morale (Q2) has the highest gap. Here, the values of the German survey peak (0.5), while the values of the Romanian survey remain at a low level (0.1). From Q3 onward, the values are almost the same, with a gap of 0.1.

4.2 *Descriptive Comparison Based on Age*

In the following, we take a closer look at the results in descriptive form. First, we look at the results as a function of age. With regard to tax compliance, it can be seen that contrasting attitudes emerge within the countries. While the age groups of the Romanian and German surveys between 26 and 45 years are almost identical, the values of the 16- to 25 -year-olds and the 46- to 65 -year-olds are slightly different. In both divergent age groups, tax compliance worsens by about 0.5 score points for the German respondents. Looking fundamentally at tax compliance, it is clear that the level in Romania is better than in Germany. It is also evident that the level in Romania is almost constant in all age groups.

When looking at tax morale, it is evident that the Germans have worse morale than the Romanians. While in Germany the 16- to 25-year-olds and the 46- to 65-year-olds have the lowest tax morale, it is the 26- to 45-year-olds who place a higher value on morale. In contrast, the values in Romania are almost constant (Fig. 1.3).

When looking at the perception of corruption, it becomes clear that here, too, there is an almost contrasting relationship between Romania and Germany. The level differs by 2 score points, with a significantly higher level of corruption found in

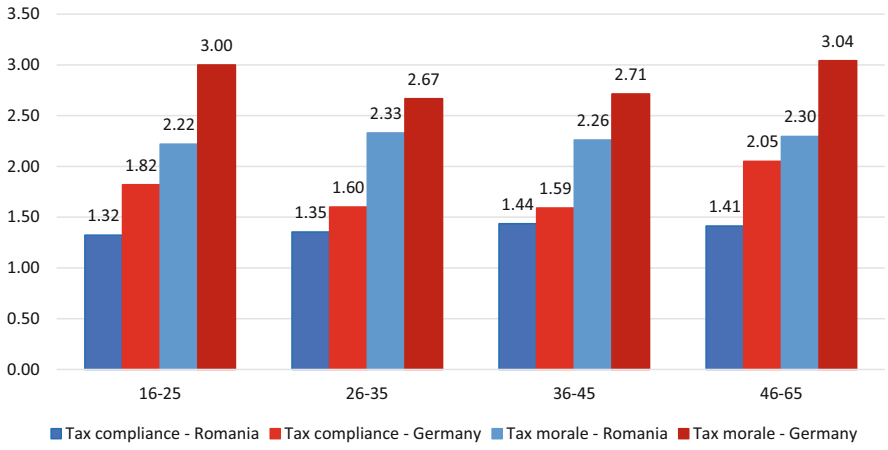


Fig. 1.3 Tax score by age–comparison in Germany/Romania. *Note:* Data survey, with a sample of 1742 individuals. Source: Own composition based on the survey

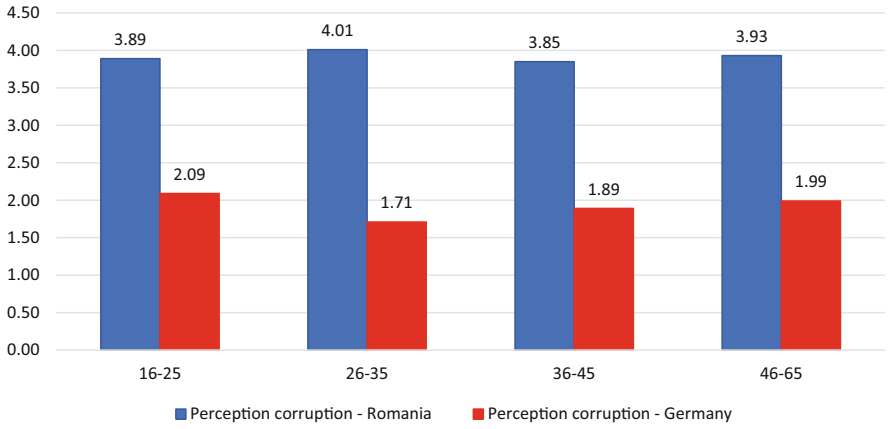


Fig. 1.4 Perception level of corruption score by age–comparison in Germany/Romania. Note: Data survey, with a sample of 1742 individuals. Source: Own composition based on the survey

Romania. The 2 score point difference says that the perception varies from low to very high. Basically, there are no large swings in either Germany or Romania. In Germany, all groups of people hold themselves almost constant, except for the 26- to 35-year-olds, who perceive slightly less corruption. In Romania, on the other hand, all respondents remain constant except for the 26- to 35-year-olds, who perceive a slightly higher level of corruption. The group of persons between 26 and 35 years of age also experiences a slightly opposite trend in Germany than in Romania (Fig. 1.4).

Money laundering is examined in more detail as a function of age. When looking at the attribution of competence to bank employees, it becomes clear that Romanians still have slightly more trust in bank employees at a young age than at the age of 26 and older. It is also striking that young Romanian respondents between 16 and 25 attribute a higher level of competence to bank employees than young German respondents. In Romania, there is a constant progression from the age of 26 onward to an assessment of the low level of competence of bank employees. In Germany, on the other hand, there is an almost constant progression to a low to medium level.

Finally, we look at the willingness to cooperate in checking possible money laundering transactions. Basically, it can be said here that both the German and Romanian respondents are very cooperative. Overwhelmingly, they cooperate with a great understanding of the work and the questions. In Germany, there is a rising line from the young age to the older generation. This ranges from a very high and understanding willingness to cooperate to a willingness to cooperate with a lack of understanding. This means that the respondents are willing to cooperate at a young age and have an understanding that decreases with age. In Romania, there is a constant line across all groups of people. They consider that they do cooperate, but a part has a high understanding and the other half without understanding. There is a small improvement from year 36 (Fig. 1.5).

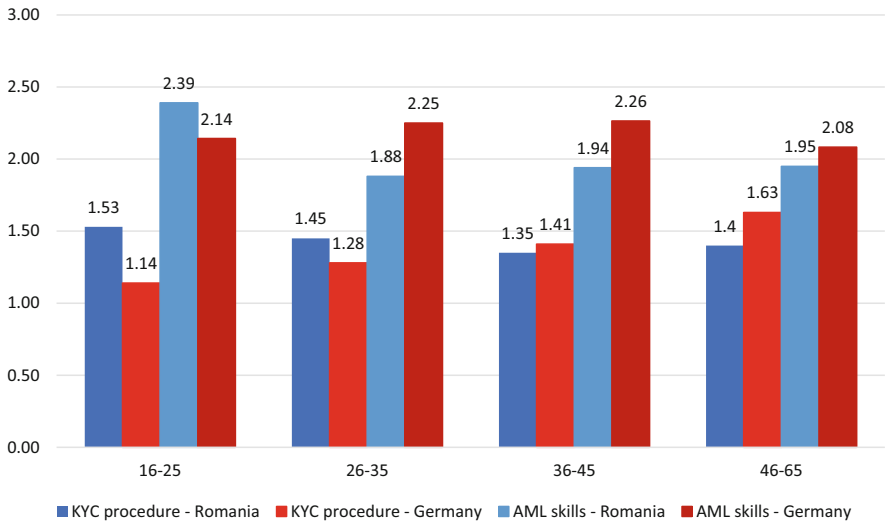


Fig. 1.5 Money laundering score by age–comparison in Germany/Romania. *Note:* Data survey, with a sample of 1742 individuals. Source: Own composition based on the survey

4.3 Descriptive Comparison Based on Gender

In the following figures, the results are compared by gender. Surprisingly, there is only a minimal difference between women and men in both Romania and Germany. Neither in Germany nor in Romania are gender-specific tax peculiarities discernible here.

When it comes to tax compliance, Romanian men and women are somewhat more lax than their German counterparts. When it comes to tax compliance, it is the other way around. Here, the German men and women have a worse attitude regarding tax morality than the Romanian respondents.

From the results, it is clear that tax compliance is perceived as more important than tax morality in both countries. However, no gender-specific behavioral pattern can be discerned (Fig. 1.6).

With regard to the perception of corruption, it can be seen in both Romania and Germany that women have a minimally higher perception of corruption than men. In Romania, it is 0.2, and in Germany, 0.1. In addition, it can be seen that in Romania both men and women perceive a significantly higher level of corruption than in Germany (shift of about 2 score points) (Fig. 1.7).

In the next category of money laundering, German men are more confident (men: 2.27; women: 2.1) than women about the ability of bank employees to detect money laundering transactions. Romanian men, on the other hand, have almost the same opinion as women. When looking at the level, the Romanian and German women are almost equal (about 2.1) by which an identical perception of banking competence is

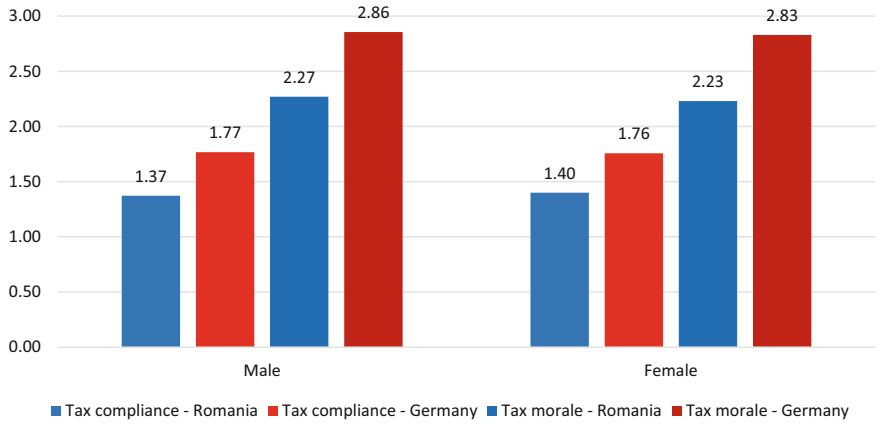


Fig. 1.6 Tax score by gender–comparison in Germany/Romania. Note: Data survey, with a sample of 1742 individuals. Source: Own composition based on the survey

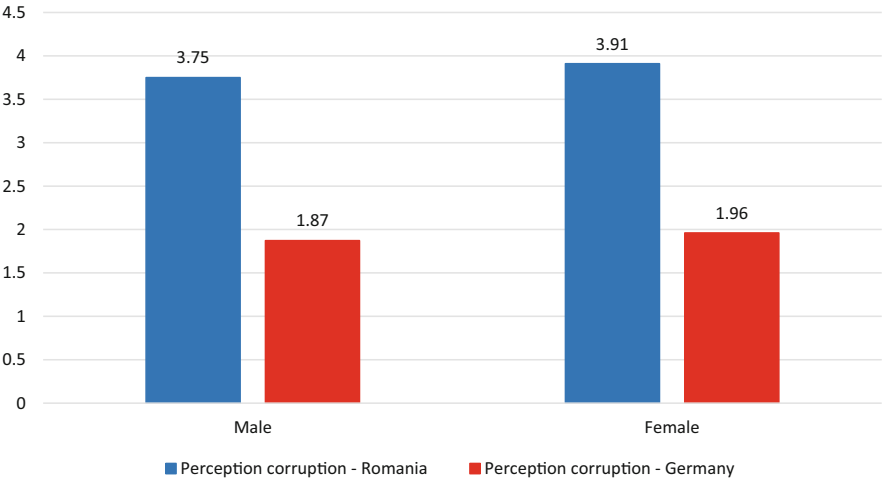


Fig. 1.7 Perception level of corruption score by gender–comparison in Germany/Romania. *Note:* Data survey, with a sample of 1742 individuals. Source: Own composition based on the survey

perceived. Among men, however, German men attribute a higher level of competence to bank employees than Romanian men (ROU: 1.99; DEU: 2.27).

As far as KYC processes are concerned, the level between Romania and Germany is almost identical (ROU/DEU men: 1.4; ROU/DEU women: 1.3). Both the differences with 0.1 are evident in Germany and in Romania. Men are minimally less cooperative than women (Fig. 1.8).

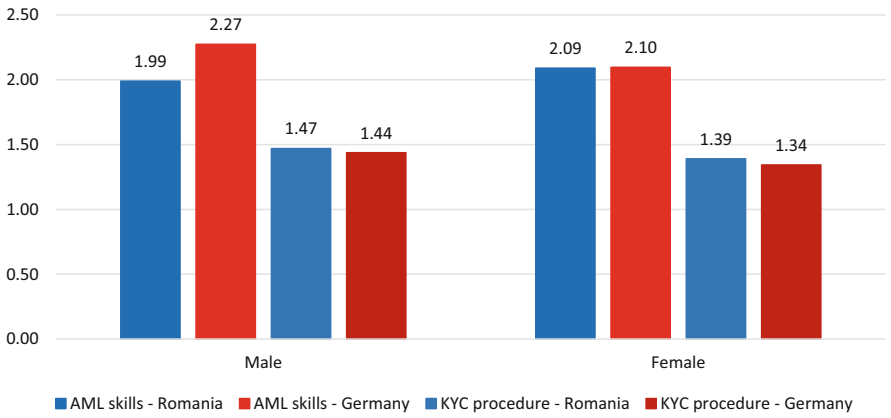


Fig. 1.8 Anti-money laundering score by gender–comparison in Germany/Romania. Note: Data survey, with a sample of 1742 individuals. Source: Own composition based on the survey

4.4 Descriptive Comparison Based on Education

In the following, the results are considered as a function of education. In general, tax compliance is at a good level in both Germany and Romania. In the case of tax honesty, it can be seen that attitudes are almost the same across all levels of education. The higher the level of education, the more similar the behavior patterns. Germans have a slightly lower level of tax honesty than Romanians.

Tax morale shows an almost identical trend at different levels. Romania shows higher tax morale (1 point), while the level in Germany is mediocre. In Romania, doctoral students place the highest value on tax morale, followed by university graduates, and in last place are bachelor's and master's students. However, all groups of people are in a good range (2 and 2.4). In Germany, on the other hand, doctoral students are also the most moral and are almost on par with Romanian doctoral students. They are followed at a considerable distance by German master's students and university graduates (doctoral students: 2.2; master's students: 2.9). Bachelor's students bring up the rear (Fig. 1.9).

The perception trajectory of corruption in Romania is the same as in Germany. In Germany, the level of corruption perception is significantly lower than in Romania (DEU: 1.5; ROU: 4). Interestingly, the perception of corruption decreases with increasing education. In Germany and Romania, the highest perception of corruption is among university graduates and less. The lowest corruption is perceived by PhD graduates (Fig. 1.10).

Lastly, the education category takes a closer look at money laundering. Here, it can be seen that the Romanian and German figures are almost identical. A closer look at the competency attributed to bank employees with regard to the detection of money laundering transactions reveals that the competency attributed decreases as the level of education increases. While high school graduates assume a medium to

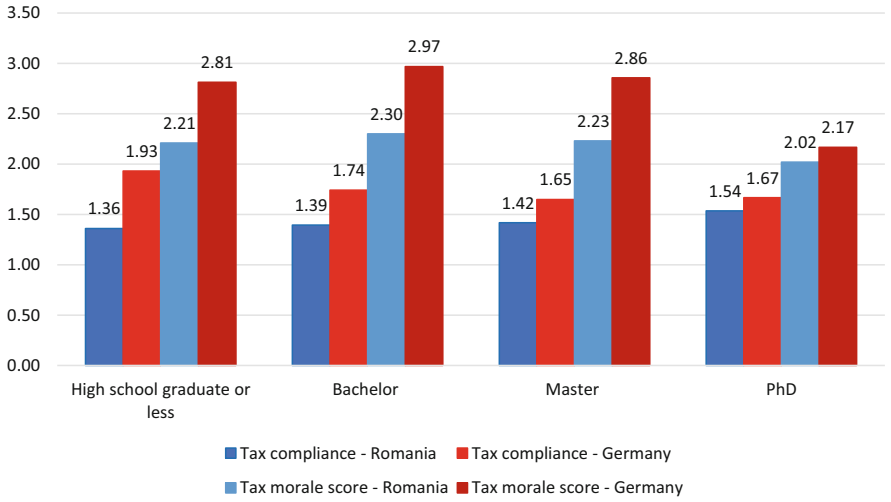


Fig. 1.9 Tax score by education–comparison in Germany/Romania. *Note:* Data survey, with a sample of 1742 individuals. Source: Own composition based on the survey

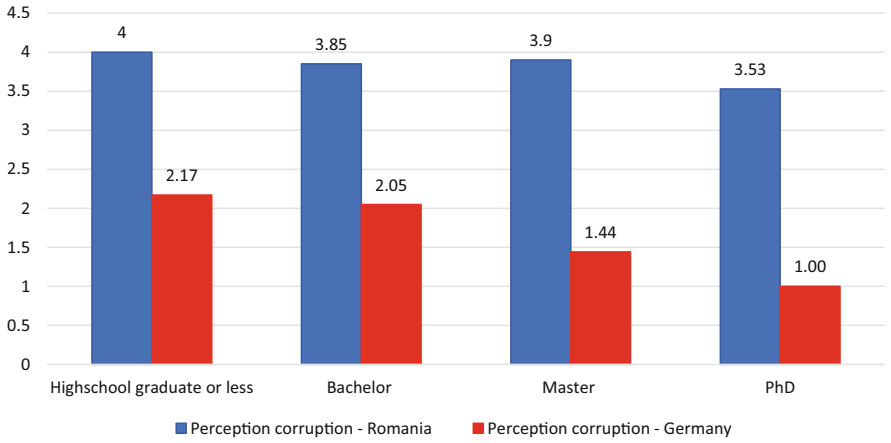


Fig. 1.10 Perception level of corruption score by education–comparison in Germany/Romania. Note: Data survey, with a sample of 1742 individuals. Source: Own composition based on the survey

low level of competence, doctoral students assume a very low to low level of competence.

In the case of willingness to cooperate, on the other hand, there is also a slight upward trend within the range of 0.2 score points. While high school graduates fluctuate between understanding cooperation and annoyed cooperation, doctoral students tend to be at the level of understanding cooperation (Fig. 1.11).

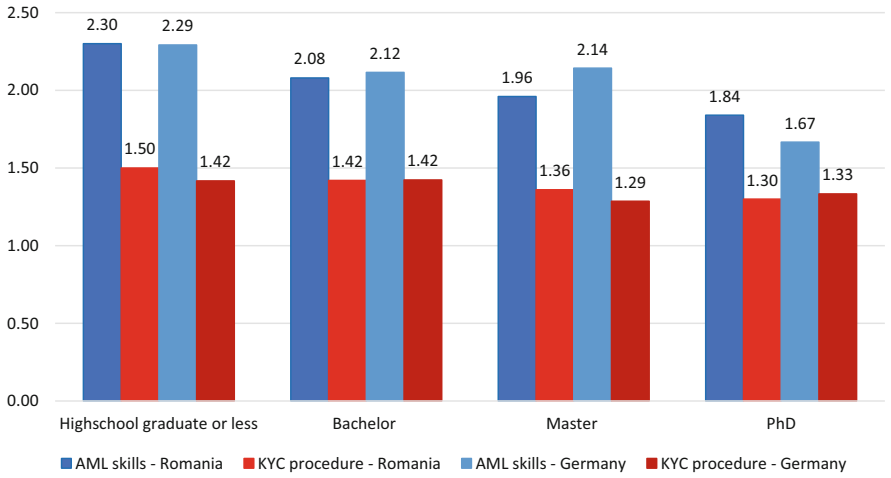


Fig. 1.11 Money laundering score by education–comparison in Germany/Romania. Note: Data survey, with a sample of 1742 individuals. Source: Own composition based on the survey

4.5 Descriptive Comparison Based on Professional Status

Finally, economic and financial crime is considered in the context of the professional status. In the first chart, the tax aspects are considered. As far as tax compliance is concerned, it can be seen that the Romanian and German trends are very similar, although at slightly different levels. Romanian tax compliance is about 0.5 points better than the German values. Romanian and German pensioners and managers are very close to each other and have almost identical values. Employees and students are at similar levels.

Looking at tax morale, a contrasting picture emerges between the German and Romanian respondents. In general, morale is significantly worse in Germany than in Romania. German students are at a similar level to managers, while employees have better tax morale. German retirees register the worst tax morale, forming a peak in the graph. The Romanian values run in the opposite direction. Pensioners form the low point and have the best tax morale. They are closely followed by managers and students. Salaried employees have the worst tax morale. However, the Romanian respondents' scores are all between 2 and 2.4, while the Germans have a higher swing, ranging from 2.6 to 3.8 (Fig. 1.12).

The next pillar of economic and financial crime is the perception of corruption. This is where the tide turns to a certain extent. In Romania, the perception is very high. This perception is held from the young student to the pensioner. In Germany, on the other hand, the perception of corruption in public institutions is low to very low. Managers in particular perceive almost no corruption in their environment (Fig. 1.13).

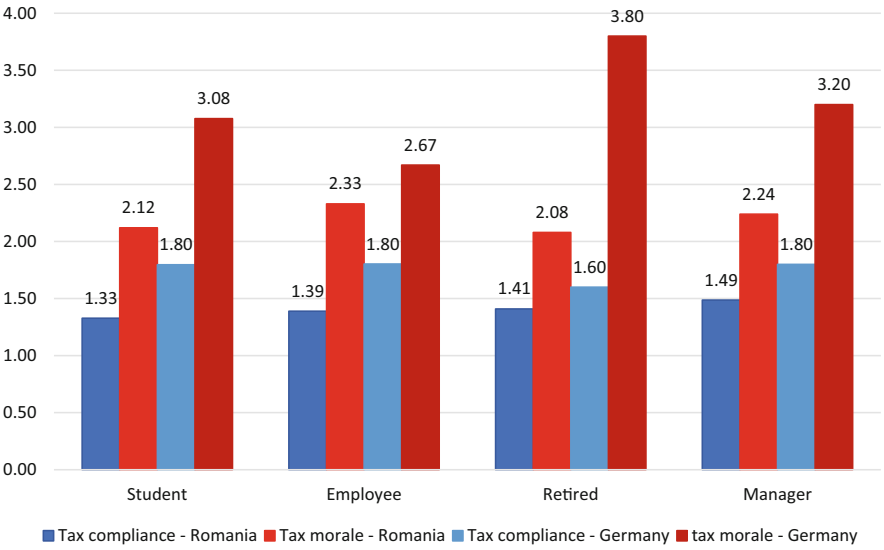


Fig. 1.12 Tax score by professional status–comparison in Germany/Romania. *Note:* Data survey, with a sample of 1742 individuals. Source: Own composition based on the survey

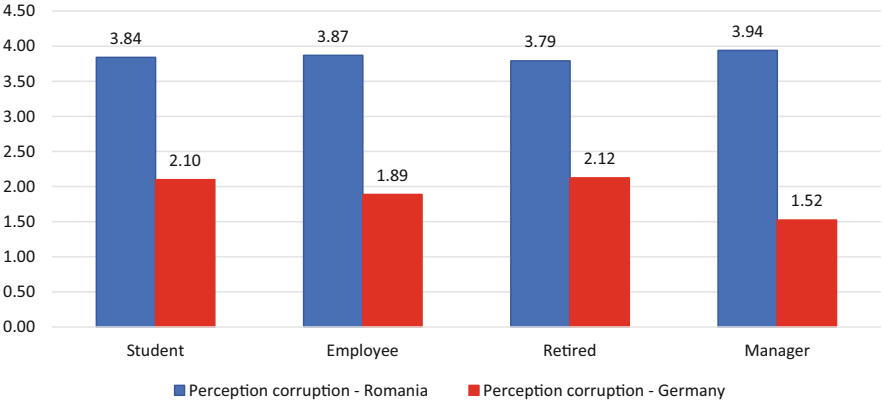


Fig. 1.13 Perception level of corruption score by professional status–comparison in Germany/Romania. Note: Data survey, with a sample of 1742 individuals. Source: Own composition based on the survey

Lastly, money laundering is considered from the perspective of professional status. Basically, it becomes clear that the Romanian values and the German values on the attribution of competence and the willingness to cooperate run almost parallel and differ strongly from country to country. A more detailed examination of the competence attribution of bank employees for the detection of money laundering shows that employees and managers in Germany and Romania are identical. Both occupational groups and countries are on a low attribution of bank employees'

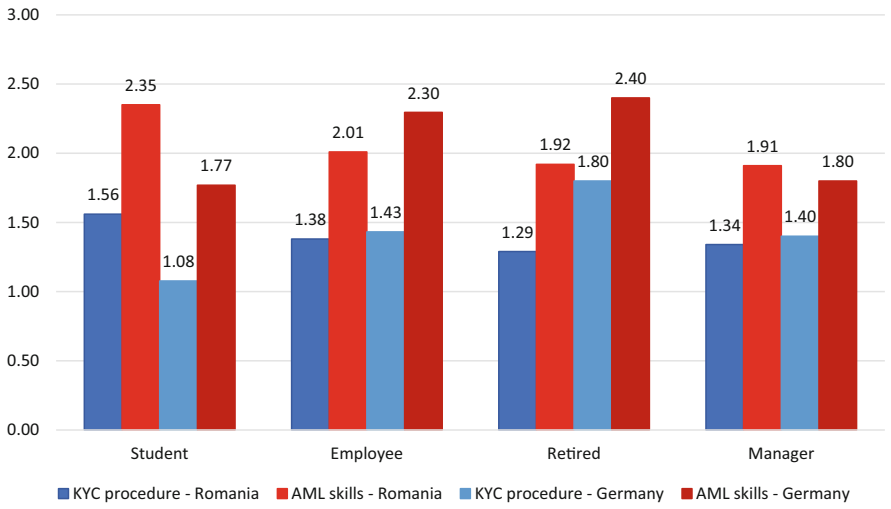


Fig. 1.14 Money laundering score by professional status–comparison in Germany/Romania. *Note:* Data survey, with a sample of 1742 individuals. Source: Own composition based on the survey

competence. The students and the pensioners deviate from each other. In the Romanian results, the students consider that the bank employees have a low to medium level of competence, while the German students record very low to low competence. In the case of the retirees, on the other hand, the view is reversed, with the Romanian retirees attributing very low to low competence to bank employees and the German retirees, in turn, a low to medium competence.

When considering the willingness to cooperate, both the Germans and Romanians are at a very good to good level. Here, too, there are two intersections: among employees and among managers. Both meet at the midpoint between cooperative with understanding and cooperative without understanding. Here, too, the opinions of the students and the retirees diverge in the same way as in the attribution of competence. The Romanian students are less cooperative than the Germans, whereby the Romanian pensioners are more cooperative than the German pensioners (Fig. 1.14).

5 Discussions

With the statistical and descriptive analysis of the Romanian and German survey data, it is now possible to answer the formulated hypotheses. When looking at economic and financial crime as a function of **age**, it is evident that a great deal of dependency can be seen from a tax perspective. A picture can be seen in both the German and Romanian values. Whereas in Romania, an almost constant trend can be

observed, in Germany, there are differences between the younger and older generations. It is clear that the younger and older generations (16–25; 46–65 years) behave similarly, and the 26- to 45-year-olds follow a pattern of behavior. In the case of corruption, on the other hand, there is almost the same trend in Romania as in Germany, with a difference of 2 score points. The trend is almost constant. In the case of money laundering activities, it can be seen that the competence attribution of the bank employees from the 26-year-old respondent onwards runs in parallel with a level difference of 0.25. The Germans attribute slightly higher competence to bank employees than the Romanians. The reverse is true for the 16- to 25-year-olds. Romanian respondents are more convinced of bank employees than Germans. In terms of willingness to cooperate, it is clear that all are very cooperative. In Romania, there is a small increase in the willingness to cooperate in relation to age, while in Germany a small decrease is evident.

When looking at economic and financial crime in relation to **gender**, it becomes clear that no gender-specific behavior is evident in tax matters and in money laundering aspects. When it comes to the perception of corruption, on the other hand, women in both Germany and Romania perceive a somewhat higher level of corruption. It is evident here that Romania has a significantly higher perception of corruption than Germany.

When analyzing economic and financial crime as a function of **education**, different patterns of behavior are evident. In the beginning, the fiscal behavior patterns are examined. What is striking here is that Romanian and German university graduates and PhD graduates behave similarly or even identically. Bachelor's and master's students, on the other hand, behave in opposite ways in Romania and Germany. In Romania, tax compliance is less pronounced than in Germany. Tax morale is significantly better than in Germany. The perception of corruption follows a similar course across all educational classes in both Germany and Romania. Although the level differs by 2 score points, in both Romania and Germany the perception of corruption decreases as the level of education increases. Finally, the money laundering aspects are considered. Here, a very similar trend can be seen both in the willingness to cooperate and in the attribution of competence. As the level of education rises, there is a slight increase in the willingness to cooperate and a slight decrease in the competence attributed to bank employees.

Lastly, the professional status is examined in more detail for possible characteristic behavioral patterns. In the case of the tax topics, no uniform behavior can be identified. In Romania, the values are rather constant and fluctuate at a level of around 0.25 score points, whereas in Germany, both the level between tax morality and tax compliance deviate strongly from each other and also allow large fluctuations within a category.

When looking at individual **professions** based on tax morale, only similar behavior can be observed among white-collar workers. Tax compliance shows a similar trend with a difference of 0.5 score points. In the case of corruption, the assessment in Romania and Germany is similar, with the difference that they behave at different levels. Only German managers deviate and have a significantly lower perception of corruption. Lastly, money laundering activities are considered. Here, it can be seen that the country-specific behavioral patterns are almost the same in terms

of both the willingness to cooperate and the attribution of competence among bank employees, with the difference at different levels. If the results of the two countries are compared with each other, it becomes clear that the employees and the managers show an identical course. The students and retirees, on the other hand, show the opposite trend. The Romanian students attribute greater competence to the bank employees and are less cooperative. The Romanian pensioners are less pleased with the competence of the bank employees and are more cooperative with regard to the information on bank transactions.

A closer look at economic and financial crime in relation to age does not reveal any general behavior. However, behavioral patterns per manifestation are evident. When examining tax compliance, it becomes clear that it is almost impeccable in Romania. This can presumably be attributed to the incentive of the 10% discount on the tax burden. Almost every Romanian respondent takes advantage of the discount and pays their taxes before the deadline. In Germany, on the other hand, there is no such incentive, which means that taxes are paid around the deadline on average. Interestingly, 26- to 45-year-olds also pay more often before the deadline, although there is no incentive to do so. Looking at tax morale, it is evident that German morale is worse than Romanian morale. The 26- to 35-year-old German and Romanian respondents converge somewhat, while the other age groups diverge. In Romania, the trend is almost constant, which suggests that external influence, for example, from the government, the news, or other sources, has set an example or propagated a behavior. In Germany, it is the younger generation (16–25) and the older generation (46–65) that are the most negligent in terms of tax morals. It may be that the older generation has had a bad experience with the government or the tax office. It is also possible that the younger generation is ignorant of what it means when they do not want a bill. In Germany, little is reported about tax morality or tax evasion, which may mean too little education for the younger generation.

When looking at behavior based on gender, it is apparent that there is no discernible pattern in tax crimes. There are no serious differences between men and women in either Romania or Germany. This result can possibly be attributed to the emancipated behavior of women and the convergence of a woman's professional and private career with that of a man. There are no longer any differences in who pays at the restaurant or who prepares and submits the tax return. As a result of the fact that the formerly typical distribution of tasks no longer exists, the boundaries and the "typical" behavior patterns of a woman or a man become blurred as far as tax compliance and tax morale are concerned.

In Germany and Romania, education is a factor that influences the motivation for tax morality and tax compliance. The higher the level of education, the higher the tax morale and the higher the tax compliance. This can be explained by the fact that the higher the level of education, the more enlightened the respondents are about the background of taxes and how they are used. This makes them more aware of what it means, for example, not to receive a bill and what the consequences of this behavior are. In Romania, there is an almost constant trend when it comes to tax compliance. The tax compliance can also be explained by the 10% discount, which most of the respondents would like to benefit from.

Lastly, the professional status is considered. In Romania, it does not have a major impact on tax compliance and tax morale. There is also no discernible pattern of behavior in German tax compliance. In the case of German tax compliance, on the other hand, it is clear that employees and students have the best tax compliance. Managers are in the midfield and pensioners have the worst tax morale. Retirees may have experienced a lot in their lives and can draw on their experiences and possible disappointments on the part of the tax office or the government. A concrete behavioral pattern cannot be derived from the results.

During corruption, it becomes clear that there is no age-specific behavioral pattern in perception. Whether it is the 16-year-olds or the 65-year-olds, all respondents have almost the same perception about corruption on a country-by-country basis. Both in Romania and in Germany, there is an almost constant opinion about it. It can be concluded that corruption in the country is equally pronounced in all different areas of life. It does not matter if an 18-year-old person is trying to get a university place or a 70-year-old person is trying to get a place in an old people's home. The same level of corruption is felt in all areas of life. The level differences between Romania and Germany can probably be explained by the fact that corruption is more widespread in Romania. This is also confirmed by the statistics on transparency (International (2023)). When looking at the perception of the level of corruption depending on gender, a minimally higher level of corruption is perceived by women in both Romania and Germany. However, at 0.1 score points, this is so little that it is hardly possible to speak of gender-typical behavior.

When looking at education, it is also evident in the perception of corruption that the higher the level of education, the less corruption is perceived. Possible explanations could be that people with a higher level of education are aware of the financial consequences of such actions for the government's budget, for the economy, and also for society. In addition, more educated people may also know the consequences for them if they are caught committing such an act. A person with a higher level of education probably has more risk to bear than a person without a high school diploma.

No differences can be seen in the various occupational relationships in Romania. There are hardly any differences in Germany either, except for the managers, who perceive a somewhat but not serious lower level of corruption. The pattern of behavior, which is not dependent on profession, suggests that corruption is ubiquitous regardless of profession, age, or gender.

When looking at the money laundering instruments, it can be seen that when it comes to attributing competence to bank employees, it is precisely the Germans who attribute a somewhat higher level of competence. The exception is the 16- to 25-year-olds, who attribute a lower competence to banking than the Romanians. Basically, the Germans are of the opinion that the banks have a low to mediocre competence, while the Romanians attribute a low competence to the banks. This result may be due to the fact that the development of banking transparency and money laundering detection tools in Romania is not yet as developed as in Germany. Nevertheless, the results of the German survey can be questioned in that competence is rated as low to medium. Various publications about how widespread money

laundering is in Germany raise doubts about the banks' competence. Only this year, the Central Office for Financial Transaction Investigations Financial Intelligence Unit (FIU) has published a statistic, which says that in Germany a new peak in money laundering cases was reached. Last year, 300,000 reports of criminal activity related to money laundering were noted. In 2020, the figure was 144,000, less than half that number. When considering gender, it becomes clear that no particular pattern of behavior is evident. Thus, in conclusion, in the case of gender-specific economic and financial crime, it can be said that no particular behavior or pattern can be discerned, as the behavior in the most diverse areas of men and women has adapted both in Romania and in Germany.

A closer look at education in both Germany and Romania reveals that a slight downward trend is associated with rising educational attainment. This means that the more educated a person is, the more cooperative he is toward the banks and the less competence he attributes to bank employees. The result can be interpreted to mean that more educated people understand the background of why bank employees need to ask such questions. Likewise, in addition to being educated about the subject, understanding also applies. The persons would like to contribute to the clarification of money laundering transactions. With regard to the topic of attributing competence, it is also evident that the slight decrease is possibly influenced by one's own knowledge. People with a higher level of education possibly compare this with the level of education of bank employees and thus find fault with their competence.

Finally, the professional relationship is examined in more detail. It can be seen that employees and managers in particular exhibit identical behavior in Germany and Romania. Students, on the other hand, show a lower willingness to cooperate in Romania, while bank employees' attribution of competence is higher, and the opposite is true for retirees. Salaried employees and managers have arrived in professional life. They may know why bank employees ask such specific questions and the respondents want to contribute to clarification. The differences among retirees can possibly only be attributed to experience. In Germany, the experience with bank employees may have been positive, resulting in a higher level of competence being attributed to them, while in Romania no good experience with bank employees was made.

6 Conclusions

Findings reveal that there are some similarities in terms of the influence of education and age. Occupation exerts only partial influence, while again, gender does not represent a specific pattern of behavior. Findings also emerged from the different levels of tax compliance and tax morale, which can be explained by the Romanian government's incentivizing of a rebate for earlier payment of taxes. It also became apparent that the level of corruption in Romania is almost twice as high as in Germany. These comparative analyses reflect the importance of the role played by education in building a high level of tax morale and tax compliance in Germany. On

the other hand, Romania is far behind Germany because of the low quality of the educational system in general and because of the lowest level of tax morale. Thus, important improvements are required in the Romanian educational system in order to change the taxpayer behavior and their compliance with the tax laws.

Education plays a key role in reducing economic and financial crime. By means of the chi-square model and the intensity assessment in connection with the survey, a negative correlation could be confirmed in Germany and in Romania. The negative impact illustrates that the higher the level of education, the lower the perception and willingness to engage in economic and financial crime activities.

Economic and financial crime has different forms and is constantly evolving, and in some cases, it is very difficult to predict and anticipate. The main concern of the governments should be the adaptation of the methods and means to combat illegal activities. On the one hand, using various blockchain technologies and AI to curb these activities could be a possible solution. On the other hand, improving the education system and the general education of citizens through various information campaigns and presenting the negative consequences of economic and financial crimes can be an important way to reduce the prevalence of underground activities.

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.

Appendix

Questionnaire

Thank you for participating in the questionnaire on the subject of perceptions of economic and financial crime in Germany. By answering the following questions, you will help the community better understand the current sentiment and gather future action for government, organizations, or many others.

1. **Regarding paying your tax duties, which one of the following behaviors is common for you and the people around you:**

   (a) Taxes are paid long before the deadline
   (b) Taxes are paid very close to the deadline
   (c) Taxes are paid over the deadline

2. **When you buy goods and services from shops, restaurants, hotels, salons, etc., please choose one or more of the following that better fit you:**

   (a) Always receiving the receipt
   (b) Usually receiving the receipt
   (c) Always asking for the receipt
   (d) Receiving the receipt but leave it there
   (e) Not bothered by not receiving the receipt

3. **How do you perceive the level of corruption in German public institutions, on a scale from 1 (very low) to 5 (very high)? Please choose one of the following:**

   (a) Very low level of corruption
   (b) Low level of corruption
   (c) Medium level of corruption
   (d) High level of corruption
   (e) Very high level of corruption

4. **Regarding the risk of money laundering, do you think that people have suitable knowledge to be able to recognize a suspicious transaction in a business? Please choose one of the following:**

   (a) Very low skills to detect the risk of money laundering in a business
   (b) Low skills to detect the risk of money laundering in a business
   (c) Medium skills to detect the risk of money laundering in a business
   (d) High skills to detect the risk of money laundering in a business
   (e) Very high skills to detect the risk of money laundering in a business

5. **When you or the people around you ask for bank transactions (making a bank deposit, withdrawing cash from the account, etc.), and the bank officer asks you to complete some details regarding the provenience of the money, or where the amount goes, then you or the people around you generally have different reactions. To help us analyze your responses, please indicate which of the following categories represents you best.**

   (a) You offer any required details; banks must apply their "know your clients" principle to do their job.
   (b) You are bothered by the asked details but finally you provide the required information.
   (c) You refuse to offer any asked details; banks have to satisfy the people's needs that's all.

6. **How old are you? Choose one of the following categories:**

   (a) Between 16 and 25 years old
   (b) Between 26 and 35 years old
   (c) Between 36 and 45 years old
   (d) Between 46 and 55 years old
   (e) Between 56 and 65 years old
   (f) Over 65 years old

7. **Which is your gender? Choose one of the following:**

   (a) Male
   (b) Female
   (c) Other

8. **Which is your professional status? Choose one or more of the following:**

   (a) Student
   (b) Employed
   (c) Manager
   (d) Unemployed
   (e) Retired

9. **Which is your last level of acquired degree? Choose one of the following:**

   (a) High school graduate diploma or less
   (b) Bachelor studies
   (c) Master studies
   (d) Doctoral studies
   (e) Postdoctoral studies

Thank you for making it to the end of this short survey.

References

Achim, M. V., & McGee, R. W. (2023). *Financial crime community pulse: A Romanian survey. Financial crime community pulse: A Romanian survey*. Springer Brief.

Country Data. (2023). https://www.laenderdaten.info/laendervergleich.php?country1=ROU&country2=DEU.

Dabla-Norris, E., Gradstein, M., & Inchauste, G. (2008). What causes firms to hide output? The determinants of informality. *Journal of Development Economics, 85*(1–2), 1–27.

Entorf, H., & Spengler, H. (2002). *Crime in Europe: Causes and consequences*. Springer Science & Business Media.

European Union. (2023). https://european-union.europa.eu/principles-countries-history/key-facts-and-figures/life-eu_de.

Federal Government of Germany. (2023). https://www.bundesregierung.de/breg-de/themen/deutsche-einheit/geteiltes-deutschland#:~:text=Nach%20dem%20Zweiten%20Weltkrieg%20%C3%BCbernehmen,die%20oberste%20Regierungsgewalt%20in%20Deutschland.

Federal Statistical Office. (2023). https://www.destatis.de/DE/Themen/Laender-Regionen/Regionales/_inhalt.html.

Khasanova, G. K. (2021). *The success and education system of South Korea and Japan*. In Наука сегодня: проблемы и пути решения (pp. 94–95).

Madani, R. A. (2019). Analysis of educational quality, a goal of education for all policy. *Higher Education Studies, 9*(1), 100–109.

Medina, L., & Schneider, F. (2022). New COVID-related results for estimating the SE in the global economy in 2021 and 2022. *International Economics and Economic Policy, 19*, 299–313.

Melgar, N., Rossi, M., & Smith, T. W. (2010). The perception of corruption. *International Journal of Public Opinion Research, 22*(1), 120–131.

Mocan, N. (2008). What determines corruption? International evidence from microdata. *Economic Inquiry, 46*(4), 493–510. https://doi.org/10.1111/j.1465-7295.2007.00107.x

National Agency for Civic Education. (2023). https://osteuropa.lpb-bw.de/rumaenien-wirtschaft

Saha, S., Beladi, H., & Kar, S. (2021). Corruption control, SE and income inequality: Evidence from Asia. *Economic Systems, 45*(2021), 1000774.

Schleicher, A. (2006). The economics of knowledge: Why education is key for Europe's success.
Statista. (2022). https://www.destatis.de/Europa/DE/Thema/Basistabelle/Uebersicht.html#424346.
Statista. (2023). https://de.statista.com/statistik/daten/studie/347262/umfrage/anteile-der-laender-am-bruttoinlandsprodukt-bip-in-eu-und-euro-zone/.
Tascu, M. V., Noftsinger, J., & Bowers, S. (2002). The problem of post-communist education: The Romanian example. *The Journal of Social, Political, and Economic Studies, 27*(2), 203.

Sandra Clement is a PhD student at the PhD School in Finance at the Faculty of Economics and Business Administration of Babeş-Bolyai University in Cluj-Napoca, Romania. Her research focuses on financial crime, with particular interest in the shadow economy, corruption, money laundering, and tax evasion. In the subject area of the same name, she has participated in scientific conferences and is the author and coauthor of numerous articles. In addition to her academic career, she works as a managing director in a well-known German company. Due to the different cases and topics in her professional career, she can benefit from them in her scientific development.

Monica Violeta Achim is a full professor and doctoral supervisor in the field of Finance at the Faculty of Economics and Business Administration, Babeş-Bolyai University, Cluj-Napoca, Romania. With over 24 years of experience in academia, she has published as author and coauthor, over 150 scientific articles and 25 books. Her most recent reference work is the book Economic and Financial Crime. Corruption, Shadow Economy, and Money Laundering, published by Springer. In 2020, she earned an Award for Excellence in Scientific Research at Babeş-Bolyai University, Faculty of Economics and Business Administration, Cluj-Napoca, Romania, in recognition of the results obtained in her research activity. She heads a big grant titled "Intelligent analysis and prediction of economic and financial crime in a cyber-dominated and interconnected business world," conducted over the period 2021–2023, financed from the Romanian Ministry of Education and Research, CNCS–UEFISCDI, project number PN-III-P4-ID-PCE-2020-2174 (www.fincrime.net).

Chapter 2
Frauds in Banking System: Frauds with Cards and Their Associated Services

Daniela-Georgeta Beju and Codruța-Maria Făt

Abstract From the early stages of cards' existence, a certain class of humans tried and unfortunately succeeded to commit frauds with this electronic payment instrument. The fraud with cards is a "disease" that affects the banking systems internationally, shaking the trust in this payment instrument and in the issuing banks. The paper starts with a short revision of the card typology and of the associated services that arise in time as an effect of the banks' desire to acquire more and more clients. The recent pandemic offered a perfect motivation for banks to diversify their online platforms and services that can be used only if you have a card to perform online payments. Internet payments, so common today, increased the number of methods to do frauds with card payments and transactions, growing up the level of this type of financial criminality. The aim of this paper consists of reviewing the economic literature related to the methods old and new through which frauds with cards are committed in our days. Also, we highlight the methods that are used to prevent this type of frauds, and we reveal which are efficient in the fight against this scourge. We also analyze the evolution of frauds with cards at the international level. We find that the increasing card usage during the last years has led to a rise of the card scams. Finally, we discuss the measures required to prevent and mitigate the card fraud magnitude and policy implications.

Keywords Banking · Payment card · Online payments · Fraud · Scam · Phishing

JEL Classification G21 · G32 · G50 · O31

D.-G. Beju (✉) · C.-M. Făt
Faculty of Economics and Business Administration, Babeș-Bolyai University, Cluj-Napoca, Romania
e-mail: Daniela.beju@econ.ubbcluj.ro

M. V. Achim (ed.), *Economic and Financial Crime, Sustainability and Good Governance*, Contributions to Finance and Accounting,
https://doi.org/10.1007/978-3-031-34082-6_2

1 Introduction

The wide variety of cards, the safety, and convenience to carry them (Li et al., 2023) determined the incredible growth of this cashless payment instrument in recent years and especially of credit cards, as can be seen in the chart below. Today, the credit cards represent one of the most popular financial products. For instance, in the USA, around 70% of households get a credit card, and nearly 40% of them borrow funds making use of this instrument (Li, 2022).

According to Abdallah et al. (2016), "fraud is a crime where the purpose is to appropriate money by illegal means." Fraud was defined by the Association of Certified Fraud Examiners (ACFE) as follows: "the use of one's occupation for personal enrichment through the deliberate misuse or misapplication of the employing organization's resources or assets" (ACFE, 2002). Online banking activity such as online payments, online commerce, and online financial transactions rose exponentially in the last decades, which happened in the meantime with Internet spread all around the world. COVID-19 pandemics act as a catalyzer for card payments, which increased dramatically last years. These online card payments became a real attraction for criminal minds. Card frauds arrived to be one of the biggest menaces for individuals, companies, and of course banks in two words for the card issuers and users. Criminality in this area grew exponentially.

We speak about card fraud or scam when a person uses another person's card, and the owner of that card does not realize this, which means that the card is used without cardholder's consent. The fraudulent person usually does not have anything to do with the real card owner and does not have any intention to contact cardholders to repay the money that he forged.

Criminal activity with cards supposes compromising and obtaining personal data of card owner in order to use it for printing forged cards; cash withdrawal from banks ATMs; and buying online goods and services, all these with a minimum effort.

Grace to Internet spread, it became an ideal environment for card scams, reuniting consumers from all around the world highly exposed to card felony. Fraudsters have brilliant minds, along the time inventing different fraud formulas, and being aware on card evolution.

The card fraud is considered a white-collar crime affecting the card issuer, the cardholder, and the retailer. The most affected part usually is the card issuer (the bank) because it will assume the client's loss repaying them the lost amount of money. Card owners are protected through law being the least affected participants in this circuit. The big responsibility is in retailer area who accepts the card payment.

To defeat card fraud menace, the banks are trying to strengthen the security level by developing new measures to discover earlier fraud attempts by creating complex systems to detect fraud (van Belle et al., 2023). The steps of credit card frauds are represented in Fig. 2.1.

The main purpose of this work is to review the key issues regarding card fraud methods, their typology, and measure applied to detect and prevent them. An

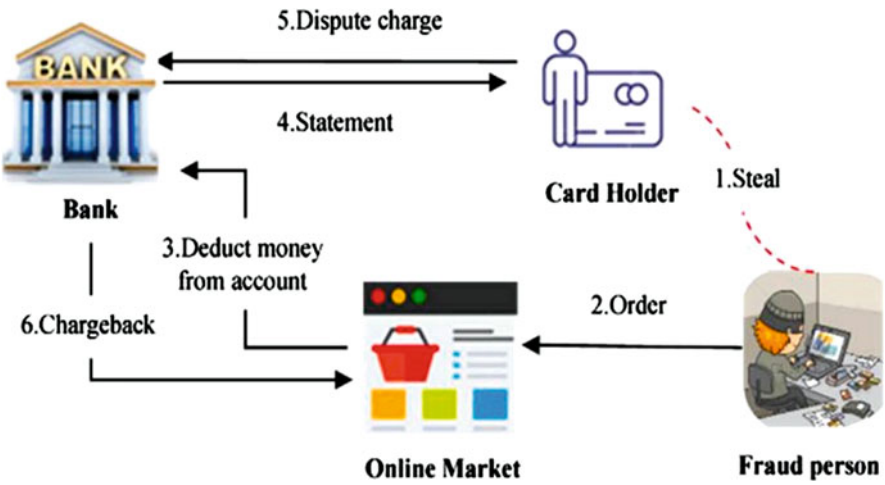


Fig. 2.1 Steps of credit card fraud (Source: Rtayli & Enneya, 2020, p. 2)

examination of the evolution of card frauds worldwide is also achieved, suggesting that the increasing use of cards in the last years has amplified the card scam amount. After all, we debate the measures needed to avoid and alleviate the card fraud level.

Despite the significant expansion of card frauds observed recently, there is still a shortage of research focused on this topic. To the best of our knowledge, this work covers the lack in the economic literature linked to the payment cards and card fraud typologies. The novelty of this work resides in the presentation of the main features of cards and frauds and proposal of a taxonomy of them.

The paper is organized as follows. Section 1 is an introduction in the investigated area. Section 2 presents the theoretical framework related to cards, associated services, and card frauds. Section 3 reviews the literature on the subject matter. Section 4 explains the research methodology and data collection. Section 5 illustrates the empirical results. Section 6 debates the findings and outlines the policy implications. The final section reiterates the conclusions, paper's limitations, and further research directions.

2 Theoretical Framework

2.1 The Card and Their Associated Services

The card is an electronic payment instrument, which allows an electronic transfer of value (European Central Bank, 2021). There are a lot of different types of cards issued by banks or companies. They can be classified on different criteria.

(a) Card Function:

- Debit Card

  A debit card allows the holder to use the funds underlining the card to do payments. The funds underlining the card have been deposited by the cardholder in his account. In certain circumstances, it can be the beneficiary of an overdraft namely a credit line offered by the card issuer. This will not transform the debit card into a classical credit card, being just a debit card with an overdraft.
- Credit Card

  In the case of a credit card, from the very beginning the card issuer offers to the cardholder the possibility to use a certain amount of money, from the issuer's funds to make payments. In fact, a credit card is given with a line of credit permitting its owner to borrow financial resources constantly at an interest rate that can range between 10% and 30% (Li, 2022). The card beneficiary can repay the total used amount or just a part of it, but he is obliged to repay the minimum amount agreed in the contract signed with the issuer. A type of credit card is the charge card, which must be paid entirely once the statement balance is issued, normally every month. By contrast, a credit card can carry a negative balance a longer period, in some cases even years.
- Prepaid Card

  A prepaid card (also known as stored value card or cash card) can be rechargeable or not, customized, or not, through which the owner can realize specific payments using the funds that were deposited on this card with that aim. In this category are included gift cards offered by retailers, transportation cards, phone cards, and other cards offered by service providers.

(b) The Issuer

- Bank Card

  Bank card is issued by a banking institution, being the first payment card type, and is the most used card all over the world. It had a spectacular development rhythm. In the developed countries, a preoccupation in unifying the card offer to eliminate the bank competition in this area is observed. In this way, the phenomenon of interbank cooperation has emerged, which allows the use of a card in all cash dispensers, ATMs, POS, or retailers no matter the issuing bank. Issuing and expanding the use of bank cards represented the ideal solution for banks in reducing the operating expenses generated by the management of checks and cash.
- Store Card

  A store card is issued by a retailer, store chains, commercial centers, or companies serving the population (gas stations, private clubs, companies with mail, or Internet commercial activities) resembling white cards issued by banks. In this case, the main objective is to keep the clients loyal. To achieve this goal, it is very important that they can be used in the same manner as bank cards, to be considered useful by their owners. This is why the retailers attach

more and more facilities to their cards: special discounts, credit facilities, insurances, etc., all this to increase the sales volume and to offer a modern image of the company. There are two types of store cards: store-only cards, which can just be used for purchases in card-issuing store, and cards for general purpose, which can be used for purchases in card-issuing store and out of it. At present, store cards have been converted into an everyday shopper tool (Sarofim et al., 2020).

- Co-Branded Cards

  A co-branded card is usually issued by a bank in partnership with another entity implied in retail or services area. The co-branded card is the result of two partners association, which will split the revenues obtained through collaboration, offering usually special discounts in retailer sales. For example, a client who holds an airline co-branded credit card could profit of both the advantages of usual bank-issued credit card and supplementary benefits such as admission to the airline membership club lounges in airports (Wang & Hsu, 2016). The mutually beneficial partnership made between airlines companies and banks is remarkable and the business has gotten an instrument that exploits visible returns, which can considerably aid in supporting the financial future in an increasingly changing environment (Reales & O'Connell, 2017).

(c) Implied Technology

- Magnetic Stripe Card

  The first issued card contained a magnetic memory stripe, which was added to the back of the conventional embossed card in the seventh decade of the last century. The security of transactions made by magnetic stripe card is primarily attained using a personal identification number (PIN), which works as a password to the system (Madan & Reid, 1992). These cards have gained a huge popularity very fast in the developed countries. It is considered the first form of electronic money.
- Chip Card (Smart Card)

  The need for an increased operational and applications' security has led to the development of the integrated circuit (IC) card. This is also a plastic card as magnetic stripe card but comprises within its body a silicon integrated circuit chip that incorporates not only a processor but also a memory, allowing the use of data encryption techniques (Madan & Reid, 1992). Due to microprocessor, memory, and power provided by the microchip, the chip card is an intelligent or smart one. The smart card offers better services than strip band card: a faster connection to the issuer net, higher volume payments on overdraft, higher security level, which makes it almost impossible to counterfeit or forged, low operating costs, etc.

(d) Card Form

- Physic Card

  It is the classic card that requires a physical support, the small plastic invested with great powers. It is required in classical payments in retailer's

shops, banks offices, or ATM transactions, where the magnetic band or the chip is electronically read.

- Virtual Card

  Virtual card intervenes when the physical support is not demanded to be used in online virtual payments, where the physical card presence is not required, but the card user must provide passcodes or passwords.

Banks in their permanent struggle to retain and attract a higher number of clients create new digital alternatives of financial services attached to their cards.

(a) Internet Banking

It was created in order to provide information regarding the client's personal accounts, a safe medium to make online payments and online transactions or other operations such as card blocking/unblocking; account opening in domestic or foreign currency; foreign exchange; inter-/intra-banking transfer national and international of national and foreign currency; payments including credit repayment or invoice payments; payment scheduling; bank statement, payment order mailing; password change; SMS alerts; granted access with password or access code; beneficiary data's saving; and phone card recharge.

(b) Mobile Banking

It is a service provided to mobile phone users, companies, or individuals, debit card owners issued in home or foreign currency. Through mobile banking, the users can visualize home and foreign currencies sold; visualize the last transactions; transfer money between a client own account's; receive information about their town transactions; block card accounts; password or digital footprint login; and SMS alert activation.[1]

(c) Multicash

This service is provided, especially for companies. The companies can connect to a bank if they have at least, a Pentium II processor, 128 MB memory, a 20GB hard disk, Windows 98 operating system, and Internet connection. The companies can get customized information and can realize banking transactions such as bank statements, payment orders and account situation; interbank and intrabank in home and foreign currency transactions; foreign exchange; and term deposits in home or foreign currency opening/closing.

(d) App Contactless Payments

Transactions through app contactless payments are secure due to direct mobile phone confirmation on app such as BT Pay, George Pay, Google Pay, RaiPay, CEC Pay, etc. All these apps are working as digital cards having the same characteristics as the physical ones. In order to provide a higher security, they can be activated or deactivated quick and easy. The clients find this service useful because it provides time economy and comfort; guarantees an easier access to information; ensures permanent technical assistance; and offers operations and information confidentiality and security.

[1] A permanent information service about account proceeds and card transactions (e.g., transaction day and time, amount, and location).

(e) Current Services

Card issuers provide apps and other services such as 3D secure[2]; free travel insurance; priority pass[3]; discounts to retailers; and SMS alerts.

2.2 Cards Fraud Typology

Card scams are like a virus, which can easily infect any card user if he/she does not pay enough attention to how and for what they use their card. As we know, scammers are inventive in finding new strategies to trick card owners. In a 2020 paper, Rtayli and Enneya studying the existing literature conclude that card scams can be divided into two categories:

- Online frauds committed with a physical stolen card.
- Offline frauds committed by stealing cardholder identity features (card number, PIN, control number, expiry day, and so on).

The most frequent nowadays scams are presented in the next sections.

2.2.1 Skimming

It is a scam that is working on magnetic band cards. The scammer using a device named skimmer captures data or cardholder's PIN. This device can be installed on bank ATMs or on retailer's POS. The stolen data are used to print fake cards to steal money from original cardholder's accounts. According to FBI,[4] more than one billion USD per year is stolen through skimming strategies.

The skimmers appear in different forms, but in all cases the undetectable skimming device is installed over the card reader or is inserted in the card reader so when the cardholder introduces the card in the card reader the card data are stolen and used after to be encoded on a blank card or on a stolen or lost card.

To get the cards' PIN code, the scammer:

- Installs a pinhole camera on an ATM in order to record the card user PIN. Usually, these cameras are used in conjunction with the skimming device. They are very small and post it in areas where the client does not even think to check.

  or
- Installs a false keypad overlaid on the original one. These are smart keypads, which replace concealed cameras. When the cardholder punches the PIN numbers, the phony keypad internal circuits memorize the PIN code and store it.

[2] Protection against fraud program initialized by Mastercard and Visa. It requests an account login for payment consent.

[3] Priority pass provide independent travelers access to all-world airport lounge.

[4] https://www.fbi.gov/how-we-can-help-you/safety-resources/scams-and-safety/common-scams-and-crimes/skimming.

Another skimming method consists of literally replacing original ATMs with modified ones. The modified ATM will register the card information. It looks like it is working, and the card owners tries to use it. During their attempt, their data are stolen and stored in the fake ATM and used later by scammers.

2.2.2 Phishing, Smishing, and Vishing

The common thing of these scams is the attempt to steal the cardholder personal information and to access their bank accounts by directing them to a fraudulent website created by scammers. These websites are replicating the original bank or well-known brand retailer's websites, imitating almost perfect even the ad spots.

- ***Phishing*** is a term conceived in 1996 by hackers. It consists of phony emails, which try to convince the cardholder to send by email card identification data such as holder name and surname as it is written on the card, address, email address, card number, CVV/CVC code, numerical personal code or insurance number, PIN code, and even the authorization code received as SMS, email, or on app notification or the message urges the cardholder to access a certain Internet link, to download an attachment or an application as Any Desk, as soon as possible, to avoid certain unwanted actions as it is the account close.

  A common card fraud is realized on marketplace platform where the victims post selling announcements. The scammers are pretending to be interested to buy or they are pretending to be sellers. Their strategy is to gain victim confidence and to convince it to continue the negotiation, for instance, on WhatsApp. The scammers will attach in the WhatsApp messages links to fake sites using brand's visual identity claiming payment or delivery validation to obtain the card victim data that will be used to withdraw or spend their money.
- ***Smishing*** is conducted through text messages. The fraudster sends fake phone messages claiming the message is from a cardholder bank or other institutions (as fiscal institutions) or retailers. As in the phishing the potential deceived client is asked to take an urgent action by making a call or log on a certain Internet link, to verify devices, transactions, or if new payments are registered. The message looks almost legitimate, but at a closer look it will contain words that usually are avoided by the genuine organization. Another sign that it can be a scam is related to the message provenience: The message will come all the time from a national or international unknown phone number.
- ***Vishing*** is when the card owner receives an unexpected phone call from somebody claiming that they represent a bank or another authority (like police) or even a retailer that the cardholder knows and trust, for example, the accident method when the criminals pretend to represent the local police and announce the future victim that a relative had an accident and needs financial help. The scammers may know personal information about the phoned person and can use "number spoofing" technique to make the phone number look real. The problem arises when that person asks the cardholder: to transfer money to a safe account or to

somebody else account because the cardholder account was compromised; to process a number on the phone in order to speak with client service where in fact a scammer will be the contacted person; and to disclose card identification data and personal or financial information.

If the victim (the called person) tells the caller (the scammer) that he is suspicious about the phone call and thinks it is a scam, then the caller can advise him to contact the bank using the number on the back of the card. Unfortunately, the criminal is prepared with a fake dial tone keeping the line opened and making the client believe that he is talking with the bank representative. In fact, the conversation is still with the same scammers. The client can avoid these situations by being sure that they disconnected from the former conversation, using a genuine phone number available on official sites, waiting at least 1 min before dialing the phone number, etc.

2.2.3 Gift Cards Scams

The gift cards can be used by scammers in phishing, smishing, and vishing scams. The fraudsters will ask the victim to pay with a gift card or to buy and offer them the gift card. To avoid gift card scams, everybody must know that neither a bank nor an official institution will not claim payments with gift cards. As the US Federal Trade Commission[5] conclude, the villains are very creative so they can pretend they represent: a government agency (government impersonator scam); the technical support team of Microsoft or Apple; a social security administrator (social security impersonator scam); a tax collector as IRS in US; the medical insurance agency as Medicare in US, National Health Insurance House in Romania, and so on; the national consumer protection agency; the national supervision commission of capital markets; the immigration authorities; the Maire office; the court of justice; and the list can continue.

They will ask the victim to use a gift card to pay a tax, or a fine, to get technical support because the called person computer has a malfunction, to pay a fee in order to get a supposed gained prize, and the examples do not stop here. Google Play, MoneyPak, Steam, iTunes, eBay, and Amazon have lists with the most usual gift card scams and the signs to recognize it, available for everybody.

2.2.4 Carding and Malware

Carding and malware are using performant programming to steal and use card data (Aurand, 2020). Carding can be realized through phishing and smishing tactics but often this fraud type is working by buying the stolen card data on Darknet. Carding forums or carding websites are illegal website where the stolen card data are

[5] https://consumer.ftc.gov/articles/how-avoid-government-impersonator-scam.

shared between the scammers who intend to use it to perform illegal activities. Other users, like criminal groups, seek to purchase big quantities of stolen card data in order to sell them on Darknet.

Carding, in fact, use robots (bots), which are software used to check and find the cards with enough resources to be used in illegal purchases. Carding affects the credit cards, or generally the regular type of cards. The villains created bots specialize in detecting active gift cards, which can be used in gift card scams, performing unauthorized purchases with them.

In the case of malware, the scammers use malicious software, viruses as the "banking Trojans" installed on victim's personal computers, tablet, or mobile phones. We can categorize these attacks as electronic skimming or e-skimming, which grow tremendously during COVID-19 pandemics, due to exponential online commerce growth, but in this case no physical skimmer must be used. For instance, a malware soft as a malicious Java Script code is designed to attack the online shopping sites or any website, by inserting it into the site or into the third-party platform from where the attacked site loads remote resources. These are named **Magecart Attacks** from the Magento software used to built-up a lot of online shops and are nothing else than hacking the website payment system.

The main characteristic is that all the malicious acts after the virus is planted in the companies' network are remote done. The hacker arrives to control through malware the cash register, the POS transaction, and the data are stolen without a physical approach to POS. It is possible to be done even recording all the information typed on keyboard by victim using keyword stroke software.

Another example is the **Flubot** scam. In this case, the victim is asked by an SMS to download an app, which in fact is a malware designed to cause technical damages to the phone. Once downloaded, the criminals get access to the phone owner personal data. Moreover, they can control the damaged phone. For instance, they can access the phone owner agenda and send messages to all the contacts inviting them to install the same app. All the data obtained by malware are forwarded automatically from the victim's account or Web browser directly into the attacker's server using an encoded network and from there it can arrive on the Dark Web being sold for significant prices.

This malware can affect even the ATMs to facilitate cash withdraw without physical card presence, using just a code that activates the cash withdraw interface.

In all frauds, the fraudsters rely on victim openness to new, their confidence in banks, companies, police, and other institutions. Another factor is usually the lack of time that affects the victims, which are trying to do a lot of things in a short time, so they do not pay attention to important details.

3 Literature Review

Several research papers investigating the social cost of payments have shown that, on average, cash and debit cards have similar social costs per transactions, but in some countries debit cards carry lower unit costs than cash transactions. Thus,

electronic payment instrument such as debit cards must be promoted to reduce the costs of payment transactions (Schmiedel et al., 2012). Considering both services provided by a debit card to consumers, namely cash withdrawal and payment, the research of David et al. (2016) has indicated that the adoption of debit cards has an overall negative effect on the demand for cash.

Even if the debit card has evolved in an important alternative to cash, there are significant cross-country differences regarding its usage. These differences are due to discrepancies in card acceptance, the policies implemented by retail payments banks in order to encourage card usage, payment scheme developments, the policies promoted by merchants. For example, in the USA 76% of consumers hold a debit card, in France the proportion is 83%, and in Austria the percentage is 85%, the highest share being recorded by Australia with 93% of population (Bagnall et al., 2016). However, in the less developed countries the percentage of consumers that holds a debit card is much lower.

Nowadays, credit cards have become a conventional type of consumer credit products, showing an excellent vigor in the consumer credit market, especially in developed countries where around 60–70% of customers carry at least one credit card, whereas in developed countries only a proportion of 30% of consumers benefits of this financial product (Li et al., 2023). Credit card accounts are the most popular household debt instrument in advanced nations, and in the USA, the aggregate card balances account for almost 4% of GDP (Campbell et al., 2022).

Prepaid cards are more and more widespread these days. The cash cards are branded products, such as Starbucks, C&A, Zara, or Mastercard. On these cards are stored amounts of money that can be used in the issuer's shops. Usually, the prepaid cards are not linked with a person and are infrequently reloaded with money. Therefore, the store cards have a short lifespan, commonly from months to a year (Robinson & Aria, 2018).

The retailers, which accept the bank cards as payment instruments, must pay a fee to the issuing bank, every time the clients pay by bank cards. They usually argue that it is too high. The costs generated by the payments made by bank cards were the main cause of dispute between the issuing banks and retailers that should accept these payment instruments. This was the reason of why the retailers have come up with strategies designed to lower the costs of payment card transactions, starting to implement their own "private" or store cards (Bourreau & Verdier, 2010).

The menace of card frauds rose dramatically in the last decades and especially during pandemics. Ryman-Tub et al. (2018) underline that the patterns of fraud called fraud vectors evolved slowly until disruptive technologies such as smartphones, mobile payments, cloud computing, and contactless payment burst, in the meanwhile with data breach outbreak. This led to new fraud vectors activation, declining the efficiency of existing methods. As a response to this real threat, as Van Belle et al. (2023) noticed, financial institutions try hardly to increase and improve security measures and to deploy security systems to detect and prevent fraud. Banks and other financial institutions developed an entire series of fraud detection systems to build up grace to artificial intelligence (AI), so new methods are blooming constantly.

The early attempts to detect and prevent card frauds relied on fraud vectors. This is specific set of operations determined by a card payment underlining a payment card fraud, which was observed, recognized, and reported by fraud experts or by official institutions law enforced. Based on fraud vectors are created the card fraud classifiers, which are algorithms conceived to analyze and identify similarities or certain patterns in data content and structure.[6] They are applied in data mining and machine learning.

In 2018, the study of Ryman-Tubb reviewed the methods that use artificial intelligence and machine learning methods. Other researchers, such as Bagga et al. (2020) focused on pipelining and ensemble learning. Rtayli and Enneeya (2020) identify two card fraud detecting approaches: supervised and unsupervised. The supervised approach relies on a learning algorithm meant to classify the card transactions as scams or no scam using the recorded transactional data. The unsupervised approach creates algorithms made to find the hidden paths in non-labeled transaction card data. They found the self-organized map (SOMs) and K-means method, which try to solve the problems generated by unexpected events.

Resuming the findings of already mentioned researchers, we conclude that nowadays exist a huge number of methods using AI techniques to detect as early as possible the card fraud attempts. Some of them are presented in the following lines:

(a) Expert systems are the most used AI technique to detect card frauds. The expert systems are based on human capacity to perform symbolic representations of known elements this is why they are also named knowledge-based systems. To build up such systems are used symbolic approaches such as rules, decision trees or random forest, and case-based reasoning.
(b) Supervised neural network introduces models that are generating functions, which infer the training data with inputs and outputs associated with initial inputs. In fact, the models will classify the transactions into two classes: genuine transactions or fraud.
(c) Unsupervised neural networks and clustering go further, using a transactions classification considering the geographical approach. The input data are similar card transactions, with the same characteristics placed in the same area, in the same nearby location that permit to be successfully clustered. It will detect the unusual transactions or strange transactions, compared with the benchmark pattern, that will be considered a potential fraud sign. It is presented by other authors as K—nearest Neighbors.
(d) Bayesian network is the next level in card fraud detecting models based on probabilistic approach. In this case, the conditional dependencies are deduced from input data.
(e) Evolutionary algorithms are inspired from biology. They are trying to reveal a method to search the optimum functions set needed to detect card scams. They

[6] https://www.sciencedirect.com/topics/computer-science/classification-machine-learning.

are based on heuristic algorithms tracking biological mechanisms. An example is artificial immune system that replicates the way how biological immune system works.

(f) Hidden Markov model (HMM) relies on a statistical model detecting the probability of certain sequence appearance during an event.

(g) Support vector machine (SVM) is designed to make classifiers combining the input data with their associated outputs to determine a unique boundary between two classes.

(h) Challenger model of Kim et al. (2019) based on deep learning methods is constructed with more hidden layers, which provides multiple patterns to check the authenticity of card transaction alerts. This model significantly reduces the false alarms.

(i) Long short-term memory recurrent neural network (LSTM-RNN) is proposed to predict illegal behavior on card payments and prevent card scams based on deep learning technique (Femila et al., 2022).

(j) Hybrid models are combining different methods in order to get the best features proved by each one. The aim is to obtain a better card fraud detecting system than the existing ones on the market. As an example, Rtayli and Enneeya (2020) mixt the recursive feature elimination used to find the best forecasting features with GridSearchCV in order to obtain optimized hyper-parameters and with synthetic minority oversampling to solve the problem of imbalanced data.

A criminal card fraud system designed to detect and prevent card scams depends both on the manner of parameters estimation used by the model and on the selection criteria applied to forecasting features.

4 Methodology and Data

The purpose of this paper is to review the literature on the methods applied in the frauds with cards, which are practiced in present. The paper begins with a revision of the card typology and of the associated services, emphasizing the features of each one. We discover a growing number of methods to do frauds with card payments and transactions, expanding the level of this kind of financial criminality. We focused on a qualitative analysis of the methods that are used to prevent the scams, and we make a comparative investigation to reveal which are efficient in combating this scourge. A horizontal analysis is performed on worldwide data collected for the period 2010–2022. The data are annually and are collected from Statista and Euromonitor databases. The evolution of fraud losses in card payments worldwide and fraud losses in e-commerce payments are analyzed. Moreover, the evolution of fraud detection methods is explored. Some projections of the value of fraudulent payment card transactions worldwide are also included in our research. Based on the investigation accomplished on annual worldwide data, we identify the causes that can fuel the anticipated growth of card fraud and we discuss the policy implications of these evolutions in the future for both banking industry and cardholders.

5 Results

5.1 The Evolution of Fraud Losses in e-Commerce Payments

After the arrival of the COVID-19 crisis, e-commerce turns out to be more widespread among citizens (Cheba et al., 2021; Eriksson & Stenius, 2022). The shoppers' approach regarding e-commerce has enhanced because individuals intended to avoid infection risk and keep up with social distancing and safety rules (Kawasaki et al., 2022). For example, in 2020, the global average of the clients who shopped online was 85% (Statista a).

However, the remarkable growth of e-commerce has opened a window for opportunistic fraudsters (Fig. 2.2). In 2021, for instance, 75% of online sellers have faced a huge rise in scammers assaults compared with pre-pandemic year. The regions have been affected in a different way, the higher fraud losses from e-commerce payments being recorded in Asia-Pacific and Latin America. As the credit and debit cards are the preferred payment instruments used by online shoppers, the card frauds represent an important component of e-commerce payment fraud losses. The primary instrument for fraud in online shopping globally in 2021 was debit card which accounted for 67% of online frauds, followed by credit card, which accounted for 61% (Statista b). The most popular kind of e-commerce fraud attack is the friendly fraud, which arises when clients deliberately make a purchase with a debit or credit card. Later, they dispute that purchase with their bank requesting a refund. In 2021, almost 40% of online retailers globally reported that have suffered this form of damage (Statista c).

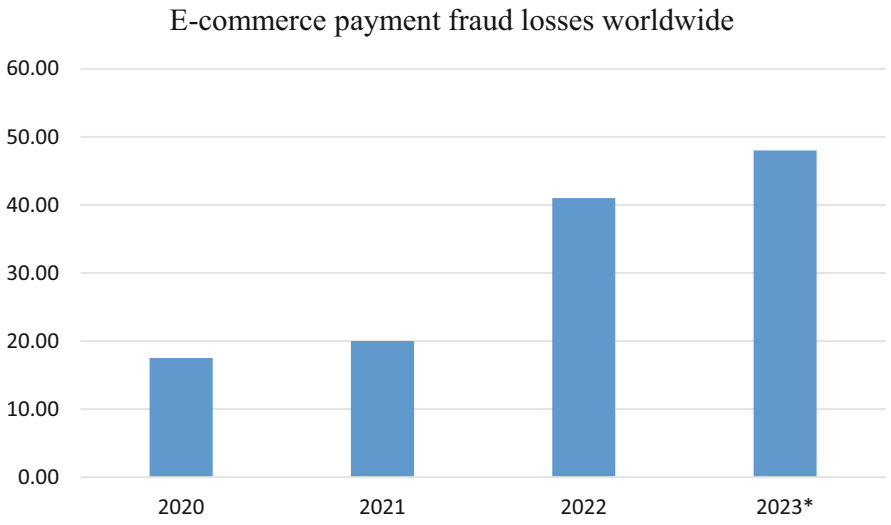


Fig. 2.2 E-commerce payment fraud losses worldwide 2020–2023 (billion U.S. dollars). Source: authors' own processing based on Statista databases

5.2 The Evolution of Fraud Losses in Card Payments

Of all worldwide sales paid by a payment card, the average annual fraud losses per 100 U.S. dollars was 6.6 cents for the period 2010–2020, with a peak of 7.2 cents in 2016 sales, as can be observed in the chart below (Fig. 2.3). In 2020, the total loss from card fraud worldwide was of 28.58 billion US dollars from issuers, retailers, shopping, and ATM transactions (Nilson Report, 2021).

The value of fraudulent transactions made with payment card worldwide has increased significantly in recent years and is projected to reach the amount of 38.5 billion dollars in 2027 (Fig. 2.4). The expected expansion of illegal transactions is fueled by the increasing use of cards for payments and by the difficulty of detecting them among the huge volume of bona fide transactions carried out daily.

5.3 The Evolution of Fraud Detection Methods

As the fraudsters are very ingenious and manage to create various forms of frauds, the banks and merchants were forced to develop methods for prevention and detection of card frauds, the most important being presented in the next session. Furthermore, the Kosse empirical research (2013) has reported that the newspaper articles regarding card frauds have a negative impact on debit card usage, especially

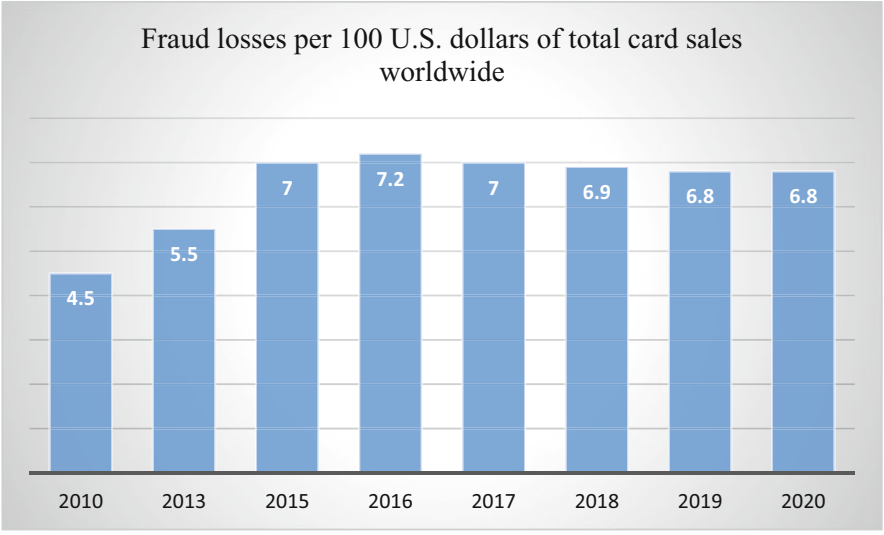


Fig. 2.3 Fraud losses per 100 U.S. dollars of total card sales worldwide from 2010 to 2020. Source: authors' own processing based on Statista databases

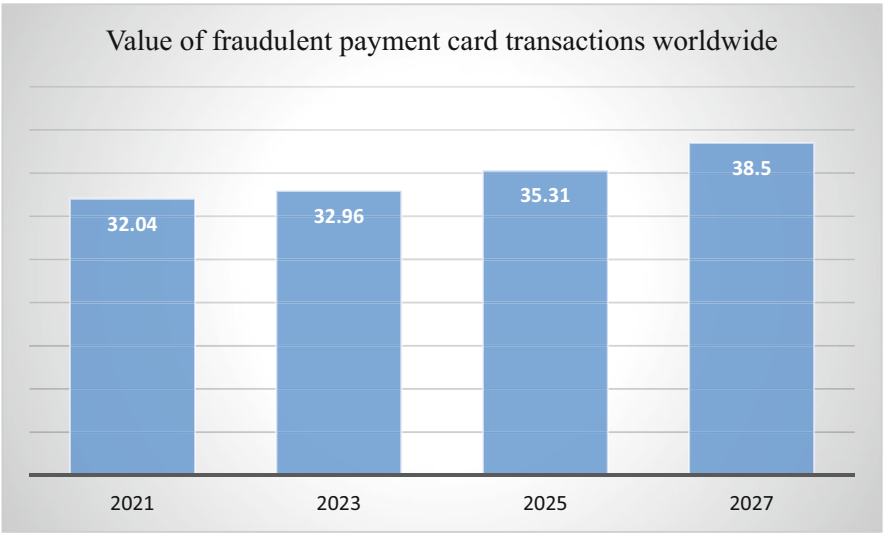


Fig. 2.4 Value of fraudulent payment card transactions worldwide in 2021 and its projections until 2027 (billion' U.S. dollars). Source: authors' own processing based on Statista databases

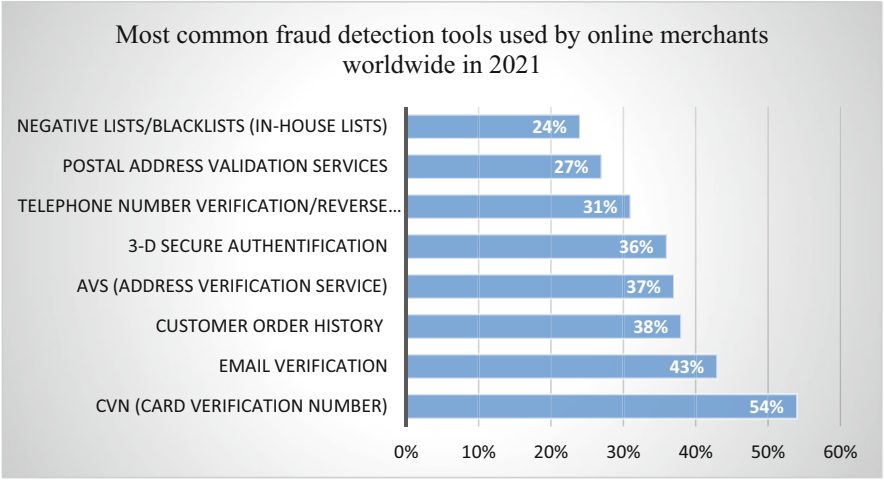


Fig. 2.5 Most common fraud detection tools used by online merchants worldwide in 2021 (%). Source: authors' own processing based on Statista databases

in the day when the articles are published. In 2021, the most popular fraud detection method used by 54% of online sellers was the card verification number, followed by email verification with 43% and customer order history with 38% (Fig. 2.5).

6 Discussions and Policy Implications

Card fraud detection and prevention are a difficult task for all implied parties in card payments. Several studies have focused on credit card fraud detection (Carcillo et al., 2021; Cherif et al., 2022; Forough & Momtazi, 2021; Madhurya et al., 2022; Malteseva, 2022). Detection and prevention must not be a major preoccupation only for banks or companies, which issued the cards, but in the same measure it must be a concern of card users too.

The bank and other card issuer's policy to prevent the malicious actions of fraudsters is to ask the cardholders to apply some simple measures. These measures are focused on the use of physical devices, on improving the card security features, on the bank statement verifications, on the device's strange behavior, and not at least on the services that can be used by cardholders to improve the payment security level. In the first category, the measures are related to the verifications performed on ATMs, POS, or other payment devices before a physical payment or a check and double-check of the retailer in the online payments. In the case of improving the card security features, the clients are advised to create a complex PIN or to check if the cards have intact protective stickers namely in the case of gift cards. The bank statement verifications involve checking at least monthly the account statement to survey money movement during the month, or during a certain period, to ask for the bill for any performed transaction on ATMs or POS, approved or rejected. When cardholders use frequently online payments by phones or other devices, they are advised to enable SMS alert service provided by the bank just to be able to perform a real-time check on every transaction performed in that account, to not access strange or unknown sites, links, or emails from unfamiliar sources; to not answer to SMS messages or phone calls received from strangers or unknown phone numbers, or international unknown phone numbers; and to pay attention to unprofessional mistakes in messages or on website such as spelling mistakes, difficult navigation on the website, and differences in website design namely bank or company's logo. They are prevented to pay attention to odd computer, tablet, or phone behavior, it works slower, it became suddenly hotter, or the sound is louder; to be aware if new icons or animation appear on computer, tablet, or phone because it can be a sign of malware; to use antivirus and phishing protection software; to upgrade and update the owned software and devices; and to sign up for identity theft protection.

The cardholder can contest online transactions for different reasons, so he will complain to the card-issuing bank or merchant (if it is a gift card), which will contact the retailer to initiate the money reimbursement in the cardholder account as the card system regulation permits.

The burst of e-commerce increased by COVID pandemics leads to a fulminant card fraud growth related to online payments. The e-commerce retailers improved their cybersecurity measures and practices. The most common are claiming transaction authorization, demanding a CAPTCHA test, and accessing payment authentication system which supposes to contact the cardholder to check the transaction and to employ security features as verifying if it is used the same device or if the

purchase is in the usual store. Moreover, to approve or reject transaction verifying the card verification value—CVV (in the case of VISA cards) or the card verification code—CVC (in the case of Mastercard cards), namely the three number code that is impressed on the card backside above the cardholder signature but not on the magnetic strip. The retailer demands this code even when the payment is done with the physical card to increase the payment security. Because it is data that appear just physical on the card, it is a little bit more difficult to fraudsters to obtain it and to be sold with all card data on Dark Web. Other measures more complex are the velocity check performed by merchants by numbering the transactions realized with that card in each timeframe discovering patterns in transactions or using AVS—address verification system, which compares the billing address with the address that is in the issuer card system if appears mismatches the payment can be denied. The bad news in this last case is that fraudsters arrived to compromise the addresses using change in address scams (Toohil, 2022).

A useful technique practiced by e-commerce retailers consists of creating the black/whitelist to identify the highly risk transactions.

The blacklist contains the card numbers used in several frauds, and the bill number, address, email addresses from where scams were performed. The blacklist is also created by banks aiming to restrict transactions in the listed cardholder's benefit. Mastercard and Visa are issuing a file forwarded to banks and retailers containing the card numbers stolen or lost, which were not blocked yet and it can be used by scammers.

The whitelist contains the card data of trustworthy clients who are regular clients of the same merchant and can be exempted of some verification or can benefit of smaller transaction processing delays.

The detecting fraud technologies permit to banks and merchants to verify all transactions and to detect earlier fraud attempts (Asha & Suresh Kumar, 2021), but to eliminate frauds they use a combination of methods, measures, and techniques complementary one to another. These antifraud systems are not cheap from financial point of view. It supposes a lot of work and resources, banking industry, and online companies trying to improve constantly their antifraud systems. Beneath artificial intelligence solutions already mentioned, banks introduce in their fraud detection and prevention systems some functions as login to client account using the biometrical parameters as face ID or digital fingerprint, and 3D secure—an authentication measure that ask cardholder to use a one-time password (OTP) validated by the card issuer. The online shopping is performed after this validation, and the online payment becomes safer and is done in secure conditions. 3D comes from 3 domain model formed by acquirer domain, issuer domain, and interoperability domain.[7] In the same direction of tightening antifraud measures, another initiative is to issue virtual card for one-off use, making impossible any other attempt to use it again and issue virtual cards, which can be activated or deactivated anytime or any card

[7] https://www.paycec.com/products-and-services/3d-secure-transaction?gclid=EAIaIQobChMIwPqG_IqA_AIVDvt3Ch19UQlpEAAYAyAAEgI0MfD_BwE.

function activation/deactivation authorization using the phone apps. For instance, cardholder can deactivate the magnetic strip making impossible card cloning with skimmer devices, or it can cut off contactless function, online payments, or cash withdraw.

All these measures and techniques suggested to cardholders or used by banks and other card issuers have as final goal to avoid the loss of their credibility and image damage and to increase the confidence in the services that they offer to their clients.

7 Conclusions

The aim of this paper was to review the major aspects related to card frauds, emphasizing cards' typology, their associated products and services, fraud typology, and the most important measures for detection and prevention of card frauds. The COVID-19 pandemic supported the banks' incentive to expand their online platforms and services that allow online payments made through payment cards. The Internet payments, so widespread these days, expanded the number of card fraud methods, growing up the amount of this type of financial criminality. Therefore, the essence of this paper consisted of describing the old and new card fraud methods. The most important measures used to detect and prevent card frauds are also shown. An analysis of the evolution of frauds with cards at international level is also performed, indicating that the growing card use in the last years has boosted the card scams amount. Finally, we debate the measures needed to avoid and alleviate the card fraud level and we reveal some policy implications.

Despite the substantial development of card frauds noted recently, there is still a scarcity of investigations centered on this subject. To the best of our knowledge, this research covers a lack in the financial literature related to the payment cards and card fraud typologies. Our contribution consists in presenting the main features of cards and frauds and proposing a taxonomy of them. However, this study has some limitations. The evolution of card frauds focuses on international level, and the frauds are treated undifferentiated. We intend to consider different regions and countries in our future research. Moreover, a separate analysis on each type of frauds should be taken into consideration into our upcoming studies.

References

Abdallah, A., Maarof, M. A., & Zainal, A. (2016). Fraud detection system: A survey. *Journal of Network and Computer Applications, 68*, 90–113. https://doi.org/10.1016/j.jnca.2016.04.007

ACFE. (2002). Occupational Fraud Abuse. Available at https://www.peoriamagazine.com/archive/ibi_article/2007/occupational-fraud-andabuse/#:~:text=Occupational%20fraud%20can%20be%20defined,employing%20organization's%20resources%20or%20assets.%E2%80%9D, Visited on 5 December 2022

Asha, R. B., & Suresh Kumar, K. R. (2021). Credit card fraud detection using artificial neural network. *Global Transitions Proceedings, 2*(1), 35–41. https://doi.org/10.1016/j.gltp.2021.01.006

Aurand J. (2020). What is carding, available at: https://www.binarydefense.com/what-is-carding/, visited on 15 December 2022.

Bagga, S., Goyal, A., Gupta, N., & Goyal, A. (2020). Credit card fraud detection using pipeling and ensemble learning, international conference on smart sustainable intelligent computing and applications under ICITETM2020. *Procedia Computer Science, 173*, 104–112. https://doi.org/10.1016/j.procs.2020.06.014

Bagnall J., Bounie D., Huynh K. P., Kosse A., Schmidt T., Schuh S., & Stix H. (2016). Consumer cash usage: a cross-country comparison with diary survey data. *International Journal of Central Banking*, *12*(4), 1–61. Available at https://www.ijcb.org/journal/ijcb16q4a1.pdf, visited 1st December 2022.

Bourreau, M., & Verdier, M. (2010). Private cards and the bypass of payment systems by merchants. *Journal of Banking & Finance, 34*(2010), 1798–1807. https://doi.org/10.1016/j.jbankfin.2009.10.004

Campbell, D., Grant, A., & Thorp, S. (2022). Reducing credit card delinquency using repayment reminders. *Journal of Banking and Finance, 142*(2022), 106549. https://doi.org/10.1016/j.jbankfin.2022.106549

Carcillo, F., Le Borgne, Y. A., Caelen, O., Kessaci, Y., Oble, F., & Bontempi, G. (2021). Combining unsupervised and supervised learning in credit card fraud detection. *Information Sciences, 557*, 317–331. https://doi.org/10.1016/j.ins.2019.05.042

Cheba, K., Kiba-Janiak, M., Baraniecka, A., & Kołakowski, T. (2021). Impact of external factors on e-commerce market in cities and its implications on environment. *Sustainable Cities and Society, 72*, 103032. https://doi.org/10.1016/j.scs.2021.103032

Cherif, A., Badhib, A., Ammar, H., Alshehri, S., Kalkatawi, M., & Imine, A. (2022). Credit card fraud detection in the era of disruptive technologies: A systematic review. *Journal of King Saud University—Computer and Information Sciences, 35*, 145–174. https://doi.org/10.1016/j.jksuci.2022.11.008

David, B., Abel, F., & Patrick, W. (2016). Debit card and demand for cash. *Journal of Banking and Finance, 73*(2016), 55–66. https://doi.org/10.1016/j.jbankfin.2016.08.009

Eriksson N., Stenius, M. (2022). Online grocery shoppers due to the Covid-19 pandemic—an analysis of demographic and household characteristics. Procedia Computer Science 196 (2022) 93–100. http://doi.org/https://doi.org/10.1016/j.procs.2021.11.077.

Femila, R. J., Naidu, G. B. S. R., Samuthira, P. V., Alamelu, S., & Mageswari, N. (2022). Autonomous credit card fraud detection using machine learning approach. *Computers and Electric Engineering, 102*. https://doi.org/10.1016/j.compeleceng.2022.108132

Forough, J., & Momtazi, S. (2021). Ensemble of deep sequential models for credit card fraud detection. *Applied Soft Computing Journal, 99*. https://doi.org/10.1016/j.asoc.2020.106883

Kawasaki, T., Wakashima, H., & Shibasaki, R. (2022). The use of e-commerce and the COVID-19 outbreak: A panel data analysis in Japan. *Transport Policy, 115*. https://doi.org/10.1016/j.tranpol.2021.10.023

Kim, E., Lee, J., Shin, H., Yang, H., Cho, S., Nam, S., Song, Y., Yoon, J., & Kim, J. (2019). Champion-challenger analysis for credit card fraud detection: Hybrid ensemble and deep learning. *Expert Systems with Applications, 128*, 214–224. https://doi.org/10.1016/j.eswa.2019.03.042

Kosse, R. (2013). Do newspaper articles on card fraud affect debit card usage? *Journal of Banking & Finance, 37*(2013), 5382–5391. https://doi.org/10.1016/j.jbankfin.2013.01.016

Li, Q., Zha, Y., & Dong, Y. (2023). Subsidize or not: The competition of credit card and online credit in platform-based supply chain system. *European Journal of Operational Research, 305*, 644–658. https://doi.org/10.1016/j.ejor.2022.06.003

Li, T.-H. (2022). Credit card and payday loan borrowing: Evidence in the SCF 2010–2019. *Economics Letters, 221*, 110872. https://doi.org/10.1016/j.econlet.2022.110872

Madan, M. S., & Reid, M. A. (1992). Data processing aspects of the integrated circuit and magnetic stripe cards. *Information & Management, 22*, 41–52. North-Holland. Available at: https://www.sciencedirect.com/science/article/abs/pii/037872069290005Z, visited on 29 December 2022

Madhurya, M. J., Gururaj, H. L., Soundarya, B. C., Vidyashree, K. P., & Rajendra, A. B. (2022). Exploratory analysis of credit card fraud detection using machine learning techniques. *Global Transition Proceedings, 3*(1), 31–37. https://doi.org/10.1016/j.gltp.2022.04.006

Malteseva I. (2022). 10 Ways to prevent credit card fraud (and avoid scams), Available at: https://www.aura.com/learn/how-to-prevent-credit-card-fraud, visited on 14 December 2022.

Reales, C. N., & O'Connell, J. F. (2017). An examination of the revenue generating capability of co-branded cards associated with frequent flyer programmes. *Journal of Air Transport Management, 65*(2017), 63e75. https://doi.org/10.1016/j.jairtraman.2017.08.001

Robinson, W. N., & Aria, A. (2018). Sequential fraud detection for prepaid cards using hidden Markov model divergence. *Expert Systems with Applications, 91*(2018), 235–251. https://doi.org/10.1016/j.eswa.2017.08.043

Ryman-Tub, N. F., Krause, P., & Garn, W. (2018). How artificial intelligence and machine learning research impacts payment card fraud detection: A survey and industry benchmark. *Engineering Applications of Artificial Intelligence, 76*, 130–156. https://doi.org/10.1016/j.engappai.2018.07.008

Rtayli, N., & Enneeya, N. (2020). Enhanced credit card fraud detection based on SVM-recursive feature elimination and hyper-parameters optimization. *Journal of Information Security and Applications, 55*. https://doi.org/10.1016/j.jisa.2020.102596

Sarofim, S., Chatterjee, P., & Rose, R. (2020). When store credit cards hurt retailers: The differential effect of paying credit card dues on consumers' purchasing behavior. *Journal of Business Research, 107*(2020), 290–301. https://doi.org/10.1016/j.jbusres.2018.08.031

Schmiedel H., Kostova G., & Ruttenberg W. (2012). The social and private costs of retail payment instruments: A European perspective. ECB Occasional Paper No. 137, visited on 28 December 2022.

Van Belle, R., Baesens, B., & De Weerdt, J. (2023). CATCHM: A novel network-based credit card fraud detection method using node representation learning. *Decision Support Systems, 164*. https://doi.org/10.1016/j.dss.2022.113866

Wang, S. W., & Hsu, M. K. (2016). Airline co-branded credit cards. An application of the theory of planned behavior. *Journal of Air Transport Management, 55*, 245e254. https://doi.org/10.1016/j.jairtraman.2016.06.007

Toohil R. (2022). Carding: The fraud technique destroying your credit, Available at: https://www.aura.com/learn/what-is-carding, visited on 11 December 2022.

Further Reading

European Central Bank. (2021). Eurosystem oversight framework for electronic payment instruments, schemes and arrangements. November 2021, Available at: https://www.ecb.europa.eu/paym/pol/activ/instr/html/index.en.html, visited on 29 November 2022.

Carding. Available at: https://www.imperva.com/learn/application-security/carding-online-fraud/, visited on 16 December 2022.

Gift cards scams. Available at: https://consumer.ftc.gov/articles/gift-card-scams, visited on 2 December 2022.

How to avoid a government impersonator scam. Available at: https://consumer.ftc.gov/articles/how-avoid-government-impersonator-scam visited on 5 December 2022.

How to recognize phishing. Available at: https://consumer.ftc.gov/articles/how-recognize-and-avoid-phishing-scams, visited on 5 December 2022.

Nilson Report. 2021 Issue 1209. (2021). Available at: https://nilsonreport.com/publication_newsletter_archive_issue.php?issue=1209, visited on 28 December 2022.
Skimming. Available at: https://www.fbi.gov/how-we-can-help-you/safety-resources/scams-and-safety/common-scams-and-crimes/skimming, visited on 10 December 2022
Statista a. Available at: https://www.statista.com/statistics/1192578/worldwide-share-of-consumers-that-shop-online/, visited on 28 December 2022.
Statista b. Available at: https://www.statista.com/statistics/1298838/leading-payment-methods-online-fraud-worldwide/, visited on 28 December 2022.
Statista c. Available at: https://www.statista.com/statistics/1273177/ecommerce-payment-fraud-losses-globally/, visited on 28 December 2022
Tipuri de fraude. Available at: https://www.bancatransilvania.ro/siguranta-online/tipuri-de-fraude, visited on 15 December 2022.
What is 3D secure. Available at: https://www.paycec.com/products-and-services/3d-secure-transaction?gclid=EAIaIQobChMIwPqG_IqA_AIVDvt3Ch19UQlpEAAYAyAAEgI0MfD_BwE, visited on 10 December 2022
https://www.portal.euromonitor.com, visited on 16 December 2022.

Daniela-Georgeta Beju is an associate professor, affiliated at Babeş-Bolyai University, Faculty of Economics and Business Administration, Department of Finance, Cluj-Napoca, Romania. She graduated in Finance—Credit specialization at the Faculty of Economics and Business Administration, "Babeş-Bolyai" University, Cluj-Napoca, Romania, in 1996. She acquired her PhD. diploma in Finance in 2001, at Babeş-Bolyai University, Cluj-Napoca, Romania. Since 2009, she is an associate professor at the Department of Finance, Faculty of Economics and Business Administration, Babeş-Bolyai University, Cluj-Napoca, Romania. She teaches the courses "Monetary mechanisms and institutions" and "Inflation, deflation and monetary systems" at the bachelor level and "Monetary policies" and "Risk management techniques in credit institutions" at the master level. Her research interests focus on banking risks, monetary financial institutions, monetary policies, fraud in banking sector, and digital money.

Codruța-Maria Făt is an associate professor affiliated at Babeş-Bolyai University, Faculty of Economics and Business Administration, Department of Finance Cluj-Napoca, Romania. She obtained her PhD. in the Finance field in 2003, at Babeş-Bolyai University, Cluj-Napoca, Romania. Since 2006, she has been an associate professor at the Department of Finance, Faculty of Economics and Business Administration, Babeş-Bolyai University, Romania. She teaches the disciplines "International finance," "Financial derivatives," "International Banking," and "Commodities exchanges" at the Faculty of Economics and Business Administration, Babeş-Bolyai University, Romania, and modules of International Economics and Financial derivatives at IAE de Caen, France. She has research concerning the area of international finance, international banking, financial derivatives, economic and monetary union, and business performances. She is responsible for Banks and Capital Markets Master Program of Department of Finance, Faculty of Economics and Business Administration, Babeş-Bolyai University, Romania.

Chapter 3
A SWOT Analysis on Illegal Logging and Corruption: Romania Case Study

Adeline-Cristina Cozma and Monica Violeta Achim

Abstract Illegal logging has come to the attention of the public eye for several years. Violent conflicts resulting even into murdering the rangers that tried to protect the forests represent a serious alarm for the general population regarding the extent to which corruption can go. As one of the three pillars of economic and financial crimes, corruption represents the core of illegal logging, which brings ultra-high incomes to those involved. Interested groups become organized crime networks as they exploit wood without permits and avoid taxes. There is a stringent need for a clear and deep understanding of this phenomenon. The aim of this study was to provide a SWOT analysis of the role that corruption plays in the exploitation of wood and to find practical countermeasures by interviewing experts involved in protecting the forests. Even though the legislative framework in Romania is appreciated to be of good quality, its implementation seems to be the problem. The politicians, who are also considered to be highly responsible for the theft of the wood, are not eager to take and implement decisions in their power to stop these environmental crimes. Education and technology are identified as the key drivers for protecting the forests more efficiently. It is a general expectation of those interviewed that Romania will achieve higher sustainability over time.

Keywords Corruption · Illegal logging · SWOT analysis · Interviews · Countermeasures

Jel Classification D73 · F18 · F64 · K32 · L73 · O17

A.-C. Cozma (✉) · M. V. Achim
Faculty of Economics and Business Administration, Babeș-Bolyai University, Cluj-Napoca, Romania
e-mail: adeline.cozma@econ.ubbcluj.ro

M. V. Achim (ed.), *Economic and Financial Crime, Sustainability and Good Governance*, Contributions to Finance and Accounting,
https://doi.org/10.1007/978-3-031-34082-6_3

1 Introduction

Illegal logging phenomenon is both an environmental crime considering its negative effects as it is an economic and financial crime because of its means. Achim and Borlea (2020) classify the types of economic and financial crime into three main pillars: corruption, shadow economy, and money laundering. Illegal logging can only happen when the people involved are corrupt. Because there are no proxies for illegal logging, the most accurate measurement for research is the difference in forestland in time. The relationship between corruption and deforestation was studied by Cozma et al. (2022) and by Cozma et al. (2021), who proved that economic and financial crime and deforestation have a significant relation, meaning that, statistically, corrupt countries and/or countries that have high levels of shadow economy also have a higher level of deforestation. Having this hypothesis confirmed, the next step is to qualitatively analyze this phenomenon, in order to have a holistic understanding of it and to be able to identify proper solutions.

Two-thirds of Europe's last virgin woods, which are home to the biggest wolf, bear, and lynx populations on the continent, are in Romania. Yet, massive degradation in once-pristine forests has been caused by illicit logging and bad forest management. The University of Maryland and Greenpeace examined satellite data and discovered that Romania lost 280,000 hectares of forest between 2000 and 2014, according to Environmental Investigation Agency (2017). National parks and other protected areas housed about half of the lost forest. Since more than 10 years ago, illegal logging in Romania has been generally acknowledged by the authorities, the media, and environmentalists as a significant issue. According to a recent assessment by the Romanian National Forest Inventory, 49% of the wood harvested between 2008 and 2014—or 8.8 million m3 of timber—was illegally exploited.

A more recent investigation by Der Spiegel (Kuchlmayr et al. 2023) shows that Romanian forests, some of the oldest in Europe, provide more than half of the wood that is illegally harvested globally. Major Austrian corporations are charged with making money off of illegal logging in Romania. According to a report by the German magazine Der Spiegel, despite having some of Europe's oldest woods, those forests are in danger due to widespread illegal deforestation. In the study, the journalists detail how Austrian businesses with tens of thousands of employees amassed wealth by signing contracts with Romanian suppliers that harvested wood illegally. The German journalists focused their investigation mostly on the forests in Suceava, a northern county in Romania. A prior extensive investigation by the Romanian authorities in the town of Bogdănești, in which 1800 Romanian investigators took part, served as the basis for the Der Spiegel story. Illegal deforestation, money laundering, and tax evasion are among the offenses that the Romanian police are looking into. The huge Austrian timber businesses Egger and HS Timber were also the subject of the Romanian authorities' inquiry, which the German journal speaks about. With a revenue of more than four billion euros and more than 11,000 workers, Egger is one of the most significant mast manufacturers in the industry. According to Der Spiegel, HS Timber, the other significant Austrian business in the

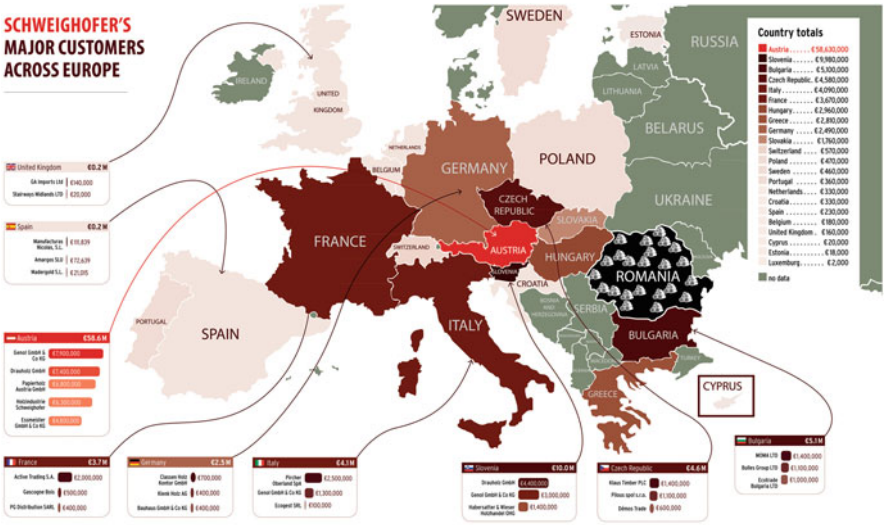


Fig. 3.1 Schweighofer's (HS Timber) major customers across Europe. Source: https://us.eia.org/blog/romania-widespread-illegal-logging-within-the-european-unions-borders/

sector, has a facility not far from the Egger branch in Rădăuți. HS Timber was the subject of a scandal in 2015 over the processing of wood from illegal deforestation (Fig. 3.1). The two businesses are now being accused of collaborating with some illegal forest exploitation in Romania.

However, even though there are several academic studies regarding environmental crimes based on interviews, the vast majority of them lack diversity in the expertise of the interviewees, limiting the horizon of the analysis, and mostly focusing on tropical forests. Moreover, some research fails to compile the results in order to identify key drivers and suitable solutions, stating only the main finding of the analysis. All these create a gap in research regarding the holistic analysis and practical approach to illegal logging countermeasures.

The aim of this paper was to identify efficient and effective countermeasures for illegal logging by using a SWOT analysis created based on interviews with experts involved in protecting the forests from different fields of professional activity and from different countries. This type of analysis gives a complete, in-depth, yet structured perspective on this phenomenon that offers the basis for identifying suitable solutions that can not only be applied to Romania but also in every country that faces this problem.

Although Romania's legislative structure is acknowledged to be of high quality, its enforcement appears to be the issue. The people on the political stage, who are also considered to have a significant role in the theft of wood, are not eager to take and put into action measures in their sphere of competence that might prevent these

environmental crimes. The most important factors for more effective forest protection are considered to be technology and education.

Among the solutions proposed, the most effective one seems to be the independence of the control bodies, along with the depoliticization of forestry organizations, the continuous development of technology used in the field, educational programs for children, supporting investigative journalism in order to expose potential crimes and to create public pressure, the involvement of citizens, simpler normative acts without loopholes, environmental courts, and so on.

2 Literature Review

In the field of illegal logging, very few articles discuss the phenomenon from an economic point of view. In the Web of Science database, only 140 indexed articles include the keywords "corruption" and "deforestation," in the Scopus database 145, in Springer Link Journals 391, in the ACM Digital Library 20, in the ScienceDirect database 24, in the Emerald Insight database only 1, and in the IEEE Transactions none.

The largest type of research on this topic considering the methodology is descriptive studies, which are based either on the analysis of primary qualitative data (interviews and focus groups) or on the analysis of secondary data. These studies are chosen to be further discussed as the most impactful ones based on the quality of the journal and the number of citations.

Several academic researchers have published studies based on interviews. The articles discuss the factors underlying illicit logging and its relationship with corruption. For instance, Harwell (2009) observes that illegal logging is a widespread and diversified activity in Indonesia, which he analyzed through interviews with government representatives, journalists, and activists. According to Pellegrini (2011), Pakistani forest officials tolerate certain companies collecting more timber than is permitted by law. The governmental system has been extensively penetrated by a "wood mafia" that pays bribes to sanction timber trafficking. Another research in this area was carried out in Southern Tanzania by Milledge et al. (2007), and they concluded that corruption is the key factor in the facilitation of illegal wood exports. After conducting 162 interviews with Indian foresters, Robbins (2000) finds out that some local barons are able to avoid the law and to clear out the forests at an excessive rate due to corrupt tactics. Miller (2011) discusses the findings of 15 expert interviews and identifies the most used method by corrupt officials to enable illegal logging: police accepts bribes to permit the transport of wood without the required documentation, and forestry officials issue permits that are never stamped, allowing an operator to reuse this document repeatedly. Teye (2013) undertakes a thorough investigation based on interviews with 24 enterprises engaged in illegal forestry activities, 105 residents of Amutu and Bami, and 102 personnel of Ghana's Forest Service Division. The results of this study demonstrate that corruption is partially to blame for Ghana's high rate of illicit exploitation. He comes to the conclusion that

governmental officials' and private timber corporations' interests come above the general needs of the country.

Another category of the methodology used in the papers that discuss illegal logging and corruption is the one based on the analysis of other studies. These articles offer innovative ideas for future study, comprise the findings, and/or and indicate the present gaps in the literature. The causes of deforestation are identified by Angelsen and Kaimowitz (1999) after analyzing 140 studies. They include final agricultural production costs, agricultural raw material costs, wages and employment, credit availability, technological advancements on farms, accessibility, ownership and tenancy laws for forested lands, land security, and wood prices, but they leave out corruption. Sundstrom (2016) examines 27 empirical studies and 10 other research, noting that they all concur in suggesting that illegality in forest management is often permitted by corruption at various levels and that this is true in both time and place. A number of recommendations were made to the World Bank by Callister (1999), including the formation of a working group to combat unlawful forestry practices and a partnership between the World Bank and the World Wide Fund for Nature. The process behind bribery, forest management decisions (legal and illegal) of foresters, and government policy decisions—while taking into account various assumptions about various forms of corruption, markets, information, and bargaining power of every country—all need to be understood, according to Amacher (2006), if we are to understand the relationship between corruption and deforestation. With the purpose of eradicating corruption, Adela and Saragih (2017) concentrate on research in Indonesia and make the case for collaborative management in government. According to Maina (2018), previous research has shown that corruption has the potential to destroy a nation's forests, and it is urgently necessary for studies to explain how much corruption contributes to the ongoing loss of forested area in the context of numerous reforms intended to boost the performance of the forestry sector. Lopez and Mitra (2000) arrive at a significant conclusion: Pollution levels are always above what is desirable from a social perspective, regardless of the form of interaction between the enterprise and the government, at any amount of per capita income.

Also, there is a category of studies that uses case studies, benchmarking, or other techniques to process secondary data. Although the time periods, geographic regions, topical stances, and particular situations vary, they all demonstrate the corruption-related reasons for illicit forestry. Siebert and Elwert (2014) analyze deforestation in Benin, Africa, and discover that corruption of civil workers has a significant part in the illegalities that occur in public property woods. According to Bulkan and Palmer (2008), corruption is the main obstacle preventing government authorities in Guyana, South America, from effectively controlling concessions for long-term deforestation. Due to extremely cheap forest taxes and substantial earnings from unreported wood exports, corruption exists in a favorable environment. The state itself acts in a criminal manner, permitting the disregard of technical restrictions designed to enhance forest management or using them selectively to target loggers without political clout. Relationships between senior and junior forest officers and forest managers are maintained. Small-scale loggers raise their revenues

by exceeding the quota, and in exchange, they pay lower-level government employees to conduct fraudulent inspections. According to Brockington (2008), who focuses on resource management operations in Tanzania, creating an effective ministry of natural resources would be a protracted battle that requires creating accountable institutions and developing a democratic culture. However, Søreide (2007) compiles a list of recommendations on inter-institutional dependencies, conditionality, good practices adopted from developed countries, concession mode, transparency, firms as whistle-blowers, and independent forestry authorities.

It can be observed that most studies focus on tropical forests, only a small of researchers collected interview from a variety of experts, very few draw some recommendations, and none of them use SWOT analysis as a basis for the identified solutions. This is the gap identified in the literature that this article tries to fill.

3 Methodology

This study is based on six interviews with Romanian experts involved in protecting the forests from various fields of activity. Interviews were collected using video meetings and in writing, from December 2022 to February 2023.

The highest-ranked official interviewed is Ms. Adriana-Doina Pană (DP), who is a Romanian politician, and deputy in the Romanian Parliament in the 2012–2016 legislation from PSD Bistrița. In the second half of 2017, she was Minister of Water and Forests, in the government of Mihai Tudose. Previously, she was Minister Delegate for Social Dialogue in the Second Ponta Government and Minister Delegate for Water, Forests and Fisheries in the Third Ponta Government. In January 2018, Doina Pană resigned from the position of Minister of Forests, citing that she has health problems and complained that she was poisoned with mercury, pointing to the "wood industry mafia" as possible culprits.

Another important vector in combating illegal logging is represented by investigative journalists. Mr. Andrei Ciurcanu (AC) graduated from the Faculty of Journalism in Iași in 2006. Since then, he worked for Evenimentul Zilei—a national newspaper, Realitatea TV, and Antena 3—national television and he was the head of the Agent Green investigations department. Now, he is an investigative reporter at Rise Project and Organized Crime and Corruption Reporting Project and also a contributor to Dilema Veche, Courrier de Balkans, Arte TV, and Al Jazeera International. Some of the investigations carried out were awarded at competitions in the country and abroad (United States of America and Great Britain). In 2011, he was awarded by the Association for International Broadcasting in London for Highly Commended Award/Best Investigation Report. He also obtained a Gold Award for Best Investigation at the New York Film Festival in April 2016. He won the first TV & Video Journalism Award at Superscrieri Gala 2017 and a Jury Prize in 2021 at the same gala.

The work of NGOs also has an impact on minimizing illegal logging. The Conservation Carpathia Foundation was created in 2009 by 12 philanthropists and

conservationists with the aim of stopping illegal logging and preserving a large area of the Carpathian forests as a fully protected area for future generations. This was done by buying land and assigning hunting rights, for the complete protection of all-natural elements, with private and public money. They intend that eventually the ownership of their lands will return to the public domain, under permanent protection, in the form of a National Park. Their technical director, Mr. Mihai Zotta (MZ), forestry engineer, has previously worked at two Forest Ranges and at the National Directorate of Forests. He works for the foundation for more than 12 years.

The research field is represented by Mr. Florin Stoican (FS), a geologist with expertise in the management of protected areas, biodiversity and geodiversity conservation, ecotourism, and ecological education. He is also an environmental activist, specialist in sustainability, and one of the founders of the Văcărești Natural Park Association, an organization that established the only urban nature park in Romania. He is now the director of Oltenia de sub Munte UNSECO aspiring Geopark and the president of the Kogayon Association, a national NGO in the environmental protection field specialized in the management of protected areas, geodiversity and biodiversity conservation, ecotourism, ecological education, promotion, and informing and creating public awareness on environmental issues and local sustainability development.

As for Forest Ranges representatives, Mr. Nicolae-Cătălin Dinucă (CD) and Mr. Ion Gavrilescu (IG) were also interviewed. The first one is an office manager at the Gorj County Forest Range and has a Ph.D. in Forestry—ecological reconstruction, as Mr. Gavrilescu is a senior councilor of the Brașov Forestry Range and a former employee of the Forestry Research and Development Institute—National Forestry Inventory Service. Because the first layer of illegal logging is represented by forestry workers, their perspective is of great importance.

The interview was based on 18 general questions regarding the causes, the measures, the direct and indirect effects, the used techniques, the improvements in the field, the accomplices, and the third parties involved in the illegal logging phenomenon in Romania but also few specific questions for each interviewee depending on their professional activity. Its structure is entirely reproduced in Appendix.

4 Results and Discussion

A SWOT analysis is further conducted, as it offers the possibility to present the results of the interviews in an organized and comprehensive way and to create the proper basis for identifying the most efficient and effective solutions that might be applied not only in Romania but also in any country that faces this problem. The main strengths and weaknesses of the forest protection system, with all its actors, from public institutions to NGOs, and from foresters to ministers and to citizens, as they resulted from the interviews, are further discussed. The opportunities and threats to protecting the forests, to sustainably exploiting the wood, and to

minimizing illegal logging are also analyzed in the following subchapters. This analysis serves as a solid and complete basis for the identification of efficient and effective countermeasures to illegal logging, as it takes into consideration all the elements involved in protecting and sustainably exploiting the forests.

4.1 Strengths

The main positive aspect identified from the discussion with the experts is the legislative framework, which is appreciated to be mostly adequate by all the respondents, yet perfectible. DP was directly responsible for the forestry laws as Minister of Water and Forests. She says that the primary legislative framework (at the level of laws) regarding the sustainable exploitation of forests was and is ensured at a high level by the Forestry Code. If there were no cases of illegal logging, Romania would be an example of good practice worldwide, the Romanian School of Forestry being excellent. However, the primary legislative framework for forest protection (Forestry Code, Forestry Offenses Law, Forestry Personnel Statute) has been substantially improved only since 2014, with very big obstacles encountered by DP on the legislative path, although illegal logging had already reached alarming levels. She says that it can still be improved in some places, but, even as it is, if the state institutions would follow the correct and consistent application of the existing legislation at the present time, the level of illegal cutting would decrease a lot. Thus, she considers the quality of the primary legislative framework in Romania to be good in terms of both sustainable exploitation and protection of forests in Romania. She also talks about the Forest Radar, an application that is based on an extension of the SUMAL computer system, a development in addition to the requirements of Regulation (EU) no. 995/2010 establishing the obligations of operators who introduce wood and wood products to the market, so that the path of the wood from the time it leaves the forest to the final recipient (furniture or export) is tracked in real time through the Forest Radar. It is a unique system in Europe, possibly in the world, and very efficient. The application of the Forest Radar no longer allows complicity between the forester, the economic agent, and the police regarding the legality of wood transport, being an IT application that follows the path of the wood from the forest to the final recipient in real time, no matter how long this path is and how many warehouses does it go through.

After almost 10 years of investigations in the area of the environment and ecological crime, years in which AC interacted with specialists in the forest timber sector, he believes that the legislation in the area of the forest sector and forest management was always one that could be perfected, but which covered the big loops and weaknesses in the system.

On the same note, IG states that the exploitation of forests is allowed and is done in compliance with the restrictions of the legislation of the forestry regime, at the same time taking into account the protection of the soil and the existing vegetation, promoting mainly treatments that promote the natural regeneration of most species

from the forestland, with small exceptions species like spruce or poplar monocultures, where no other silvicultural treatments are possible and clear cuts with artificial afforestation are allowed. Moreover, he explains that the "traceability of timber" system—SUMAL 2.0—is established by the Ministry of Environment and developed by the Special Telecommunications Service. It represents a big step forward in combating illegal timber harvesting in Romania, IG believes. The SUMAL computer system also has an extension intended for the population. For the immediate verification of the legality of the transport of wood materials on forest and public roads, there is the Forest Inspector app, an application that represents a component for the population of the Integrated Information System for real-time monitoring of timber in Romania. The application is accessible free of charge to the population for the purpose of verifying a wood mass transport where there are suspicions. It also allows immediate verification of the legality of the transport by entering a registration number, facilitating the involvement of civil society in monitoring the wood mass transport. Through the SUMAL application, every wood shipment is monitored and can be controlled. The way the Timber Traceability Tracking System is designed, the carrier is required to take photographs (front, back, and side and onboard mileage) of the means of transport being loaded into the system. On the whole, the route of the means of transport with wooden material will be seen online, the carrier is obliged to keep the device on which the information was loaded with all the open data in GPS coordinates, and this way the suspicions of multiple transport were eliminated. At the final unloading point of the wood material, the carrier will hand over the notice to the manager of the respective warehouse, and he closes the notice. Practically, in this way, multiple shipments cannot be made.

All in all, the legislative framework and the digital tools (SUMAL and Forest Radar) are the main strengths in protecting the forests in Romania.

4.2 Weaknesses

AC thinks that as in any field of crime, the controlling authority is always one step behind the criminals—if only for the simple fact that the criminals can hatch the scheme of theft without the authority preventing it. It is almost impossible for an authority to foresee a crime, especially in a state where policies and strategies are not made for the medium and long term, regardless of the field concerned—education, security, economy, and in this case the administration and judicious management of the forest fund. Faced with the phenomenon of illegal logging, we must recognize that the Romanian state, through the control, verification, and regulation authorities, has lost the start, AC says. This is visible from the satellite, with mountain areas where entire slopes have been exploited illegally and without any respect for the environment and the local community, areas where regeneration is extremely difficult to achieve, if not impossible.

CD explains how, in 2017, through Law 175/2017, an article was introduced that, from his point of view, promotes these illegal cuttings. Before the promulgation of

this law, foresters were patrimonially responsible for any damages. Certain diligence was done: The foresters drew up reports, which were analyzed by the head of the Control Department and by the head of the Patrol Department, and which entailed patrimonial responsibility. After the introduction of this law article, the report drawn up by the forester is submitted at the Forest Range, and within 24 h, it is forwarded to the police or the prosecutor's office, and thus, these illegal cuttings are justified. In most of the cases, the perpetrators are not found. In his view, this article should be removed, because it leaves a lot of slack for public servants. It lets them not do their jobs, even though they are paid for it. Then, he says that Law 171/2010 on forestry offenses should be tightened a bit. For example, before 2017, if the forestry structure cut more than permitted by the forestry management, it was punished, in addition to the contravention, by calculating amounts obtained from the difference in volume multiplied by the average price per meter, money that was transferred to the land improvement fund with forestry destinations. This measure was, however, repealed. He says that the punishments are very mild compared to the scale of the phenomenon and the acts committed by the forestry personnel. From his point of view, these coercive measures should be tightened. For example, if you know that you get a 10,000 lei (2000 euros) fine for authorizing a few thousand cubic meters, there is no problem, because you pay half of the minimum in 15 days, an amount that is usually paid by the economic agent who wanted the cutting and so the problem was solved. All subsequent legislation on the forest fund should be updated so that the forest has an ecological role and is exploited sustainably, CD says. Another legislative change would be related to Ministerial Order 530/2019, CD thinks, more precisely the procedure for taking over all non-administered surfaces. Forest Ranges were nominated in each locality that should take over these areas, but this has been postponed since 2017. At the level of Gorj county, there was 36,000 ha, CD got involved a lot, and at the moment there is still 5000 ha to be taken over. From his point of view, if a term of 60 days were introduced to take over these surfaces, there would be a minimization of these illegal cuttings, because there would be a manager. The delay in taking over these areas also has an economic role for the beneficiaries of illegal logging in these areas, be they local people, forestry personnel, or the political environment.

MZ believes that one of the problems at least as big as illegal logging is the fact that certain forests of very high biodiversity and scientific value are being lost through legal logging. These are old forests that have not been classified as virgin forests that are over 140–150 years old and that have an inestimable scientific value compared to the value of the wood that results from it.

On another note, IG thinks that the human quality factor remains the largest problem in combating the illegal logging phenomenon, referring to the moral principles and education values of each individual responsible for protecting the forests.

The reactive mindset of those in power, few legislative loopholes, the wrong classification of the forests, and the lack of fairness of those involved in protecting the forests represent the main weaknesses for Romania's forests sustainable management.

4.3 Threats

Obviously, the main threat in protecting forests is the "wood mafia," as the Romanian media calls the groups of interest that benefit from the illegal exploitation of forests.

Asked about who might be involved in such groups, AC starts by defining the mafia as a group of individuals who act together to commit an illegality that can benefit the group. The Criminal Code article 367 paragraph 6 describes the organized criminal group as one "structured, made up of three or more persons, established for a certain period of time and to act in a coordinated manner for the purpose of committing one or more crimes." To identify the organized groups that revolve around the commission of illegal acts in the forest fund or related to the exploitation of wood, we only have to look at the timber trail to identify the mechanisms and professional categories involved/actors. The forest is managed and guarded by foresters, based on legislation. No forestry work can be carried out in the forest fund without the presence of an employee involved in the administration. The marking of trees, compliance with forestry plans, and assessment of volumes are done by forestry employees. The exploitation of the forest is carried out by commercial agents who either won a lot at the auction, in the case of the state public forest, or signed exploitation contracts in the private forests. Exploitation is carried out (both state and private) based on forestry plans (10-year plans outlining the works to be carried out on certain areas of land and the estimated volume to be extracted), which are voted on by order of the minister. Logged wood from the forest must be transported by specialized companies that have special transport equipment. The employees of these companies are required by law to draw up legal transport documents for the goods they load. The processing of the wood that is exploited and transported from the forest fund is ensured by economic agents who, like the exploiters and transporters, must draw up the documents required by law for the wood received at the factory gate. After analyzing the wood route and identifying the "actors," we turn our attention to the authorities that have the right to control the case of the exploitation and transport of wood materials. These institutions are the Romanian Police (Ministry of the Interior), the Forest Guard (Ministry of the Environment), and in some cases the Control Body of Romsilva (Ministry of the Environment). These bodies can verify whether the exploitation and management of the forest fund were done judiciously and complied with the legal criteria. The last level is represented by magistrates—prosecutors and judges. This professional category is involved in the good administration of the forest fund (private and public) when there are investigations and criminal complaints made by those from the Ministry of the Interior and the Ministry of the Environment level. If the failure of administration in the forest fund is found, then one or more of these "organisms" did not fulfill their purpose and/or collaborated for group interest. From the perspective of creating the image of the wood mafia in the context of the exploitation and processing of wood without legal documents, AC thinks that the following paragraph is representative, a component part of the 2015 control act of the Territorial

Forestry and Hunting Inspectorate Cluj, in the case of investigations into the activity of Holzindustrie Schweighofer (HSR), a company investigated by the prosecutors of the Directorate of Investigation of Organized Crime and Terrorism Offenses: "From the presented cases, the suspicion arises that forestry personnel from some authorized forestry structures, some representatives of HSR Sebeș from the territory and some commercial companies that provide exploitation services or supply wood material to HSR Sebeș, make available to this company wood material without legal provenance, on a chain that gives an appearance of legality to the value of the wood mass—the authorization of the parquets—their exploitation—the exploitation controls—the reception of HSR Sebeș in the primary platform (following the controls in the field, it appears that the company does not draw up documents in this sense)—issuance of accompanying notices with fictitious volumes—resumption of prosecutions—value settlement of contracts by HSR Sebeș."

He concludes that it is difficult to pencil in/identify exactly the characteristics of the wood mafia. These characteristics and the composition of the criminal group differ from case to case, depending on the complexity of the criminal scheme and the purpose of the criminal group.

CD believes that these interested groups are made up of forestry personnel, forestry directors, and forest guards. There are many involved, in all structures, who have been making these little deals for years, including the police, from the level of head of the station to the central structure, at the level of inspectorates; and the political factor, from the local level to the party leader. There are many people in the system who, although they do not have results, resist due to the fact that they serve the electoral interests in the campaigns and serve the economic interests of the political factors. Hiring is done for an amount of money. There is no transparency in the hiring process, and it is done according to the affiliation of a political party or the decision of influential people.

On the same note, FS thinks that these groups, larger or smaller, are often made up of owners, foresters, logging companies, and representatives of the authorities, who take advantage of the current system to obtain untaxed and illegal benefits from forest exploitation.

DP states that there is no one person who leads the timber mafia, even if the means of attack are discussed in a very narrow circle composed of the big exploiters, inside the Association of Foresters in Romania (ASFOR), an association used in sight to support some requests at the government level. Mafia-type attacks are not practiced by ASFOR as an association. They are practiced individually or in extremely small groups of people with huge financial possibilities, through a dragon-like system with many heads and enormously many arms that buy or blackmail or, in the last resort, eliminate people in positions of decision or influence regarding the taking of measures that would bring them great financial losses. When it comes to huge financial losses, then the mobilization is maximum, and all ends of the dragon intervene a lot of money to buy as many people with influence and/or political decision-making power as possible, in parallel with as many blackmails as possible, in parallel with paid specialists/paid press to denigrate the initiator of the measures by false manipulation as if those measures would not do the field good but, on the

contrary, bad, etc. As a first example to sustain her affirmations, DP talks about how she and her colleagues in the Parliament amended the Forestry Code, and among the many disturbing measures for all logging and wood processing companies, there was also a measure that provided for the prohibition of monopoly, which only affected the Schweighofer Company. The inconvenience was huge, estimated by them at about 150 million euros annual loss. There was only one head of the dragon that fought for this measure, but with many arms: through parliamentarians who were absent from the final vote (the Forestry Code is an organic law that, in order to pass, requires at least half plus one of the total number of deputies, not only to those present), through TV studios where specialists in the field or even parliamentarians talked about how bad all the changes are, including this one, and how they will lead to an increase in illegal logging, not a decrease, and through pressure on ministers, reaching the Prime Minister and the President of Romania. One of the arms also reached the Competition Council, which sent a letter to Parliament saying that the measure is anti-competitive and harms the free market. They wrote to the Prime Minister that they would have to close all the companies and there would be tens of thousands of unemployed people, and when Prime Minister Victor Ponta was not impressed, the Austrian ambassador asked for an audience and declared that if the measures DP proposed will come into force, all Austrian companies will leave Romania, not only those in the wood sector. Still without success! Instead, they succeeded with the President of Romania, who instead of promulgating the law that was so difficult to vote (many deputies were absent, citing various reasons) returned it to the Parliament citing the exact amendment of the articles, which were bothering those in Schweighofer's management and sustained with the arguments of the Competition Council! If the American Environmental Investigation Agency had not sought her out to give her hidden camera footage of the Schweighofer company in which they not only bought illegally cut wood but also gave bonuses for it, footage that she presented to her fellow parliamentarians and then she sent it to the television with the largest audience at that time, the new Forestry Code, without the changes requested by the president, would certainly not have been voted on! The second example is when the Forestry Code was amended again, also at her initiative. In the last minutes of the Chamber of Deputies meeting, without passing through the Senate and, therefore, unconstitutionally, an amendment was introduced in the Agriculture Committee. It specified that firewood from the state's forests will bring back the economic agents as intermediaries, even though a year before, DP had succeeded to implement a procedure that removed the economic agents from the auction and wood from fallings and thinning and hygiene products were sold directly to the population. In order to succeed in convincing the deputies to vote for the amendment of its return to the economic agents, three deputies, forestry engineers by trade, from three different parties (Social Democratic Party, National Liberal Party, and Alliance of Liberals and Democrats Party), claimed that all the arguments presented by her are wrong, as she does not have forestry studies and that in fact the firewood crisis will increase if that change is not made, through which economic agents bid and sell firewood to the population. The three being from different parties, the vote being political, it went to the committee vote, to be voted on in the Plenary

in the autumn parliamentary session, because the parliamentary vacation was coming up, but surprise, in the last Plenary (parliamentary vacation started the next day), it was put on the agenda the three deputy forestry engineers from three different parties supported what they also supported in the committee, upsetting the majority of the deputies. DP went to the microphone again and explained once again, in simple terms, for everyone to understand, what the mechanism is, insistently asking her fellow deputies not to vote for that amendment. She also explained that, from the statistical data, when bidding, only 3% of the total firewood was sold by the economic agents to the population, the rest went to the big processors, being one of the causes of the firewood crisis. They all understood what was going on, but at the vote, because the group leaders of the three parties raised their hands to vote, even though many assumed and voted as she asked, it passed. The arms of the mafia reached the leadership of the three parties. One of them was her party, whose president was absent that day for the vote, even though he was the president of the Chamber of Deputies, and who later calmly lied to me that he did not know it would be on the agenda and that in the fall we would adjust things. Obviously, nothing happened "in the fall." A third example is when she introduced, as a minister, in 2014, in parallel with the Government Decision on the Forest Radar, the 112 system for the transport of wood. She had to have a protocol signed between her ministry, the Special Telecommunications Service, and the Ministry of the Interior. The Minister of the Interior kept putting off signing, without citing a specific reason. She appealed to the Prime Minister of that time to mediate and after a minute of thinking he said to her: "It's urgent, so let him go without his signature. He will learn from TV that it is already working, and he will not politically allow himself to come out and say that he did not sign, so he will be forced to sign." Obviously, this was exactly the case. Because the Prime Minister supported her, all the mafia's efforts failed. She concludes that the prime minister does not take measures, you do, as a minister, but his support is vital. In any government, if the prime minister does not agree with a measure you want to take as a minister, you do not stand a chance. You can only resign by making the reason public.

4.4 Opportunities

On the opposite pole, the main factors that have a huge role in protecting the forests that were identified in the discussions with the experts are civil society and the NGOs, as well as investigative reporters.

AC states that from the perspective of democracy and the democratic game, Romania is "in the early stages." The movement and activity of NGOs started quite late—a fact recognized both at the national level and especially at the international level. In any democracy, it is society/integrity whistle-blowers who raise the first alarm bells. In the context of the attacks on the forest fund and the large quantities of illegally cut wood, until 2015–2016 the situation of Romania was not known at the European level, although at the political and administrative level it was

well known the gravity regarding the level of corruption in the sector and the destruction of the forest fund and of protected areas, drawn by treaties and international conventions. For example, in 2015 investigative journalists revealed that the Austrian giant, Holzindustrie Schweighofer, was processing illegally cut wood and that forests included in protected areas were falling victim to chainsaws. "If I were an international company and had to choose between buying land or forest in Austria or in Romania, I would definitely buy a forest in Romania. Because of the price and the Government. You have a cheap forest and an equally cheap Government. In Austria, no one would accept that the disaster in your forests should also happen in our forests. No one would accept that. Why do I, as a green politician of the Parliament of Austria, and I have not been a parliamentarian for a few months, but for 27 years, why do I have to wait for a television team from Romania to give me first-hand information about this major issue, looking at the behavior of businessmen in Austria? Why is there this incredible lack of information? What do your NGOs do?" said Peter Pilz, the president of the Green Party in Austria. As for civil society (communities), most of the time the illegal activities were done with the complicity of some residents/owners, or the illegalities were committed by not involving the majority of the community (the illegal/criminal acts were not reported at the time of their commission). This topic can of course be developed and analyzed for the reasons for non-involvement—lack of interest, fear of repercussions, mistrust of state authority.

CD also believes that the locals are accomplices, being the beneficiaries of these illegal cuttings, together with some of the forestry personnel. In those areas, local people are allowed to cut wood illegally by forestry personnel, and they share the earnings. Timber is also produced, not just firewood. In his field of activity, he tried as much as possible to deconstruct these local interests.

FS emphasizes that the role of civil society is very important. Transparency of the system and education of people would solve a lot. If everyone would check the forest exploitations they pass by and report any suspicions to the authorities, things would radically improve.

Also, MZ points out that the Forest Radar, the app where anyone could enter a log truck number to see if it was legal or not and then be automatically redirected to the police, was extremely effective, but only from the moment it became public. It was available before, but only the authorities had access to it, i.e., the forest areas only within its range, as well as the inspectorates and the police. If the application was available earlier, why was this phenomenon not controlled earlier? he asks himself. He considers this to be clear evidence that the public, seeing in the media what is happening, has led the political factor to take certain measures.

As for the role of NGO in combating illegal logging, CD thinks that some NGOs have a very good activity, in the sense that they discover certain irregularities that the forestry staff do not want to reveal. Any area of forest is subject to two background checks annually: one in spring and one in autumn, but also whenever necessary. These NGOs bring these irregularities to the surface and then there is resentment among the forest staff, but there are also situations when NGOs represent certain interest groups and then certain companies play vicious games and present fake news

and erroneous information. Some of the NGOs are beneficial and love the forest and nature, but there are also certain NGOs that are likely to play the games of the big corporations to destroy, for example, the National Forestry Authority or to destroy the timber market in Romania. There is a lot of fake news about the National Forestry Authority and how to manage forests sustainably, and not all the information presented has come true.

FS believes that the role of NGOs is extremely important. Without them and without the media, we would not have had so much attention paid to the forest. The activity is effective but more punctual, without noticeable systemic results. Some have studied virgin forests, some have established and administered protected areas, some are planting, some are doing activism with protests, lawsuits, and campaigns, and many are doing environmental and forest education.

MZ also believes that the impact of NGO activity is quite significant. In particular, in recent years, investigative journalists have been more effective than NGOs.

On the same note, IG appreciates the involvement of certain NGOs such as Greenpeace or WWF Romania who, through environmental or forest specialists, have shown concern and involvement in studies about forests, biodiversity, or environmental protection. However, he does not agree with the aggressive NGOs that promote distorted information in the public space, which are not scientifically or practically substantiated, promoting the opinions of non-specialists; in this way, we are only witnessing a media circus and the discrediting of Romania abroad.

This being said, these vectors must be carefully managed in order to enhance the opportunities, and not the threats.

5 Conclusions and Proposed Solutions

Taking into consideration the high quality of the legislative framework but also its loopholes, the "wood mafia" and the role of civil society, NGOs, and investigation media in combating the phenomenon of illegal logging, the most important part of this research is the identification of efficient and effective countermeasures, as listed as follows:

- CD proposes *higher responsibility* for forestry workers, even a patrimonial one, as a conclusion to the weaknesses listed by him.
- DP points out that based on an IT system that allows development, *the Forest Radar should have features that also measure the volume* and not just the legality of the transport, plus other important information.
- DP also points to a government decision that she insisted to the government from the rostrum of the Parliament would involve the establishment at the interministerial level of *emergency crews* composed of rangers, police, and gendarmerie, properly equipped with defense weapons, which to intervene promptly if illegal cutting is reported. At first in high-risk areas—there are statistics and risk maps on those places and then gradually throughout the country. It is true, she

says, that there are still a lot of corrupt forestry personnel, but there is also a shocking record with about 600 hospitalized and six dead rangers as a result of confrontations with those who cut wood illegally.

- Moreover, FS thinks that *a clearer demarcation between protection and production forests* is needed. Protection is not prioritized where there are natural values over the economic ones of the forests. The method of valorization and sale of wood must be changed: Forests must be managed based on some result indicators, *overregulation must be removed, and control must be strengthened*. There is a need for *a vision and strategy aligned with the European policies*, for the evaluation and valorization of all forest ecosystem services, not only wood. There is a need for *reform of key institutions* (the National Directorate of Forests Romsilva, the Forest Ranges, and the National Agency for Protected Natural Areas). There is a need for *education* so that people understand the roles of the forest: environmental, social, and economic. It is essential to *reform the way in which we valorize wood*, from marking with a hammer and estimates through the valuation act, to measuring the wood when it comes out of the forest, to exploiting it by providing services. This leads to efficiency, de-bureaucratization, transparency, cost reductions, fair competition, traceability, easy control, social and economic benefits, increased quality of exploitation services, and forest health.
- MZ thinks that *the legislation must be put into practice*. It was said that some *environmental courts* would also be established, but this did not happen yet. As legislative measures are required, our opinion is that *the legislative framework that provides for the confiscation of the means of transport of illegally transported wood must be updated*. There is also a need to *improve the legislative framework for the protection of forest monuments*, and these old forests that have not been classified as virgin forests and protected in the national catalog and which, unfortunately, are being lost through legal exploitation.
- IG states that the most important measures currently to minimize illegal logging are paying *fair wages* to forestry personnel, *ensuring their protection*, and *applying a special status and responsibility for those who are involved in defending the integrity of the forest fund*. Also, he believes that an important legislative measure would be that periodically, management positions within public or private institutions should be obtained through *competition*, not nominalization.

Talking about the future, FS thinks that everything depends on the reform and how quickly it is made and applied. The phenomenon can be consistently reduced immediately by reforming the system. In the long term, he believes that the phenomenon will decrease a lot, because Romania inevitably develops, just like the Western countries, according to European public policies. IG is also optimistic and believes in the power of change and he is certain that Romania's forest fund will be continuously protected. Obviously, the phenomenon of illegal cutting cannot be permanently eradicated, but it can be kept under control. Only through education can we all realize how important the role of forests is for our lives, IG concludes.

Limitations of the study may consist of the complexity of gathered information, the hard access to highly positioned and recognized experts in the field, and the time-consuming data processing. Future research may focus on extending the discussions with international experts and also go more in-depth regarding the causes and the appropriate measures to counteract them.

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.

Appendix

Interview related to deforestation and illegal logging in Romania

Firstly, I want to thank you for accepting to answer a few questions related to your activity in protecting forests.

1. Which do you consider to be the quality of the legislative framework in Romania regarding the protection and sustainable exploitation of forests?
2. What legislative measures are now required to minimize illegal cuts of wood?
3. What is the reason why these measures are not yet adopted and/or implemented?
4. How complex do you think this phenomenon is in Romania? But in the world?
5. What are the main used techniques in illegal logging?
6. Do you feel any pressure in carrying out your professional activity? If so, by whom and in what way?
7. What do you think is the share of those who carry out their activity correctly in the total of those who have the role of protecting the forests? Are those at the base of state institutions more corrupt or those in their leadership?
8. Starting with corrupt foresters, how high does the corruption go? How high are the stakes? What is the chain of corruption when we talk about illegal logging?
9. What do you think is the role of civil society in this phenomenon?
10. What do you consider to be the impact of NGO activity? Is their activity effective in the fight against the timber mafia?
11. Corruption Perception Index (CPI) is an indicator calculated by Transparency International, which measures the level of corruption perceived by the inhabitants of a country. In 2022, Romania is the third country in the European Union in terms of perceived level of corruption, after Hungary and Bulgaria, on the opposite pole being Finland, Denmark, Sweden, and Norway. What do you consider to be the causes, the reasons, the factors why the level of corruption in Romania is so high?
12. What are the main vectors that could destroy this “wood mafia”?
13. Is the Romanian timber mafia supported by people from other countries?
14. What do you consider to be the direct effects of illegal logging? Who is directly affected?

15. What about the indirect ones? How far do you think the negative effects of the timber mafia extend?
16. What is the major difference in approach regarding forest management between Romania and Austria, considering the involvement of the Austrians in the exploitation of Romanian timber?
17. Do you think that Austria's approach to promote forests for tourism can be a solution for Romania as well, to monetize the forest fund in a sustainable way?
18. How do you think the phenomenon of illegal woodcutting will evolve in Romania in the coming years? But in the long run?

Thank you so much for your replies and all your support!

References

Achim, M. V., & Borlea, S. N. (2020). In Studies of Organized Crime (Ed.), *Economic and financial crime: Corruption, shadow economy and money laundering* (Vol. 20). Springer.

Adela, F. P., & Saragih, A. (2017). Corruption, deforestation and disaster in the Taman National Gunung Leuser Forest. 2nd international conference on social and political development (ICOSOP 2017) (pp. 633–639). Atlantis Press.

Amacher, G. (2006). Corruption: A challenge for economists interested in forest policy design. *Journal of Forest Economics, 12*(2), 85–89.

Angelsen, A., & Kaimowitz, D. (1999). Rethinking the causes of deforestation: Lessons from economic models. *The World Bank Research Observer, 14*(1), 73–98.

Brockington, D. (2008). Corruption, taxation and natural resource Management in Tanzania. *Journal of Development Studies, 44*(1), 103–126.

Bulkan, J., & Palmer, J. (2008). Breaking the rings of forest corruption: Steps towards better forest governance. *Forests, Trees and Livelihoods, 18*(2), 103–131.

Callister, D. (1999). *Corrupt and illegal activities in the forestry sector: Current understandings, and implications for World Bank Forest Policy*. Preluat de pe World Bank. www.illegal-logging.info/papers/Corruption.rtf

Cozma, A.-C., Achim, M. V., & Safta, I. L. (2022). Economic and financial crime in the Forest industry—internationally and in Romania. 24th RSEP international conference on economics, Finance & Business (pp. 72–88). Vienna, Austria: BC GRUP INC. https://doi.org/10.19275/RSEPCONFERENCES158.

Cozma, A.-C., Cotoc, C.-N., Vaidean, V. L., & Achim, M. V. (2021). Corruption, shadow economy and deforestation: Friends or strangers? *Risks, 9*(9). https://doi.org/10.3390/risks9090153

Harwell, E. (2009). *The human rights consequences of illegal logging and corruption in Indonesia's forestry sector*. Human Rights Watch.

Kuchlmayr, F., Langhans, K., Milatz, M., Obermayer, B., & Verschwele, L. (2023). Wie Holzräuber die ältesten Wälder Europas zerstören. Preluat de pe Spiegel Wirtschaft: https://www.spiegel.de/wirtschaft/rodung-in-rumaenien-wie-holzraeuber-die-aeltesten-waelder-europas-zerstoeren-a-d6b0149e-a843-4f91-ae08-6f9afbcf29f7.

Lopez, R., & Mitra, S. (2000). Corruption, pollution, and the Kuznets environment curve corruption, pollution, and the Kuznets environment curve. *Journal of Environmental Economics and Management, 40*(2), 137–150.

Maina, P. M. (2018). Impact of poor governance on deforestation in Africa.

Milledge, S., Gelvas, I., & Ahrends, A. (2007). Forestry, governance and national development: Lessons learned from a logging boom in the southern Tanzania. TRAFFIC East/Southern Africa.

Miller, M. (2011). Persistent illegal logging in Costa Rica: The role of corruption among forestry regulators. *The Journal of Environment & Development, 20*(1), 50–68.
Pellegrini, L. (2011). *Corruption, development and the environment*. Springer.
Robbins, P. (2000). The rotten institution: Corruption in natural resource management. *Political Geography, 19*(4), 423–443.
Siebert, U., & Elwert, G. (2014). Combating corruption and illegal logging in Benin, West Africa. *Journal of Sustainable Forestry, 19*, 239–261.
Søreide, T. (2007). Forest concessions and corruption.
Sundstrom, A. (2016). Understanding illegality and corruption in forest governance. *Journal of Environmental Management, 181*, 779–790. https://doi.org/10.1016/j.jenvman/2016.07.020
Teye, J. K. (2013). Corruption and illegal logging in Ghana. *International Development Planning Review, 35*(1), 1–19.

Adeline-Cristina Cozma is a PhD student at the Faculty of Economics and Business Administration, Babeş-Bolyai University, Cluj-Napoca, Romania; postgraduate with a master's diploma in tourism, at Faculty of Business, Babes-Bolyai University; and also an undergraduate of two bachelor programs at Faculty of Business, Babes-Bolyai University: one in economics and one in tourism. She was author and coauthor of several academic articles in international journals, such as Risks, Information, Negotia, Studia, Brazilian Journal of Business; and participated as author and coauthor in several international conferences, such as R.S.E.P. International Conference on Economics, Finance and Business, B.EN.A Conference, CACTUS, Entrepreneurship in the Hospitality Industry. With considerable experience in the academic field, the research focuses on the relationship between economic and financial crime and illegal deforestation, as illegal logging becomes a serious issue for the environment, as well as for the safety of the ones trying to protect the forests. She is also a contributor to the project titled "Intelligent analysis and prediction of the economic and financial crime in a cyber-dominated and interconnected business world," conducted over the period 2021–2023, financed by the Romanian Ministry of Education and Research, CNCS-UEFISCDI, project number PN-III-P4-ID-PCE-2020-2174 (www.fincrime.net).

Monica Violeta Achim is a full professor and doctoral supervisor in the field of Finance at the Faculty of Economics and Business Administration, Babeş-Bolyai University, Cluj-Napoca, Romania. With over 24 years of experience in academia, she has published as author and coauthor, over 150 scientific articles and 25 books. Her most recent reference work is the book Economic and Financial Crime: Corruption, Shadow Economy and Money Laundering, published by Springer. In 2020, she earned an Award for Excellence in Scientific Research at Babeş-Bolyai University, Faculty of Economics and Business Administration, Cluj-Napoca, Romania, in recognition of the results obtained in her research activity. She heads a big grant titled "Intelligent analysis and prediction of economic and financial crime in a cyber-dominated and interconnected business world," conducted over the period 2021–2023, financed by the Romanian Ministry of Education and Research, CNCS-UEFISCDI, project number PN-III-P4-ID-PCE-2020-2174 (www.fincrime.net).

Part II
Economic and Political Determinants of Financial Crime

Chapter 4
Identifying Determinants of Informal Entrepreneurship Using Bibliometric and Cross-Country Analysis: Evidence from the European Union Countries

Monica Violeta Achim, Viorela Ligia Văidean, Sorin Nicolae Borlea, and Decebal Remus Florescu

Abstract Recently, the phenomenon of the informal economy has attracted the attention of policymakers and researchers alike in order to fight against its causes. This study has two main objectives. First, using bibliometric analysis, it comes up with a detailed literature review of the field of informal entrepreneurship in order to dimension its widespread in time and space. Second, through empirical analysis, it identifies the main determinants that stimulate engagement in informal entrepreneurship using the European Union (EU) as a case study. For sample collection, articles are selected from the International Web of Science database. In addition, an empirical cross-country analysis is performed for the 28 EU member states, and separately for old and new EU countries, using data extracted from the 2019 Special Eurobarometer Survey 92.1.

Our findings suggest that agriculture, cash in labor, trust morale, trust in tax and social security authorities, economic development, and urbanization are important determinants of the level of informal entrepreneurship. In addition, some economic and financial factors have a greater influence on old EU countries compared to new EU countries, while cultural factors sting harder in the new EU countries than in the

M. V. Achim (✉) · V. L. Văidean
Faculty of Economics and Business Administration, Babeș-Bolyai University, Cluj-Napoca, Romania
e-mail: monica.achim@econ.ubbcluj.ro

S. N. Borlea
Faculty of Economics, University of Oradea, Oradea, Romania

Faculty of Economics, Computer Science and Engineering "Vasile Goldiș" Western University of Arad, Arad, Romania

European Research Institute, Babeș-Bolyai University, Cluj-Napoca, Romania

D. R. Florescu
Faculty of Political, Administrative and Communication Sciences, Babeș-Bolyai University, Cluj-Napoca, Romania

M. V. Achim (ed.), *Economic and Financial Crime, Sustainability and Good Governance*, Contributions to Finance and Accounting,
https://doi.org/10.1007/978-3-031-34082-6_4

old EU countries. These findings are very important for policymakers who have to consider various factors in a different manner, in their analyses of people's behaviors regarding involvement in informal work.

Keywords Informal entrepreneurship · Bibliometric analysis · Economic factors · Political factors · Culture

Jel Classification E20 · E26 · K31 · J45

1 Introduction

In recent years, numerous studies have focused on underground activities. A special part of underground activities is represented by activities conducted through informal entrepreneurship. According to the specialized literature, informal entrepreneurship refers to those working on an own-account basis and engaging in monetary transactions not declared to the state for tax, benefit, and/or labor law purposes (Williams, 2014, 2020; Williams & Shahid, 2016). However, more efforts need to be made to fill the research gaps through empirical analyses to measure the dimension of the informal sector and identify its determinants, functioning mechanisms, and existing correlations (Elgin & Erturk, 2019).

Therefore, the present study has two main objectives. First, using bibliometric analysis, it provides an extensive literature review of the field of informal entrepreneurship. Second, through empirical analysis, it identifies the main determinants that stimulate engagement in informal work. For these purposes, we use qualitative and quantitative analyses. In order to provide an answer to our research questions, a bibliometric analysis of the research papers is performed using the VOSviewer software. For sample collection, articles on this topic are selected from the International Web of Science database. In addition, an empirical cross-country analysis is performed for the 28 European Union (EU) member states at the time of research (before the withdrawal of the United Kingdom (UK)), using data extracted from the 2019 Special Eurobarometer Survey 92.1. Moreover, we discuss specific results for the two subgroups of countries (i.e., old and new EU member states). The novelty of this study expresses itself in the following contributions: on the one hand, it identifies determinants of informal entrepreneurship using both bibliometric and cross-country analysis; on the other hand, specific results are extracted separately for old and new EU countries.

The remainder of this paper is structured as follows. Section 2 offers an extensive literature review of the field of informal entrepreneurship, including a bibliometric analysis of a large sample of articles. Section 3 presents the methodology and data for the empirical part of our study. Section 4 includes the results and their interpretations. Finally, Section 5 summarizes the main conclusions of the study, identifies its limitations, and explores the scope of future research.

2 Literature Review

2.1 *Data on Informal Entrepreneurship: Bibliometric Mapping with VOSviewer*

Based on various studies related to the topic of informal entrepreneurship, we first conduct a bibliometric analysis to capture the main issues concerning informal entrepreneurship. First, to describe research data on informal entrepreneurship, we intend to answer the following research questions:

Research questions (RQ1): How did research evolve in the field of informal entrepreneurship over time?
Research Questions (RQ2): Which journals have the highest frequency of articles written or cited on the topic of informal entrepreneurship?
Research Questions (RQ3): Which countries have the most publications on this topic?

For this purpose, we review all articles published on the Web of Science that contain the word "informal entrepreneurship," and then, using the VOSviewer software, we check for their strongest links with the most related words. Simultaneously, the information retrieved shows how to display the results shaped as scientific maps. Using the search key "informal entrepreneurship" to be captured in the title and abstract through the Web of Science, we obtain a number of 1743 articles. These articles represent our database for bibliometric analysis.

To answer our first research question (RQ1), we have to analyze Fig. 4.1 in detail. In Fig. 4.1, research concerns on "informal entrepreneurship" show rapid growth. Within the time span of the last 10 years (from 2010 to 2020), the number of published articles on this topic has increased from 45 to 246, that is, a growth of approximately 5.5 times.

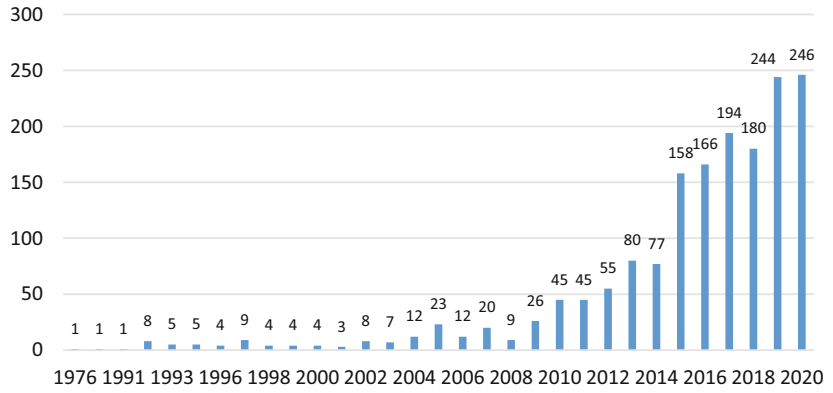


Fig. 4.1 Evolution of the number of published articles on "informal entrepreneurship." Source: Authors' processings in VOSviewer—Web of Science index articles

Fig. 4.2 Top 10 journals that publish articles in the field of "informal entrepreneurship." Source: Authors' processings in VOSviewer—Web of Science index articles

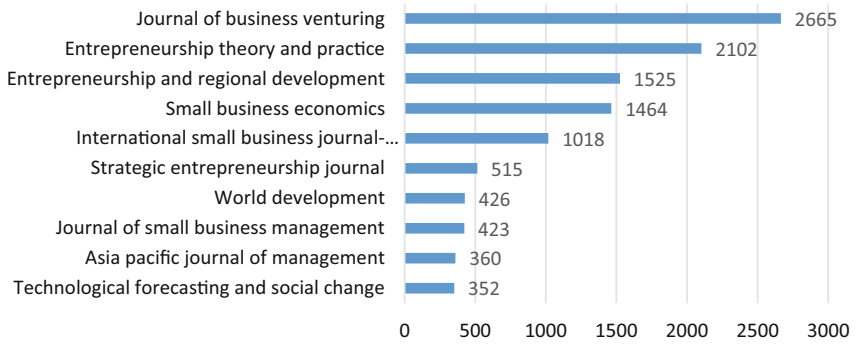


Fig. 4.3 Top 10 most-cited journals on the topic of "informal entrepreneurship." Source: Authors' processings in VOSviewer—Web of Science index articles

To answer our second research question (RQ2), we check for journals with the highest frequency of articles written or cited on the topic of informal entrepreneurship (Figs. 4.2 and 4.3). Figure 4.2 highlights the top 10 journals that have published articles on the topic of "informal entrepreneurship": Entrepreneurship and Regional Development (47), Small Business Economics (41), Journal of Developmental Entrepreneurship (40), Journal of Business Venturing (26), International Small Business Journal-Researching Entrepreneurship (22), International Entrepreneurship Theory and Practice (22), International Entrepreneurship and Management Journal (21), Sustainability (19), Journal of Business Ethics (16), and Strategic Entrepreneurship Journal (15).

The most-cited journals on the topic of "informal entrepreneurship" are generally the same journals that have the most publications on this research topic (Fig. 4.3).

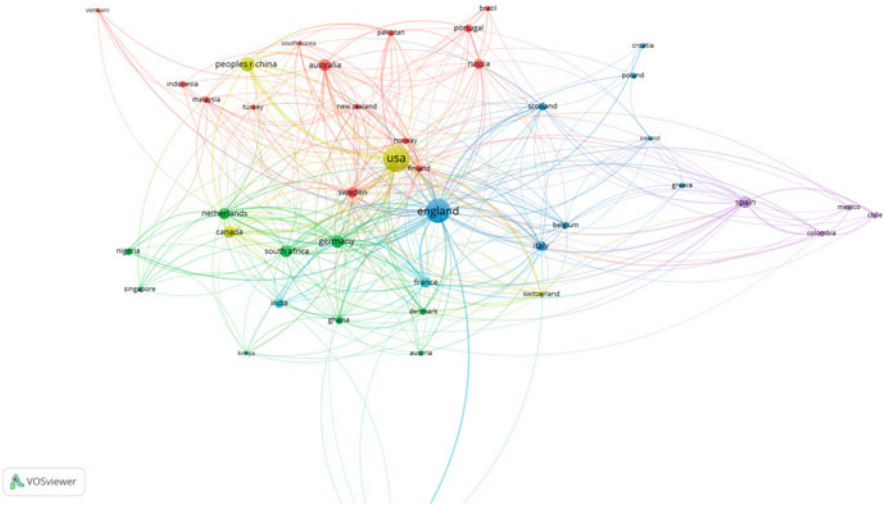


Fig. 4.4 Bibliometric analysis of countries that publish articles in the field of "informal entrepreneurship." Source: Authors' processings in VOSviewer—Web of Science index articles

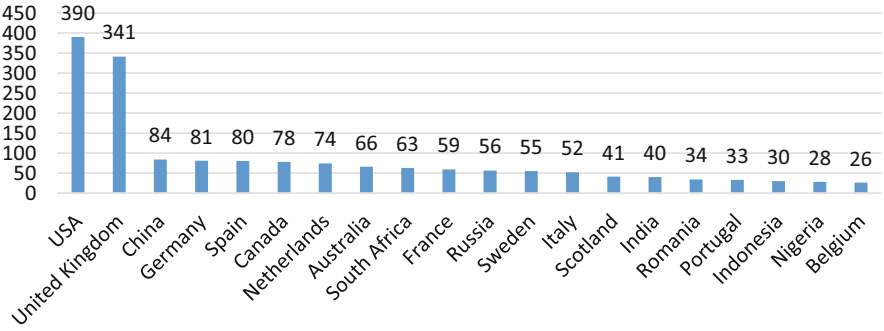


Fig. 4.5 Top countries that publish articles in the field of "informal entrepreneurship." Source: Authors' processings in VOSviewer—Web of Science index articles

However, Fig. 4.3 shows four new entry journals that appear in the most-cited journals' list, different from the main 10 journals, which published papers on the topic of "informal entrepreneurship", namely the Journal of Small Business Management, World Development, Asia Pacific Journal of Management, and Technological Forecasting and Social Change. These appear supplementary as being among the top 10 most-cited journals on the topic of informal entrepreneurship.

Regarding the third research question (RQ3), we identify countries with the most published papers on "informal entrepreneurship" (Figs. 4.4, 4.5, and 4.6). From Figs. 4.4 and 4.5, it can be seen that the United States (US) and the UK are, by far, on

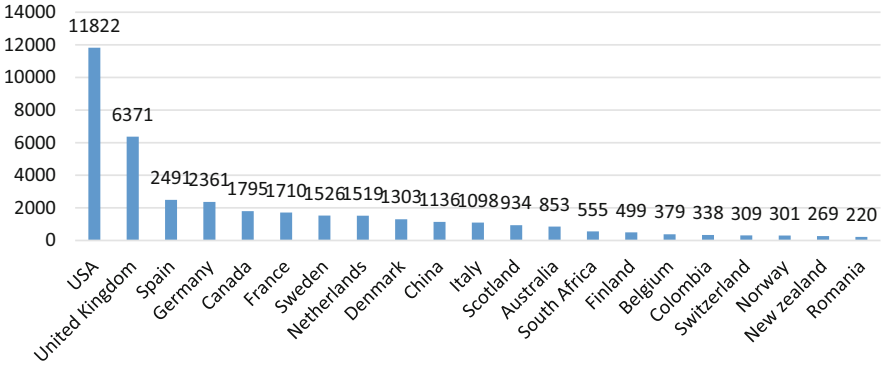


Fig. 4.6 Countries with the most-cited journals in the field of "informal entrepreneurship." Source: Authors' processings in VOSviewer—Web of Science index articles

the very top, with 390 and 341 published papers, respectively (Fig. 4.3 and Fig. 4.4), followed by emerging China (84), Germany (81), Spain (80), Canada (78), the Netherlands (74), and Australia (66). However, some less developed countries such as South Africa, Romania, Indonesia, and Nigeria have entered the list, ranking among countries that pay special attention to the topic of "informal entrepreneurship." Countries with the most-cited journals on "informal entrepreneurship" are very similar to the ones with the largest number of published papers on the same topic (Fig. 4.6).

Overall, informal entrepreneurship has become an extremely attractive research topic, capturing the interest of an increasing number of researchers, especially in the current worldwide economic context.

2.2 Determinants of Informal Entrepreneurship: Bibliometric Mapping with VOSviewer and Synthesis

Furthermore, we perform a *bibliometric analysis* of the literature on informal entrepreneurship using the VOSviewer program. Consequently, using the keyword "informal entrepreneurship, " we identify 1742 indexed articles on the Web of Science at the time of our research (May 21st, 2022). Figure 4.7 illustrates the graphical distribution of the number of occurrences of papers published on the topic of informal entrepreneurship, together with the associated terms; the higher the number of bullets, the higher the occurrence of terms and the more powerful the relationships between terms. Different clusters mapping the way in which the relationships are realized are displayed in different colors. Figure 4.7 shows that "informal entrepreneurship" is related to various terms that can be grouped as follows: economic factors (emerging economy/economic development/poverty/ developing country/China, entrepreneurship, informal economy, informality,

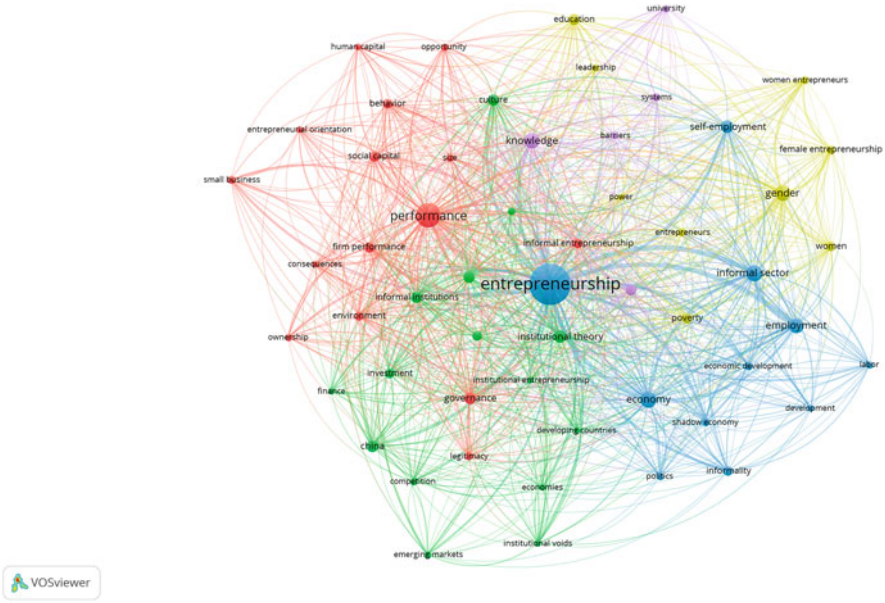


Fig. 4.7 Bibliometric analysis of keywords from existing publications in the literature on "informal entrepreneurship." Source: Authors' processings in VOSviewer—Web of Science index articles

performance, self-employment, small business, and informal sector); political factors (informal institution, policy, legitimacy, and institutional theory); and sociocultural factors (social capital, trust, gender, behavior, women, knowledge, female entrepreneurship, and culture). Thus, our fourth research question (RQ4) regarding the pursuit of the main determinants of informal entrepreneurship is partially checked. In the following section, we empirically demonstrate the validity of some of these determinants.

To identify the determinants of engagement in economic activities outside the jurisdiction of laws, we review numerous studies presented in Table 4.1. We synthesize and classify all these determinants as follows: economic factors (e.g., economic development, cash usage, unemployment, self-entrepreneurship, share of agriculture within the total economy, technical and scientific revolutions, crises, preventive measures, and detecting risk); political factors (e.g., institutional quality, rule of law, governance effectiveness, and bureaucracy); and sociocultural factors (e.g., greed, education, age, intelligence, tax morale, and social norms such as various attitudes, culture, institutional trust, and happiness).

Table 4.1 Determinants of informal entrepreneurship

Type of factor	Variable	Authors	Results
Economic factors	Economic development	Chelliah (1971), Torgler (2004), Torgler and Schneider (2009), Achim and Borlea (2020)	The studies show that an increased level of economic development and prosperity brings along an improved capacity for paying and collecting taxes and an improved demand for public goods and services. They conduct lower incentives to engage in informal activities
	Cash usage	Medina and Schneider (2018), Schneider and Buehn (2016)	A larger shadow economy and informal entrepreneurship are associated with the use of more cash
	Unemployment	Medina and Schneider (2018), Schneider and Buehn (2016)	The higher unemployment is, the higher informal entrepreneurship is as well
	Self-entrepreneurship	Schneider and Williams (2013), Feld and Schneider (2010), Schneider and Buehn (2016), Medina and Schneider (2018)	Researchers validate a positive relationship between independent economic activities (natural persons authorized to carry out economic activities) and the level of the underground economy. The higher the rate of independent activities, the higher the rate of activities carried out in the underground economy. In theory, independent activities are expected to provide more freedom to entrepreneurs from the point of view of the level and structure of declared economic activities. However, we keep this determinant as slightly validated by the research literature
	Share of agriculture in the total economy	Medina and Schneider (2018), Hassan and Schneider (2016), Kelmanson et al. (2019)	Agriculture and its related sectors (along with lower enforcement) have been analyzed and the size of the agricultural sector

(continued)

Table 4.1 (continued)

Type of factor	Variable	Authors	Results
			positively contributes to the shadow economy
	Technical and scientific revolutions	Gaspareniene et al. (2016), Remeikiene et al. 2017), Satalkina and Steiner (2020), Şcheau (2018)	*The technical and scientific revolutions and online transaction growth* led to the development of the digital economy along with that of digital entrepreneurship. In addition, they lead to the occurrence of a new category of informal activities in the shape of a digital shadow economy and digital informal entrepreneurship
	Crises	Webb et al. (2020)	Evidence exists that there are considerable short- and long-term implications of crises such as the pandemic for informal employment and the informal economy This is due to the unresolved tensions stemming from informal workers' desire for greater job security on the one hand, and employers' efforts to keep labor flexibility up, while shifting the costs toward the government and workers, on the other. The COVID-19 pandemic can accelerate current trends and force the implementation of new solutions to better protect basic job security while also helping organizations to stay competitive
Political factors	Institutional quality, rule of law, governance effectiveness, bureaucracy	Kirchler (2007), Johnson et al. (1997), Enste (2010), Williams and Shahid (2016)	Besides fiscal pressure and fiscal morality, the degree of regulation existing within economies leads to boosted levels of the underground economy. On the contrary, a high regulation of the labor market

(continued)

Table 4.1 (continued)

Type of factor	Variable	Authors	Results
			or of the goods market restricts individual freedom and that of the entrepreneur to act in the formal economy
		Webb et al. (2013)	They analyze the incentives, constraints, motivations, strategies, and abilities of entrepreneurs to operate in the informal economy in the view of three separate theories: Institutional theory, motivation-related theories from a sociological perspective, and resource allocation theory. Based on this background, the authors assume 10 important propositions Therefore, the authors state that the stringency of policies, the degree to which policy changes are radical, proactivity usages of avoidance and manipulation tactics, the ambiguous jurisdiction and conflicting interests across institutional centers, the formation of group-level institutions, the perceived costs of operating informally relative to institutional benefits, the failure of the society to help individuals, and the distrust in formal institutions are positively related to the opportunity to slip into informal entrepreneurship. In addition to these, the authors find that bureaucracy has a curvilinear, inverted U-shaped relationship with opportunity recognition in the informal economy

(continued)

Table 4.1 (continued)

Type of factor	Variable	Authors	Results
	Preventive measures	Williams (2020)	The finding is that participation in informal entrepreneurship is not significantly associated with the deterrent measures of raising the penalties and probability of being caught but is significantly associated with the preventive measures of improving vertical and horizontal trust
	Detecting risk	Schneider and Buehn (2016), Williams (2020)	Schneider and Buehn (2016) find that there is little empirical evidence that fines and penalties do not have a negative influence on the underground economy but it is actually the risk of detection, which is subjectively perceived by individuals, that has a positive influence. In the same view, Williams (2020) finds a significant association between engaging in informal entrepreneurship and the perceived risk of detection. No relationship is identified between the perceived levels of penalties and participation in informal sector entrepreneurship
Sociocultural and individual factors	Greed	(Bucur, 2011, p. 50)	*Greed,* as a universal human motivation, is considered to be an important component for figuring out the legal conformity behavior
	Education and age	Chan et al. (2000), Kasipillai et al. (2003), Bordean et al. (2020)	Researchers find that U.-S. respondents' decisions to respect tax laws are mainly driven by their age and education. In the same spirit, the study of Kasipillai et al. (2003) assesses the influence of education on tax

(continued)

Table 4.1 (continued)

Type of factor	Variable	Authors	Results
			compliance among students in Malaysia. Statistical findings confirm the prevalence of a relationship between the level of education and of tax compliance. This relationship is generally consistent, especially with respect to issues concerning avoiding general and personal taxes. An improvement in the degree of personal tax compliance is registered among students, especially among women, after a semester of taking a preliminary taxation course
		Jiménez et al. (2015)	The fundamental role of education is particularly materialized throughout the training stages of entrepreneurs because that is when an appropriate mentality toward entrepreneurship is created. Specifically, this study shows that both secondary education and tertiary education have a very different effect on engaging in formal or informal entrepreneurial activities. Thus, in particular, formal entrepreneurship is positively associated with secondary and tertiary education, while informal entrepreneurship is negatively affected by tertiary education only
	Intelligence	Potrafke (2012), Lv (2017), Čiutienė et al. (2015), Salahodjaev (2015)	The studies find that a high IQ in the population is associated with less corruption and a lower level of engagement within the informal economy

(continued)

Table 4.1 (continued)

Type of factor	Variable	Authors	Results
	Tax morale, social norms (attitude), culture	Alm and Torgler (2006), Kirchler, 2007), Çule and Fulton (2009), Cubillas et al. (2018), Alm and Torgler (2006), Kirchler (2007), Kogler et al. (2013), Medina and Schneider (2018), Schneider and Buehn (2016)	There is extensive literature investigating the existing variations in values, social attitudes and norms, *culture, lifestyle, and historical heritage* for different countries and if these variations impact tax morale and tax compliance behaviors. Various cultural traits imply different degrees of tax compliance due to the varying levels of tax morale. Furthermore, the inner motivation of people to pay taxes, which represents the mere definition of "tax morale," differs from one state to another and creates varying incentives to engage in informal activities
	Trust (institutional trust)	Kirchler (2007), Torgler and Schneider (2009), Park and Blenkinsopp (2011), Fritzen et al. (2014), Çule and Fulton (2009), Marinkovic (2005), Petrakis (2014, p. 61), Austwick and Berga (2016)	Several papers have highlighted the importance of ensuring a high degree of trust within government institutions, in order to ensure the good functionality of the state. The inefficiency of public goods generates a low trust in the authorities and causes individuals and entrepreneurs to act in an underground manner with the purpose of getting quicker benefits
		Thai et al. (2020)	The results of this study show that in the formal and informal sectors, social networking enables business creation with varying levels of impact. It establishes that *institutional trust* has an indirect effect on informal business creation and a direct effect on business registration; interpersonal trust drives

(continued)

Table 4.1 (continued)

Type of factor	Variable	Authors	Results
			entrepreneurship in the informal sector but has less impact on business registration; norms of trustworthiness are related to business registration than informal business creation
	Happiness	Schneider and Klinglmair (2004), Bergheim (2007)	The studies reveal that in countries where people feel happy, the level of engagement in informal economical activities is smaller than in countries where people feel unhappy

3 Methodology and Data

3.1 Sample

Our data comprise variables for the 28 EU member states, at the time of research, extracted from the 2019 Special Eurobarometer Survey 92.1. (no. 498), in September 2019 for 27,565 respondents, including the UK, which was still an EU member state at that time. A clear advantage of collecting variables from Eurobarometer surveys is represented by the fact that each level of the sample is representative in proportion to its population size by construction. Our database also includes variables from the World Data Bank for the year 2019. Nonetheless, the cultural dimensions of these member states are reflected by Hofstede's 6D cultural model. Overall, our cross-sectional data cover the 28 EU member states for the year 2019, which represents the most recent data available at this moment.

3.2 Data

We extracted data on informal entrepreneurship (IE), people working within the agricultural sector (Agriculture), cash in labor (CashLabor), tax morale (TaxMorale), and trust in tax and social security authorities (TrustTaxSS) from the Special Eurobarometer Survey 92.1. IE is a dummy variable with a value of 1 for respondents who answered "yes" to the question of "have you yourself carried out any undeclared paid activities in the last 12 months?" and 0 otherwise. Similarly, Agriculture is a dummy variable with a value of 1 only for respondents who declared having jobs in the agricultural sector and 0 otherwise (various types of services or industries). CashLabor is a dummy variable with a value of 1 for an affirmative

answer to "Sometimes employers prefer to pay all or part of the salary or the remuneration (for extra work, overtime hours, the amount above the legal minimum wage or bonuses) in cash and without declaring it to tax or social security authorities. Has your employer paid you any of your income in the last 12 months in this way?" and 0 otherwise. TaxMorale is a simple average of the scaled answers given by the respondents to five questions. Respondents rated the acceptability of engaging in five types of informal sector activities using a 10-point Likert scale (1 = absolutely unacceptable and 10 = absolutely acceptable). TaxMorale was then computed as the *mathematical average* of the answers given to these five questions, while 0 was for "Other" or "do not know." TrustTaxSS is a proxy for institutional quality. This variable refers to how much trust respondents have in certain authorities or institutions that are involved in tackling undeclared work, with the value of 1 if they tend to trust tax and social security authorities that are in charge of ensuring adequate payment of taxes and social security contributions, and 0 if they tend not to trust them (other answers included here as well).

Furthermore, the variables taken from the database of the World Bank are the per capita gross domestic product (GDP, the logarithmic value of per capita GDP in current US dollars, to meet the assumptions of multivariate data analysis) and urbanization (the weight of urban population within the whole population of member states).

Hofstede's cultural dimensions (the culture vector from Eq. (4.1)) include the following six variables: power distance (PD), individualism versus collectivism (IDV), masculinity versus femininity (MAS), uncertainty avoidance (UAI), long-term orientation (LTO), and indulgence versus restraint (IND). Consequently, significant variables were kept within our multiple regression model.

Figure 4.8 shows our expected results by linearly fitting the data. The average values of informal entrepreneurship percentage dimensions for each EU member state (IE) were approximated through the countries' average values of Agriculture, CashLabor, TaxMorale, TrustTaxSS, per capita GDP, and Urban, revealing the direct and positive impact of these determinants on IE. For some of these explanatory variables, such as CashLabor and TrustTaxSS, the slope was rather mild, and the correlation coefficients were low. Nevertheless, there were many other determinants that might further capture the interest of researchers in the field of informal entrepreneurship.

3.3 Descriptive Statistics of Data

From Fig. 4.9, we find that the highest levels of informal entrepreneurship are found in the Netherlands and Luxembourg (with approximately 6%), Belgium, Latvia, and Denmark (with approximately 5%), and Bulgaria, Sweden, and Estonia (with approximately 4%). The average level of informal entrepreneurship is 3.48% (Table 4.2).

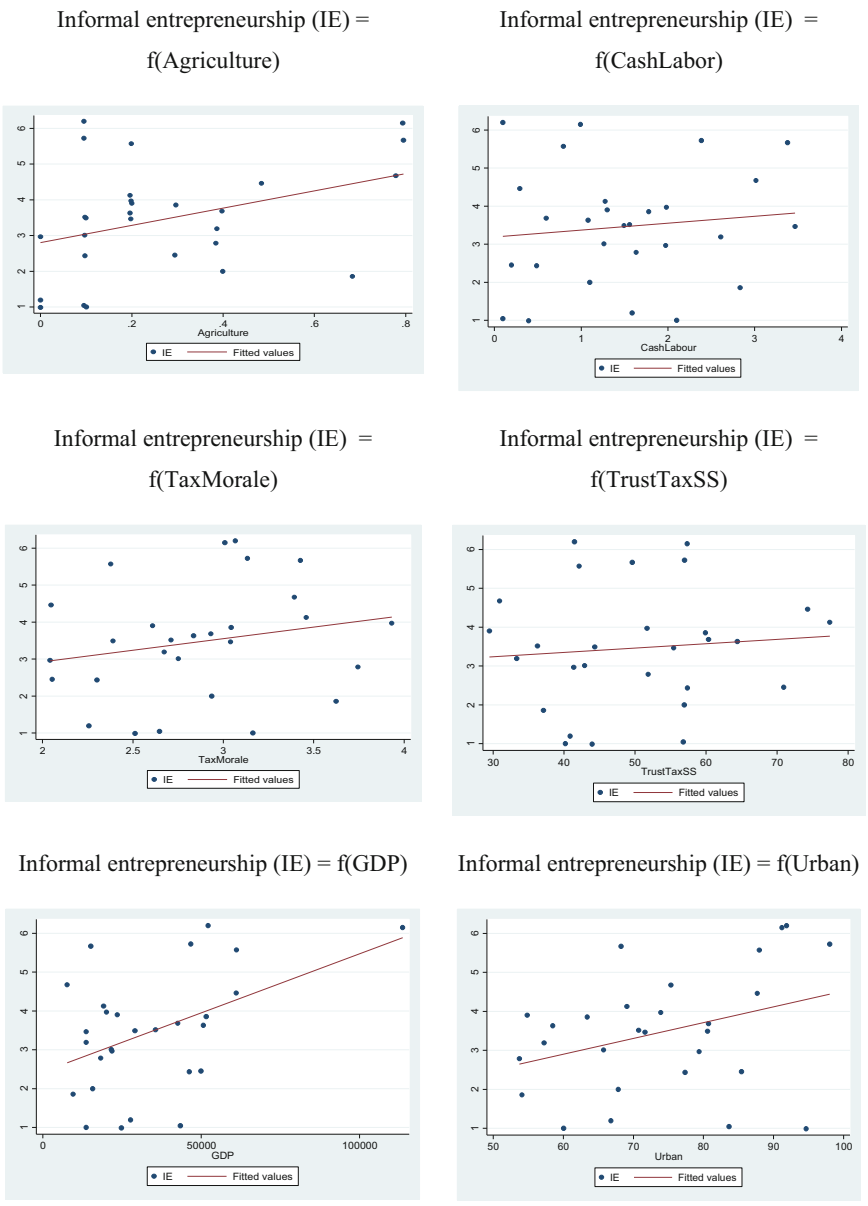


Fig. 4.8 Linear fitting of data: informal entrepreneurship as a function of various determinants. Source: Authors' processings in Stata

The summary statistics for our entire sample of 28 EU member states were further divided into two subsamples: 15 old EU member states (i.e., Belgium, Denmark, Greece, Spain, Finland, France, Ireland, Italy, Luxembourg, the Netherlands,

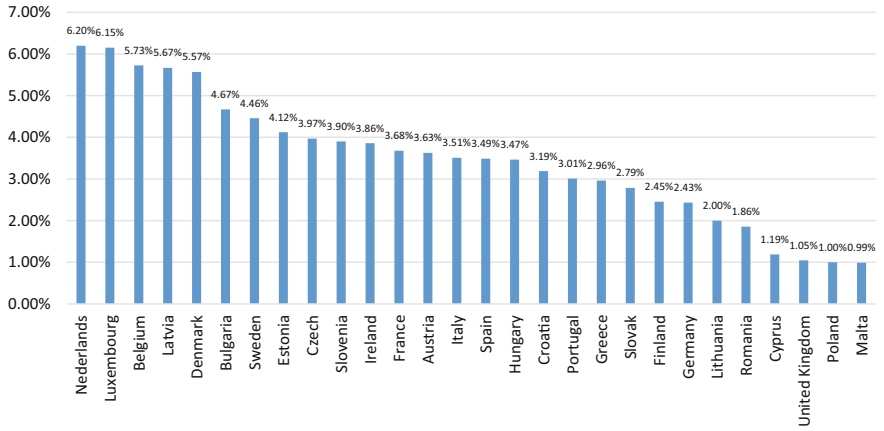


Fig. 4.9 Acceptability of the informal sector, by EU Member States 2019. Source: The authors' own processing based on data from Eurobarometer, 2019

Austria, Portugal, Sweden, Germany, and the UK) and 13 new member states (i.e., Bulgaria, Cyprus, Czech Republic, Estonia, Hungary, Latvia, Lithuania, Malta, Poland, Romania, Slovakia, Slovenia, and Croatia), as presented in Table 4.2. The mean percentage of people who admitted to engaging in undeclared paid activities in the last 12 months was 3.75% and 3.14% for the old and new countries, respectively. That is, although there were no high discrepancies in the level of informal entrepreneurship among the two subgroups of old and new EU member states, the level was somewhat higher for old countries than for the new ones. Regarding the considered independent variables, there were significant differences in the average values calculated for the new and old countries' subsamples. Although the percentage of people who declared having jobs in the agricultural sector was 0.26% for the entire sample, it significantly differed between the two subgroups, with the percentage of the old countries' subgroup being approximately double than that of the new countries' subgroup. Further, the percentage of people whose labor was remunerated in cash was about 1.51% on average for all EU countries. However, this percentage for the new countries' subgroup was double that of the old countries' subgroup (i.e., the average values for the old and new EU states' subsamples were 1.01% and 2.14%, respectively). In addition, tax morale, meaning the acceptability of engaging in informal activities, was 23% higher for new EU countries than for old countries (i.e., the average Tax Morale scores for the old and new states' subsamples were 2.599 and 3.2007, respectively). In addition, the level of trust in tax and social security authorities (TrustTaxSS) was 15% higher for old countries than for new countries. About half of the respondents from this Eurobarometer expressed their trust in the quality of their public institutions, which could be further extrapolated to the entire European population. The levels of economic development (represented by per capita GDP) and urbanization were also significantly higher for old countries compared to new countries. The average per capita GDP for the old and news states'

Table 4.2 Summary statistics

Variable	Obs	Mean	Std. Dev.	Min	Max
InformalEntrepreneurship_all	27,565	0.0348	0.1834	0	1
InformalEntrepreneurship _OLD	15,384	0.0375	0.1901	0	1
InformalEntrepreneurship _NEW	12,181	0.0314	0.1745	0	1
Agriculture_all	27,565	0.0026	0.0517	0	1
Agriculture_OLD	15,384	0.0019	0.0441	0	1
Agriculture_NEW	12,181	0.0036	0.0599	0	1
CashLabor_all	27,565	0.0151	0.1219	0	1
CashLabor_OLD	15,384	0.0101	0.0998	0	1
CashLabor_NEW	12,181	0.0214	0.1448	0	1
TaxMorale_all	27,565	2.8649	2.5307	1	12
TaxMorale_OLD	15,384	2.599	2.3009	1	12
TaxMorale_NEW	12,181	3.2007	2.7578	1	12
TrustTaxSS_all	27,565	0.5034	0.4999	0	1
TrustTaxSS_OLD	15,384	0.5351	0.4987	0	1
TrustTaxSS_NEW	12,181	0.4635	0.4986	0	1
GDP_all	27,565	34,566.35	20,066.05	9828.148	114,685.2
GDP_OLD	15,384	46,869.38	18,875.57	19,580.99	114,685.2
GDP_NEW	12,181	19,028.22	5347.424	9828.148	29,737.25
Urbanization_all	27,565	73.4615	12.5083	53.729	98.041
Urbanization_OLD	15,384	79.7464	10.7552	58.515	98.041
Urbanization_NEW	12,181	65.5239	9.7508	53.729	94.678
Culture_PD_all	26,556	51.1869	20.9087	11	100
Culture_PD_OLD	15,384	41.9632	16.9521	11	68
Culture_PD_NEW	11,172	63.888	19.1052	40	100
Culture_IDV_all	26,556	58.8017	17.9139	27	89
Culture_IDV_OLD	15,384	64.6001	16.0622	27	89
Culture_IDV_NEW	11,172	50.8173	17.2485	27	80
Culture_MAS_all	26,556	46.3449	24.7461	5	100
Culture_MAS_OLD	15,384	46.3552	22.5352	5	79
Culture_MAS_NEW	11,172	46.3307	27.5021	9	100
Culture_UAI_all	26,556	69.4523	21.4107	23	100
Culture_UAI_OLD	15,384	65.0644	24.8451	23	100
Culture_UAI_NEW	11,172	75.4946	13.2921	51	93
Culture_LTO_all	26,556	58.3749	16.8644	24	83
Culture_LTO_OLD	15,384	54.254	17.8326	24	83
Culture_LTO_NEW	11,172	64.0495	13.5122	38	82
Culture_IND_all	26,556	42.3422	19.0895	13	78
Culture_IND_OLD	15,384	54.6846	14.0048	30	78
Culture_IND_NEW	11,172	25.3464	9.8739	13	48

subsamples were 46,869 and 19,028 US dollars, respectively. That is, for the new members' subsample, it was 2.46 times smaller than for the old members' subsample, indicating strong differences in economic development between the two subsamples of member states.

3.4 Methods

We used cross-sectional analysis for data from the 28 EU countries for the year 2019, which are the most recent data available. We analyzed our cross-sectional data from the viewpoint of the existing correlations, added the determinants of informal entrepreneurship as explanatory variables in the simple and multiple OLS regressions (based on the forward addition method, in a decreasing order of their explanatory power), and paid considerable attention to avoid multicollinearity. Our baseline model is described by the following specific equation:

$$\begin{aligned}\text{InformalEntrepreneurship}_i = {} & \beta_0 + \beta_1 \text{Agriculture}_i + \beta_2 \text{CashLabor}_i \\ & + \beta_3 \text{TaxMorale}_i + \beta_4 \text{TrustTaxSS}_i + \beta_5 \text{GDP}_i + \beta_6 \text{Urban}_i + \beta_7 \text{Culture}_i \\ & + \varepsilon_i \end{aligned} \tag{4.1}$$

where i ranges from the first respondent to the last one, β stands for the estimated coefficients of the linear effects, and ε represents the residuals.

4 Results and Discussion

4.1 Main Results

Our findings show that agriculture accounted for 7.45% of informal entrepreneurship for the whole sample of the 28 EU member states, according to regression (4.1) from our main results table (Table 4.3—models (1) to (7)). Thus, the more people work within the agricultural sector, the more they engage in informal entrepreneurship activities. The results are in line with those of Medina and Schneider (2018) and Hassan and Schneider (2016), who also found that the larger the agricultural sector is, the greater the possibility of working in the shadow economy. No significant differences were found when the two subgroups of countries were analyzed (Table 4.4, models (1) to (6), and Table 4.5, models (1) to (6)).

Cash in labor was also found to have a positive impact on informal entrepreneurship, as shown in Table 4.3 (models (2) to (7)); that is, the higher the payment of work in cash, the greater the level of engagement in informal entrepreneurship. This result aligns itself with other findings from the specialized literature, such as Medina and Schneider (2018), Schneider and Buehn (2016), and Achim and Borlea (2020),

Table 4.3 Main results, entire sample

	OLS regressions						
Informal entrepreneurship determinants	(1)	(2)	(3)	(4)	(5)	(6)	(7)
Agriculture	0.9677***	0.9301***	0.9201***	0.9195***	0.9205***	0.9206***	0.9176***
CashLabor		0.3518***	0.3454***	0.3443***	0.3477***	0.3479***	0.3518***
TaxMorale			0.0057***	0.0055***	0.0057***	0.0058***	0.0059***
TrustTaxSS				−0.0074***	−0.0094***	−0.0094***	−0.0101***
LogGDP					0.0162***	0.0111***	0.0127***
Urbanization						0.0004***	0.0003***
Culture (MAS)							−0.0002***
Culture (LTO)							0.0001**
Constant	0.0322***	0.0270***	0.0106***	0.0151***	−0.1517***	−0.1306***	−0.1371***
R^2	0.0745	0.1291	0.1354	0.1358	0.1382	0.1388	0.1411
Adj R^2	0.0745	0.1290	0.1353	0.1357	0.1380	0.1386	0.1408
Observations	27,565	27,565	27,565	27,565	27,565	27,565	26,556

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

Table 4.4 Main results EU 15 old

Informal entrepreneurship determinants	(1)	(2)	(3)	(4)	(5)	(6)
Agriculture	0.9643***	0.9269***	0.9069***	0.9069***	0.9041***	0.9022 ***
CashLabor		0.4149***	0.4048***	0.4038***	0.4049***	0.4074***
TaxMorale			0.008***	0.0077***	0.0075***	0.0076***
TrustTaxSS				−0.0083***	−0.0096***	−0.0096***
LogGDP					0.014***	0.0116***
Urbanization						
Culture (MAS)						−0.0003***
Culture (LTO)						0.0002***
Constant	0.0356***	0.0315***	0.0108***	0.0161***	−0.1323***	−0.1021 **
R^2	0.0501	0.0975	0.1068	0.1073	0.1081	0.1101
Adj R^2	0.0500	0.0974	0.1067	0.1071	0.1078	0.1097
Observations	15,384	15,384	15,384	15,384	15,384	15,384

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

Table 4.5 Main results EU 13 new

Informal entrepreneurship determinants	(1)	(2)	(3)	(4)	(5)	(6)
Agriculture	0.9721***	0.9354***	0.9305***	0.9296***	0.9298***	0.9282***
CashLabor		0.3173***	0.3136***	0.3125***	0.3125***	0.3172***
TaxMorale			0.0044***	0.0042***	0.0042***	0.0042***
TrustTaxSS				−0.0079***	−0.0083***	−0.0102***
LogGDP						
Urbanization					0.0002**	0.0018***
Culture (PD)						−0.0004***
Culture IDV						−0.0008***
Culture (MAS)						
Culture (UAI)						−0.00203***
Culture (LTO)						−0.0014***
Culture (IND)						0.0004**
Constant	0.0279***	0.0212***	0.0072***	0.0116***	−0.0071	0.2068
R^2	0.1117	0.1809	0.1857	0.1862	0.1865	0.1945
Adj R^2	0.1116	0.1807	0.1855	0.1860	0.1861	0.1938
Observations	12,181	12,181	12,181	12,181	12,181	11,172

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

who found that both a large shadow economy and informal entrepreneurship are associated with the use of more cash. Regarding the magnitude of the estimated coefficients for the two subsamples of old versus new EU member states, although the cash in labor variables have the same positive signs, they have a higher positive impact on informal entrepreneurship (IE) for the subsample of old EU member states, compared to the new subsample (Table 4.4—models (2) to (6), and Table 4.5—models (2) to (6)).

As expected, tax morale has a direct impact on informal entrepreneurship, as the more people who favor informal sector activities, the higher the informal entrepreneurship (Table 4.3, models (3) to (7)). The specialized literature (e.g., Alm & Torgler, 2006; Kirchler, 2007; Çule & Fulton, 2009; Cubillas et al., 2018; Achim & Borlea, 2020 p. 218) has also emphasized that the *attitude regarding taxes* or *tax morale* is decisive for the inclination toward engaging in illicit activities. In addition, our results show that the effect exerted by tax morale on old EU states was twice as high as the impact on new states (i.e., the estimated coefficients, as shown in regressions (3) to (6) in Table 4.4, were approximately doubled compared to the corresponding estimated coefficients and regressions from Table 4.5).

Moreover, the trust in tax and social security authorities (TrustTaxSS) had an indirect relationship with informal entrepreneurship. The more trust people have in the quality of institutions, the less inclined they are to engage in informal entrepreneurship activities (Table 4.3, models (4) to (7)). These results are supported by other specialized studies (e.g., Kirchler, 2007; Torgler & Schneider, 2009; Park & Blenkinsopp, 2011; Fritzen et al., 2014; Çule & Fulton, 2009; Marinkovic, 2005; Austwick & Berga, 2016) highlighting the importance of trust for effective functioning of the state mechanisms. In addition, inefficiency in providing public goods determines the incentives to work in the shadow to obtain higher and quicker benefits. Tables 4.4 and 4.5 show that the impact of trust in tax and social security authorities (TrustTaxSS) is slightly higher in old EU member states than in the new ones (the estimated coefficients from regressions (4) to (6) in Table 4.4 are higher in modulus than the corresponding estimated coefficients and regressions (4) to (6) in Table 4.5).

Economic prosperity seems to be directly related to informal entrepreneurship, as the estimated coefficients for LogGDP were positive in regressions (5), (6), and (7) from Table 4.3. That is, the more a nation develops economically, increasing its per capita GDP, the more incentives are created for entrepreneurial activities of any type, including informal entrepreneurship. Indeed, using a sample of 125 worldwide countries from 2006 to 2016, Achim et al. (2019) found a positive effect of economic development on the level of entrepreneurship. In this view, at a higher scale of entrepreneurship, there are higher levels of openings, including those for informal entrepreneurship. Further, the estimated coefficients from Tables 4.4 and 4.5 show the significant positive influence of GDP on the level of informal entrepreneurship for old EU member states (Table 4.4, models (5) and (6)); however, no significant influence was found for the new states (Table 4.5, model (6)). Similarly, Achim et al. (2019) pointed out that the level of development has a different type of

influence on the new business entry rate in two groups of high-income and low-income countries.

Urbanization also has a positive impact on informal entrepreneurship, showing that the more urbanized an area is, the more developed the informal entrepreneurship activities are, to the detriment of rural areas, according to regressions (6) and (7) from Table 4.3. Further, Tables 4.4 and 4.5 show no significant influence of urbanization on the level of informal entrepreneurship in old EU member states (Table 4.4, model (6)), but a significant positive influence of urbanization was maintained in new EU member states (Table 4.5, models (5) and (6)). Our results are to those of Williams (2020), who found that people from rural areas and villages are more prone to get involved in informal sector activities.

Regarding culture, among the six dimensions of Hofstede's model, masculinity (MAS) and long term orientation (LTO) were found to be significant within the most complex multiple regression from Table 4.3, model (7), with an indirect impact for the former and a direct impact for the latter. Culture also seems to have a differentiated impact on the development of informal entrepreneurship within the two subsamples of countries: if MAS and LTO are significant for old EU members (Table 4.4, model (6)), LTO has a reversed impact for new EU members while MAS is not significant (Table 4.5, model (6)). Moreover, for the subsample of new EU member states, PD, IDV, and UAI have a negative impact on IE, whereas IND has a positive impact (Table 4.5—model (6)).

Thus, our study shows that the higher the masculinity, the lower the level of informal entrepreneurship (Table 4.3, model (7)). Conversely, higher femininity creates higher incentives for engaging in entrepreneurship activities. Other studies (i.e., Tsakumis et al., 2007) find that a higher level of femininity is correlated with higher levels of working in the shadow. A possible explanation of such a correlation may be found in the study of Hofstede (2001, 319), which identified that masculinity and the national permissiveness index are negatively correlated. Thus, a highly masculine society is less permissive and focuses on punishments more than a highly feminine society that is rather concerned with "correction and rehabilitation" (Tsakumis et al., 2007). In this view, a society that is highly masculine seems to be "more conscious of its tax compliance obligations" (Tsakumis et al., 2007, 138), and therefore less prone to engage in informal entrepreneurship. Our study conducted on the two subgroups of old and new EU member states reveals that the negative coefficient of MAS was retained in the estimations performed for the old group (Table 4.4, model (6)), whereas the coefficient was not significant for the new one ((Table 4.5, model (6)).

In addition, we found that the higher the LTO level of a society, the higher its level of informal entrepreneurship (Table 4.3, model (7)). Similarly, Dan (2015) found the size of the shadow economy and LTO of 26 EU member states in 2013 to be positively correlated. The type of orientation of a certain culture may determine the incentives for informal working because LTO cultures have thrift and preparation for the future as a main characteristic of theirs (Réthi, 2012). However, when we conducted our analysis of the two subgroups, we estimated different signs. Thus, we found the same positive coefficient of LTO for old EU countries (Table 4.4, model

(6)), whereas for new countries, surprisingly, the sign of this estimated coefficient was negative (Table 4.5—model (6)). Thus, for new EU countries, the level of informal entrepreneurship increases with the level of short-term orientation of the society. A possible explanation is that people from new EU countries are more inclined to obtain immediate benefits from working informally due to the higher financial difficulties they face and the many legislation gaps that an evolving regulation system offers. In line with our results, Réthi (2012) pointed out that a short-term-oriented culture increases the dimension of the shadow economy.

For the remaining cultural dimensions (PD, IDV, UAI, and IND), we found that they do not exert an influence on informal entrepreneurship for old EU countries; however, surprisingly, we obtained significant coefficients for the group of new EU member states (Table 4.5, model (6)). Thus, for new EU countries, lower PD, lower IDV, lower UAI, and higher IND increase the level of informal entrepreneurship.

Additionally, people belonging to societies exhibiting a larger degree of PD accept a hierarchical order in which everybody has a place that needs no further justification (Hofstede Centre, 2022). Indeed, people from new EU countries had a significantly higher level of PD than those from old EU countries. From the summary statistics in Table 4.2, we can see that the average level of PD for new EU countries was 63.99 compared to only 41.95 for the average value for old countries. As it is accustomed to newly entered EU member states to express high levels of PD, the potential reduction in their PD level may disrupt their traditional system of values and general habits, which may further generate different types of imbalances, including engagement in informal entrepreneurship.

Individualism (IDV) is the inclination for a "loosely-knit" social frame in which individuals protect themselves and their close family members only while collectivism is the preference for a "tightly-knit" framework of society in which individuals look after their relatives or members of a particular in-group in exchange for unquestioning loyalty (Hofstede Centre, 2022). In this view, for collectivistic societies, people tend to violate the law in order to sustain their own group out of unquestioning loyalty. Our findings show that people in a collectivistic society have a tendency to engage in informal entrepreneurship, as in the case of new EU countries. Additionally, a lower individualistic society (i.e., a higher collectivistic one) is also significantly associated with the engagement in shadow economy in the studies of Richardson (2008) and Tsakumis et al. (2007).

UAI reflects the degree to which society members get to feel uncomfortable with uncertainty and ambiguity (Hofstede Centre, 2022). This dimension deals with how people confront the fact that the future can never be known: to attempt to control or just let it happen. The results confirmed that people from new EU countries have higher levels of UAI (of 75.49 on average; see Table 4.2) compared to people from old EU countries (65.06 on average, Table 4.2). That is, people from new EU countries feel more uncomfortable and intolerant of risk and ambiguity. High UAI cultures are related to ambiguous situations that can imprint higher levels of anxiety (Tsakumis et al., 2007). For such cultures, corruption would be regarded as a mechanism to reduce uncertainty and obtain more certain results (Husted, 1999). Furthermore, in such cultures, people consider tax systems as being extremely

complex, and therefore, they tend to avoid taxes (Richardson, 2008). Therefore, a decrease in the level of UAI for new EU countries causes an increase in the level of informal entrepreneurship. As in the case of PD, the reduction in the level of UAI for new EU countries can disrupt the usual system of accepting risk and maintaining order, which may generate different types of imbalances, including engagement in informal entrepreneurship.

In addition, indulgence (IND) is the degree to which society permits relatively free gratification of basic and natural human drives for enjoying life and having fun as opposed to the suppression and regulation of needs according to strict social norms (Hofstede Centre, 2022). In this view, we expect that an indulgent society is more prone to fulfilling immediate needs regardless if they comply with the law or not. Indeed, the positive sign of IND supports these assumptions.

4.2 Robustness Checks

To test the robustness of our results, we tested our model on a different sample of observations, extracting the variables from Eurobarometer no. 402 (79.2), a similar survey from April to May 2013 with 26,257 respondents. Unfortunately, the ratios of people working in specific sectors and the level of trust in the authorities were not declared then. Thus, the variables Agriculture and TrustTaxSS were not included in the database we have prepared for robustness tests. Nevertheless, the variables Cash in Labor and Tax Morale were found in the 2013 and 2019 Special Eurobarometer on informal entrepreneurship. Furthermore, our database for robustness checks was supplemented with LogGDP and Urban for 2013 from the World Data Bank and

Table 4.6 Robustness checks: the reduced model without Agriculture and TrustTaxSS

	OLS regressions		
Informal entrepreneurship determinants	1. Entire sample	2. Old	3. New
CashLabor	0.2297***	0.2505***	0.2189***
TaxMorale	0.0218***	0.0211***	0.0228***
LogGDP	0.0095***	0.0164***	
Urbanization	−0.0003***		
Culture (PD)			−0.0016***
Culture IDV			−0.0018***
Culture (MAS)	−0.0006***	−0.0005***	
Culture (UAI)			−0.0023
Culture (LTO)	0.0004***	0.00028***	−0.0015
Culture (IND)			
Constant	−0.0792***	−0.1767***	0.4655***
R^2	0.0624	0.0493	0.0732
Adj R^2	0.0622	0.049	0.0727
Observations	25,000	14,858	10,142

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

with Hofstede's cultural dimensions. The reduced model, due to data constraints (Eq. (4.1), excluding $Agriculture_i$ and $TrustTaxSS_i$), is presented in Table 4.6.

The robustness tests show that our main results are supported for the whole sample of the 28 EU countries and for the two subsamples of old and new EU member states. Based on data taken from the 2013 Eurobarometer survey, for a totally different sample of respondents, the estimated signs and significances of the considered variables stand strong as determinants of informal entrepreneurship.

5 Conclusions

In this study, first, using bibliometric analysis, we provide an extensive literature review in the field of informal entrepreneurship to identify the main trends and patterns. Our results highlight a 5.5-fold increase in the number of published papers in the area of informal entrepreneurship in the last decade. The journals that published the highest number of publication articles on "informal entrepreneurship" topic are Entrepreneurship and Regional Development, Small Business Economics, Journal of Developmental Entrepreneurship, Journal of Business Venturing, International Small Business Journal-Researching Entrepreneurship, Entrepreneurship Theory and Practice, International Entrepreneurship and Management Journal, Sustainability, Journal of Business Ethics, and Strategic Entrepreneurship Journal. Most of these journals are also the most-cited journals on the same topic. In addition, countries that published the largest volume of research papers on the topic of "informal entrepreneurship" are, in order, the US and the UK, followed by emerging China, Germany, Spain, Canada, the Netherlands, and Australia.

Second, using a large sample of observations from 28 EU member states, we conduct empirical cross-country analysis to identify the main determinants that stimulated engagement in informal work. We use data extracted from the 2019 Special Eurobarometer Survey 92.1, World Bank Data, and the six cultural dimensions from Hofstede's model. Our findings suggest that agriculture, cash in labor, trust morale, trust in tax and social security authorities, economic development, and urbanization are important determinants of the level of informal entrepreneurship. Moreover, we conduct a comparative analysis between the two subgroups of countries (old and new EU countries). On the one hand, we find that the determinants of cash in labor, trust morale, trust in tax and social security authorities, economic development, and urbanization have a greater influence on the old EU countries compared to new EU countries. On the other hand, for new EU countries, the impacts of cultural factors (PD, IDV, UAI, and IND) are more significant than in old EU countries. These findings highlight the importance of social attitudes and norms, values, culture, lifestyle, and historical heritage in new EU countries, where the intrinsic motivation for individuals to choose between working for the "formal" or "informal" sector is mostly related to sociocultural factors rather than to economic and/or political factors.

These findings are very important for policymakers who have to include cultural factors in their analyses of people's behaviors regarding involvement in informal work, especially for new EU countries, so that they can take the best decisions on how to tackle this undesirable phenomenon. Our findings are also important in an international context, as the estimations are performed on a large sample of cross-sectional respondents, covering all EU countries, on the most recent data available at the time of writing this chapter. The limitations of our study include that we only employed OLS regression as a multivariate data analysis technique. For future research, we intend to use probit regression to surpass this limit, for data extracted from Special Eurobarometers on informal entrepreneurship only. Moreover, we intend to employ panel data analysis as well, including three Eurobarometers (no 284–67.3 from May–June 2007, no 402–79.2 from April–May 2013, and no 498–92.1 from September 2019), by further including more potential determinants of informal entrepreneurship.

Funding and 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 conflicts of interest.

References

Achim, M. V., & Borlea, N. S. (2020). *Economic and financial crime. Corruption, shadow economy, and money laundering*. Springer Nature Switzerland AG. https://doi.org/10.1007/978-3-030-51780-9

Achim, M. V., Borlea, N. S., & Văidean, V. L. (2019). Culture, entrepreneurship and economic development. An empirical approach. *Entrepreneurship Research Journal*. https://doi.org/10.1515/erj-2018-0091

Alm, J., & Torgler, B. (2006). Culture differences and tax morale in the United States and Europe. *Journal of Economic Psychology, 27*(2), 224–246.

Austwick, S., & Berga, I. (2016). *Foreign investors viewpoint on the shadow economy in Latvia may 2016, KPMG*. Available at https://docplayer.net/140175931-Foreign-investors-viewpointon-the-shadow-economy-in-latvia-may-2016.html. Accessed 18 Feb 2020.

Cubillas, A. F., Morales, O., & Rees, G. H. (2018). Understanding the intentions of informal entrepreneurs in Peru. *Journal of Entrepreneurship in Emerging Economies, 10*(3), 489–510. https://doi.org/10.1108/JEEE-02-2018-0022

Bergheim, S. (2007). The happy variety of capitalism. *Deutsche Bank Research, 25*, 1–22.

Bordean, O. N., Rácz, D. S., Ceptureanu, S. I., Ceptureanu, E. G., & Pop, Z. C. (2020). Gender diversity and the choice of conflict management styles in small and medium-sized enterprises. *Sustainability, 12*, 7136. https://doi.org/10.3390/su12177136

Bucur, D. (2011). *Criminalitatea transfrontalieră şi economia globalizată (cross-border crime and the globalized economy)*. Pro Universitaria Publishing House.

Chan, C. W., Troutman, C. S., & O'Bryan, D. (2000). An expanded model of taxpayer compliance: Empirical evidence from the United States, *83*(103), 9.

Chelliah, R. J. (1971). Trends in taxation in developing countries. *Staff Papers, International Monetary Fund, 18*, 254–0331.

Čiutienė, R., Meilienė, E., Savanevičienė, A., & Vaitkevičius, S. (2015). Interdependence between human capital and the power of a shadow economy: Lithuanian case study. *Technological and Economic Development of Economy, 21*(3), 460–482.

Çule, M., & Fulton, M. (2009). Business culture and tax evasion: Why corruption and the unofficial economy can persist. *Journal of Economic Behavior & Organization, 72*(3), 811–822.

Dan, H. (2015). The influence of cultural elements on fiscal behaviour in the European Union. *Journal Modelling the New Europe, 16*, 3–19.

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

Enste, D. H. (2010). Shadow economy—the impact of regulation in OECD-countries. *Economics, 24*(4), 555–571. https://doi.org/10.1080/10168737.2010.525996

Feld, L. P., & Schneider, F. (2010). Survey on the shadow economy and undeclared earnings in OECD countries. *German Economic Review, 11*(2), 109–149.

Fritzen, S. A., Serritzlew, S., & Svendsen, G. T. (2014). Corruption, trust and their public sector consequences: Introduction to the special edition. *Journal of Comparative Policy Analysis: Research and Practice, 16*(2), 117–120.

Gaspareniene, L., Remeikiene, R. R., & Navickas, V. (2016). The concept of digital shadow economy: Consumer's attitude. *Procedia Economics and Finance, 39*, 502–509.

Hassan, M., & Schneider, F. (2016). Size and development of the shadow economies of 157 worldwide countries: Updated and new measures from 1999 to 2013. *Journal of Global Economics, 4*(218), 2. https://doi.org/10.4172/2375-4389.1000218

Hofstede Centre. (2022). Available at https://hi.hofstede-insights.com/national-culture. Accessed May 2022.

Husted, B. W. (1999). Wealth, culture, and corruption. *Journal of International Business Studies, 30*(2), 339–359. https://doi.org/10.1057/palgrave.jibs.8490073

Jiménez, A., Palmero-Cámara, C., González-Santos, M. J., González-Bernal, J., & Jiménez-Eguizábal, J. A. (2015). The impact of educational levels on formal and informal entrepreneurship. *Business Research Quarterly, 18*(3), 204–212.

Johnson, S., Kaufmann, D., & Sleifer, A. (1997). The unofficial economy in transition. *Brooking Papers on Economic Activity, 1997*, 159–221.

Kasipillai, J., Aripin, N., & And Amran, N. A. (2003). The influence of education on tax avoidance and tax evasion. *eJournal of Tax Research, 1*(2), 134–146.

Kirchler, E. (2007). *The economic psychology of tax behavior*. Cambridge University Press.

Kelmanson, B., Kirabaeva, K., Medina, L. , Mircheva, B., & Weiss, J. (2019). Explaining the shadow economy in Europe: Size, causes and policy options, IMF working paper WP/19/278.

Kogler, C., Bătrancea, L., Nichita, A., Pantya, J., & Belianin, A. (2013). Trust and power as determinants of tax compliance: Testing the assumptions of the slippery slope framework in Austria, Hungary, Romania and Russia. *Journal of Economic Psychology, 34*, 169–180.

Lv, Z. (2017). Intelligence and corruption: An empirical investigation in a non-linear framework. *Journal of Behavioral and Experimental Economics, 69*, 83–91.

Marinkovic, D. (2005). Corruption in history and today, have we choice. *Economic Perspective, 10*(1), 5–20. Serbia: Society of Economists.

Medina, L., & Schneider, F. (2018). Shadow economies around the world: What did we learn over the last 20 years? (Working Paper WP/18/17). International Monetary Fund.

Park, H., & Blenkinsopp, J. (2011). The roles of transparency and trust in the relationship between corruption and citizen satisfaction. *International Review of Administrative Sciences, 77*(2), 254–274.

Petrakis, P. E. (2014). *Culture, growth and economic policy*. Springer.

Potrafke, N. (2012). Intelligence and corruption. *Economics Letters, 114*, 109–112.

Richardson, G. (2008). The relationship between culture and tax evasion across countries: Additional evidence and extensions. *Journal of International Accounting, Auditing and Taxation, 17*, 67–78. https://doi.org/10.1016/j.intaccaudtax.2008.07.002

Remeikiene, R., Gaspareniene, L., & Schneider, F. (2017). The definition of digital shadow economy. *Technological and Economic Development of Economy, 24*(2), 1–22.
Réthi, G. (2012). Relation between tax evasion and Hofstede's 4+2 model. *European Journal of Management, 12*(3), 61–71.
Salahodjaev, R. (2015). Intelligence and shadow economy: A cross-country empirical assessment. *Intelligence, 49*, 129–133.
Satalkina, L., & Steiner, G. (2020). Digital entrepreneurship: A theory-based systematization of Core performance indicators. *Sustainability, 12*(10), 4018. https://doi.org/10.3390/su12104018
Schneider, F., & Buehn A (2016). Estimating the size of the shadow economy: Methods, problems and open questions, IZA Discussion Papers 9820, Institute of Labor Economics (IZA).
Schneider, F., & Williams, C. C. (2013). *The shadow economy*. Institute of Economic Affairs.
Schneider, F. H., & Klinglmair, R. (2004). *Shadow economies around the world: What do we know?* Working paper no. 0403. Universität Linz.
Şcheau, M. C. (2018). *Criminalitatea informatică privind transferurile financiare (Cybercrime on financial transfers)*. Economica Publishing House.
Thai, M. T. T., Turkina, E., & Simba, A. (2020). The impact of national social capital on business creation rates in the formal vs informal sectors. *International Journal of Entrepreneurial Behavior & Research, 26*(8), 1739–1768. https://doi.org/10.1108/IJEBR-02-2020-0071
Tsakumis, G. T., Curatola, A. P., & Porcano, T. M. (2007). The relation between National Cultural Dimensions and tax evasion. *Journal of International Accounting, Auditing and Taxation, 16*, 131–147. https://doi.org/10.1016/j.intaccaudtax.2007.06.004
Torgler, B. (2004). Tax morale in Asian countries. *Journal of Asian Economics, 15*, 237–266.
Torgler, B., & Schneider, F. (2009). The impact of tax morale and institutional quality on the shadow economy. *Journal of Economic Psychology, 30*(3), 228–245.
Webb, A., McQuaid, R., & Rand, S. (2020). Employment in the informal economy: Implications of the COVID-19 pandemic. *International Journal of Sociology and Social Policy, 40*(9/10), 1005–1019. https://doi.org/10.1108/IJSSP-08-2020-0371
Webb, J. W., Bruton, G. D., Tihanyi, L., & Ireland, R. D. (2013). Research on entrepreneurship in the informal economy: Framing a research agenda. *Journal of Business Venturing, 28*(5), 598–614.
Williams, C. C. (2020). Tackling informal entrepreneurship in east-Central Europe: From a deterrence to preventative approach. *Journal of Developmental Entrepreneurship, 25*(4), 1–20.
Williams, C. C. (2014). Informal Sector Entrepreneurship A background paper for the OECD Centre for Entrepreneurship, SMEs and Local Development *(3) (PDF) Informal Sector Entrepreneurship*. Available from: https://www.researchgate.net/publication/294089575_Informal_Sector_Entrepreneurship?channel=doi&linkId=56be16a608ae44da37f88de8&showFulltext=true. Accessed May 2022.
Williams, C. C., & Shahid, M. S. (2016). Informal entrepreneurship and institutional theory: Explaining the varying degrees of (in)formalization of entrepreneurs in Pakistan. *Entrepreneurship & Regional Development, 28*(1–2), 1–25. https://doi.org/10.1080/08985626.2014.963889

Monica Violeta Achim is a full professor and doctoral supervisor in the field of Finance at the Faculty of Economics and Business Administration, Babeş-Bolyai University, Cluj-Napoca, Romania. Having over 24 years of experience in academia, she has published over 150 scientific articles and 25 books as the main author or coauthor. Her most recent reference work is the *Economic and Financial Crime: Corruption, Shadow Economy and Money Laundering* book, published by Springer. In 2020, she obtained a prestigious Award for Excellence in Scientific Research from Babeş-Bolyai University, Faculty of Economics and Business Administration, Cluj-Napoca, Romania, in recognition of the great results obtained in her research activity. She is the principal investigator on her large research grant titled "Intelligent analysis and prediction of economic and financial crime in a cyber-dominated and interconnected business world," conducted over the

period 2021–2023, financed by the Romanian Ministry of Education and Research, CNCS-UEFISCDI, project number PN-III-P4-ID-PCE-2020-2174 (www.fincrime.net).

Viorela Ligia Văidean is an associate professor for the Finance Department of the Faculty of Economic Sciences and Business Administration, Babeş-Bolyai University, Cluj-Napoca. She obtained a Bachelor's degree in Finance and Banking from Babeş-Bolyai University Cluj-Napoca, Romania, in 2006, further graduating from a Master's Program in Corporate Finance and Insurance and another degree in Project Management and Evaluation. She successfully followed a full-time PhD program, obtaining her PhD in the Finance field, in 2010. In 2015, she graduated from a postdoctoral study program. She has worked as a teaching assistant and then a lecturer for the Finance Department within Babeş-Bolyai University Cluj-Napoca. She has also worked as an expert for different EU-financed projects and grants. She has published more than 50 research papers and attended several international conferences. She has been the author or coauthor of 10 books and international book chapters. Her research interests cover the areas of Health Economics, Corporate Finance, Financial Management, Organized Crime, and Fiscal Policies. She is a member of the project titled "Intelligent analysis and prediction of the economic and financial crime in a cyber-dominated and interconnected business world," conducted over the period 2021–2023, financed by the Romanian Ministry of Education and Research, CNCS-UEFISCDI, project number PN-III-P4-ID-PCE-2020-2174 (www.fincrime.net).

Sorin Nicolae Borlea is a full professor and doctoral supervisor in the field of Finance at the University of Oradea and Vasile Goldiș University and associate scientific researcher at the European Research Institute of Babeş-Bolyai University, Cluj-Napoca. He has more than 16 years of experience in the field of academia and more than 30 years in the business field. He has published more than 90 scientific papers and 20 books. His most recent reference work is the coauthored book *Economic and Financial Crime: Corruption, shadow economy and money laundering,* published by Springer. In parallel with the academic field, he works in the business environment as a financial auditor, accounting expert, tax consultant, and financial analyst, being strongly anchored in economic and financial crime issues in the files managed by the Court of Cluj-Napoca. He is well known in the business environment as a perfectionist, being ranked in the top 10 accounting experts in Cluj County (2017). He is a member of the project titled "Intelligent analysis and prediction of the economic and financial crime in a cyber-dominated and interconnected business world," conducted over the period 2021–2023, financed by the Romanian Ministry of Education and Research, CNCS-UEFISCDI, project number PN-III-P4-ID-PCE-2020-2174 (www.fincrime.net).

Decebal Remus Florescu is deputy editor-in-chief of Adevărul newspaper, coordinating its Transylvanian counties. He is a graduate of the Faculty of Law from Babeş-Bolyai University Cluj-Napoca, and he has been working as a journalist for over 15 years. Among the media institutions he worked for there are Ziarul Clujeanului, Clujeanul, Ziarul Financiar, and the Adevărul de Seară network. In 2015, he was elected president of the Cluj Press Professionals' Association, a position he has held until 2021, further continuing as its vice president. In 2020, he defended his PhD thesis titled "Creating viral content in the digital age," within the Faculty of Political, Administrative and Communication Sciences (FPACS), Babeş-Bolyai University Cluj-Napoca, becoming a PhD in Communication Sciences. He has been working as a teaching associate for the Journalism Department of the FPACS since 2015, and his research interests cover media, democracy, corruption, public policies and fake news. He is a member of the project titled "Intelligent analysis and prediction of the economic and financial crime in a cyber-dominated and interconnected business world," conducted over the period 2021–2023, financed by the Romanian Ministry of Education and Research, CNCS-UEFISCDI, project number PN-III-P4-ID-PCE-2020-2174 (www.fincrime.net).

Chapter 5
The Impact of Minimum Wage on the Shadow Economy: A Panel Data Analysis for EU Countries

Eugenia Ramona Mara

Abstract This chapter investigates the impact of minimum wage on the shadow economy considering a panel data analysis for European Union countries from 2012 until 2021, using panel EGLS (estimated generalized least squares) and panel two-stage EGLS. The minimum wage is applied in 22 European Union member states in 2023 (it was applied only in 21 EU countries in 2021) and represents a crucial tool in labor policy strategy, which targets employee protection. In this study, we try to test if minimum wage can play a role in reducing the shadow economy. Based on empirical results, we found that minimum wage can reduce the shadow economy if certain conditions are accomplished. The minimum wage has to be established considering a minimum threshold, which can assure employees a decent standard of living and for employers an affordable labor force cost. In this context, the tax wedge represents another important factor with a positive influence on the shadow economy, validated by our empirical model. Based on the empirical estimations, increasing the minimum wage can lead to a decrease in shadow economy in more developed EU countries, in which the minimum wage is higher than 1000 euros and has a significant positive impact in less developed countries, where this minimum wage is below this threshold of 1000 euros. The main contribution of this paper consists in delimitating the different impacts of minimum wage considering a more complex system of factors and conditions necessary to be accomplished for a successful labor policy in reducing the shadow economy.

Keywords Shadow economy · Minimum wage · Informal work · Tax wedge

JEL Classification O17 · J31 · C23

E. R. Mara (✉)
Faculty of Economics and Business Administration, Babeș-Bolyai University, Cluj-Napoca, Romania
e-mail: ramona.mara@econ.ubbcluj.ro

M. V. Achim (ed.), *Economic and Financial Crime, Sustainability and Good Governance*, Contributions to Finance and Accounting,
https://doi.org/10.1007/978-3-031-34082-6_5

1 Introduction

Can minimum wage be an obstacle to the expansion of the shadow economy, or it can stimulate it? Does the minimum wage level contribute to limiting the flourishing of informal activities? This paper contributes to answering these questions by considering the minimum wage policy applied in European Union countries based on the panel data analysis. The minimum wage represents an essential instrument in labor policies strategy, which aims firstly the employee protection. This protection covers many areas, from preventing abuses in the labor market to reducing the risk of poverty for employees. The minimum wage is enforced through national laws in each country, which establish a basic wage rate for hourly, weekly, or monthly work. In most cases, the national minimum wage applies to either all employees or a significant majority of the workforce within the country. This minimum wage is considered a gross wage, implying that employees will receive a lower net wage because the social security contributions and personal income tax are deducted from the gross wage.

The first minimum wage legislation was passed in New Zealand in 1894 by adopting the Industrial Conciliation and Arbitration Act and was later introduced in various countries after World War II (Jiménez Martínez & Jiménez Martínez, 2021). Minimum wage policies are implemented as public policy tools to address income inequality and poverty and are meant to be indicators of labor productivity and compensation levels in each country (Bruckmeier & Bruttel, 2021).

Introducing minimum wage as an enforcement measure on the labor market can have multiple consequences. For employers, this measure leads to higher labor costs due to the increase in the gross wage and a higher tax burden. A benefit of minimum wage is increased labor productivity because employees can become more motivated in their work. For governments, an expected positive outcome will be a higher amount of fiscal revenue collected from income tax and social security contributions. According to Tonin (2005), the minimum wage can increase fiscal revenues by expanding the tax base for income tax and social security contributions.

For employees, assuring a minimum wage is an important step in reducing poverty and income inequality. Minimum wage laws set a baseline for wages, ensuring that employees receive a minimum level of compensation for their work. This can lead to increased earnings for those who previously earned less than the minimum wage. When workers are paid fairly, they may feel more valued and respected, which can improve their self-esteem and job satisfaction. These positive benefits of the minimum wage depend on institutional factors such as the effectiveness of the inspection system (Rani et al., 2013).

The minimum wage can influence the shadow economy through the following channels. On one hand, the shadow economy can flourish if the government imposed a minimum wage that cannot be supported by employers. In this situation, employers are unable to pay this minimum wage because of the economic conditions, and this fact is more prevalent in less developed countries. Consequently, the unemployment rate will be higher, and informal work represents an alternative solution for both

employers and employees. On the other hand, a minimum wage can contribute to a decrease in the shadow economy if certain conditions are accomplished. First, this minimum wage must be correlated with the level of development of the country and must represent a labor cost that is easy to afford for employers. Second, this minimum wage must be set up to assure a decent standard of living for the employees, so that they are not interested in developing informal activities to supplement their incomes. Third, the impact of the minimum wage on the decrease of the shadow economy can be realized in an economic context where controls and audits are carried out at the level of employers for compliance with labor legislation. Thus, the impact of minimum wage on the underground economy is influenced by specific factors of the countries in which it is applied, but also by the level at which it is established.

Previous studies have focused on analyzing the impact of minimum wage on the shadow economy for individual countries, particularly low-income countries. The situation in European Union, as far as we know, has not been analyzed considering the implications generated by the minimum wage policy promoted in these countries. To address this gap in the literature, we are coming up with a different approach. First, we conduct our analysis based on panel data for all EU countries where the minimum wage is implemented, and then, we split the countries into two groups considering a threshold of the minimum wage. This study's novelty is that we attempt to determine if the minimum wage level significantly contributes to the spread of the shadow economy.

The rest of this chapter comprises Sect. 2, which provides a literature review on the impact of minimum wage on the shadow economy. The next section presents the empirical methodology and the main results of this study. In Sect. 4, we discuss the results obtained considering a broad view of the policy implications of minimum wage. The chapter ends with concluding remarks, limitations of our research, and the future direction of the study.

2 Literature Review

There are two strands of literature concerning the influence of the minimum wage on the shadow economy. One strand highlights the significant contribution of the minimum wage to increase the shadow economy through informal work due to the ineffectiveness of labor policies that are implemented. In some countries, the enforcement of minimum wage laws may be weak, making it easy for employers to continue paying low wages and avoiding taxes. Additionally, some workers may choose to develop informal activities, where they can avoid taxes and regulations, even if the pay is lower.

The other strand of literature underlines the fact that implementing a minimum wage policy can have a significant negative impact on the size of the shadow economy. A higher minimum wage can reduce the incentive for employers to hire

workers informally and pay them less than the legal minimum wage. This can lead to a contraction in the size of the shadow economy and an increase in tax revenues.

There is extensive literature regarding the impact of minimum wage and how can its objective are accomplished in different countries. Regarding the impact of minimum wage on the shadow economy, there is a scarcity of studies. Most of the studies are considering a particular case of one country (Davidescu & Schneider, 2017; Carneiro, 2000; Groisman, 2015; Heemskerk et al., 2018).

Davidescu and Schneider (2017) investigate the relationship between minimum wage policies and the size of the shadow economy in Romania using the Granger causality approach with vector error correction models. The authors find that there is a positive relationship between minimum wage levels and the size of the shadow economy, meaning that as minimum wage levels increase, so does the size of the shadow economy. The study suggests that this may be due to increased labor costs, leading companies to operate in the informal sector to avoid paying higher wages and taxes. Considering the results of this study, we assume a similar impact in developing countries from European Union.

Carneiro (2000), using time series data for the case of Brazil, demonstrated a robust and significant positive contribution of the real minimum wage increase to the expansion of the informal sector. Groisman (2015) finds that changes in the minimum wage can have an insignificant impact on the economic participation of the population in informal activities in Argentina.

Another study performed by Heemskerk et al. (2018) examines the consequences of the increase in the minimum wage during 2013–2016 in Romania. Their results reflect the fact that a minimum wage increase leads to a lower shadow economy and to reducing the poverty. According to their study, the decision to apply a higher minimum wage generates a positive impact on the public budget.

Tonin (2005) explores the effects of minimum wage on the informal work sector using a complex model of the labor market. The study focuses on an economy where there is a significant amount of tax evasion, which is a common phenomenon in many developing countries. The author suggests that implementing a minimum wage can have both positive and negative effects on informal work. On the one hand, a higher minimum wage can increase the incentives for workers to move from informal work to formal work, which can increase tax revenue and reduce the prevalence of tax evasion. On the other hand, a higher minimum wage can also make it more difficult for informal workers to find employment, as employers may not be able to afford to pay the higher wage.

There are some papers regarding the influence of minimum wage on the shadow economy for some groups of countries. Nataraj et al. (2014) consider a meta-analysis of low-income countries to investigate how minimum wages can have consequences on formal and informal employment. They conclude that higher minimum wages are associated with lower formal employment and an expansion of informal workers. Adam and Buffie (2020) explored the impact of minimum wage policies on the shadow economy in less developed countries using a dynamic general equilibrium model.

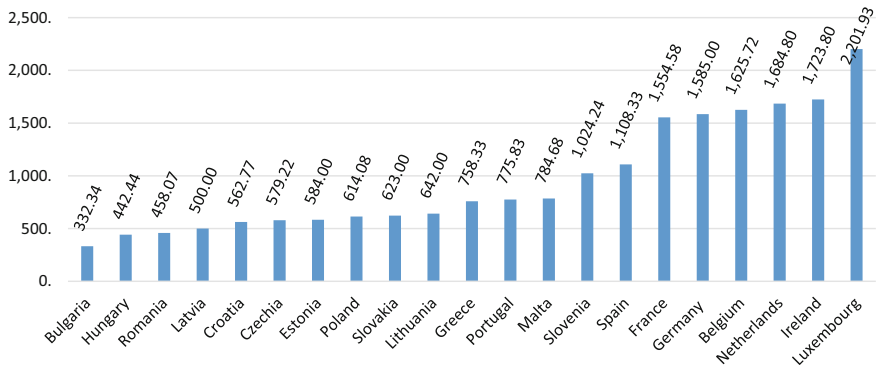


Fig. 5.1 Minimum monthly wages in 2021 (Euro) in EU countries. Source: own composition based on data provided by Eurostat

In our study, we aim to contribute to the existing literature by analyzing EU countries through panel data analysis. Therefore, we address the gap in knowledge related to the effectiveness of minimum wage policies in reducing the size of the shadow economy.

As there are different opinions in the literature regarding the impact of minimum wage on the shadow economy, we take a different approach in our study by examining the impact based on the level of minimum wage. To achieve our research objective, we assume that only countries, with a high minimum wage, can limit the incentive of their citizens to engage in informal activities. Many studies demonstrated a strong correlation between the level of development and the size of the shadow economy (Navickas et al., 2019; Hoinaru et al., 2020; Achim et al., 2021; Mara, 2021). The minimum wage in European Union is still under debate, and the idea of coordinating this policy across EU countries was first proposed in France (Schulten, 2008, 2012). Despite important progress, minimum wages in Europe are still below the subsistence minimum in many countries and thus are unable to prevent the risk of poverty (Schulten, 2014).

The level of minimum wage depends on the degree of development in one country, and based on the descriptive statistics (Fig. 5.1), we find that the highest amounts of the minimum wage are in Luxemburg, Ireland, Netherlands, France, and Germany. Considering all these aspects, we split the European Union countries into two clusters based on the level of minimum wage enforced in 2021. The first group of countries (Group A) has a minimum wage higher than 1000 euros (Luxemburg, Ireland, Netherlands, Belgium, Germany, France, Spain, and Slovenia). In this group, only Slovenia is a new member state of the European Union; the rest are old member states. The second group (Group B) includes countries with a level of minimum wage below 1000 euros such as Bulgaria, Croatia, Czech Republic, Greece, Estonia, Hungary, Latvia, Lithuania, Malta, Poland, Portugal, Romania,

and Slovakia. We chose this threshold of 1000 euros in accordance with a similar classification provided by Eurostat,[1] which uses minimum wages expressed in purchasing power standards. It is important to note that some EU countries do not have a minimum wage policy implemented in 2023, such as Denmark, Italy, Austria, Finland, and Sweden.

Based on the aspects considered thus far, we aim to answer the following research question:

Can minimum wage be an effective instrument in limiting the shadow economy?

To find an answer to our research question, we will formulate the first hypothesis of our inquiry:

Hypothesis #1: Minimum wage can reduce the shadow economy if is set up higher than a certain minimum level, ceteris paribus.

Another important factor that can significantly contribute to the shadow economy is represented by the tax burden. In the previous research, the impact of the tax burden was extensively studied and confirmed as a significant driver of increasing the shadow economy. In our research, we aim to delimit the impact of wage tax on the spread of the shadow economy. According to Eurostat, the tax wedge represents the difference between the employer's labor costs and the employee's net take-home pay, including any cash benefits from government welfare programs.

Hypothesis #2: *Increasing the tax wage can lead to a higher shadow economy, ceteris paribus.*

In recent years, the tax burden on labor continuously increased to compensate for the decreases in capital tax rates, especially lower corporate tax rates. In this empirical research, we aim to demonstrate the fact that not only tax burden in general, as it was included in other studies, is an important driver of the shadow economy, but the most significant role is also played by tax wage.

3 Empirical Analysis

3.1 Data

We perform the empirical analysis using yearly data for 21 European Union countries from 2012 to 2021. The variables used in the econometric model, along with their sources, are presented in Appendix 1.

Our empirical research aims to capture the impact of minimum wage by considering as an intrinsic factor a threshold for the minimum wage. We are aware of the

[1] https://ec.europa.eu/eurostat/statistics-explained/index.php?title=Minimum_wage_statistics#Variations_in_national_minimum_wages

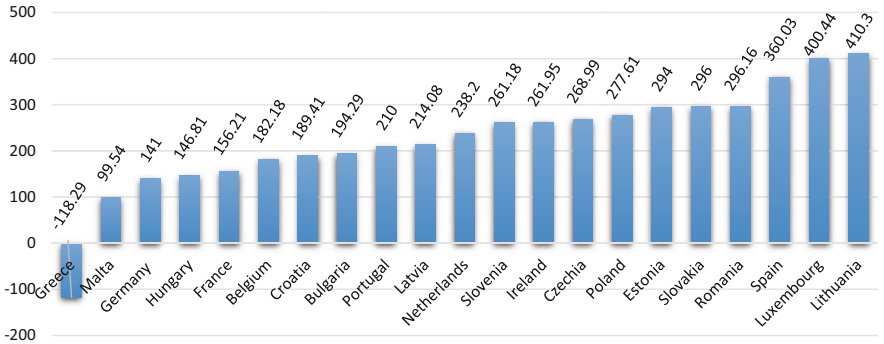


Fig. 5.2 Change of minimum wages between 2012 and 2021. Source: own composition based on data provided by Eurostat

fact that this threshold can be a topic of debate, but considering the descriptive statistics offered by Eurostat, we established this threshold of 1000 euros for minimum wage only for clustering the countries in two groups to see if there are differences in the empirical estimations between these clusters. We emphasize that this threshold can vary from year to year in the same country, and it is not considered the optimum level for EU countries.

In this study, we try to show the fact that the impact on minimum wage is conditioned by its level, and each country must consider multiple perspectives when setting its minimum wage. *Firstly,* the macroeconomic context, labor market characteristics, and the level of development of each country are relevant barometers for choosing the appropriate minimum wage level. *Secondly,* the level of tax wage (the tax rates for salary tax and social security contributions applied to employees and employers) must be considered from a fiscal perspective. The tax wedge can have a significant impact on the shadow economy's spread. If the labor tax burden is too high, both employers and employees will be tempted to prefer informal jobs to declared work agreements. In some cases, it is possible that this influence is higher compared with the level of minimum wage imposed by the government.

Figure 5.1 shows that the minimum wage in the new member states of the EU is lower than in the old member states. Only eight EU countries have a minimum monthly wage higher than 1000 euros. The discrepancies between EU member states are significant, ranging from 332 euros in Bulgaria to 2200 euros in Luxembourg.

It is interesting to analyze the evolution of the minimum wage. Based on Fig. 5.2, we can observe changes from 2012 until 2021. Only one country experienced a decrease in its minimum wage, which was Greece (by 118 euros). On the other hand, many new member states of the EU registered significant increases, such as Lithuania and Romania.

Because we are testing if the minimum wage can have an impact on the shadow economy, we will compute a simple correlation between these two variables for EU countries in 2021 (Fig. 5.3). The result shows a negative correlation, which reflects the fact that any increase in minimum wage can lead to a decrease in the level of the

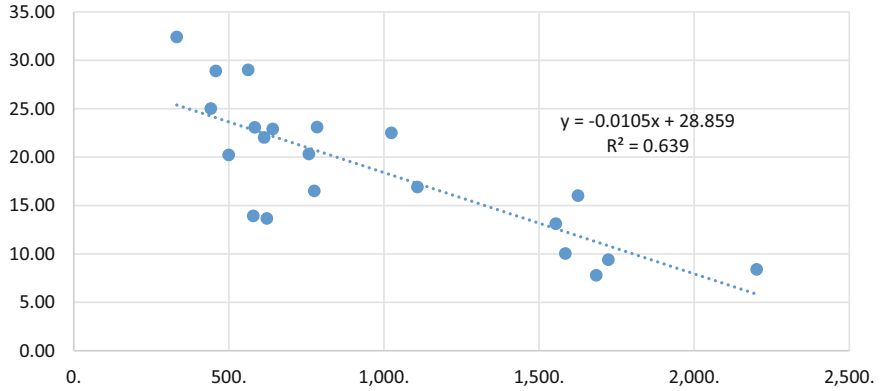


Fig. 5.3 Correlation between shadow economy and minimum wages in EU countries in 2021. Source: own composition based on data provided by Eurostat

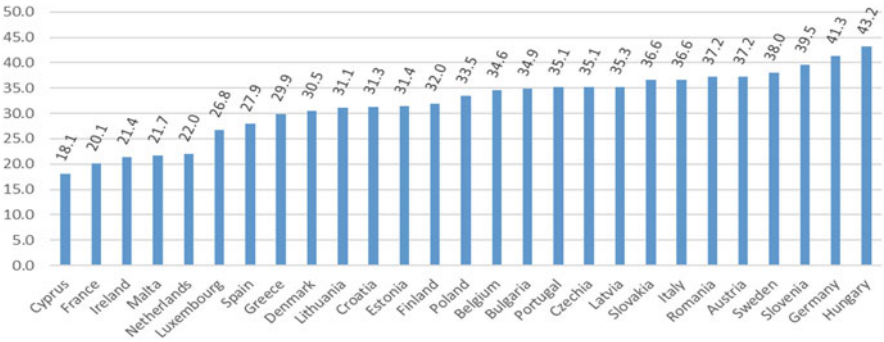


Fig. 5.4 Tax wedges for a single worker with 50% of average earnings and no children for EU countries in 2021. Source: own composition based on data provided by Eurostat

shadow economy. However, we also need to consider other factors that contribute significantly, such as the tax burden on labor and audits carried out by specialized institutions in the labor market.

According to data provided by Eurostat, there are significant disparities in the tax wedge among EU countries. In 2021, the tax wedge ranges from 18.1% in Cyprus to 43.2% in Hungary based on data provided in Fig. 5.4.

Thirdly, from the employers perspective is important to analyze their ability to pay the minimum wage. *Lastly*, the employee's point of view is important because a decent standard of living is necessary to be ensured by the minimum wage.

Figure 5.5 shows the distribution of the countries included in these two clusters (Group A—countries with a higher minimum wage than 1000 euros; Group B—countries with a minimum wage below 1000 euros). It is important to take into account the correlation between the shadow economy and minimum wage. For the

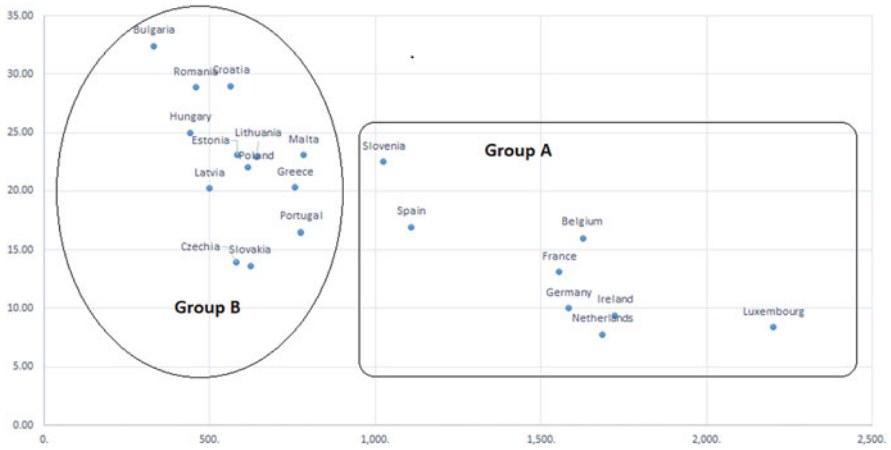


Fig. 5.5 Clusters of EU countries based on the wage minimum threshold based on the 2021 data. Source: own composition based on data provided by Eurostat

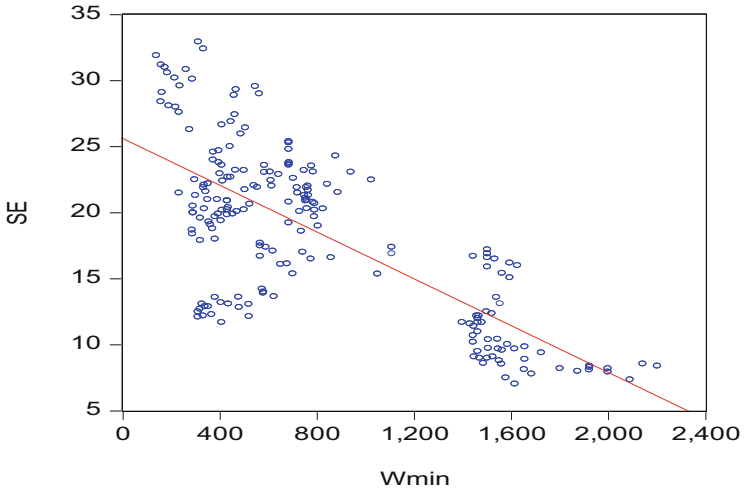


Fig. 5.6 Relationship between shadow economy and minimum wage in panel data for 2012–2021. Source: own composition realized in EViews 10

countries from Group A, except Slovenia, all the countries have a shadow economy below 20%.

Considering the panel data, we compute the correlation in EViews between the shadow economy and minimum wage (Fig. 5.6), and again it is confirmed as an indirect correlation. Another significant aspect is the fact that the countries with the lowest minimum wage registered the highest value of the shadow economy.

3.2 Model Specification and Empirical Results

Based on the theoretical background, we will use the econometric model developed by Goel et al. (2016) as a starting point for our analysis:

$SE = f_1$ *(government intervention, macroeconomic variables, political system).*

We adapt this model to the context of labor policies implemented in EU countries based on the two pillars: minimum wage and tax wedge.

$SE = f$ (labor market factors, institutional factors).

We will specify the equations in the baseline model as follows:

$$SE_{i,t} = \alpha + \beta_1 \ln MinWage_{i,t} + \beta_2 FD_{i,t} + \beta_3 Unempl_{i,t} + \beta_4 CPI_{i,t} + \beta_5 CONTROL_{i,t} + \varepsilon_{i,t} \quad (5.1)$$

$$SE_{i,t} = \alpha + \beta_1 TaxWage_{i,t} + \beta_2 PolStab_{i,t} + \beta_3 CPI_{,t} + \beta_4 Trade_{i,t} + \beta_5 CONTROL_{i,t} + \varepsilon_{i,t} \quad (5.2)$$

We estimate Eqs. (5.1) and (5.2) using panel EGLS (cross-sectional weights) method while assuming the existence of cross-sectional heteroscedasticity. Panel estimated generalized least squares is a commonly used method for estimating panel data models in order to correct heteroscedasticity across cross sections. The use of cross-sectional weights in panel EGLS can lead to more accurate parameter estimates and improved statistical inference.

Based on the results provided in Table 5.1, the minimum wage has a significant negative impact on the shadow economy in EU countries, particularly in countries with a minimum wage higher than 1000 euros. However, in less developed countries where the minimum wage is below the threshold of 1000 euros, the minimum wage has a significant positive impact on the spread of the shadow economy resulting in an increase in informal activities. Therefore, we can conclude that the minimum wage can be an effective tool in reducing the shadow economy only in developed countries, where the minimum is established to discourage both employers and employees from engaging in informal work.

Regarding institutional factors such as financial development and corruption, we can observe different results. Financial development has a significant negative influence on the development of the shadow economy, but only in Group A. Reducing corruption is another important condition in fighting against underground activities. It is necessary to have a strong quality of institutions and less corruption especially when labor inspections try to verify if the labor regulations regarding the minimum wage are applied.

Concerning the impact of tax burden quantified in this empirical model through the tax wage, the results are reported in Table 5.2. An increase in income tax and social security contributions has a significant positive contribution to the shadow economy, and this effect is stronger in countries where the level of minimum wage is

Table 5.1 Empirical results based on panel EGLS (cross-sectional weights)

	(1) 21EU countries	(2) Group A	(3) Group B
Dependent variable SE			
LnWage min	−2.17*** (0.44)	−7.17*** (1.04)	3.94*** (0.67)
FD	−4.69*** (1.35)	−7.01*** (2.13)	0.87 (5.18)
UNMPL	0.05* (0.03)	0.16** (0.06)	0.17*** (0.04)
CPI	−0.28*** (0.02)	−0.17*** (0.03)	−0.06* (0.03)
INFLA	0.05 (0.10)	−0.13 (0.17)	−0.003 (0.06)
C	51.88*** (2.03)	81.22*** (6.04)	−1.25*** (4.95)
R-squared	0.91	0.93	0.97
Observations	186	69	117

Notes: standard errors in parentheses. *, **, *** denote statistical significance at the 10%, 5% and 1% level, respectively
Method: panel EGLS (cross-sectional weights)
Source: own elaboration using the EViews software

Table 5.2 Empirical results based on panel EGLS (Cross-sectional weights)

	(1) 21EU countries	(2) Group A	(3) Group B
Dependent variable SE			
Tax wage	0.61*** (0.03)	0.35*** (0.03)	0.22*** (0.04)
POLSTAB	−0.65 (1.003)	−3.00** (1.29)	−7.69*** (1.21)
CPI	−0.12*** (0.01)	−0.01 (0.02)	0.21*** (0.03)
TRADE	0.018*** (0.004)	0.009** (0.004)	0.03*** (0.005)
UNEMPL	0.36*** (0.03)	0.49** (0.04)	0.12*** (0.05)
R-squared	0.79	0.81	0.34
Observations	197	80	117

Notes: standard errors in parentheses. *, **, *** denote statistical significance at the 10%, 5% and 1% level, respectively
Method: panel EGLS (cross-sectional weights)
Source: own elaboration using the EViews software

higher (Group A). Political stability can also play an important role in the shadow economy decrease, especially in the countries from Group B. Similar results to the literature are obtained for the case of control variables.

To conduct robustness checks, we re-estimate using the method of panel two-stage least squares (panel 2SLS). This method is commonly used for estimating

Table 5.3 Empirical results based on panel two-stage least squares

	(1) 21EU countries	(2) Group A	(3) Group B
Dependent variable SE			
LnWage min	−1.99*** (0.56)	−8.13*** (2.72)	3.13*** (0.76)
AGRI	0.76** (0.31)	1.77 (1.23)	0.08 (0.36)
CPI	−0.26*** (0.02)	−0.08 (0.08)	−0.08*** (0.03)
INTERNET	−0.03*** (0.02)	0.01 (0.04)	−0.03 (0.02)
C	48.57*** (4.00)	74.84*** (17.57)	8.79** (3.79)
R-squared	0.92	0.96	0.97
Observations	201	76	125

Notes: standard errors in parentheses. *, **, *** denote statistical significance at the 10%, 5% and 1% level, respectively
Source: own elaboration using the EViews software

panel data models that suffer from endogeneity. Endogeneity arises when there is a correlation between the explanatory variables and the error term in the model, leading to biased parameter estimates. Panel 2SLS is particularly useful for panel data models because it allows for the inclusion of both time-invariant and time-varying instruments, improving the precision of the estimates. Moreover, it can handle unobserved heterogeneity and dynamic panel data structures (Table 5.3).

Again, the first hypothesis is confirmed and minimum wage can lead to a decrease in the shadow economy in countries where its level is higher than 1000 euros. On the other hand, for the countries from Group B, the minimum wage cannot be considered an efficient instrument in combating and limiting the shadow economy for many reasons. First, in many of these countries, the level of the shadow economy is higher than 20% of the GDP, and informal activities are spread in all the economic sectors. Second, in these countries, the role of the shadow economy in reducing the poverty and income inequality is not accomplished, and for many employers due to economic conditions, it is hard to assure a minimum wage for their employees. Moreover, institutional factors such as financial development, political stability, or limiting corruption have also a stronger impact on limiting the shadow economy.

4 Discussion and Policy Implications

The empirical results reflect the complexity of minimum wage policy and the duality of the implications on the underground economy. Our results are consistent with those of Hazans (2011), who, based on European Social Survey data for 30 countries between 2004 and 2009, found that an increase in the minimum wage led to a higher

share of informal employment in Eastern and Southern Europe. In contrast, Western European and Nordic countries experienced a significant negative impact of minimum wage on informal employment. In our study, we considered the shadow economy, which includes not only informal employment but also other underground activities, such as unregistered sales of goods and services, unreported income, and bartering.

The impact of the tax wage on the shadow economy was confirmed as an important determinant of the spread of shadow activities, generating higher labor costs for employers. This finding is consistent with previous studies that considered the impact on informal employment (Loayza et al., 2005; Hazans, 2011; Lehmann & Muravyev, 2012).

Overall, due to the dual impact of the minimum wage on the shadow economy, policymakers should be cautious about raising the minimum wage in countries with weak labor market institutions and governance, as it may lead to unintended consequences such as increased underground activities. Instead, policies that strengthen labor market institutions and governance may be more effective in reducing informal activities along with an efficient system of penalties and a moderate tax burden.

5 Conclusions

Our results have relevant policy implications because underline the future direction of diminishing the shadow economy. The minimum wage is a powerful instrument that can be implemented to decrease the shadow economy, especially in developed UE countries, where the level of minimum wage can accomplish social and economic objectives, and the institutional capacity can assure the efficiency of labor market regulations through forceful inspections or sanctions. In less developed EU countries, the results prove that the minimum wage can increase the incentive to develop underground activities, as long as this minimum wage remains below a minimum level that assures a decent standard of living. Moreover, if we will consider the tax wedge applied to this minimum wage for some countries, net benefit received by employees will reach approximately half of the value of the minimum salary, which worsens the situation even more for the employees who live in the poverty line.

As a general conclusion, we can state that minimum wage policies can be effective in reducing the size of the shadow economy, but policymakers should carefully consider the specific context in which they are being implemented. In this regard, they should pay attention to the level of enforcement, the preferences of workers, and the potential unintended consequences of the policy minimum wage correlated with the level of economic development.

One main limitation of this study is the fact that our analysis cannot include the system of penalties for noncompliance in the labor field applied in each country. This system of sanctions for informal activities can be an important element along with

minimum wage in reducing the shadow economy. As a future direction of study, we can consider a composite index for capturing the efficiency of penalties applied.

Another future research direction will be to analyze the impact of minimum wage according to the welfare policies developed by the European countries considered in clusters of the welfare models.

Declaration of Competing Interest Declarations of Interest: None.

Appendices

Appendix 1: Description of Variables

Variable	Specification	Source	Expected sign
SE	Shadow economy (% GDP)	Medina and Schneider (2019), Schneider (2022)	
WMIN	The minimum wage in euros Minimum wage statistics published by Eurostat refer to monthly national minimum wages.	Eurostat, 2023, https://ec.europa.eu/eurostat/web/main/data/database	+/−
LNW	Natural logarithm minimum wage		
UNEMPL	Unemployment, total (% of total labor force) (modeled ILO estimate)	World Bank (2022), https://data.worldbank.org/indicator/SL.UEM.TOTL.ZS	+
CPI	Corruption perception index (CPI—Ranges from 0 (highly corrupt) to 100 (very clean))	Transparency International (2020), https://www.transparency.org/en/cpi/2020/index/nzl	−
INFL	Inflation, consumer prices (annual %)	World Bank (2022), https://data.worldbank.org/indicator/FP.CPI.TOTL.ZG	+
FD	Financial development index	Financial Development—IMF, 2022, https://data.imf.org/?sk=f8032e80-b36c-43b1-ac26-493c5b1cd33b	−
TAXW	Tax wedges for a single worker with 50% of average earnings, no children	Source: European Commission, DG economic and financial affairs, tax and benefits	−
POLSTAB	Political stability and absence of violence/terrorism: Estimate Estimate gives the country's score on the aggregate indicator, in units of a standard normal distribution, i.e., ranging from approximately −2.5 to 2.5	World Bank (2022), https://databank.worldbank.org/metadataglossary/1181/series/PV.EST	−

(continued)

Appendix 1: (continued)

Variable	Specification	Source	Expected sign
TRADE	Trade (% of GDP)	World Bank: World Bank national accounts data, and OECD National Accounts data files (2022), https://data.worldbank.org/indicator/NE.TRD.GNFS.ZS	_
AGRI	Agriculture, forestry, and fishing, value added (% of GDP)	World Bank (2022), https://data.worldbank.org/indicator/NV.AGR.TOTL.ZS	+
INTERNET	Individuals using the Internet (% of population)	World Bank (2022), https://data.worldbank.org/indicator/IT.NET.USER.ZS	_

Source: own elaboration based on cited sources

Appendix 2: Summary Statistics

	Observations	Mean	Median	Maximum	Minimum	Std. Dev.
SE	210	18.26	19.50	32.93	7.04	6.45
WMIN	207	817.15	623.00	2201.93	138.05	531.40
LNW	207	6.49	6.43	7.70	4.93	0.67
UNEMPL	208	8.67	6.99	27.47	2.01	5.13
CPI	208	60.96	59.00	85.00	36.00	12.54
INFLA	208	1.38	1.33	5.65	−1.74	1.42
FD	189	0.52	0.49	0.91	0.20	0.19
TAXW	199	32.35	33.62	42.62	15.79	6.14
POLSTAB	208	0.69	0.74	1.44	−0.23	0.35
TRADE	208	142.67	138.51	380.10	56.86	72.36
AGRI	208	2.31	2.19	5.38	0.20	1.20
INTERNET	204	79.11	80.24	98.83	45.88	10.55

Appendix 3: Matrix Correlation

	SE	WMIN	LNW	UNEMPL	CPI	INFLA	FD	TAXW	POLSTAB	TRADE	AGRI	INTERNET
SE	1											
WMIN	−0.73	1										
LNW	−0.71	0.96	1									
UNEMPL	0.25	−0.17	−0.10	1								
CPI	−0.74	0.83	0.80	−0.36	1							

(continued)

Appendix 3: (continued)

	SE	WMIN	LNW	UNEMPL	CPI	INFLA	FD	TAXW	POLSTAB	TRADE	AGRI	INTERNET
INFLA	−0.01	−0.07	−0.09	−0.32	0.02	1						
FD	−0.54	0.75	0.77	0.20	0.56	−0.17	1					
TAXW	0.28	−0.44	−0.47	0.01	−0.30	0.15	−0.50	1				
POLSTAB	−0.51	0.28	0.27	−0.51	0.43	0.13	0.08	−0.32	1			
TRADE	−0.35	0.38	0.31	−0.41	0.33	0.09	0.03	−0.42	0.70	1		
AGRI	0.73	−0.79	−0.81	0.36	−0.74	0.00	−0.61	0.43	−0.60	−0.58	1	
INTERNET	−0.72	0.69	0.72	−0.38	0.76	0.06	0.37	−0.28	0.44	0.44	−0.68	1

References

Achim, M. V., Borlea, S. N., Văidean, V. L., Florescu, D. R., Mara, E. R., & Cuceu, I. C. (2021). Economic and financial crimes and the development of society. Improving quality of life: exploring standard of living, wellbeing, and community development, (vol. 25).

Adam, C., & Buffie, E. F. (2020). The minimum wage puzzle in less developed countries: Reconciling theory and evidence. IMF working paper, 20/23. Retrieved from https://ssrn.com/abstract=3545289

Bruckmeier, K., & Bruttel, O. (2021). Minimum wage as a social policy instrument: Evidence from Germany. *Journal of Social Policy, 50*(2), 247–266. https://doi.org/10.1017/S0047279420000033

Carneiro, F. G. (2000). Time series evidence on the employment effect of minimum wages in Brazil. Retrieved from https://doi.org/10.2139/ssrn.231875

Davidescu, A. A., & Schneider, F. (2017). Nature of the relationship between minimum wage and the shadow economy size: An empirical analysis for the case of Romania (no. 11247), Institute for the Study of Labor (IZA). https://www.econstor.eu/bitstream/10419/177051/1/dp11247.pdf

Goel, R. K., Michael, A., & Nelson, M. A. (2016). Shining a light on the shadows: Identifying robust determinants of the shadow economy. *Economic Modelling, 58*, 351–364. https://doi.org/10.1016/j.econmod.2016.06.009

Groisman, F. (2015). Social protection to the informal sector: The role of minimum wage and income transfer policies. PEP working paper series 2015-05. Retrieved from https://doi.org/10.2139/ssrn.2665225

Hazans, M. (2011). What explains prevalence of informal employment in European countries: The role of labor institutions, governance, immigrants, and growth. World Bank Policy Research Working Paper, (5917). Retrieved from https://ssrn.com/abstract=1972832

Heemskerk, F., Voinea, L., & Cojocaru, A. (2018). Busting the myth: The impact of increasing the minimum wage: The experience of Romania. Policy research working paper no. WPS 8632, Washington, DC: World Bank Group; https://elibrary.worldbank.org/doi/abs/10.1596/1813-9450-8632

Hoinaru, R., Buda, D., Borlea, S. N., Văidean, V. L., & Achim, M. V. (2020). The impact of corruption and SE on the economic and sustainable development, do they "sand the wheels" or "grease the wheels"? *Sustainability, 12*(2), 481. https://www.mdpi.com/2071-1050/12/2/481

Jiménez Martínez, M., & Jiménez Martínez, M. (2021). Are the effects of minimum wage on the labour market the same across countries? A meta-analysis spanning a century. *Economic Systems, 45*(1), 100849. https://doi.org/10.1016/j.ecosys.2020.100849

Loayza, N., Oviedo, A. M., & Servén, L. (2005). The impact of regulation on growth and informality cross-country evidence. Retrieved from https://doi.org/10.2139/ssrn.755087

Lehmann, H., & Muravyev, A. (2012). Labour market institutions and labour market performance. *The Economics of Transition, 20*(2), 235–269. https://doi.org/10.1111/j.1468-0351.2012.00435.x

Mara, E. R. (2021). Drivers of the shadow economy in European Union welfare states: A panel data analysis. *Economic Analysis and Policy, 72*, 309–325. https://doi.org/10.1016/j.eap.2021.09.004

Medina, L., & Schneider, F. (2019). *Shedding light on the shadow economy: A global database and the interaction with the official one* (CESifo working paper, no. 7981). CESifo. https://doi.org/10.2139/ssrn.3502028Mellios

Nataraj, S., Perez-Arce, F., Kumar, K. B., & Srinivasan, S. V. (2014). The impact of labor market regulation on employment in low-income countries: A meta-analysis. *Journal of Economic Surveys, 28*, 551–572. https://doi.org/10.1111/joes.12040

Navickas, M., Juščius, V., & Navickas, V. (2019). Determinants of shadow economy in eastern European countries. *Scientific Annals of Economics and Business, 66*(1), 1–14. https://doi.org/10.2478/saeb-2019-0002

Rani, U., Belser, P., Oelz, M., & Ranjbar, S. (2013). Minimum wage coverage and compliance in developing countries. *International Labour Review, 152*(3–4), 381–410. https://onlinelibrary.wiley.com. https://doi.org/10.1111/j.1564-913X.2013.00197.x

Schneider, F. (2022). New COVID-related results for estimating the shadow economy in the global economy in 2021 and 2022. *International Economics and Economic Policy, 19*, 299–313. https://doi.org/10.1007/s10368-022-00537-6

Schulten, T. (2008). Towards a European minimum wage policy? Fair wages and social Europe. *European Journal of Industrial Relations, 14*(4), 421–439. http://digamo.free.fr/schult8.pdf

Schulten, T. (2012). European minimum wage policy: A concept for wage-led growth and fair wages in Europe. *International Journal of Labour Research, 4*(1), 85–104. http://nationalminimumwage.co.za/wp-content/uploads/2015/09/0204-European-minimum-wage-policy-A-concept-for-wage-led-growth-and-fair-wages-in-Europe.pdf

Schulten, T. (2014). *Contours of a European minimum wage policy?* Friedrich Ebert-Stiftung. https://www.epsu.org/sites/default/files/article/files/Contours_of_a_Minimum_Wage_Policy_Schulten.pdf

Tonin, M. (2005). *The effects of the minimum wage in the economy with tax evasion*. IIES, Stockholm University. https://www.mnb.hu/letoltes/minimu-wage.pdf

Eugenia Ramona Mara is Associate Professor of Public Finance at the Faculty of Economics and Business Administration, Babeş-Bolyai University, Cluj-Napoca, Romania. She holds a Ph.D. in Finance, and currently, she teaches Public Finance, Fiscal policy, and Taxation. Her research interests include public finance, fiscal policy, tax havens, shadow economy, tax evasion, and financial sector taxation. In addition to academia, she was involved as an expert consultant in several projects financed by the European Commission in the field of taxation.

Part III
The Effects of Economic and Financial Crimes on the Society

Chapter 6
The Impact of Corruption on Human Well-Being Within an Economic Framework: Evidence from a Cross-National Study

Cristina Boța-Avram

Abstract No doubt, corruption is a serious threat to human well-being and its development. The purpose of this chapter is to investigate the impact of perceived level of corruption in public sector on human well-being, by using cross-national data for a large sample of countries. Thus, the cross-national sample covers 132 countries (45 high-income, 39 upper-middle-income, and 48 lower-income countries) during the 2013–2020 period, and the analysis is developed for both the full sample and sub-samples. To measure well-being, we use two of the most well-known and well-documented composite indicators of well-being, such as the Legatum Prosperity Index (LPI) and the Human Development Index (HDI). The main results indicate clear evidence that the perceived level of corruption significantly influenced the level of well-being and human development, after controlling for some economic and governance dimensions such as the index of economic freedom, GDP growth, unemployment, press freedom, and country-level governance. The findings of this study could have relevant implications for policymakers and governments from all over the world who need to acknowledge the impact of anticorruption measures on people's well-being and its development.

Keywords Corruption · Well-being · Development · Economic freedom · Income · Governance

Jel Classification Is3 · I38 · M21

C. Boța-Avram (✉)
Faculty of Economics and Business Administration, Babeș-Bolyai University, Cluj-Napoca, Romania
e-mail: cristina.botaavr@econ.ubbcluj.ro

M. V. Achim (ed.), *Economic and Financial Crime, Sustainability and Good Governance*, Contributions to Finance and Accounting,
https://doi.org/10.1007/978-3-031-34082-6_6

1 Introduction

Corruption is a controversial topic, and its negative influences on various aspects of human beings and its development cannot be neglected. In its various forms, corruption was proven to be a *"very harmful and destroying factor to any economy for countless reasons"* (Akouwerabou, 2014, p. 199). Previous scholars also provided significant evidence on the destructive role of corruption in people's lives and population health (Achim & Borlea, 2018; Achim et al., 2020; Sommer, 2020). For instance, using cross-sectional data from 185 countries for the period 2005–2017, Achim et al. (2020) argued that a high level of corruption will significantly affect more the physical health of population in low-income countries, while, for high-income countries, the effect of corruption will be more strongly felt on the mental health of population. Using two-way fixed-effects models for a sample of 90 low- and middle-income nations from 1996 to 2012, Sommer (2020) investigated how the interaction between corruption in the executive and public sector and health expenditure affects infant and child mortality. Therefore, Sommer (2020) underlined the negative impact of corruption on infant and child mortality, highlighting the importance of controlling corruption in improving the effectiveness of health expenditure development.

Among the negative consequences of corruption and its perceived level, especially in the public sector, is the one particularly related to well-being, often corruption being considered a threat to well-being (Magalhaes et al., 2019). As Yan and Wen (2020) suggested, corruption is one of the most important indicators to assess the quality of the institutional environment, and so it is expected to have a significant effect on human well-being. As some authors (Ma et al., 2022; Tay et al., 2014) admitted that even if corruption and human well-being were of great interest to various scholars, the relationship between perception of official corruption and well-being is still unknown or still unclear. Additionally, we notice that some gaps emerge from the related literature, seeing that most studies focused on analysing the relationship between corruption and well-being for a specific country or a small sample of countries, whereas this study proposes to analyse the potential impact of corruption on human well-being by including in the analysis much larger samples of worldwide countries. Thus, the research question that the study presented in this chapter is trying to answer is as follows:

RQ: Does corruption significantly affect human well-being as measured at the national level? Is this impact felt differently for countries classified into income categories?

This chapter intends to contribute to the existing literature on the consequences of corruption on well-being by employing a comprehensive analysis of data for a large sample of 132 worldwide countries, for a large period of 8 years, from 2013 to 2020. To capture human well-being and human development, we employ two of the most well-known composite indicators of well-being, namely the Legatum Prosperity Index (PROSP) and the Human Development Index (HDI), which were previously

confirmed by other authors as some of the most reliable measures of human well-being (see, for instance, Otoiu et al., 2014). The study presented in this chapter argues that the impact of corruption is significant for human progress and well-being, even if this impact could be felt differently by countries classified into various income categories.

Thus, empirically we examine the impact of corruption in the public sector (as measured by the corruption perception index developed by Transparency International) on well-being (measured by two proxies such as the Legatum Prosperity Index (PROSP) and the Human Development Index (HDI)). For both empirical analyses, we consider some economic and governance control variables such as the index of economic freedom, GDP growth, unemployment, press freedom, and country-level governance (as captured by governance indicators developed by the World Bank). Furthermore, all the empirical analyses were conducted for both full sample and sub-samples of countries classified into high-income, upper-middle-income, and lower-income economies according to the World Bank classification. The empirical findings of this study support the conclusion that there are also some indicators that are significant control variables in the regression analysis of the corruption–well-being nexus such as index of economic freedom, GDP growth, unemployment, press freedom, and country-level governance, even if the impact of these control variables on well-being is felt differently by countries classified into high-income and upper-income categories compared to countries in the lower-income category.

The remainder of the chapter is structured as follows. Section 2 presents a brief synthesis of the background literature that supports the development of the working hypotheses. Section 3 describes the main data, data sources, and sample included in the empirical analysis, Sect. 4 presents the method and models used, while Sect. 5 presents the results and discussions. Finally, Section 6 concludes.

2 Literature Review

As Yan and Wen (2020) recently admitted, along with the increasing complexity of the society, researchers interested in determining the influencing factors for subjective well-being have gradually moved their focus from the field of psychology and sociology to the field of economics. If at the very beginning of the economic perspective on subjective well-being, the researchers were more interested in examining the influence of variables such as education level, health status, religion, or marital status, recently, more and more economists started to include in their investigations the impact of various economic indicators on well-being such as inflation, unemployment, income inequality, or governance effectiveness (Yan & Wen, 2020).

There is a large body of literature that uses country-specific economic micro-data sets of variables when analysing the impact of various factors on well-being. For instance, in the case of the United States, Luttmer (2005) found that an increase in

the neighbours' earnings and a similarly sized decrease in own income each have roughly the same negative effect on well-being. Analysing subjective well-being and its determinants in rural China, Knight et al. (2009) found that conventional economic variables increase happiness, in line with basic economic theory, but the contributions of the absolute levels of income and financial wealth are relatively weak. On the other hand, using data from the European Quality of Life survey with data from more than 70,000 respondents, Evans et al. (2019) suggested that income inequality has no statistically significant impact before, during, or after the Great Recession, while money does increase well-being, but inequality itself, the gap between rich and poor, is irrelevant.

Another strand of previous literature was focused on analysing the impact of various macroeconomic variables on human well-being. In this vein, Wasmmer et al. (2009) suggested that the increase in the proportion of national expenditure devoted to public safety, education, and health could have a positive impact on the increase of personal happiness, while the ideology mediates the impact of fiscal variables on well-being. Investigating, the subjective well-being and relative poverty in rural Bangladesh, Asadullah, and Chaudhury (2012) found that institutional quality measured in terms of confidence in police exerts a positive and significant coefficient in the well-being function.

When scrutinizing previous literature on the major determinant of human well-being, especially at macro-level, one can note that institutional environment is frequently considered as one of the main macroeconomic factors with a significant role in affecting well-being (Yan & Wen, 2020). Corruption weakens the quality of institutions and increases economic inequality and limitations of growth, while corruption is frequently associated with lower life satisfaction (Ciziceno & Travaglino, 2019). Based on cross-national data from 68 countries and survey data from 16 European democracies, Tavits (2008) provided strong evidence that the quality and performance of their governments (e.g. are cleaner rather than corrupt) could have a significant impact on human well-being. Using data from the World Value Survey on life satisfaction, Helliwell and Huang (2008) found that people living in countries where government is less corrupt registered an increased life satisfaction. The same conclusions have been reached by other authors also (Welsch, 2008; Kim & Kim, 2012). The detrimental effect of corruption on well-being was also confirmed by Heukamp & Ariño (2011) who found that the lower the corruption, the higher the chance of well-being in a country. Analysing the individual and macro-level determinants of individual life satisfaction in 10 CEE countries, Rodriguez-Pose and Maslauskaite (2012) found that the individual levels of life satisfaction are mostly impacted by institutional factors such as corruption, government spending, and decentralization.

The attention paid by various scholars to the relationship between corruption and human well-being has increased particularly in the recent years. Analysing the drivers of well-being in Latin America, Rojas (2020) and his contributors to his book found that while Latin American institutions are highly characterized by weak institutions and many corrupt practices, Latin American perceptions of corruption in most state institutions reach very high levels, and therefore, these perceptions tend to

be negatively associated with human well-being in these countries. Because often Latin Americans are used to pay bribes to public representatives of various state institutions, this seems to negatively affect human well-being and their satisfaction with life, but, on the other hand, these people are convinced that paying bribes will provide a more facile access to various public services with a corresponding well-being increase (Rojas, 2020). By using data from Chinese General Social Survey, Yan and Wen (2020) found that corruption has a significant negative impact on the subjective well-being of urban and rural residents. Li and An (2020), using cross-national data for 126 countries found that the national average of subjective well-being would decrease by 0.23 points if a government became more corrupt by 10 points, and unemployment rate had to decrease equivalently by 9.2% to keep the national average subjective well-being unimpacted.

Recently, Ma et al. (2022), while employing data from China General Social Survey, examined the relationship between perceived official corruption and the subjective well-being in the context of China and found that the perception of official corruption is negatively related to subjective well-being, whereas the satisfaction with government performance plays a mediating role in this relationship. Using micro-level data from 1566 households from Punjab, Pakistan, Danish, and Nawaz (2022) argued that the tendency of the people is to feel happier and with an increasing level of life satisfaction, when government and public institutions are perceived as being less corrupted. Even more, Danish and Nawaz (2022) claimed that governments and policymakers should make all possible efforts to enhance the trust of the public in the quality of public institutions.

No doubt, the relationship between corruption and well-being was of great interest to scholars, academics, and policymakers and certainly will continue to be in the next years (Li & An, 2020). Generally, the main premise in studies related to corruption and well-being is that corruption will negatively affect well-being, but even so sometimes, there is some evidence (Tay et al., 2014) that could suggest the opposite conclusion that corruption can improve the economy and thus human well-being. For instance, Tay et al. (2014) using cross-national data from 150 countries argued that the perceptions of national corruption are high across many nations, and if the mediation analyses and longitudinal modelling support the conclusion that corruption negatively affects national income and institutional trust, which in turn affects the human well-being, still there are some moderating factors that could determine that perception of corruption will enhance the effect of income on well-being. Also, the same authors found that the detrimental effect of corruption on well-being is more strongly felt in Western countries compared to non-Western economies. In the same vein, Li and An (2020) suggested that corruption has a significant impact on national well-being only in democratic or high-income countries.

Consistent with the background literature presented above and in light of the purpose of this chapter, this study proposes the following hypotheses to be tested through the empirical analysis as follows:

H1. A higher level of CPI score (which means less corruption) has a significant and positive impact on well-being (when well-being is proxied by the Legatum Prosperity Index), for both full sample and sub-samples of countries considered.
H2. A higher level of CPI score (which means less corruption) has a significant and positive impact on well-being (when well-being is proxied by the Human Development Index), for both full sample and sub-samples of countries considered.

3 Data Description

To investigate the impact of perceived corruption in the public sector on well-being and human development, this study uses international country-level data for 132 countries (45 high-income countries, 39 upper-middle-income countries, and 48 lower-income countries) during the 2013–2020 period. The analysis is developed for both the complete sample and sub-samples of high-income, upper-income, and lower-income countries classified according to the World Bank's income classification (World Bank, 2022a). The rationales and sources of data for the variables used in this study are disclosed below.

3.1 Dependent Variable: Well-Being

Defining human well-being is a controversial issue, and there is no general accepted definition on this topic. In terms of indicators that could best capture the substance of human well-being and its progress, there are many indicators that were largely used in the previous literature related to well-being. According to Otoiu et al. (2014), the most comprehensive, widely known, and applied well-being and human development indicators are the Human Development Index, the Happy Planet Index, and the Legatum Prosperity Index. These indicators were mostly used in previous studies due to their advantages in measuring a comprehensive range of indicators that assess certain dimensions of well-being, for larger samples from countries. Of course, there were also criticisms of these indicators due to their high correlation between components, computational form, and component weighting (Kovacevic, 2011). In this vein, a significant contribution was provided by the study by Otoiu et al. (2014) that examined the relevance of indicators that define well-being and human development. Thus, based on a cluster analysis and with an optimal classification of countries according to their multidimensional performance on well-being, the findings obtained by Otoiu et al. (2014) validated two reliable measures of well-being, namely the Human Development Index and the Legatum Prosperity Index. Therefore, for the purpose of the study presented in this chapter, we run two separate econometric analyses, considering two different proxies for the dependent variable—well-being, namely:

- First, when well-being is proxied by the Legatum Prosperity Index (PROSP), an indicator that aims to evaluate countries in promoting the flourishing of their residents, reflecting both economic and social well-being. For that purpose, the developers of this index created the optimal structure of the prosperity index, comprised of 12 pillars of prosperity divided into 67 policy-focused variables, while using 300 different indicators from more than 70 different data sources and grouped into three domains relevant to prosperity: inclusive societies, open economies, and empowered people (The Legatum Institute, 2021). A higher score for this index means higher prosperity for a certain country.
- Second, when well-being is proxied by the Human Development Index (HDI), a composite index that captures average achievement in three basic facets of human development: a long and healthy life, knowledge, and a decent standard of living (UNDP, 2021a, 2021b). This index ranges from 0 (lowest human development relative to the rest of the countries) to 1 (highest possible relative human development relative to the rest of the world).

3.2 Independent Variable: Corruption

Corruption measurement is another controversial issue (Brunetti & Weder, 2003), but even so the Transparency Corruption Perception Index (CPI) is assessed as one of the best indicators of perceived level of corruption in public sector (Achim et al., 2020; Dutta, 2018; Ben Ali & Gasmi, 2017; Mornah & Macdermott, 2018; Achim, 2016). The composite index of corruption (CPI) has become one of the most used indicators in the previous empirical studies related to corruption due to its methodology that combines data from various sources that quantify the perceptions of businesspeople and different specialists about the perceived level of corruption in the public sector (Mornah & Macdermott, 2018).

According to Transparency International (2021), the CPI index ranks 180 countries and territories by their perceived levels of public sector corruption according to experts and businesspeople, whereas relying on 13 independent data sources and employing a scale of 0 to 100, where a score of 0 assigned to a country means highly corrupt, and a score of 100 means a very clean country. For the purposes of the analysis, this study uses the CPI scores and not their ranks because of some advantages as emphasized by Dutta (2018), who highlighted the benefit of using the CPI score instead of the CPI rank is *"to avoid the problem of cardinalisation of ordinal variables which might lead to ambiguous results"* (Dutta, 2018, p. 4).

3.3 Control Variables

Because various economic and governance indicators could exert some interferences that might outshine the results of the empirical analysis in what regards corruption–

well-being nexus, we have also included some control variables related to economic, governance, and press freedom dimensions as follows:

- *The index of economic freedom (IEF)* is an index computed by the well-known Heritage Foundation, and it assesses 12 specific instruments of economic freedom, each of which being graded on a scale from 0 to 100. Based on these calculations, the general score associated with the index of economic freedom captures four large areas over which governments usually exercise control, namely the rule of law, government size, regulatory efficiency, and market openness (Heritage Foundation, 2022). The final score assigned to this index ranges from 0 (means lowest level of economic freedom) to 100 (means highest level of economic freedom). We include this control variable because of its frequent usage in the previous literature to investigate the consequences of corruption on economic environment (Graeff & Mehlkop, 2003; Ekici & Ekici, 2021).
- *GDP growth (GDP_growth)* rates compare the year-on-year growth rate of a country's economic production to measure the speed at which the economy grows (World Bank, 2022b). Considering previous studies (Sacks et al., 2010; Stevenson & Wolfers, 2013; Altindag & Xu, 2017; Rodriguez-Pose & Maslauskaite, 2012) that argued that an increase in per capita income will positively impact the life satisfaction of people, we include GDP growth as a control variable. For instance, investigating the individual and macro-level determinants of individual life satisfaction in 10 CEE countries, Rodriguez-Pose and Maslauskaite (2012) found that GDP growth is still a source of increasing well-being, but the happiness bonus associated with it is becoming smaller.
- *Unemployment (UNEMP)* is defined as the proportion of the labour force that is unemployed (World Bank, 2022b). Another relevant control variable in the relationship between corruption and well-being highlighted by previous scholars is unemployment. For instance, Li and An (2020), analysing a large sample of observations for 126 countries, highlighted the significance of keeping a certain level for unemployment rate so as to maintain the national average life satisfaction unaffected, when governments tend to become more corrupt. Also, frequently, this indicator was frequently considered as a control variable when corruptive practices were analysed (Romero-Martínez & García-Muiña, 2021).
- *Press freedom (PRESS_F)* is an index of press freedom calculated by the organization Reporters without frontiers (RSF, 2022) and assesses the degree of freedom of press and journalists in 180 countries, using a combination of qualitative and quantitative data on abuses and acts of violence committed against journalists and journalists' representatives. The scores assigned to each country range from 0 to 100, where 0 is the best possible score (the greatest freedom of the press in that country) and 100 is the worst (the lowest freedom of the press in that country). We also include this control variable in the regression analysis of the corruption–well-being nexus due to the opinion of previous scholars (Newton et al., 2004; Rao, 2008) that press freedom is one of the most important tools for fighting corruption, especially in the public sector. Also, there were some

researchers (Kalenborn & Lessmann 2013; Hamada et al., 2019) who argued that greater press freedom is frequently correlated with lower levels of corruption.

- *Country-level governance (GOV_PCA)* represents an index of country-level governance computed based on the six worldwide governance indicators (voice and accountability; political stability and absence of violence/terrorism; government effectiveness; regulatory quality; rule of law; control of corruption) published by the World Bank (Kaufmann et al., 1999, 2010). We consider this control variable in the regression analysis of the corruption–well-being nexus because of previous studies that argued the significance of institutional quality for the satisfaction of people's life and their human well-being (Asadullah & Chaudhury, 2012; Altindag & Xu, 2017; Ciziceno & Travaglino, 2019; Yan & Wen, 2020; Danish & Nawaz, 2022). Because of their high interdependence and multicollinearity, we use principal component analysis to generate a composite country-level governance indicator, based on the six World Bank governance indicators (World Bank, 2022c). This approach is in line with many previous studies that have adopted the same approach (Chipalkatti et al., 2021; Asongu et al., 2019; Rachisan et al., 2017).

In the following, Table 6.1 presents the descriptive statistics of the variables used in this study. Table 6.2 discloses the correlation coefficients between these variables, indicating a high and direct correlation between corruption and well-being (when proxied by the Human Development Index—HDI) greater than 0.7 ($r = 0.735$). The same higher and direct correlation was also identified between the corruption perception index and well-being (when proxied by the Legatum Prosperity Index—PROSP) higher than 0.9 ($r = 0.917$).

4 Method and Models

The study presented in this chapter aims to examine the impact of corruption on well-being, while controlling for some economic and governance dimensions specific to each country included in the sample. For that purpose, we employ panel data analysis which combines both the cross-sectional data (identified for each country i) and the time dimension (year t), and the baseline forms of the tested models are as follows:

$$\begin{aligned}\text{Prosperity}_{it} = {} & \alpha_0 + \alpha_1 \text{Corruption}_{it} + \alpha_2 \text{ Index of economic freedom}_{it} \\ & + \alpha_3 \text{ GDP\_growth}_{it} + \alpha_4 \text{ Unemployment}_{it} + \alpha_5 \text{ Press Freedom}_{it} \\ & + \alpha_6 \text{ Country} - \text{level governance}_{it} + \varepsilon_{it} \end{aligned} \quad (6.1)$$

Table 6.1 Summary statistics for the dependent and independent variables

	Full sample (132 countries)					High income (45 countries)					Upper income (39 countries)					Lower income (48 countries)				
Variable	Obs	Mean	Std. Dev.	Min	Max	Obs	Mean	Std. Dev.	Min	Max	Obs	Mean	Std. Dev.	Min	Max	Obs	Mean	Std. Dev.	Min	Max
HDI	1056	0.74	0.16	0	0.957	360	0.89	0.04	0.77	0.96	311	0.76	0.05	0.54	0.85	385	0.59	0.13	0	0.79
PROSP	1056	59.60	12.78	32.35	84.26	360	73.82	7.09	47.43	84.26	311	57.37	5.85	38.38	68.91	385	48.11	6.97	32.35	60.99
CPI	1056	45.11	19.87	8	92	360	66.99	15.03	19	92	311	37.10	9.64	14	59	385	31.13	10.11	8	59
IEF	1056	59.96	16.91	0	90.2	360	71.53	7.86	36.3	90.2	311	57.87	16.07	0	77.1	385	50.82	17.52	0	76
GDP growth	1056	2.09	4.66	−27.99	32.49	360	1.60	3.39	−10.82	25.18	311	1.43	5.29	−25.91	32.49	385	3.08	4.98	−27.99	20.72
UNEMP	1056	5.86	5.63	0	31.31	360	6.46	4.39	0	27.47	311	8.24	6.77	0	29	385	3.39	4.57	0	31.31
PRESS F	1056	66.92	16.68	0	93.62	360	78.44	11.27	33.98	93.62	311	63.45	14.62	0	90.12	385	58.94	16.57	0	85.68
GOV PCA	1056	0	1	−2.32	1.77	360	0.81	0.92	−2.32	1.77	311	−0.24	0.76	−1.71	1.16	385	−0.57	0.71	−2.24	0.99

Table 6.2 Pairwise correlations coefficients

Variables	(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)
(1) HDI	1.000							
(2) PROSP	0.885***	1.000						
(3) CPI	0.735***	0.917***	1.000					
(4) IEF	0.618***	0.732***	0.711***	1.000				
(5) GDP_growth	−0.163***	−0.060*	−0.014	0.044	1.000			
(6) UNEMP	0.302***	0.246***	0.174***	0.232***	−0.053*	1.000		
(7) PRESS_F	0.446***	0.596***	0.596***	0.523***	−0.044	0.224***	1.000	
(8) GOV_PCA	0.579***	0.762***	0.750***	0.592***	−0.049	0.274***	0.780***	1.000

*Statistically significant at *** $p < 0.01$, ** $p < 0.05$, * $p < 0.1$*

$$\text{Human Development}_{it} = \gamma_0 + \gamma_1 \text{ Corruption}_{it} + \gamma_2 \text{ Index of economic freedom}_{it} + \gamma_3 \text{GDP\_growth}_{it} + \gamma_4 \text{ Unemployment}_{it} + \gamma_5 \text{ Press Freedom}_{it} + \gamma_6 \text{ Country} - \text{level governance}_{it} + \varepsilon_{it} \quad (6.2)$$

where (α_i) and (γ_i) indicate the parameters, (i) the country, and (t) is the time.

The purpose of this study is to estimate the effect of corruption on the outcomes of well-being for country i in the year t, while considering alternatively well-being being proxied by the Legatum Prosperity Index, but also proxied by the Human Development Index.

As mentioned above, the sample employed in this study consists of 132 countries (45 high-income countries, 39 upper-middle-income countries, and 48 lower-income countries) and the period of analysis is 2013–2020. The analysis is developed for both the full sample and sub-samples of high-income, upper-income, and lower-income countries. Based on the World Bank's income classification (World Bank, 2022a, 2022b, 2022c), countries are classified into high-income, upper-middle-income, lower-middle-income, and low-income economies. For the purposes of this study and considering the hypotheses mentioned above, the analysis is conducted for the full sample and sub-samples of high-income, upper-middle-income, and lower-income countries (which includes both categories of World Bank lower-middle-income and low-income economies).

The properties of the selected independent variables are verified through some diagnostic tests, such as the Jarque–Bera test for the normality test, which indicates that the selected data are normally distributed. Next, the issue of multicollinearity is checked through the variance inflation factor (VIF) because otherwise the precision of estimated coefficients could be affected, leading to misleading findings. The low correlation among independent variables is indicated by smaller VIF values, whereas a higher collinear relationship is highlighted by higher VIF values. According to Daniels and Minot (2020), a VIF value smaller than 10 is acceptable, and a VIF value greater than 10 demands specific attention. According to the results disclosed in Table 6.3, the independent variables are not highly correlated, and multicollinearity is not an issue for the sample considered.

In the first stage of the panel data analysis, the unbalanced panel structured data for 132 cross sections over a period of 8 years (2013–2020) is examined using the pooled OLS method. But due to the disadvantage of the pooled OLS regression of

Table 6.3 Variance inflation factor

	VIF	1/VIF
GOV PCA	3.875	0.258
CPI	3.098	0.323
PRESS F	2.599	0.385
IEF	2.145	0.466
UNEMP	1.106	0.904
GDP growth	1.014	0.986
Mean VIF	2.306	

ignoring the heterogeneity of the data, subsequently, the panel data analysis is extended to the use of the fixed-effects model (FE) and a random-effects model (RE). The identification of the best estimation models between random-effects model (RE) and fixed-effects model (FE) is carried out through the application of Hausman tests.

5 Results and Discussions

The main econometric findings for panel data analysis on well-being (proxied by the Legatum Index Prosperity Index) and corruption, while controlling for certain economic and governance dimensions are disclosed in Tables 6.4 and 6.5. According to the results of the least square method for panel data (pooled OLS) and presented in Table 6.4, one can note that the relationship between perceived level of corruption in the public sector and human prosperity is statistically significant for both the full samples and the sub-samples of high-income, upper-income, and lower-income economies.

While controlling for some economic and governance dimensions, the main findings disclosed in Table 6.4 revealed that the coefficients of the corruption perception index (CPI) are positive and significant, promoting the idea that countries with higher scores for the corruption perception index (which means they are cleaner and therefore lower corruption) obtain higher scores for the Legatum prosperity

Table 6.4 Multiple regression analysis of well-being (proxied by Legatum Index Prosperity Index) and corruption

	Model 1—Pooled OLS (dependent variable PROSP)			
Variables	Full sample	High-income countries	Upper-income countries	Lower-income countries
CPI	0.456***	0.268***	0.258***	0.219***
IEF	0.109***	0.167***	0.167***	0.117***
GDP_growth	−0.132***	−0.038	−0.048	0.018
UNEMP	0.117***	0.044	−0.119***	0.276***
PRESS_F	−0.03**	0.12***	−0.09***	−0.079***
GOV_PCA	2.024***	1.359***	2.674***	2.706***
Constant	34.081***	33.203***	45.543***	40.505***
Adjusted R^2	0.8675	0.8599	0.7870	0.5913
Prob > F	0.0000	0.000	0.000	0.000
F-test	1151.97	368.286	191.918	93.577
N cross-sectional units	132	45	39	48
Observations	1056	360	311	385

Notes: The dependent variable is well-being expressed by Legatum Index Prosperity Index
*Statistically significant at *** $p < 0.01$, ** $p < 0.05$, * $p < 0.1$*

Table 6.5 Panel data analysis of well-being (proxied by Legatum Index Prosperity Index) and corruption

	Model 2 (Dependent variable PROSP)			
Variables	Full sample FE	High-income countries FE	Upper-income countries FE	Lower-income countries FE
CPI	0.109***	0.054***	0.073***	0.175***
IEF	0.024***	0.134**	0.182***	−0.01
GDP_growth	−0.062***	−0.041***	−0.051**	−0.079***
UNEMP	−0.055***	−0.16***	−0.064***	0.025*
PRESS_F	−0.022**	−0.072***	0.005	−0.025*
GOV_PCA	1.171***	0.415	1.789***	1.072**
Constant	55.186***	66.988***	44.822***	45.436***
Overall R^2	0.8416	0.3523	0.7326	0.4807
Within R^2	0.2590	0.5228	0.4631	0.2935
Between R^2	0.8537	0.4919	0.7024	0.4823
Prob > F	0.000	0.000	0.000	0.000
F-test	53.491	55.515	36.804	22.428
Rho	0.9934	0.9943	0.9520	0.9791
N cross-sectional units	132	45	39	48
Observations	1056	360	311	385

Notes: The dependent variable is well-being expressed by Legatum Index Prosperity Index
*Statistically significant at *** $p < 0.01$, ** $p < 0.05$, * $p < 0.1$*

index, which means higher overall prosperity in various fields such as health, education, investor protection, government integrity, and environmental protection actions. One can note that lower influences of perceived corruption in the public sector on prosperity are identified for lower-income countries, where the variation in prosperity due to the corruption, economic, and governance indicators is only 59.13% (Table 6.4, Model 1, lower-income countries) compared to the higher variations for the full sample (86.75%) or the high-income countries (85.99%).

After applying the Hausman tests and selecting the most appropriate models between fixed-effects and random-effects models, the findings presented in Table 6.5 also confirm the significance of their relationship for both full sample and the sub-samples of high-income, upper-income, and lower-income economies. Therefore, based on the results of the Hausman tests, the optimal models selected for the full sample and sub-samples are listed in Table 6.5. One can note that the significance of having less corruption (and so being in the top position in corruption perception index with higher CPI scores) has a significant and positive effect on overall prosperity (Table 6.5, Model 2) for all samples (full sample and the sub-samples of high-income, upper-income, and lower-income economies). Thus, for a country, a higher position in corruption perception index (a higher CPI score, which means a reduced level of perceived corruption) should lead to an increase in

the perceived level of well-being, when proxied by the Legatum prosperity index, indicating an increase of overall human prosperity. *Rho* is a percentage of variation caused by a specific term of the individual element (country) included in the sample. According to the findings presented in Table 6.5, there is a large percentage of variation explained by the individual specific term (99.34%—full sample, 99.43%—high-income countries, 95.20%—upper-income countries, 97.91%—lower-income countries), and the rest is due to idiosyncratic error. Therefore, *the first hypothesis* that the impact of corruption on well-being (when proxied by the Legatum Prosperity Index) is significant for all samples is accepted.

In what regards the control variables used in this analysis, one may note that GDP_ growth and unemployment are significant variables for both full sample and sub-samples. In terms of the Index of Economic Freedom (IEF), it has a substantial and positive impact on the full sample as well as sub-samples of high-income and upper-income economies. A higher score for IEF means healthier and cleaner societies. Thus, it can be seen that for upper-income countries, IEF registers the highest statistically coefficient (0.182, p-value<0.01) indicating that an increase of one unit, on a scale from 0 to 100, would conduct an increase of 0.182 in the level of well-being (when proxied by Legatum Prosperity Index) compared to the full sample (0.024, p-value<0.01). It is interesting to note the significant and negative relationship between index of press freedom and well-being (proxied by Legatum Prosperity Index) for full sample, high-income, and lower-income countries (Table 6.5, Model 2). Starting from the premise that index of press freedom ranges from 0 to 100, where 0 is the best possible score (the greatest freedom of the press in that country) and 100 is the worst (the lowest freedom of the press in that country), these findings are quite expected. In other words, according to the results presented in Table 6.5 (Model 2), for both full sample and sub-samples of high-income and lower-income countries, higher scores on the press freedom (meaning lower press freedom in that economy) would conduct to lower scores on well-being scores when proxied by Legatum Prosperity Index (meaning lower prosperity for that country). In what regards country-level governance, according to the findings presented in Table 6.5 (Model 2), there is a significant and positive relationship between country-level governance and well-being (when proxied by Legatum Prosperity Index), especially in the case of full sample and sub-samples of upper-income and lower-income economies. In other words, a better country-level governance would lead to a higher prosperity for the citizens of that country, especially for upper-income and lower-income countries.

Next, when well-being is proxied by the Human Development Index (HDI), the results disclosed in Tables 6.6 and 6.7 indicate the same positive significance of the level of perceived corruption in the public sector for human well-being, even if the impact is felt differently on selected sub-samples. According to the results of the least square method for panel data (pooled OLS) and presented in Table 6.6, one can note that the relationship between perceived level of corruption in the public sector and Human Development Index is statistically significant for both the full-sample and the sub-samples of high-income and upper-income countries, except for lower-income economies where the significance of this relationship is no longer confirmed.

Table 6.6 Multiple regression analysis of well-being (proxied by Human Development Index) and corruption

Variables	Model 3—Pooled OLS (dependent variable HDI)			
	Full sample	High-income countries	Upper-income countries	Lower-income countries
CPI	0.005***	0.002***	0.001***	0.001
IEF	0.002***	0.001**	0.001***	0.003***
GDP_growth	−0.005***	−0.003	−0.002***	−0.005***
UNEMP	0.004***	0.001**	0.0003	0.007***
PRESS_F	−0.001**	0.0001	−0.001***	−0.001***
GOV_PCA	0.004	0.003	0.004	0.029**
Constant	0.454***	0.704***	0.730***	0.520***
Adjusted R^2	0.6068	0.5995	0.1935	0.3151
Prob > F	0.000	0.000	0.000	0.000
F-test	272.302	90.557	13.395	30.441
N cross-sectional units	132	45	39	48
Observations	1056	360	311	385

Notes: The dependent variable is well-being expressed by Human Development Index
*Statistically significant at *** $p < 0.01$, ** $p < 0.05$, * $p < 0.1$*

The main findings presented in Table 6.6 emphasize the idea that countries that are cleaner and with less corruption (and therefore with higher scores for the CPI) will receive higher scores for the Human Development Index, which represents a *"summary measure of average achievement in key dimensions of human development: a long and healthy life, being knowledgeable and having a decent standard of living"*.[1] It can be noted that the significance of the perceived level of corruption on well-being (proxied by HDI) is no longer confirmed in the case of lower-income countries, while lower influences of perceived corruption in the public sector on human development can be identified for upper-income countries, where the variation in human development due to corruption and economic and governance indicators is only 19.35% (Table 6.6, Model 3, upper-income countries) compared to the higher variations for the full sample (60.68%) or the high-income countries (59.95%).

Next, Table 6.7 discloses the optimal models after applying the Hausman tests and selecting the most appropriate models between fixed-effects and random-effects models. Corruption is statistically significant for well-being (when proxied by Human Development Index) for the full sample and the sub-sample of lower-income countries (Table 6.6, Model 4). Thus, an increase in CPI score (which means less corruption) would lead to an increase in Human Development index, which means a longer and healthier life, with a more decent standard of living. According to the

[1] https://hdr.undp.org/data-center/human-development-index#/indicies/HDI.

Table 6.7 Panel data analysis of well-being (proxied by Human Development Index) and corruption

	Model 4 (dependent variable HDI)			
Variables	Full sample FE	High-income countries FE	Upper-income countries FE	Lower-income countries FE
CPI	0.0004***	0.0001	0.0003	0.002***
IEF	0.0005***	0.002***	0.002***	0.0001
GDP_growth	−0.001***	−0.001***	−0.001***	−0.001***
UNEMP	−0.001***	−0.002***	−0.001***	0.0002
PRESS_F	0.0004	−0.001***	0.0001	−0.001***
GOV_PCA	0.003	−0.009	0.006	0.009
Constant	0.724***	0.862***	0.666***	0.604***
Overall R^2	0.4441	0.0034	0.1212	0.1319
Within R^2	0.2667	0.5286	0.3864	0.3196
Between R^2	0.5036	0.0030	0.0905	0.1524
Prob > F	0.000	0.000	0.000	0.000
F-test	55.646	56.822	26.872	25.360
Rho	0.9952	0.9860	0.9700	0.9919
N cross-sectional units	132	45	39	48
Observations	1056	360	311	385

Notes: The dependent variable is well-being expressed by Human Development Index
*Statistically significant at *** $p < 0.01$, ** $p < 0.05$, * $p < 0.1$*

results presented in Table 6.6, there is a large proportion of variation (99.52%—full sample, 99.19%—lower-income countries) explained by the individual specific term. Finally, *the second hypothesis* that the impact of corruption on well-being (when proxied by the Human Development Index) is significant for all samples is partially accepted (only for full sample and lower-income economies).

In what regards the control variables used in the second analysis (Table 6.7, Model 4), one may note that GDP_ growth and unemployment are significant variables for both full sample and sub-samples (high-income, upper-income, and in the case of GDP_growth for lower-income economies too). In terms of the index of economic freedom (IEF), same as in the previous analysis, also, in the second analysis (when well-being is proxied by the Human Development Index), a higher score for IEF is significant, especially for the full sample and sub-samples of high-income and upper-income economies, but the coefficients are much lower (see, for instance, in case of high-income and upper-income countries, the coefficients are only 0.002, p-value<0.01). It is interesting to note that in the case of this second analysis, the significant and negative relationship between index of press freedom and well-being (proxied by Human Development Index) is confirmed only for sub-samples of high-income and lower-income countries (Table 6.7, Model 4), while for full sample and upper-income countries press freedom seems to be

insignificant for the human well-being (when proxied by Human Development Index). In other words, according to the results presented in Table 6.7 (Model 4), higher scores for the index of press freedom index (meaning lower press freedom for that country) would lead to lower well-being scores when proxied by the Human Development Index, especially in the case of high-income and lower-income economies. It is interesting to note that in terms of country-level governance, its significance for well-being when proxied by the Human Development Index is no longer confirmed for any of the full sample or sub-samples.

6 Conclusions

This study aims to investigate the role of corruption in determining human well-being and its development, while controlling for some economic and governance dimensions. In other words, this study tries to answer the research question: *Does corruption significantly affect human well-being as measured at the national level? Is this impact felt differently for countries classified into income categories?* Using macro-level data for 132 countries classified into income categories according to the World Bank classification, this study came to the following general conclusions.

- Corruption has a significant negative impact on well-being, when proxied by Legatum prosperity index, for both full sample and the sub-samples of high-income, upper-income, and lower-income economies. Or, in other words, a cleaner country with a reduced level of perceived corruption (higher CPI scores) would have better chances to register an increased level of overall human prosperity. Statistically, *the first hypothesis* was confirmed for all income categories (high-income, upper-income, and lower-income economies).
- Corruption has a significant negative impact on well-being, when proxied by the Human Development Index, for the full sample and the sub-sample of lower-income countries. This would mean that a cleaner country with a reduced level of perceived corruption (higher CPI scores) would have better chances to register an increased level of human development, which means a longer and healthier life with a more decent standard of living. Statistically, *the second hypothesis* was partially confirmed, especially for the full sample and lower-income economies. This finding is in line with previous ones, such as the findings of Helliwell and Huang (2008) who suggested that *"the ability of governments to provide a trustworthy environment and to deliver services honestly and efficiently appears to be of paramount importance for countries with worse governance and lower incomes*" (Helliwell & Huang, 2008, p. 595). On the other hand, this finding is contrary to the ones suggested by Altindag and Xu (2017), who argued that in poor countries, the extent of corruption, democracy, or civil rights has no effect on happiness or life satisfaction, but an increase in per capita income impacts well-being positively. In the same vein, Li and An (2020) suggested that corruption has a significant impact on national well-being only in democratic or high-income countries.

The significant role of certain economic development indicators for human well-being was also confirmed in both analyses (once when well-being was proxied by the Legatum prosperity index and, second, when well-being was proxied by the Human Development Index). Thus, GDP_growth and unemployment are significant variables for both full sample and sub-samples. Also, a higher score for index of economic freedom (that means healthier and cleaner societies) has a significant and positive effect on well-being (when proxied by Legatum prosperity index) for full sample and sub-samples of high-income and upper-income economies. Next, when well-being is proxied by the Human Development Index, a higher score for index of economic freedom is also significant, especially for the full sample and sub-samples of high-income and upper-income economies, but the coefficients are much lower than in the first analysis. In terms of the impact of press freedom on human well-being, it is interesting to note that in both analyses (once when well-being was proxied by the Legatum prosperity index and, second, when well-being was proxied by the Human Development Index), the significant and negative relationship between index of press freedom and well-being was confirmed, especially, for high-income and lower-income economies, meaning that lower press freedom in those countries would lead to lower scores on well-being scores (regardless of whether well-being is proxied by the Legatum prosperity index or by the Human Development Index). Finally, regarding country-level governance, the significant and positive relationship with well-being was confirmed only in the case of the first analysis (when well-being was proxied by Legatum Prosperity Index), especially in the case of full sample and sub-samples of upper-income and lower-income economies.

As further research, we propose the investigation of the moderating role of some other factors (such as education or cultural dimensions) on the relationship between corruption and human well-being and its development. Furthermore, our findings disclosed in this chapter could be reconfirmed or not when rerunning all the regressions but on different samples (classified based on geographical regions or other development criteria). Also, in these additional studies, some new and relevant control variables could also be included, such as democracy quality, health expenditures, or other indicators of economic development.

The conclusions of the study presented in this chapter could be considered as another significant and relevant argument that supports the idea that governments and policymakers should make all possible efforts to increase the trust of the public in the quality of public institutions and its representatives, while substantial and concrete efforts could be made to develop a rigorous legal system that condemns as strictly as possible bribery and corruption in the public sector. No doubt, in the near future, it is absolutely necessary that policymakers should be more and more focused on implementing adequate measures and policies to fight efficiently against corruption, both in the public and private sectors, so as to contribute to the improvement of well-being and human progress for their citizens.

Funding

No external funding was used for supporting the research presented in this chapter.

Disclosure Statement No potential conflict of interest was reported by the author.

Availability of data and materials: All the data used in this chapter are available in public databases.

References

Achim, M. V., & Borlea, S. N. (2018). The impact of corruption on population health. *Population Health Management, 21*(1), 84–84. https://doi.org/10.1089/pop.2017.0051

Achim, M. V., Văidean, V. L., & Borlea, S. N. (2020). Corruption and health outcomes within an economic and cultural framework. *The European Journal of Health Economics, 21*, 195–207. https://doi.org/10.1007/s10198-019-01120-8

Achim, M. V. (2016). Cultural dimension of corruption: A cross-country survey. *International Advances in Economic Research, 22*, 333–345. https://doi.org/10.1007/s11294-016-9592-x

Akouwerabou, B. D. (2014). Corruption in government procurement: On the motivations of small and medium enterprises in Burkina Faso. In D. Seck (Ed.), *Private sector development in West Africa, book series advances in African economic social and political development* (pp. 199–216). https://doi.org/10.1007/978-3-319-05188-8_10

Altindag, D. T., & Xu, J. (2017). Life satisfaction and preferences over economic growth and institutional quality. *Journal of Labor Research, 38*(1), 100–121. https://doi.org/10.1007/s12122-016-9235-2

Asadullah, M. N., & Chaudhury, N. (2012). Subjective well-being and relative poverty in rural Bangladesh. *Journal of Economic Psychology, 33*(5), 940–950. https://doi.org/10.1016/j.joep.2012.05.003

Asongu, S., le Roux, S., Nwachukwu, J. C., & Pyke, C. (2019). The mobile phone as an argument for good governance in sub-Saharan Africa. *Information Technology & People, 32*(4), 897–920. https://doi.org/10.1108/ITP-01-2018-0011

Ben Ali, M. S., & Gasmi, A. (2017). Does ICT diffusion matter for corruption? An economic development perspective. *Telematics and Informatics, 34*(8), 1445–1453. https://doi.org/10.1016/j.tele.2017.06.008

Brunetti, A., & Weder, B. (2003). A free press is bad news for corruption. *Journal of Public Economics, 87*(7–8), 1801–1824. https://doi.org/10.1016/S0047-2727(01)00186-4

Chipalkatti, N., Le, Q. V., & Rishi, M. (2021). Sustainability and society: Do environmental, social, and governance factors matter for foreign direct investment? *Energies, 14*, 6039. https://doi.org/10.3390/en14196039

Ciziceno, M., & Travaglino, G. A. (2019). Perceived corruption and individuals' life satisfaction: The mediating role of institutional trust. *Social Indicators Research, 141*, 685–701. https://doi.org/10.1007/s11205-018-1850-2

Daniels, L., & Minot, N. (2020). *An introduction to statistics and data analysis using Stata* (1st ed.). SAGE Publications.

Danish, M. H., & Nawaz, S. M. N. (2022). Does institutional trust and governance matter for multidimensional well-being? Insights from Pakistan. *World Development Perspectives, 25*., Article 100369. https://doi.org/10.1016/j.wdp.2021.100369

Dutta, M. (2018). Globalisation, corruption and women empowerment. *Economic Papers: A Journal of Applied Economics and Policy, 37*(3), 327–343. https://doi.org/10.1111/1759-3441.12227

Ekici, A., & Ekici, S. O. (2021). Understanding and managing complexity through a Bayesian network approach: The case of bribery in business transactions. *Journal of Business Research, 129*, 757–773. https://doi.org/10.1016/j.jbusres.2019.10.024

Evans, M. D. R., Kelley, J., Kelley, S. M. C., & Kelley, C. G. E. (2019). Rising income inequality during the great recession had no impact on subjective wellbeing in Europe, 2003–2012. *Journal of Happiness Studies, 20*, 203–228. https://doi.org/10.1007/s10902-017-9917-3

Graeff, P., & Mehlkop, G. (2003). The impact of economic freedom on corruption: Different patterns for rich and poor countries. *European Journal of Political Economy, 19*, 605–620. https://doi.org/10.1016/s0176-2680(03)00015-6

Hamada, B. I., Abdel-Salam, A.-S. G., & Elkilany, E. A. (2019). Press freedom and corruption: An examination of the relationship. *Global Media and Communication, 15*(3), 303–321. https://doi.org/10.1177/1742766519871676

Helliwell, J. F., & Huang, H. (2008). How's your government? International evidence linking good government and well-being. *British Journal of Political Science, 38*(4), 595–619. https://doi.org/10.1017/S0007123408000306

Heritage Foundation. (2022). Index of economic freedom. Accessible online at https://www.heritage.org/index/download

Heukamp, F. H., & Ariño, M. A. (2011). Does country matter for subjective well-being? *Social Indicators Research, 100*(1), 155–170. https://doi.org/10.1007/s11205-010-9610-y

Kalenborn, C., & Lessmann, C. (2013). The impact of democracy and press freedom on corruption: Conditionality matters. *Journal Policy Model, 35*(6), 857–886. https://doi.org/10.1016/j.jpolmod.2013.02.009

Kaufmann, D., Kraay, A. & Zoido-Lobaton, P. (1999). *Aggregating governance indicators*, World Bank Policy, Research Working Paper No. 2195. The World Bank. HYPERLINK "https://doi.org/10.1111/j.1468-2508.2007.00552.x"

Kaufmann, D., Kraay, A., & Mastruzzi, M. (2010). The worldwide governance indicators: Methodology and analytical issues. World Bank Policy Research Working Paper No. 5430. The World Bank.

Kim, S., & Kim, D. (2012). Does government make people happy? Exploring new research directions for government's roles in happiness. *Journal of Happiness Studies, 13*(5), 875–899. https://doi.org/10.1007/s10902-011-9296-0

Knight, J., Song, L., & Gunatilaka, R. (2009). Subjective well-being and its determinants in rural China. *China Economic Review, 20*(4), 635–649. https://doi.org/10.1016/j.chieco.2008.09.003

Kovacevic, M. (2011). Review of HDI critiques and potential improvements. In: United Nations Development Programme, Human Development Reports, Research Paper 2010/33.

Li, Q., & An, L. (2020). Corruption takes away happiness: Evidence from a cross-national study. *Journal of Happiness Studies, 21*, 485–504. https://doi.org/10.1007/s10902-019-00092-z

Luttmer, E. (2005). Neighbors as negatives; relative earnings and well-being. *Quarterly Journal of Economics, 120*(3), 963–1002.

Ma, J., Guo, B., & Yu, Y. (2022). Perception of official corruption, satisfaction with government performance, with subjective wellbeing—an empirical study from China. *Frontiers in Psychology, 13*., Article 748704. https://doi.org/10.3389/fpsyg.2022.748704

Magalhaes, K. E., Portes, J. H., Domenech, A. M., & Junqueira, L. A. P. (2019). Impacts of corruption on innovation and well-being on countries represented in the ICIM by OECD members. *RISUS—Journal on Innovation and Sustainability, 10*(4), 4–15. https://doi.org/10.23925/2179-3565.2019v10i4p4-15

Mornah, D., & Macdermott, R. J. (2018). A non-proxied empirical investigation of cultures effect on corruption. *Business and Society Review, 123*(2), 269–301. https://doi.org/10.1111/basr.12142

Newton, L. H., Hodges, L., & Keith, S. (2004). Accountability in the professions: Accountability in journalism. *Journal of Mass Media Ethics, 19*(3–4), 166–190. https://doi.org/10.1080/08900523.2004.9679687

Otoiu, A., Titan, E., & Dumitrescu, R. (2014). Are the variables used in building composite indicators of well-being relevant? Validating composite indexes of well-being. *Ecological Indicators, 46*, 575–585. https://doi.org/10.1016/j.ecolind.2014.07.019

Rachisan, P. R., Bota-Avram, C., & Grosanu, A. (2017). Investor protection and country-level governance: Cross-country empirical panel data evidence. *Economic Research-Ekonomska Istraživanja, 30*(1), 806–817. https://doi.org/10.1080/1331677X.2017.1311226

Rao, S. (2008). Accountability, democracy, and globalization: A study of broadcast journalism in India. *Asian Journal of Communication, 18*(3), 193–206. https://doi.org/10.1080/01292980802207041

Rodriguez-Pose, A., & Maslauskaite, K. (2012). Can policy make us happier? Individual characteristics, socio-economic factors and life satisfaction in central and Eastern Europe. *Cambridge Journal of Regions, Economy, and Society, 5*(1), 77–96. https://doi.org/10.1093/cjres/rsr038

Rojas, M. (2020). Well-being in Latin America. *Human well-being research and policy making*. Part of the Human Well-Being Research and Policy Making book series (HWBRPM) https://doi.org/10.1007/978-3-030-33498-7_1.

Romero-Martínez, A. M., & García-Muiña, F. E. (2021). Digitalization level, corruptive practices, and location choice in the hotel industry. *Journal of Business Research, 136*, 176–185. https://doi.org/10.1016/j.jbusres.2021.07.032

RSF. (2022). World press freedom index. Reporters without borders. Accessible online at https://rsf.org/en/actions/reports-and-statistics.

Sacks D., Stevenson B., & Wolfers J. (2010). Subjective well-being, income, economic development and growth. NBER Working Papers no. 16441.

Sommer, J. M. (2020). Corruption and health expenditure: A cross-national analysis on infant and child mortality. *The European Journal of Development Research, 32*, 690–717. https://doi.org/10.1057/s41287-019-00235-1

Stevenson, B., & Wolfers, J. (2013). Subjective well-being and income: Is there any evidence of satiation? *American Economic Review: Papers & Proceedings, 103*(3), 598–604. https://doi.org/10.1257/aer.103.3.598

Tavits, M. (2008). Representation, corruption, and subjective well-being. *Comparative Political Studies, 41*, 1607–1630. https://doi.org/10.1177/0010414007308537

Tay, L., Herian, M. N., & Diener, E. (2014). Detrimental effects of corruption and subjective well-being. *Social Psychological and Personality Science, 5*(7), 751–759. https://doi.org/10.1177/1948550614528544

The Legatum Institute. (2021). *The 2021 Legatum prosperity index—a tool for transformation*. The Legatum Institute. Accessible on-line at https://www.prosperity.com/download_file/view_inline/4429

Transparency International. (2021). Corruption perception index. Accessible online at https://images.transparencycdn.org/images/CPI2021_Report_EN-web.pdf.

UNDP. (2021a). Human development report 2021–2022. UNDP. Available at https://hdr.undp.org/content/human-development-report-2021-22.

UNDP. (2021b). Human development index technical notes. UNDP. Accessible on-line at http://hdr.undp.org/sites/default/files/hdr2022_technical_notes.pdf.

Wassmer, R. W., Lascher, E. L., & Kroll, S. (2009). Sub-national fiscal activity as a determinant of individual happiness: Ideology matters. *Journal of Happiness Studies, 10*(5), 563–582. https://doi.org/10.1007/s10902-008-9109-2

Welsch, H. (2008). The welfare costs of corruption. *Applied Economics, 40*(14), 1839–1849. https://doi.org/10.1080/00036840600905225

World Bank. (2022a). World Bank country and lending groups. Accessible online at https://datahelpdesk.worldbank.org/knowledgebase/articles/906519-world-bank-country-and-lending-groups.

World Bank. (2022b). World Bank development indicators. Accessible online at https://databank.worldbank.org/source/world-development-indicators.

World Bank. (2022c). Worldwide governance indicators. Accessible online at https://databank.worldbank.org/source/worldwide-governance-indicators.

Yan, B., & Wen, B. (2020). Income inequality, corruption and subjective well-being. *Applied Economics, 52*(12), 1311–1326. https://doi.org/10.1080/00036846.2019.1661953

Cristina Boța-Avram is an Associate Professor, PhD, at Babes-Bolyai University, Faculty of Economics and Business Administration, Department of Accounting. She holds PhD from Babes-Bolyai University in 2009 and habilitation degree in the field of Accounting from the University of West in 2018, Timisoara. With over 19 years of experience in academia, she has published as author and co-author over 70 scientific articles, 4 books chapters and 3 books. Her research interests include governance, corruption, digitalization, audit, ethical behaviour, sustainable business performance, and sustainability reporting assurance.

Chapter 7
The Main Aspects of the Impact of Cybercrimes on the Business Environment in the Digital Era: Literature Review

Sorinel Căpușneanu, Dan Ioan Topor, Ileana-Sorina Rakoș, Cristina-Otilia Țenovici, and Mihaela Ștefan Hint

Abstract The aim of this research is to identify the main aspects of the impact of cybercrime on the business environment through quantitative research and comparative analysis by reviewing international literature. The applied research methodology also consisted of processing and analysing information gathered from the literature of international regulatory bodies, which formed the basis for syntheses and extracts of judgements and findings. The results obtained revealed a significant increase in cybercrime over the last decade, which is why several measures to combat cybercrime in business were proposed and discussed. The chapter concludes with the authors' conclusions, the limitations of this study and future research directions proposed by them.

The importance of this chapter is aimed at both academic and business specialists, as well as at all readers interested in learning more about the subject.

Keywords Cybercrime · Business environment · Digital age

JEL Classification K20 · K22

S. Căpușneanu
Faculty of Economic Sciences, Titu Maiorescu University, Bucharest, Romania

D. I. Topor (✉) · M. Ș. Hint
Faculty of Economic Sciences, University of Alba-Iulia, Alba-Iulia, Romania
e-mail: dan.topor@uab.ro

I.-S. Rakoș
Faculty of Sciences, University of Petroșani, Petroșani, Romania

C.-O. Țenovici
Faculty Marketing Management in Economic Affairs, Pitești, Romania

M. V. Achim (ed.), *Economic and Financial Crime, Sustainability and Good Governance*, Contributions to Finance and Accounting,
https://doi.org/10.1007/978-3-031-34082-6_7

1 Introduction

Digital evolution has also enabled the fast evolution of business, and digital systems and information and communication technology (ICT) have become essential in all sectors of economic activity worldwide. As digital evolution has increased, so have cybersecurity incidents, either intentional or accidental, which have led to an increase in cybercrime worldwide. As such, companies need to embrace these challenges and respond in a swift manner, countering cyberattacks and protecting themselves from the negative impact on their business. In other words, companies need to invest in cybersecurity to prevent cybercrime and train their staff to do so. Furthermore, each country should invest in its IT infrastructure using appropriate protection tools to anticipate possible cyberattacks and protect itself in the future by taking appropriate measures.

Until legislation in the area of cyberattacks is harmonised, international cooperation is needed to establish certain objectives, conventions, and guidelines necessary to prevent, combat, investigate, and fight cyberattacks. In this respect, this chapter sets the following objectives: (1) presenting the most important conceptual approaches to cybercrime and the taxonomy of cybercrime in the business environment; (2) presenting the main causes and effects of cybercrime; (3) presentation of cybersecurity and cyberforensics with business impact; and (4) presentation of the main ways to combat cybercrime in the business environment. The purpose of our research is to identify the main aspects of the impact of cybercrimes on the business environment by carrying out a quantitative research and a comparative analysis by reviewing the international specialised literature.

Therefore, this chapter fills in some existing gaps in the specialised literature and brings together many unspecified aspects regarding cybercrime in the business environment, and thus, our study represents a true synthesis of the international specialised literature. The results obtained indicate some effective measures to combat crime in the business environment. The paper is organised as follows: Sect. 2 is dedicated to carrying out a synthesis of the specialised literature in the field of cybercrime and its taxonomy in the business environment followed by their causes and effects; Sect. 3 includes the research methodology; Sect. 4 results obtained and related interpretations and Sect. 5 is dedicated to general conclusions, own contributions, and limitations of the research conducted, including establishing future research directions.

2 Literature Review

2.1 Cybercrime and Taxonomy of Cybercrime in the Business Environment

The emergence of the term "cyber" is linked to the field of cybernetics and the use of computer technology between the 1980s and 1990s. Positive meanings of the term were used until 2000 to describe all aspects of cyberspace use, cyberbrowsing, or cybershopping (Yar & Steinmetz, 2019). After 2000, negative meanings of the use of the term that had links to the conduct of illicit or harmful activities (cyberbullying, cyberterrorism, cyberoffense) or cybercrime emerged (Yar & Steinmetz, 2019; McGuire, 2020).

The systematic and reasoned approach to defining cybercrime is an important issue that we seek to clarify below. As it is well-known, cybercrime includes a diverse set of crimes and harmful behaviours (Phillips et al., 2022) of which the most well-known include among others: computer-related fraud, copyright infringements, cyberfraud, illegal access (hacking/cracking), ransomware, spam, data interference, digital piracy, espionage, phishing, system interference, and trademark-related offences (Tsakalidis & Vergidis, 2017).

The concept of cybercrime has been widely debated in the literature, but there is no agreement on its international definition (Collin, 1996; Viano, 2017; Paoli et al., 2018; Broadhead, 2018; Sarre et al., 2018; Black et al., 2019; Donalds & Osei-Bryson, 2019; Akdemir et al., 2020), which is why the most significant definitions and approaches have been selected:(1) using computers as targets to attack other computers by infecting them with viruses and spreading malware and committing fraud, illegally storing information or data (Mativat & Tremblay, 1997); (2) activities that are considered illegal or illicit by certain parties and that are carried out via global electronic networks using computers; (3) offences committed against individuals or groups of individuals with a view to intentionally damaging the reputation of victims or causing physical or psychological harm or loss to them, directly or indirectly using telecommunications networks and mobile phones (Halder & Jaishankar, 2011); and (4) the commission of a large number of unlawful acts, crimes, or behaviours by some individuals against other individuals or groups against computers, computer-related devices, or technological information, as well as fraud carried out or maintained through the use of the Internet and/or information technology (Gordon & Ford, 2006; Donalds & Osei-Bryson, 2019).

According to international organisations, the concept of cybercrime does not have a widely accepted definition, each of which has its own understanding of the composition and terms used. Among them, we report the most important meanings of cybercrime: (1) actions against the confidentiality, integrity, and availability of information systems, networks, and computer data, including their misuse for the purpose of criminal conduct (Council of Europe, 2001); (2) the use of information systems and electronic communications to commit criminal offences (Commission of the European Communities, 2007); and (3) the involvement as primary tools or

primary targets of telecommunications or information systems to carry out criminal activities (European Commission, 2013). There are several types of cybercrime, of which the most common in business are data crimes, network crimes, and related crimes.

Data Crime: This concept encompasses the interception, alteration, and theft of data by a criminal who monitors these data streams in order to gather information which may or may not be the ultimate purpose of the crime. The offender can act passively, when he simply monitors the information flow without intervening, or he can act actively, when he intervenes on the information by producing certain detections in the network traffic. There is a possibility that when the information is distributed, the offender can intervene by altering the data and committing a cybercrime. It is therefore very important to ensure the confidentiality of communications during data transfer. Through this unauthorised and illegal interception, the offender may or may not alter some of the information, copy it, and pass it on to another person. This information usually includes passwords, social security numbers, credit card information, and personal and confidential company information. By committing these types of cybercrimes, the offender will be prosecuted and subject to the rigours of the applicable laws.

Network Crime: The concept of network crime includes unauthorised access and dissemination of viruses. Unauthorised access can be translated as attempting to gain access to a website, program, server, or other services and systems using login credentials or by attempting to guess them. It can also include attempts to access certain areas of networks or servers without the consent of the system administrator. Usually, these attempts are signalled by receiving alert messages indicating unauthorised access and blocking the hacker's connection. The concept of virus spreading refers to the actions of a malicious computer program that is attached to another computer program that helps to destroy the victim's system by disrupting the functioning of the computer or damaging its database. There are many viruses that affect computer systems and programs such as polymorphic viruses, hidden viruses, tunnel viruses, cloaking viruses, and Trojan horses, which cause damage to victims' computers.

Related Crime: The concept of related crime refers to complicity in the commission of a crime and is composed of the following elements: aiding and abetting cybercrime, computer forgery and fraud, and other crimes related to its content.

According to expert studies, the most common types of cybercrime identified in the business environment are as follows: (1) denial of service (DoS);(2) botnet; (3) advanced persistent threat (APT);(4) social engineering; and (5) malicious software (Ponemon Institute, 2012; Mostafa, 2022).

Denial of Service (DoS) is the name for a cyberattack whose goal is to block legitimate users from accessing a machine or network and consists of sending massive information (flooding) into the network that triggers a crash. Most DoS attacks do not lead to theft or significant loss of information, but contribute to business disruption (Shui, 2013) generating significant costs for victims and most often target the web servers of companies, especially banking, commercial and media companies, or commercial and government organisations. Criminals typically

use either flooding services or services to lock down the servers or systems of organisations (Tan et al., 2014). Flooding services consist of receiving heavy traffic, the server being unable to cope with the requests—it automatically slows down, until it is blocked. Blocking services consist of identifying and exploiting vulnerabilities in a computer system causing it to be blocked or unusable for a certain period of time, contributing to server destabilisation.

Also included in this category is the distributed denial of service (DDoS) attack, which consists of a DoS attack being concentrated simultaneously from several locations on the target or victim. Under these conditions, the perpetrator is difficult to identify and can cause serious damage to the victim (Mirkovic et al., 2004). Due to the unique characteristics of a DDoS attack, it is very difficult to identify a defence against them with the modern security technologies currently available.

A botnet is a network of computers and devices infected with bot malware, hijacked, and remotely controlled by a criminal (hacker). These botnets can exist without a command and control (C&C) server using a P2P architecture or other bot management and transfer channels and consist of spamming and DDoS attacks. In a botnet, the client can take actions without allowing the hacker to connect to its operating system, but any clients that execute the same specific goals with others in a coordinated manner are taken care of without any interference from the hacker (Schiller & Binkley, 2007). In recent years, these networks have also developed on IoT-connected devices. Today, botnets have the ability to extract bitcoin, intercept any data in transit, consume user machine resources, and send logs of user information.

Advanced persistent threats (APTs) are those threats in the form of attacks on a network or computer networks through which an intruder (attacker) gains access and remains undetected for an extended period of time. The purpose of these APT attacks is to maintain continuous access to the targeted network and to steal data and information without causing damage to the targeted companies or organisations (corporations or large companies). To avoid detection of APT attacks, intruders resort to various social engineering techniques, taking advantage of zero-day vulnerabilities and spear phishing, and they continuously rewrite malicious code and leave backdoors (Chen et al., 2014). Cybersecurity professionals focus on detecting those anomalies on outbound data to verify APT attacks. Attackers usually follow a sequential approach whereby they gain access into a computer network (spear phishing email or other system vulnerability), use malware to rewrite code, can also gain greater access by obtaining passwords with administrative rights, move around the network stealing information which they encrypt, and then transfer to their own systems, etc.

Social engineering refers to the art of manipulating (deceiving trust, tricking) people into giving up confidential information (passwords or banking information) and gaining control over their devices (computers, tablets, phones, etc.). In other words, social engineering refers to those methods by which cybercriminals trick victims into taking certain questionable actions, allowing them to breach security, send money, or give up private information. Criminals take advantage of the fact that they never meet their victims, and by manipulating emotions (anger, love, or fear),

crooks can get people (victims) to act on impulse without thinking rationally. A hacker pretending to be an officer in some authoritative institution can easily tell the victim to remove information such as a system password or a credit card number (Krombholz et al., 2015).

Malware refers to any programs or files (computer viruses, worms, backdoors, Trojans, ransomware, spyware) that infect by inserting or implanting themselves into computers, networks, or servers intentionally causing damage to them (Stallings, 2014). These malicious programs are used to steal, encrypt, and delete sensitive data, modify or hijack basic computing functions, or monitor end-users' computer activity. All types of malware are designed to exploit devices to the detriment of the user and to the benefit of the perpetrator (hacker). Malware can be spread in various ways: USB drive via software delivery, drive-by download, other collaboration tools, etc.

With the above-mentioned and discussed, we consider that the first objective of our research, namely to present the most important conceptual approaches to cybercrime and the taxonomy of cybercrime in business, has been achieved.

2.2 Causes and Effects of Cybercrimes

Among the most known causes of cybercrime in business can be listed as (1) economic reasons; (2) personal reasons; and (3) ideological reasons (Krishna Viraja & Purandare, 2021).

Economic motives or lack of money is the main cause for cybercriminals to commit cybercrimes. They use malware and phishing and identity theft or other forms of fraudulent activities to demand very large financial rewards from companies or government organisations, hiding their identity behind the networks through which they carry out cyberattacks (Iqbal & Beigh, 2017). Lack of money is also due to other causes such as unemployment or poverty. With all the educational qualifications in the country, many people fail to get jobs, fall into depression, and see cybercrime as a way to survive. Other people are not paid enough or at all for months or years, unable to survive and on the verge of poverty, turn to cybercrime of the kind mentioned above (Pawar et al., 2021).

Personal motives are a second cause of committing cybercrime and are due to emotional states, generally revenge, especially in the case of very large companies where the offender considers himself a disgruntled victim. He either proceeds to virus the system or the programs he works with or sends threatening messages to colleagues or management demanding large sums of money as a reward (Kamruzzaman et al., 2016). Other personal causes could be related to certain unfulfillment in professional life (lack of confidence) or greed, the desire of certain people who are dissatisfied with what they have and want more, to get rich quickly by skipping certain stages of professional development, proceed to cybercrime of those mentioned above (Pawar et al., 2021).

The third cause of cybercrime is due to the ideology by which cybercriminals are motivated by certain ethical or ideological principles. They do this by blocking or

disrupting the functioning of computer equipment or even by damaging networks or servers within the companies or organisations in which they operate, thereby expressing their dissatisfaction with certain people in management, colleagues, or other institutions with which they have business relationships (Kumar Goutam & Kumar Verma, 2015).

Among the most well-known effects of cybercrime in business are (1) financial and reputational losses and (2) moderation of companies' competitive advantage.

In the case of companies, cybercriminals proceed with threats to disclose or leak sensitive information to the press or other institutions, demanding large sums of money in return and thus causing companies large financial losses (Leukfeldt et al., 2019). Along with financial losses also comes the loss or diminution of the company's reputation, as its image is compromised in the eyes of its customers due to security breaches (Pathak, 2016). All of the above-mentioned effects contribute to the impairment of a country's security and financial health causing irreparable damage and loss of time which in turn is reflected in financial and reputational losses (Pawar et al., 2021).

According to the statements of some websites specifically dedicated to cybercrime (Krazytech, 2022) among the causes of cybercrime are also: *(1) ease of access to systems; (2) complex coding; (3) carelessness; (4) insufficient data storage space; (5) loss of evidence; (6) evolution of cybercrime.*

Some companies' systems and servers are not powerful enough or protected against cyberattacks by hackers, lacking firewalls, or complex biometric systems. The very complexity of operating systems means that complex code is created in computer programming and hackers exploit this by carrying out cyberattacks. Neglecting these aspects can create open access to hackers and vulnerabilities that affect the security of the company's data that is attacked and becomes a victim. Insufficient data storage space on some companies' servers creates the perfect conditions for cyberattacks by hackers who take advantage of this vulnerability and access and transfer data to their own storage systems. With the loss of company data, evidence of hackers accessing the servers can easily be lost, making it impossible to investigate cybercrime. The evolution of computer technology has also led to the evolution of cybercrime as teenagers develop these skills in school or secondary school.

With the above presentation, we believe that the second objective of our research, namely to present the main causes and effects of cybercrime, has been achieved.

2.3 Cybernetic Security and Digital Forensics and Its Impact on Business

Cybersecurity is the advanced response of technology, processes, and methods specifically designed to protect data from attack, damage, or unauthorised access to networks, computers, software, and data by cybercriminals. According to expert

opinion, cybersecurity has several meanings including (1) the insecurity created through cyberspace and ensuring that technical or less technical practices are carried out (Dunn-Cavelty, 2010); (2) allowing operations to be carried out in cyberspace without risk of physical or digital harm (Dewar, 2014); and (3) ensuring that authorised users have unrestricted access to information and unauthorised access is prevented (Faysel & Haque, 2010).

The cybersecurity system is based on components such as confidentiality, availability, and integrity. Regardless of security procedures, standards, or technology, no system is totally secure, and companies are facing increasingly complex attacks, and in this sense, cybersecurity is also expanding (Le Compte et al., 2015). In order to ensure cybersecurity, a joint effort must be made by citizens, companies, and their own information systems. Threats to breach cybersecurity systems are becoming increasingly intense, and rapid solutions must be found to prevent and combat cybercrime. In this sense, cybersecurity is becoming the necessary guide to train, prevent, and combat criminal offences in the cyberenvironment that protects the assets of organisations and users consisting of a complex set of tools, policies, security concepts, security agents, risk approaches, best practices, safeguards, and technologies.

According to expert opinion (Perwej et al., 2014; Jensen et al., 2009) there are several types of cybersecurity identified in business including cloud security, critical infrastructure security, data loss prevention, application security, information security, network security, end-user education, IoT security, operational security, endpoint security, website security, big data security, blockchain security.

Cloud Security Some specialist IT companies offer cloud-based data storage capabilities that need to be protected from attacks by cybercriminals through advanced software-based technologies that protect and monitor the activities in individual and corporate customer accounts (Ong et al., 2017). These companies offer low-cost ways for customers to maintain and secure their data.

Infrastructure Security Ensuring cybersecurity for infrastructure is important, and the entire communication circuit through platforms connected to different systems within the vital economy depends on it.

Data Loss Prevention (DLP) Some specially designed software allows network administrators to manage sensitive or vital data flows from inside to outside the company or organisation by setting network permissions and policies (Jin et al., 2011). In other words, they ensure that vital data are kept within the organisation or company, while also developing a set of policies and practices to deal with and prevent data loss or data recovery as a result of a cybersecurity breach. Preventing data loss also ensures the protection of personal information, the protection of intellectual property, and data visibility.

Application Security Identifying or minimising security vulnerabilities is done using hardware, software, and certain procedures that help secure applications. These applications can be protected against cyberattacks with the help of cybersecurity antivirus software, firewalls, and encryption services.

Information Security Protecting data from unauthorised use, disclosure, deletion, or other malicious intent is known as information security and is achieved through data encryption. Encryption protects data from being altered, deleted, or stored on other storage media during transmission from one network to another. Various applications are currently used to manage encryption keys, network intrusion detection systems, password rules, and regulatory compliance.

Network Security Internal network security is ensured by protecting internal infrastructure and restricting access to it against intrusions from outside the networks (Perwej et al., 2019a, 2019b). Companies must implement security programs to monitor networks and internal infrastructures to combat cyberattacks and network viruses. One way to combat this relates to machine learning technology that detects unusual data traffic within networks, alerting network administrators to potential cyberattacks.

End-User Education End-user education is essential and vital to avoid cyberattacks and damage to the companies or organisations where they operate. In addition to cyber-protection solutions in the form of software or other applications, users need to be educated on best practices for avoiding and spreading cyberattacks such as not accessing unknown links, not opening strange or unknown attachments, and not accessing unidentified USB drives.

IoT Security Security risk is one of the main obstacles in the adoption and deployment of IoT in companies and organisations (Akhtar & Perwej, 2020; Parwej et al., 2019). In recent years, cyberattacks by hackers have increased through the use of IoT, and for this reason, many companies and organisations avoid its use due to security concerns and lack of funds to implement advanced security systems to protect their data (Kowtha et al., 2012).

Operational Security It is the process by which companies examine and secure their public data using various techniques that ensure that their data are protected from disclosure of certain information that must remain hidden or secret. This process involves identifying important information, analysing threats, analysing vulnerabilities, assessing risk, and implementing effective countermeasures.

End Point Security The interconnection of devices in an internal network creates access points for cyberthreats and vulnerabilities, which is why these risks, including those arising from the use of remote devices, must be avoided (Perwej, 2018a). To this end, user access perimeters within companies must be delimited and security measures implemented to protect network access points. This can be done through the use of antivirus and anti-malware software or data integrity monitoring within companies.

Web Security The aim of web security is to protect websites from cyberthreats or cyberattacks from the Internet. It consists of using security software that targets company databases, applications, source code, and files. Protecting against cyberattacks can be done in several ways such as scanning the website, removing malware, installing, and running firewalls.

Big Data Security According to expert opinion, the use of big data technology can help increase cybersecurity by quickly and efficiently detecting malware and ransomware attacks (Perwej et al., 2017), malicious internal programs, or corrupted and vulnerable equipment within companies (Pasqualetti et al., 2013). By using big data specialists can create predictive alert models in case of cyber-intrusions (Perwej et al., 2018).

Blockchain Security According to expert opinion, blockchain presents itself as a distributed ledger in the sense of sharing by multiple participants in a peer-to-peer network without the involvement of a central authority, (Perwej et al., 2019b) in order to optimise the available bandwidth of a service to increase data availability and access (Perwej, 2018b). Avoiding cyberattacks can be achieved by implementing blockchain, thus protecting sensitive data through a decentralised type of data storage.

Computer forensics is a special computer law enforcement division within the forensic branch that investigates cyber-attempts, cyberattacks, and cybercrimes committed by malicious individuals or hackers. There are now a number of computer forensic tools that are publicly available through which individuals or companies can apply auditing standards and principles and conduct investigative cases on specific suspected cybercrime situations.

In the broadest sense of the word, computer forensics deals with the recovery of data from various magnetic media (hard disk, floppy disk, or flash drive memory). In addition to this, it also investigates the possibilities of encryption, password protection, steganography, or compression of various devices or files, smart cards, electronic organisers, personal digital assistants, printer heads, printer cartridges, or toner, which may constitute evidence in various cyberforensic investigations. There are several definitions of cyberforensics and digital evidence in the literature that do not take into account how evidence is obtained from the client (Guo et al., 2010) or how evidence is managed on the client's side (Simou et al., 2014), as well as other studies that emphasize the problems of current forensic processes and challenges in the near future (Garfinkel, 2010). Some studies focus on email data management tools (Hatole & Bawiskar, 2017) and other studies on cyberforensics and digital evidence management tools (Kaur et al., 2016) and guidelines for managing digital evidence in web environments (Kaur et al., 2016; Sachdeva et al., 2020).

The main types of forensic evidence are digital evidence that is stored or transmitted by computers. They are most often used in cases of harassment, fraud, theft, or espionage in business. Cybercriminals are increasingly using computer networks to hide the traces of their crimes, and the investigators are specialised in technical or legal issues and less in those associated with digital evidence. Thus, digital evidence is insufficiently or incorrectly investigated and analysed. According to expert opinion there are two techniques that cybercrime analysts use in their investigations: (1) the non-hierarchical view technique according to which non-hierarchical views of file statistics displaying each file in a directory and its subdirectories do not take into account the relationship between the files and

directories mentioned; (2) the hierarchical view technique or hierarchical views of file statistics that take into account the relationship between files according to the structure of the directories displayed (Teelink & Erbacher, 2006).

As a result of the above discussion, we believe that the third objective of our research, namely to present cybersecurity and cyberforensics with business impact, has been met.

3 Methodology of Research

The scientific research used in the paper is based on qualitative research and literature review, based on which syntheses and extracted judgements and findings were made. The aim of the documentary research was to gather material for analysis, description, and opinion building on the topic of cybercrime and cybersecurity in business. Accordingly, a variety of specific methodological methods were used, including information gathering based on literature review, observation, data documentation and analysis, data processing, and comparative research on interpretation of results. The literature review included research papers published in various research journals, books, and online publications.

4 Results

Discussions among IT and business experts revealed a shift in focus towards combating and reducing cybercrime, which has increased significantly over the last decade. One of the sustainable goals set by the UN also refers to crime reduction, and this involves the participation of a key partner, the financial world whose willingness is crucial to the success of this partnership (UN, 2017). While the UN used to be concerned about the environmental degradation dominating the economy, it has now shifted its priorities to unlocking and reshaping finance. In addition to boosting green investment, experts also suggest focusing and coordinating efforts that could replace existing fragmented and sectoral initiatives (Clark et al., 2018). Developing countries could bring innovative environmental, climate, and sustainable development solutions supported by financial decision-makers and regulators (Zadek, 2018). Factors influencing decisions coming from the financial sector relate to (1) involvement in financing environmental degradation operations in developing countries and (2) the general trend of prioritising immediate objectives (Ruggiero, 2022).

Most companies do not take environmental goals into account in their performance, being only concerned with business and less with sustainability issues (Yasin et al., 2021), and in this way, finance can become a party to environmental crime, provoking reactions among protesters trying to defend their territories from corporations pursuing oil, gas, and mineral extraction (Ruggiero, 2020). Such unrest can

also be created on the basis of political instability which also explains the reluctance of investors to commit to long-term initiatives whose outcomes are uncertain (Ruggiero, 2022). Some financial groups continue to finance companies that pursue destructive growth rather than green growth (Global Witness, 2021), while national and international agencies seek to identify safe and sustainable areas of investment, developing a series of typologies (China, Japan, France, Netherlands) and taxonomies of sustainability finance (Canada, Indonesia) (green and sustainable, less risky and more remunerative, regulated, and more enforceable) that encourage investors to integrate climate change into their businesses (OECD, 2021).

Tax evasion is an illegal, unethical way in which certain individuals or groups (corporations) benefit from low or non-existent tax contributions. In other words, tax evasion is a crime committed mainly by certain privileged individuals and groups against a system that guarantees their privileges by adopting the conversion of legally acquired money into illegal funds (Ruggiero, 2017a, 2017b). The opposite of tax evasion is money laundering; i.e., illegally earned money is apparently transformed into legal profit and is a financial crime specific to organised crime itself. Most of the money is hidden behind a complex of secret offshore bank accounts, companies, and trusts (Christensen, 2015).

According to experts, sustainable finance will not reduce financial crime, but will stimulate its decriminalisation (Ruggiero, 2022), giving rise to another term in financial activity that has led to a certain fear among investors and avoids legal regulation: financial innovation (Krugman, 2020). The case of Panama, Paradise, and Pandora best describes the advantages gained as a result of financial criminality as a result of tax convergence and tax evasion. Encouraging waste among consumers or denigrating the output of entrepreneurs has led to the emergence of sabotage (Camic, 2020; Appiah, 2021). These activities have encouraged experimentation with techniques that contribute to increased financial crime. Institutions that provided finance had to intervene to continue funding, while financial operators aware of their imprudence relied on the help of honest taxpayers (Nesvetailova & Palan, 2013). Under these conditions, sustainable finance will become even more unsustainable due to the increase in financial criminal activities, and political choices will become a subsystem subsumed by the economy (Ruggiero, 2022).

Digitisation offers enormous opportunities and provides solutions to many of the challenges facing Europe, not least during the crisis caused by the COVID-19 pandemic, when a number of critical sectors such as health, energy, transport, and finance have become dependent on digital technology to carry out their core activities (Alecu et al., 2021).

Preventing and combating cybercrime as it relates to business are not an easy task, as cybercriminals are often difficult to identify, as they commit their crimes at considerable distances from their geographical location or the country where they live and carry out their criminal actions, does not have criminal laws against cybercrime. However, some measures can be taken against cybercrime, such as (1) user identification and authentication; (2) use of network scanning programs; (3) use of open source for security; (4) special laws for the protection of computer users; (5) intensification of cooperation actions between public structures that are

responsible for preventing and combating cybercrime; and (6) cooperation between public authorities and members of civil society (Mshana, 2015).

User identification and authentication can be done by using the username and password. Although these tools can be very easily cracked by a cybercriminal, passwords consisting of long strings of characters including numbers, uppercase and lowercase letters, and changing them at short intervals, monthly or yearly, make them difficult to crack. Also the SMART use of cards in the future is a means of stopping cyberattacks, by requiring both the card and the personal identification number known only to the cardholder, access being impossible without both.

Using Network Scanning Software For SMEs, virtual private network (VPN) technology over WLAN, which has a practical and scalable design, can be used for cybersecurity purposes. A VPN allows users of a public network or WLAN to set up a secure connection to a private network. In wired or wireless mode, the user establishes a secure VPN tunnel to the VPN server when the user is authorised. Subsequently, all data traffic sent through the tunnel are encrypted.

Using Open Source for Security Cybercrime can be prevented by using software that allows users to assess their own security or hire a party of their choice to assess the security of the Internet they are using. This software allows not just one person but a team of people to assess the security of the system, thus eliminating the dependency on one person to decide for or against a particular system.

Special Laws to Protect Computer Users Every country should have special laws to combat criminal cyber-activities, protecting computer users from cyberattacks. Internet use is a major risk for all businesses. The question is: How can these risks be minimised? Effective enforcement of national legislation and harmonisation of national legislation with that at European and international level would be a first step in terms of legislation to prevent cybercrime. Cyberspace and cybercrime are two constantly evolving elements, which makes it difficult for public authorities to create a legislative package adapted to the two methods of committing criminal offences. Given that international legislation is drafted in English, it is necessary to translate it as faithfully as possible in order to harmonise national legislation with international legislation and to avoid confusing certain terms or situations described in the legal rules adopted. In addition, in close connection with the legislation, we believe that regular training of magistrates and investigators in this field, as well as in the economic field, is advisable, since practice has shown that in most cases, starting from the first level—police officers and prosecutors do not really know where to start an investigation into a cybercrime.

Intensifying Cooperation Between Public Bodies Responsible for Preventing and Combating Cybercrime One aspect of this measure would be to increase the number of people involved in the investigation of cybercrime and to organise joint internships involving staff from different public structures or authorities, with the aim of forming inter-specialised teams that can cooperate effectively in future joint actions (cyber-data collection, searches, etc.). Due to the volatility of the data, electronic evidence collection is very difficult and requires a lot of expertise.

Therefore, judicial cooperation is essential to secure and preserve electronic data/evidence in a timely manner, ensuring its admissibility in judicial proceedings. Thus, an effective response to cybercrime requires multi-level cooperation within specific national and cross-border institutions.

Cooperation Between Public Authorities and Members of Civil Society It is very important to inform the citizens of each country about the dangers they face when using the Internet or their personal account and about the protection methods available to them to avoid becoming victims. The existence of and cooperation between various institutions specialised in this field at home and abroad ensures a high level of protection against cyberattacks, whether by small, medium-sized, or large companies or by ordinary citizens (personal card cloning). We believe that long-term cooperation should be developed between members of civil society and representatives of the authorities, resulting in the drafting of guidelines containing useful information for specific target groups who are aware that it is only a step away from becoming victims of cybercrime. Therefore, a stronger cybersecurity response to build an open and secure cyberspace can increase citizens' trust in digital tools and services (UKNCSC, 2017).

As far as the business environment is concerned, prevention measures on cybercrime could be the following: (1) educating employees; (2) implementing privileged access by company management; (3) monitoring, detection and response; (4) managing third-party risk; (5) reporting the incident to the relevant authority; (6) cleaning up affected systems; (7) getting the business back up and running as soon as possible; and (8) using antivirus software (CPST, 2021).

Employee Education Employee cybersecurity training is based on a strategy implemented by IT and cybersecurity professionals to prevent and mitigate the risk of organisational information compromise. These trainings are specifically designed to provide employees with clarity on their information security responsibilities. Awareness of the need for cybersecurity by all company employees helps them understand the security risks associated with their actions and identify potential cyberattacks they may encounter on a daily basis in their operations.

Implement Privileged Access by Company Management This refers to the technologies and strategies that business organisations use to manage privileged access and permissions of users, accounts, processes, and systems in an IT environment. By strategically assigning employees the level of access based on their role and responsibility within the company, the risk of extensive damage from a cyberattack is effectively mitigated, whether from an external perpetrator or due to internal failure (McAfee, 2017).

Monitoring, Detection, and Response Companies must monitor their systems and networks around the clock to ensure there is no suspicious activity that could indicate a fraudulent attack or breach. Lack of continuous monitoring of the IT system can lead to a delay in detecting that an attack is underway and the business of the company in question may not be able to be protected in time, prevented or the negative impact minimised.

Third-Party Risk Management This preventive measure addresses the potential threat posed to employees and customer data, financial information and related operations, and product and/or service providers who have access to the company's system. Each must have an appropriate data and information security policy in place that must be monitored and managed as effectively as possible.

Reporting the Incident to the Competent Authority Various cybercrime agencies can advise you on appropriate cybersecurity measures and help you respond to incidents or assist in the identification and prosecution of offenders if you have suffered financial loss or have been hacked as a result of responding to a phishing message; if an email has been received that you are unsure of, it is forwarded to the Reporting Service—National Crime Agency who will investigate it as a matter of priority. Online reporting is quick and easy and can be done from any device. Companies, charities, and other organisations experiencing a live cyberattack (one that is ongoing) can use the 24/7 reporting service (service available to companies 24 h a day, 7 days a week).

Cleaning the Affected Systems In the business world, computers have become an increasingly intimate part of economic entities, with information being one of the most valuable assets of companies, alongside capital and people. Worldwide, much has been written about the security aspects of information systems, but very little has been done to translate what has been written into practice. Information systems security is seen as more of a human problem than a technical one. In today's context, where four new threats appear in cyberspace every second, information systems security must be dealt with dynamically and constantly reassessed in light of the threats. Continuous threat analysis identifies, addresses, and mitigates risks, with specific security procedures and mechanisms established by experts in the field to ensure an acceptable level of security. Without the help of malicious software removal tools, eliminating a computer virus or spyware can be quite difficult. Some computer viruses or malicious software reinstall after viruses and spyware have been detected and removed, and it is recommended to install the latest updates from Microsoft Update, use the security scan to help remove potential threats identified on your computer, use the Windows tool to remove malicious software from your computer, run Microsoft Defender offline, etc.

Getting Your Business Back Up and Running as soon as Possible For any kind of business, the big challenge is secure management of applications and data, they are everything in the business world as they help the top management of organisations to make informed decisions, identify new opportunities and choose their customers. If spread across multiple systems all this data is difficult to manage, but with rigorous data management the potential dangers that can arise are greatly diminished. In the event of computer systems being affected by viruses or malicious software, in order to get the business back up and running as quickly as possible, companies providing specialised services in this field can be called in, which, after cleaning up computer systems, can significantly reduce the risks of reinfection or

cyberattacks by recommending the use of products for backing up and recovering important data and information and installing the latest antivirus software.

Using Antivirus Software Antivirus and anti-malware software are extremely important, and the most popular phone security applications can be found in app stores. Make sure you keep this software up to date and run regular security scans. Delete, uninstall, or quarantine anything that should not be on your device. Without claiming to be exhaustive of cybercrime prevention measures, the above are just a few examples of initiatives companies can take to increase their cybersecurity and reduce the chance of falling prey to a cyberattack or cyberbreach.

By presenting the results obtained and making comparisons with similar studies of IT and business specialists, we believe that the fourth objective of our research, namely to present the main ways to fight cybercrime in the business environment, has been achieved.

5 Conclusions, Limitations, and Future Research Directions

5.1 Conclusions

Along with the digital evolution, there has also been an increase in cyberattacks on companies and organisations around the world, which is why we believe that it is essential to implement increased security measures and to increase the responsibility of people using IT technology. Harmonisation of cybercrime legislation and international cooperation are becoming evident, but these come with increased demands for additional resources (data collection) for investigation and capacity building, especially within developing countries.

Improving the *Mutual Legal Assistance Treaty* (MLAT) which allows one government to request the assistance of another government in investigating cybercrime or obtaining evidence is also recommended as an effective measure in combating cybercrime. The management of cybercrime problems is becoming difficult to quantify due to their transnational nature and the complexity of the technologies affecting evidence collection. Accounting for cybercrime activities is essential in the digital age and is an effective tool for governments to systematically provide nations with information to help combat cybercrime and the costs of investigating and eliminating it.

Another effective measure would be to improve and coordinate cybersecurity requirements especially in the business sector but also standardisation related to Big Data threats. Imposing tough sanctions against countries that do not align themselves in the fight against cybercrime and imposing harsh punishments on those who violate cybercrime conventions and treaties is another measure that would help fight cybercrime globally.

5.2 Limitations and Future Research Directions

With the information presented, our research is limited only to the analysis and synthesis of the main aspects of cybercrime and its fight in the business environment. The tools used were aimed only at identifying and bringing to the forefront the causes of cybercrime, the effects they produce and the measures to combat this phenomenon in the business environment (in organisations, companies, entities, etc.). In order to broaden the scope of research on the proposed topic, we launch several future research directions by conducting a bibliometric analysis of the phenomenon of cybercrime and the causes and effects produced by it, analysing the involvement of specialised bodies in combating this phenomenon worldwide, etc.

References

Akdemir, N., Sungur, B., & Başaranel, B. U. (2020). Examining the challenges of policing economic cybercrime in the UK. Güvenlik Bilimleri Derg. (Int. Secur. Congr. Spec. Issue), Özel Sayı, (pp. 113–134).

Akhtar, N., & Perwej, Y. (2020). The internet of nano things (IoNT) existing state and future prospects, for published in the GSC. *Advanced Research and Reviews, 5*(2), 131–150.

Alecu, I., Ciuchi, C., Cîmpeanu, T., Coman, I., Găbudeanu, Larisa, Mihai, I.-C., Moghior, C., Munteanu, N., Petrică, G., Stoica, I., & Zeţu C. (2021). Ghid de securitate cibernetică, Retrieved from: https://www.cyberlearning.ro/documents/Ghid-securitate-cibernetica.pdf.

Appiah, K. A. (2021). The prophet of maximum productivity. *New York Review of Books, 14*, 51–54.

Black, A., Lumsden, K., & Hadlington, L. (2019). Why don't you block them? Police officers' constructions of the ideal victim when responding to reports of interpersonal cybercrime. In K. Lumsden & E. Harmer (Eds.), *Online othering: Exploring violence and discrimination on the Web* (pp. 355–378). Palgrave Macmillan.

Broadhead, S. (2018). The contemporary cybercrime ecosystem: A multi-disciplinary overview of the state of affairs and developments. *Computer Law and Security Review, 34*, 1180–1196.

Camic, C. (2020). *Veblen: The making of an economist who unmade economics*. Harvard University Press.

Chen, P., Desmet, L., & Huygens, C. (2014). A study on advanced persistent threats. In *IFIP international conference on communications and multimedia security* (pp. 63–72). Springer.

Christensen, J. (2015). On her majesty's secrecy service. In D. Whyte (Ed.), *How corrupt is Britain?* Pluto.

Clark, R., Reed, J., & Sunderland, T. (2018). Bridging funding gaps: Pitfalls, progress and potential private finance. *Land Use Policy, 71*, 335–346.

Collin, B. (1996). *The future of cyber terrorism, proceedings of 11th annual international symposium on criminal justice issues*. The University of Illinois at Chicago.

Council of Europe. (2001). Convention on Cybercrime; European Treaty Series No. 185 (pp. 1–25); Council of Europe: Budapest, Hungary. Available online: https://rm.coe.int/1680081561 (Accessed on 16 October 2022).

Commission of the European Communities. (2007). Communication from the Commission to the European Parliament, the Council and the Committee of the Regions: Towards a general policy on the fight against cyber crime (vol 267); Commission of the European Communities: Brussels, Belgium.

Check Point Software Technologies Ltd. (CPST). (2021). Cele mai mari provocări de securitate în cloud din 2021. Retrieved from: https://www.checkpoint.com/cyber-hub/cloud-security/what-is-cloud-native-security/the-biggest-cloud -provocări-securitate-în-2021/.

Krazytech. (2022). Accessed on September 22, 2022. Retrieved from https://krazytech.com/technical-papers/cyber-crime

Dewar, R. (2014). The triptych of cyber security: A classification of active cyber defense'. 6th international conference on cyber security (pp. 7–21), NATO CCD COE Publications, Tallinn.

Donalds, C., & Osei-Bryson, K. M. (2019). Toward a cybercrime classification ontology: A knowledge-based approach. *Computers in Human Behavior, 92*, 403–418.

Dunn-Cavelty, M. (2010). Cyber security. In A. Collins (Ed.), *Contemporary security studies*. OUP.

European Commission. (2013). Joint communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions. Cybersecurity strategy of the European Union: An open, safe and secure cyberspace; European Commission: Brussels, Belgium.

Faysel, M. A., & Haque, S. S. (2010). Towards cyber defense: Research in intrusion detection and intrusion prevention systems. *IJCSNS International Journal of Computer Science and Network Security, 10*(7), 316–325.

Garfinkel, S. L. (2010). Digital forensics research: The next 10 years. *Digital Investigation, 7*(supplement), S64–S73.

Global Witness. (2021). The true price of palm oil: How global finance funds deforestation, violence and human rights abuses in Papua New Guinea, www.globalwitness.org/en/campaigns/fores ts/true-price- palm-oil/

Gordon, S., & Ford, R. (2006). On the definition and classification of cybercrime. *Journal in Computer Virology, 2*, 13–20.

Guo, H., Jin, B., & Huang, D. (2010). Research and review on computer forensics, forensics in telecommunications, information, and multimedia, international conference on forensics in telecommunications, information, and multimedia (pp. 224–233).

Halder, D., & Jaishankar, K. (2011). *Cyber crime and the victimization of women: Laws, rights and regulations*. IGI-Global.

Hatole, P. P., & Bawiskar, D. S. K. (2017). Literature review of email forensics. *Imperial Journal of Interdisciplinary Research, 3*(4).

Iqbal, J., & Beigh, B. M. (2017). Cybercrime in India: Trends and challenges. *International Journal of Innovations & Advancement in Computer Science, 6*(12), 187–196.

Jensen, M., Schwenk, J., Gruschka, N., & Iacono, L. L. (2009). On technical security issues in cloud, IEEE 2009 international conference on cloud computing (pp. 109–116), IEEE, 21–25 September 2009.

Jin, X., Sun, W., Liang, Y., Guo, J., & Xie, Z. (2011). Design and implementation of intranet safety monitoring platform for power secondary system. *Automation of Electric Power Systems, 35*(16), 99–104.

Kamruzzaman, M., Ashraful Islam, M., Shahidul Islam, M., Shakhawat Hossain, M., & Abdul Hakim, M. (2016). Plight of youth perception on cyber crime in South Asia. *American Journal of Information Science and Computer Engineering, 2*(4), 22–28.

Kaur, M., Kaur, N., & Khurana, S. (2016). A literature review on cyber forensic and its analysis tools. *International Journal of Advanced Research in Computer and Communication Engineering, 5*(1), 23–28.

Kowtha, S., Nolan, L. A., & Daley, R. A. (2012). Cyber security operations center characterization model and analysis, IEEE conference on technologies for Homeland security (HST) (pp. 470–475).

Krishna Viraja, V., & Purandare, P. (2021). A qualitative research on the impact and challenges of cybercrimes. *Journal of Physics: Conference Series, 1964*, 042004.

Krombholz, K., Hobel, H., Huber, M., & Weippl, E. (2015). Advanced social engineering attacks. *Journal of Information Security and applications, 22*, 113–122.

Krugman, P. (2020). *Arguing with zombies*. W.W. Norton & Company.
Kumar Goutam, R., & Kumar Verma, D. (2015). Top five cyber frauds. *International Journal of Computer Applications, 119*(7), 23–25.
Le Compte, A., Elizondo, D., & Watson, T. (2015). A renewed approach to serious games for cyber security, 7th international conference on cyber conflict: Architectures in cyberspace, IEEE (pp. 203–216), 26–29 May 2015.
Leukfeldt, E. R., Kleemans, E. R., Kruisbergen, E. W., & Roks, R. A. (2019). Criminal networks in a digitized world: On the nexus of borderless opportunities and local embeddedness. *Trends in Organized Crime, 22*(3), 324–345.
Mativat, F., & Tremblay, P. (1997). Counterfeiting credit cards. *British Journal of Criminology, 37*(2), 165–183.
McAfee. (2017). Economic Impact of Cybercrime-No Slowing Down. Retrieved from: https://www.mcafee.com/enterprise/en-us/assets/executive-summaries/es-economic-impact-cybercrime.pdf.
McGuire, M. (2020). It ain't what it is, it's the way that they do it? Why we still don't understand cybercrime. In R. Leukfeldt & T. J. Holt (Eds.), *The human factor of cybercrime* (pp. 3–28). Routledge.
Mirkovic, J., Dietrich, S., Dittrich, D., & Reiher, P. (2004). Internet denial of service attack and defense mechanisms. Pearson education: The Radia Pertman series in computer networking and security. Retrieved from https://books.google.com/books?isbn=0132704544.
Mostafa, A. A. N. (2022). Cyber crime in business: Review paper. *International Journal of Academic Research in Business and Social Sciences., 12*(6), 962–972.
Mshana, J. A. (2015). Cybercrime: An empirical study of its impact in the society—a case study of Tanzania, Huria. *Journal of the Open University of Tanzania, 19*(1), 72–87.
Nesvetailova, A., & Palan, R. (2013). Sabotage in the financial system: Lessons from Veblen. *Business Horizons, 56*, 723–732.
OECD (Organization for Economic Cooperation and Development). (2021). The momentum around sustainable finance taxonomies, OECD. https://www.oecd-ilibrary.org/sites/235eb800-en/index.html?itemId=/content/component/235eb800-en.
Ong, Y. J., Qiao, M., Routray, R., & Raphael, R. (2017). Context-aware data loss prevention for cloud storage services, 2017 IEEE 10th international conference on CLOUD computing (CLOUD), IEEE, 25–30 June 2017.
Paoli, L., Visschers, J., Verstraete, C., & Van Hellemont, E. (2018). *The impact of cybercrime on Belgian businesses*. Cambridge.
Parwej, F., Akhtar, N., & Perwej, Y. (2019). An empirical analysis of web of things (WoT). *International Journal of Advanced Research in Computer Science, 10*(3), 32–40.
Pasqualetti, F., Dorfler, F., & Bullo, F. (2013). Attack detection and identification in cyber-physical systems. *IEEE Transactions on Automatic Control, 58*(11), 2715–2729.
Pathak, P. B. (2016). Cybercrime: A global threat to cybercommunity. *Ijcset.Com, 7*(3), 46–49.
Pawar, S. C., Mente, R. S., & Chendage, B. D. (2021). Cyber crime, cyber space and effects of cyber crime. *International Journal of Scientific Research in Computer Science, Engineering and Information Technology, 7*(1), 210–214.
Perwej, Y. (2018a). The ambient scrutinize of scheduling algorithms in big data territory. *International Journal of Advanced Research, 6*(3), 241–258.
Perwej, Y. (2018b). A pervasive review of Blockchain technology and its potential applications. *Open Science Journal of Electrical and Electronic Engineering, New York, USA, 5*(4), 30–43.
Perwej, Y., Hannan, S. A., Parwej, F., & Nikhat Akhtar, N. (2014). A posteriori perusal of mobile computing. *International Journal of Computer Applications Technology and Research, 3*(9), 569–578.
Perwej, Y., Kerim, B., Adrees, M. S., & Sheta, O. E. (2017). An empirical exploration of the yarn in big data. *International Journal of Applied Information Systems, Foundation of Computer Science FCS, New York, USA, 12*(9), 19–29.

Perwej, Y., Nikhat Akhtar, N., & Parwej, F. (2018). A technological perspective of Blockchain security. *International Journal of Recent Scientific Research, 9*(11A), 29472–29493.

Perwej, Y., Haq, K., Parwej, F., & Mohamed Hassan, M. M. (2019a). The internet of things (IoT) and its application domains. *International Journal of Computer Applications (IJCA) USA, 182*(49), 36–49.

Perwej, A., Haq, K., & Perwej, Y. (2019b). Blockchain and its influence on market. *International Journal of Computer Science Trends and Technology, 7*(5), 82–91.

Phillips, K., Davidson, J. C., Farr, R. R., Burkhardt, C., Caneppele, S., & Aiken, M. P. (2022). Conceptualizing cybercrime: Definitions, typologies and taxonomies. *Forensic Sciences, 2*(2), 379–398.

Ponemon Institute. (2012). The impact of cybercrime on business. Studies of IT practitioners in the United States, United Kingdom, Germany, Hong Kong and Brazil. Retrieved October 16, 2022 from https://www.ponemon.org/local/.../Impact_of_Cybercrime_on_Business_FINAL.pdf

Ruggiero, V. (2017a). *Dirty money*. Oxford University Press.

Ruggiero, V. (2017b). Networks of greed. *Justice, Power and Resistance, 1*, 3–23.

Ruggiero, V. (2020). Killing environmental campaigners. *Criminological Encounters, 3*(1), 92–105.

Ruggiero, V. (2022). Sustainability and financial crime. *International Criminology, 2*, 143–151.

Sarre, R., Lau, L. Y. C., & Chang, L. Y. (2018). Responding to cybercrime: Current trends. *Police Practice and Research, 19*, 515–518.

Sachdeva, S., Raina, B. L., & Sharma, A. (2020). Analysis of digital forensic tools. *Journal of Computational and Theoretical Nanoscience, 17*(6), 2459–2467.

Schiller, C., & Binkley, J. R. (2007). *Botnets: The killer web applications* (1st ed.) Syngress.

Shui, Y. (2013). Distributed denial of service attack and defense. Chapter 1, (pp. 1–5). Springer brief in computer science. Springer.com: Google Books online. Retrieved from October 24, 2022, https://books.google.com.tr/books?isbn=1461494915.

Simou, S., Kalloniatis, C., Kavakli, E., & Gritzalis, S. (2014). Cloud forensics solutions: A review. *Advanced Information Systems Engineering Workshops*, 299–309.

Stallings, W. (2014). Cryptography and network security: Principles and practice, International Edition: Principles and Practice. Pearson Higher Ed.

Tan, Z., Jamdagni, A., He, X., Nanda, P., & Liu, R. P. (2014). A system for denial-of-service attack detection based on multivariate correlation analysis. *IEEE Transactions on Parallel and Distributed Systems, 25*(2), 447–456.

Teelink, S., & Erbacher, R. (2006). Improving the computer forensic analysis process through visualization. *Communications of the ACM, 49*(2), 71–75.

Tsakalidis, G., & Vergidis, K. (2017). A systematic approach toward description and classification of cybercrime incidents. *IEEE Transactions on Systems, Man, and Cybernetics Systems, 49*, 710–729.

UN. (2017). Work of the statistical commission pertaining to the 2030 agenda for sustainable development, Resolution Adopted by the General Assembly on 6 July, UN.

United Kingdom National Cyber Security Centre (UKNCSC). (2017). Cyber crime: Understanding the online business model, Report. https://www.ncsc.gov.uk/content/files/protected_files/news_files/Cyber% 20crime%20-%20understabnding%20the%20online%20business%20model.pdf

Viano, E. C. (2017). Cybercrime: Definition, typology, and criminalization. In E. C. Viano (Ed.), *Cybercrime, organized crime, and societal responses* (pp. 3–22). Springer.

Yar, M., & Steinmetz, K. F. (2019). *Cybercrime and society* (3rd ed.). SAGE Publications Ltd..

Yasin, I., Ahmad, N., & Chaudhary, M. A. (2021). The impact of financial development, political institutions and urbanization on environmental degradation. *Environment, Development and Sustainability, 23*, 6698–6721.

Zadek, S. (2018). Aligning the financial system with sustainable development. In N. Saab & A.-K. Sadik (Eds.), *Financing sustainable development in Arab countries*. Arab Forum for Environment and Development.

Sorinel Căpușneanu is a PhD. Professor at the *Titu Maiorescu*, Faculty of Economic Sciences. His research focus is the area of management accounting, management performance, management information systems, audit and controlling, and green supply chain management. He is the author of the following books: *Elements of Cost Management, Management Accounting. Performance Assessment Tool* and co-author of *Deontology and Accounting Expertise: Judicial Accounting and Tax Expertise,* and *Management Accounting Standards for Sustainable Business Practices*. He has participated in numerous national and international conferences and has made a remarkable contribution to managerial accounting by publishing several articles.

Dan Ioan Topor is a PhD. Professor at the *1 Decembrie 1918 University of Alba-Iulia, Faculty of Economic Sciences*. His research focus is the area of management accounting, management performance and management information systems, audit and controlling, and business ethics. He is the author of the following books: *New Dimensions of Cost-Related Cost Information for Winemaking* and *Basics of Accounting* and co-author of *Management Accounting Standards for Sustainable Business Practices* and *Deontology and Accounting Expertise. Judicial Accounting and Tax Expertise*. He has published numerous articles on managerial accounting and management control and has participated in numerous national and international conferences.

Ileana-Sorina Rakos is a PhD. Lecturer at the University of Petroșani, Faculty of Sciences, Department of Economic Science. Her research focus is the area of management accounting, holding financial management seminars for students at enterprise specialising in accounting, management, and finance. She is the author of the following books: Management and Cost Calculation, Financial Management of the Company, Public Procurement, and co-author of Cost Management. She has participated in numerous national and international conferences and has contributed to managerial accounting by publishing several articles and books.

Cristina-Otilia Țenovici is a PhD. Lecturer at Constantin Brâncoveanu University, Faculty Marketing Management in Economic Affairs. Her research focus is the area of public accounting, management accounting, management performance and management information systems. She is the author of the following books: Management Accounting, Fundamentals of Management Accounting and Costing, National and International in the Accounting of Public Institutions, and The Fundamentals of Accounting of Public Institutions. She has participated in numerous national and international conferences and has made an outstanding contribution to management accounting by publishing several articles and books.

Mihaela Ștefan Hint is a PhD. Associate Teaching Staff at the University of December 1, 1918, in Alba Iulia, Faculty of Economic Sciences. Her research focus is the area of management accounting, environmental management accounting, financial management, treasury and risk management, controlling, management performance, management information systems and control and environmental management analysis in the field of electrical equipment production lighting. She is the author of the following books: The Usefulness of Information Provided to Management Through Accounting and Management Control, The Quality of Customer Relations, as well as co-author of the works Management Accounting Standards for Sustainable Business Practices; Sustainability Reporting, Ethics, and Strategic Management Strategies for Modern Organizations; Environmental Management Accounting: A Business Perspective on the Policies, Analyzes and Benefits of its Implementation. She participated in several national and international conferences and had an important contribution to managerial accounting and environmental management by publishing several articles in the previously mentioned areas.

Chapter 8
Effects of Economic and Financial Crime on the Government Budget and the Quality of Public Services

Rita Remeikienė and Ligita Gaspareniene

Abstract The chapter analyses the impact of economic and financial crimes, such as money laundering, corruption, tax evasion, informal employment/entrepreneurship, cybercrime, illicit financial flows, on the state budget and the quality of public services, and what measures would help control the negative effects of the considered phenomena. The analysis of scientific literature leads to the conclusion that the use of digital technologies (artificial intelligence, cloud computing, interactive information sharing methods) at the control-state, control-enterprise, and control-society levels is seen as one of the solutions to reduce the volume of economic and financial crimes and increase the government budget revenue. E-government is one of the modern concepts, a new basis for the effective provision of public services to citizens and businesses. Modern ICTs improve the performance competence of public institutions, allow to establish particular compliance units that mediate the relationship between the government and society, and help achieve the required efficiency by ensuring cohesion among the structural components of the public service provision.

Keywords Money laundering · Cybercrime · Corruption · Shadow economy · Tax evasion · Informal employment · Fraud · Government budget · Public services

JEL Classification K42 · H30 · H41 · H50

1 Introduction

Actuality of the Topic: Tax revenue is the main financial resource of any state, supplementing the national government budget every year. The quality of public services also depends on how much tax revenue the state collects. The main factors that prevent the collection of planned funds into the budget are money laundering,

R. Remeikienė (✉) · L. Gaspareniene
Vilnius University, Law Faculty, Vilnius, Lithuania
e-mail: rita.remeikiene@tf.vu.lt; ligita.gaspareniene@tf.vu.lt

M. V. Achim (ed.), *Economic and Financial Crime, Sustainability and Good Governance*, Contributions to Finance and Accounting,
https://doi.org/10.1007/978-3-031-34082-6_8

corruption, tax evasion, the shadow economy, informal entrepreneurship, corporate frauds, illicit capital flows, cybercrime, and cryptocurrency scams. These factors reduce the government's ability to conduct sound economic policies and provide citizens with essential services and other resources.

Scientific Research Problem: Money laundering, as a financial crime, significantly reduces government tax revenue. This statement has been proven in many scientific studies such as McDowell (2001), Schwarz (2011), Aluko (2012), Conyers Dill and Pearman (2013), Abiahu et al. (2016), Hendriyetty and Grewal (2017), Abu-Orabi and Al Abbadi (2019), and Vitvitskiy et al. (2021).

It has been proved that the impact of money laundering has several directions: firstly, money laundering reduces the income of the national budget, and secondly, it is difficult to determine how much of that income is lost due to the illegal phenomenon of money laundering. Meanwhile, tax fraud and tax evasion are not common crimes associated with money laundering schemes. The reluctance of economic entities to pay taxes results in lower state revenues to the budget, which could be allocated to improving public infrastructure, increasing the quality of education and developing other public services. Consequently, the national state budget and public services for the population are interrelated; i.e., if tax revenues are not collected, the public welfare of the population suffers. The impact of tax evasion on the national government budget has been examined by Carvalho (2019), Dlamini and Dube (2020), Cooray et al. (2017), Argentiero and Cerqueti (2019), Levaggi and Menoncin (2020), Herranz and Turino (2022), and others. The impact of informal employment on the collection of the government budget and, at the same time, on the quality of public services is manifested through self-employment, when all received income is not declared, by paying only part of the taxes, or through informal new entrepreneurs who, although growing as a business, do not register or officially legalize their activities. The shadow economy not only increases the public debt, but also strengthens the effect of corruption on the growth of the public debt. In a general sense, corruption and the shadow economy interact as sets or substitutes, i.e., occur together or are mutually replacing phenomena. Corporate fraud occurs when national governments grant subsidies or tax breaks to businesses, but the latter then engage in financial fraud.

Technology and digitization have caused a revolution and transfered crime to e. space. The impact of cybercrime on national governments and the services they provide means that countries have to invest huge amounts of money in security and mitigating the threats of cyberattacks, resulting in reduced budgets.

The scientific problem is formulated as a question: what measures can be taken to reduce money laundering, corruption, shadow economy, tax evasion, informal employment, cybercrime, illicit financial flows on the government budget and the quality of public services?

The purpose of the chapter is to analyse the possible impact of illegal phenomena, such as money laundering, corruption, tax evasion, informal employment, cybercrime; also to investigate an illicit flows on the government budget and the quality of public services. In order to achieve the goal, a comparative and systematic analysis of the scientific literature will be carried out; the conclusions are presented

at the end of the chapter. The phenomena 'the government budget' and 'the quality of the services' are analysed together because they are highly dependent on each other.

2 Literature Review and Research Design

The negative/destructive impact of economic and financial crimes on national budgets is confirmed by the vast majority of previous studies. McDowell (2001), who analysed the social and economic effects of ***money laundering***, notes that money laundering significantly reduces government tax revenue. This means that it becomes more difficult for national governments to collect planned budget revenue. Mohasoa (2016) adds that the principle of taxation is to generate adequate government revenue that would be used to meet the socio-economic and political needs of the citizens. With insufficient tax revenue, a country's government is unable to perform its duties. Thus, budget revenue shortfalls are often followed by higher taxes, resulting in indirect damage to taxpayers. Undermining effects of illicit income, generated through money laundering, on government budgets were confirmed by Schwarz (2011), Aluko (2012), Conyers Dill and Pearman (2013), Abiahu et al. (2016), Hendriyetty and Grewal (2017), Abu-Orabi and Al Abbadi (2019), Vitvitskiy et al. (2021), and other researchers. For instance, Abiahu et al.'s (2016) empirical research confirmed that money laundering has a negative statistically significant impact on state budget revenue at a 5 per cent significance level. Hendriyetty and Grewal (2017) note that money laundering tends to reduce the national budget revenue due to tax evasion which is considered a major crime related to money laundering and stemming from it. According to Schwarz (2011), tax evasion is an additional offence which indicates that authorities do not cooperate or are not able to identify the real origin of money. Income without an established origin cannot be taxed because it is impossible to assign this income to a certain category of taxable income (e.g. individual income, corporate profit, income from transferred property). Abu-Orabi and Al Abbadi (2019) also note that, in addition to the direct negative effect on state budget revenue, money laundering also causes another indirect effect: it is difficult to measure how much revenue has been lost. This leads to inaccuracies in the national account statistics, as a result of which budget allocation and public policy mistakes can be made.

Tax frauds and tax evasion are not ordinary offences accompanying money laundering schemes. Payment of all or part of the taxes can be evaded by individuals (e.g., they can evade paying taxes on the income received from the sale of certain assets), persons working with employment contracts, the self-employed, business enterprises, and other economic entities. For instance, Ozili (2018) observes that trying to evade taxes, larger business companies can divert funds through other channels, thus disguising their profits, while individuals can either abuse the status of a self-employed or manipulate their refundable tax credits. According to Tanzi and Shome (1993), Slemrod (2007), Mukah and Fossung (2019), Andronicean u et al.

(2019), Dlamini and Dube (2020), Rashid (2020), and many others, tax evasion causes difficulties in financing the state budget; i.e., it reduces the budget revenue, which leads to a fiscal deficit, to cover which national governments can either increase tax levels (especially for purposefully selected groups of economic entities) (Yamamura, 2014; Ukaj, 2014; Kassa, 2021, etc.) or are forced to borrow money in international financial markets, which raises public debt level and vulnerability of the economy (Cooray et al., 2017; Argentiero & Cerqueti, 2019; Levaggi & Menoncin, 2020; Herranz & Turino, 2022, etc.). Tanzi and Shome (1993) argue that tax evasion has a negative impact on productivity of the taxation system since it reduces the amount of revenue that can be collected given the current statutory system. According to Ozili (2018), tax evasion diminishes the government's capability of affecting the economy through necessary interventions because due to tax evasion national governments face a lack of funds to carry out smooth economic policies and provide citizens with essential products and services. On the contrary, having a budget surplus, national governments can stabilize and strengthen a country's financial system during the period of an economic recession or after an economic shock (by correcting financial imbalances). In the case of a budget deficit, caused by tax evasion, the potential of the relevant intervention is lost.

Carvalho (2019), who researched the economic effects of tax evasion by applying a stochastic growth model approach in discrete time, confirmed that tax evasion has a negative impact on the government budget because tax revenue is the major financial resource available to any state. Thus, unwillingness of economic agents to pay taxes leads to lower government revenue which can be spent on developing public infrastructure, education, and other public services, as well as lower public input. It may also lead to the introduction of higher tax rates, which, in their turn, reduce the real income of economic agents and households. On the other hand, it is noted that tax evasion tends to raise the real income available to economic agents. Therefore, when public spending and private capital are substitutes in productive sectors, private economic agents can use the tax evaded to make private domestic investment, which, in its turn, may help to mitigate the negative effects of tax evasion on public spending in terms of promoting productivity. At the same time, the author emphasizes that the gap between actual payments and the legally required obligation (the tax gap) is not equal to the government revenue that could be collected by imposing stricter taxation conditions. On the contrary, the net revenue collected in the budget may even decrease. Therefore, any marginal measures should be applied with caution. Dlamini and Dube (2020) note that it is necessary to raise taxpayers' education and awareness, provide tax benefits to those who obey tax regulations, and simplify the taxation system.

Rysin and Antoshchuk (2021) researched the effects of ***informal employment*** on state budget revenue. They considered the situation in Ukraine during the 2014–2020 period. The authors found that Ukraine's consolidated budget deficit in 2020 increased almost threefold compared to 2019, and this deficit was caused not by unplanned state expenditure which was needed to manage the COVID-19 pandemic, but by the quarantine restrictions that stimulated informal employment of the population to retain at least part of their previous income. The empirical

research revealed that the budget losses from personal income tax from wages accounted for 16.23 billion hryvnias in the total budget deficit of 72.03 billion hryvnias in 2014, while in 2020 the budget losses from personal income tax from wages accounted for 55.05 billion hryvnias in the total budget deficit of 223.94 billion hryvnias, i.e. about 22.53 and 24.58 per cent in 2014 and 2020, respectively. Although it is recognized that informal employment is only one of the factors determining the budget deficit (money laundering, corruption, and the shadow economy are other significant factors), it is believed that by transferring a substantial number of informally employed workers to the formal sector, it is possible to significantly increase the state budget revenue. Di Porto et al. (2017) argue that informal work is a concern of not only developing, but also developed countries because underreporting of income means lower state and municipal budget revenue. The results of their research in the markets of France, Italy, and Spain show that the measures, such as lower payroll taxes for permanent contracts and higher inspection rate for businesses operating in the informal sector, are effective when trying to normalize tax revenue collection. The Policy Brief on Informal Entrepreneurship provided by the European Commission and the OECD (2015) proposes that informal entrepreneurship, which covers informal self-employment and informally operating new entrepreneurs, is a substantial component of the shadow economy. It is more common in Southern Europe and is limited to occasional activities in Nordic countries. The report confirms that informal entrepreneurship leads to reduction in government revenue and thus saps traditional governmental duties to promote economic development and effective social policies. The latter outcome harms the most vulnerable groups of society that are most likely to engage in informal activities. The government also loses control over working conditions, and the quality of public services is likely to decrease. The above-mentioned Policy Brief puts forward the idea that informal entrepreneurship can be undertaken to help new businesses establish themselves in the market, but in the long run, the businesses are regularized and transferred to the formal sector. Thus, the policy of the iron fist is not the policy that can be proposed to fight against informal entrepreneurship. In most cases, control as a measure of deterrence is combined with regularization that promotes business development.

Rachmawati (2014) focused on the impact of the activities in the informal sector (specifically, self-employed street vendors) on local government revenue. The capability of earning their own revenue is extremely important for decentralized local governments, since the more independent revenue is collected in the municipal budget, the less dependent on funding allocations from the national budget municipalities are (national funding usually depends on the size of the area and population) and the more autonomy they have. Thus, local governments must efficiently use their resources and apply rational taxation policies. The results of the empirical study in Indonesia (Rachmawati, 2014) disclosed that the amount of IDR 208,250,000 can be collected from informal entrepreneurs in the Surakarta city regional budget. The funds allocated from the regional budget for managing informal entrepreneurship are treated as an investment that is expected to bring benefits in the future, when the regional budget is likely to be balanced after collecting taxes from informal

entrepreneurship which will gradually transfer to formal entrepreneurship. It is, however, noticed that raising taxes in the countries characterized by a large informal entrepreneurship sector can only induce tax non-compliance. This will reduce the government and municipal budget revenue, and thus, the funds that could be allocated for providing public goods and services as well as market support.

Ozekicioglu and Tulumce (2020) researched the effects of ***corruption*** on budget balance and public debt in Turkey by applying Johansen cointegration, vector autoregressive model (VAR), and Granger causality methods in the period 1995–2019. They state that corruption is a factor that tends to unbalance the state budget, reduce tax revenue, lead to inefficient state expenditure, and therefore change the structure of public expenditure. When it comes to state expenditure, both economic and functional expenditures are meant. Economic expenditures refer to investment costs. For instance, if the state is characterized by a high level of corruption, investment will not be allocated to economically efficient projects, but to those projects that were 'pushed' by bribing civil servants and officials or promising a share of the income generated by a specific project. This leads to lower investment efficiency (Shleifer & Vishny, 1993; Mauro, 1996; Tanzi & Davoodi, 1998; Everhart et al., 2009). Functional expenditures refer to the expenditures for health care, social security, education, environmental protection, etc. When the level of corruption is high, a part of the expenditures intended for the aforementioned needs are embezzled, and the invoices indicate higher prices of goods and services than the actual purchase prices. In this way, the real expenditures intended for the development of the public sector are lower. Mauro (1996) provides evidence that corruption tends to reduce education funding, while Delavallade (2006) argues that the education and health and social security sectors are those most affected by corruption. Hessami (2014) empirically confirms the decline in allocation of funds to the healthcare sector and a weak but positive relationship between corruption and protection of the environment. Knight et al. (1996) propose that corruption tends to reduce military and defence expenditure, but Gupta et al. (2001) argue that when a country's government is the only provider of defence services, corruption can be associated with higher military expenditure as a share of GDP. Delavallade (2006) and Hessami (2014) confirm an increase in military expenditure determined by corruption. Delavallade (2006) also provides the results suggesting that fuel, energy, and culture expenditure may increase as well.

When assessing the impact of corruption on the government tax revenue, the literature provides evidence that a high level of corruption tends to reduce budget tax revenue as percentage of GDP (Ghura, 1998; Hwang, 2002). Hwang (2002) points out that corruption reduces government tax revenue by stimulating tax evasion, tax exemptions, and inadequate/inefficient tax administration. It is also noted that corruption negatively affects not only direct income (profit) taxes levied on private individuals and companies, but also indirect taxes, such as VAT, turnover tax, and sales tax. Yikona (2011) researched the distortive effects of corruption and tax evasion in developing countries (Malawi and Namibia) and found that if the governments of these countries were to successfully collect the taxes lost because of the aforementioned types of financial crimes, the government budget revenue would

increase by 50 per cent. Malawi receives approximately this amount of foreign aid; i.e., if the taxes hidden as a result of economic and financial crimes were collected, developing countries like Malawi would not be so dependent on foreign aid. The research also revealed that in Namibia, corruption and tax evasion divert from the national budget towards private spending, and this private spending, in its turn, has a much smaller multiplier effect compared to state budget expenditure on infrastructure, health care, agricultural development, education, etc. Hence, corruption leads to a decrease in state budget revenue due to a decrease in the share of collected domestic taxes (Hillman, 2004), although the share of international taxes in total budget tax revenue tends to increase. Hwang (2002) found a statistically significant negative correlation between domestic tax revenue and GDP, while the correlation between corruption indices and international tax revenue was found to be statistically significant and positive. The growth of the budget deficit, in its turn, tends to increase the public debt. The results of Ozekicioglu and Tulumce's (2020) study showed that budget deficit and corruption affect each other, although causality running from budget deficit and public debt to corruption is also observed. Having conducted the panel data analysis in 166 countries worldwide, Benfratello et al. (2015) found that corruption tends to raise the public debt and thus leads to an increase in the public debt stock-to-GDP ratio. Similar results were provided by Cooray et al. (2017), who conducted the analysis in 126 countries. Thus, as stated by Myint (2000), corruption distorts the balance of the government budget both through reducing budget revenue and changing the structure of public expenditure. Puron-Cid (2021) concludes that corruption is a structural phenomenon that negatively affects financial sustainability of national governments by diminishing their ability to consistently meet financial obligations and continue to provide public services and infrastructure.

Surprisingly, Guillamon et al.'s (2021) research, focused on the effects of political corruption on municipal tax revenue in Spanish municipalities with a population of over 50,000 inhabitants over the period 2002–2013, provided the result showing that the municipalities with higher levels of corruption tend to have higher tax revenues per capita. A possible explanation for this result is that more corrupt municipalities are characterized by a higher level of public spending, so municipalities need greater revenue to fund their expenditure. A positive relationship between corruption and tax revenue was also found by Liu and Mikesell (2019) who conclude that the countries with a higher level of corruption usually have a complex tax system that is designed to create a fiscal illusion that the government is able to collect larger tax revenue. Moreover, it is observed that greater tax revenue can be collected during economic upturns. In the latter case, even if a country's government is corrupt, the level of taxes collected in the budget will increase (Guillamon et al., 2021).

Cooray et al. (2017), who researched the relationship between ***the shadow economy*** and public debt in 126 countries worldwide, confirm that the shadow economy not only leads to an increase in public debt, but also enhances the effect of corruption on the growth of public debt. By applying the Bayesian estimation, Herranz and Turino (2022) provided the evidence that a sizeable informal sector with

the associated tax evasion contributed, on average, to 23 per cent of public debt accumulation in Spain over the 1985–2015 period. Cooray et al. (2017) and Fedajev et al. (2022) provide the empirical evidence that the shadow economy tends to reduce budget tax revenue; i.e., the size of the shadow economy directly affects the level of tax revenue collected in the budget. Analysing the case of Ukraine, Mishchuk et al. (2020), who focused on the economic losses from reduction in the government tax revenue, came to the same conclusion. The relationship between the shadow economy and declining budget revenue was also confirmed by Enste (2018) who states that the shadow economy diminishes tax morale and loyalty of citizens to the national government. All this results in reduced government revenue and higher control costs which also distort the government budget balance. According to Hassan (2017), a shrinking tax base tends to reduce the government budget revenue, thus creating a vicious cycle of an inefficient tax rate increase. At the same time, when the government revenue is decreasing, the informal economy is reducing government spending and thus limits the capacity of the national government to effectively financing the public sector and providing public goods and services. Thus, the shadow economy erodes the tax base as well as viability of the social security system, which leads to a further increase in the budget deficit or to higher tax rates, deterioration of the public finance and investment (Schneider et al., 2010), and gradual weakening of the foundations of the social contract between the government and society (Enste, 2018).

Reduction of tax burden is believed to contribute to formalizing the largest possible part of the shadow economy and is, therefore, proposed as one of the measures to raise the government budget revenue. Arsic and Krstic's (2015) estimations indicate that if the VAT gap was reduced by 2–3 percentage points, it would help to increase the Serbian budget revenue by 0.2–0.5% of GDP. The share of VAT collected to the state budget is considered the largest, while the potential of the overall personal income tax and social contributions to generate additional public revenue is considered to be far lower. Taking into account the fact that the shadow economy and corruption contribute in parallel to the decline of tax revenue and the growth of public debt, Cooray et al. (2017) conclude that anti-corruption measures can help reduce the shadow economy and public debt, thus having a positive impact on the government budget balance.

On the other hand, the shadow economy (i.e. the informal economic sector which covers home production, petty trading, and wage employment such as casual labour, contract labour, and piecework and which includes many small competitive firms, petty retail and services, labour-intensive methods, free entry, and market-determined production factor and product prices (Gallaway & Bernasek, 2002)) that tends to reduce tax revenue in the state budget, thus diminishing the state's capacity to promote economic and social development, offsets the above-mentioned losses by providing the poorest and most marginalized people with opportunities to earn independent income (Rachmawati, 2014). Although this attitude is not considered ideological, it is recognized as pragmatic and is in line with the arguments suggesting that the informal economy provides a degree of security for the population in case of the diminished state support (Gallaway & Bernasek, 2002).

Raghunandan (2016) analysed the relationship between ***corporate fraud*** and government subsidies. The author focuses on the problem when national governments allocate subsidies or provide tax benefits to business companies, but the latter after some time are caught engaged in financial frauds. The research revealed that the companies that receive government subsidies or are provided tax incentives (i.e. when subsidies are raising public expenditure and tax incentives are reducing the government budget revenue) are more likely to engage in fraudulent activities and are less likely to be caught by public authorities and third parties (analysts, investors, media representatives). The estimations indicate that the probability of business companies receiving any type of subsidies to engage in fraudulent activities is 2.1 per cent higher (the research assumes that an average business company is not usually subsidized). When the government support is decreasing, the probability of corporate fraud is decreasing as well. Conversely, business companies that receive direct cash grants (i.e. when public expenditure is increasing) are less likely to engage in corporate frauds compared to those companies that do not receive direct cash grants. Thus, the results of Raghunandan's (2016) research propose that corporate fraud has a negative impact on the government budget because there is a possibility that the funds allocated to businesses through subsidies and tax incentives will be used fraudulently, which will lead to an inappropriate increase in public expenditure and a decrease in the government budget revenue. In accordance with the estimations provided by The Commonwealth Fraud Prevention Centre (2020), the losses suffered by government entities because of fraud amount to 0.5–5 per cent of their spending. A substantial part of frauds remain undetected and are difficult to categorize. The estimations provided by Crivelli et al. (2015) and Cobham and Jansky (2017) propose that corporate frauds through tax heavens cost governments between $500 and $600 billion of lost tax revenue every year; on average, developing economies lose about $200 billion of annual tax revenue more than advanced economies.

Highfield et al. (2018), Haron and Ayojimi (2019), and the OECD (2019) focused on the issues of collecting Goods and Services Tax (GST) and expressed their concerns about the rising trends of GST fraud worldwide. GST is recognized to widen the net of the government revenue that spans the entire economic chain, including the informal sector. Based on the estimations by the OECD (2019), more than 28 per cent of the economic growth in the Pacific region is financed through the GST tax. Losses of this tax caused by fraudulent business activities represent a sizeable loss in the government budget revenue. Othman et al. (2020) state that in the latter case, a decrease in the government budget revenue leads to a decrease in general consumption expenditure (composed of final consumption expenditure of households and final consumption expenditure of the government), which, in its turn, tends to reduce GDP and slow down economic growth.

The use of digital technologies at the control-state, control-enterprise, and control-society levels is seen as one of the solutions that can help reduce the volume of fraud and raise the government budget revenue (Volosovych & Baraniuk, 2019). Bierstakers et al. (2006) found that firewalls, passwords, and internal control are the technologies and techniques that can help prevent fraud. Volosovych and Baraniuk

(2019) emphasize the relevance of automation of control measures, parameterization of annual reports of controlling bodies, blockchain interoperability, the use of artificial intelligence and cloud computing technologies, employment of the services based on open data, and the use of interactive information sharing methods. Kitsios et al. (2022), who addressed the issues of cross-border tax frauds, found that the potential revenue gains of frontier digitalization only could amount to over 1.5 per cent of GDP in developing economies.

Thiao and Read (2021) researched the effects of ***illicit financial flows*** on the government budget in the West African and Monetary Union (the sample of 8 countries—Benin, Bissau Guinea, Burkina Faso, Ivory Coast, Mali, Niger, Senegal and Togo) over the 1996–2013 period. Their empirical analysis was based on the budget response modelling. The results of the research confirmed that illicit financial flows negatively affect government revenue, and this effect is linked to per capita income, corruption, and governance as the major transmission channels. The report provided by the Global Financial Integrity (2013) proposes that the highest rate of illicit financial flows, amounting to 39.6 percent, are characteristic of Asia, while in developing European and Western countries they amount to 21.5 and 19.6 percent, respectively. Combes et al.'s (2019) analysis shows that developing countries illicitly lose around $800 billion per year, and this amount surpasses accumulated foreign direct investment (FDI), official development assistance (ODA), and remittances.

Thiao and Read (2021) state that illicit capital outflows are promoted by fixed exchange rates, opening the capital account, and existence of informal networks. When governments are not able to adjust exchange rates, national economies become sensitive to economic shocks, and this factor stimulates illicit capital outflows. Opening the capital account has a similar effect: it tends to raise vulnerability of the national economy to capital flow fluctuations, which opens channels for illicit capital outflows. The informal networks, especially noticeable in the case of cross-border trade, lead to cross-border criminal trafficking and smuggling, through which capital flows out of the country. The negative impact of illicit financial flows on the government revenue was confirmed by Rapanyane and Ngoepe (2020), Cobham and Jansky (2020), and other authors. Combes et al. (2019) estimated that tackling illicit financial flows improves mobilization of domestic tax revenue by around 1.2 percentage points of GDP in a given country. Le Billon's (2011) study revealed that the problem of illicit financial flows mostly affects the countries highly dependent on natural resources, and the revenue earned from extractive industries tends to intensify these flows.

Cobham and Jansky (2020) note that apart from corruption, there are many different channels for illicit capital flows, including laundering the proceeds of criminal activities or shifting the profits of multinational corporations. Income streams and cross-border movements of assets are conducted through opaque business accounts and legal vehicles for anonymous ownership. The overall effects of illicit capital flows include a decrease in the revenue available to the national government, which weakens the quality of governance. Centralization of the budget process is proposed as a measure to reduce the negative effects of illicit capital flows

on the state budget. According to Aaskoven (2018), centralization may help to raise the level of taxation (as a share of GDP) and thus reduce budget deficits and government debt and moderate public spending. To prevent illegal activities related to generation of illegal financial flows, national governments should strengthen their tax collection capacities and promote investment of profits and savings in their countries of origin (Thiao & Read, 2021).

As society is becoming dependent on information and communication technologies, the weaknesses of the Internet and other electronic systems are increasingly being used by criminals for financial gains. When analysing the costs of ***cybercrime***, Anderson et al. (2013) indicate three categories of these costs: direct costs, indirect costs, and defence costs. Researching the group of direct costs, the authors found that the traditional costs of tax evasion and welfare fraud through cybercrime per citizen amount to the low hundreds of pounds/euros/dollars per year, while transaction fraud costs amount to just a few pounds/euros/dollars, and computer crime costs—to the tens of pence/cents per year. In other words, the study revealed that the share of direct costs incurred due to cybercrime is relatively small compared to much higher indirect and defence costs. Indirect costs are equal to how much cybercriminals earn (e.g. the botnet, i.e. a network of private computers infected with malicious software and controlled as a group without an owner's knowledge usually for sending spams, in 2010 earned nearly $2.7 million). Defence costs are estimated to exceed a billion dollars.

The report provided by the UK Cabinet Office and 'Detica' (2011) presents a somewhat different categorization of the costs incurred by national governments due to cybercrime. When analysing the impact of cybercrime on national governments, it is emphasized that, above all, this impact is manifested in the fact that national governments and other public bodies must spend significant amounts of money from their budgets on security and reversing the deterioration caused by cybercrime; i.e., it requires additional spending from the government and municipal budgets. In fact, the report by the UK Cabinet Office and 'Detica' (2011) notes that the above-mentioned costs are also incurred when combating many other types of crime and insecurities, so it is difficult to estimate which part of these costs are intended for the fight against cybercrime. With reference to the report, the direct costs of cybercrime include tax revenue losses which are incurred as a result of fiscal fraud and lead to reduction in the public sector revenue, and the costs incurred because of personal data breaches. The indirect costs incurred by national government include compensation payments to victims of cybercrime, legal or forensic procedure costs, and lost economy in case government services have been transferred to the Internet for efficiency reasons. The costs of anticipation of cybercrime (organizational security measures, physical and virtual protection, anti-virus systems, insurance costs, IT standard compliance costs) are also indicated. The report by the UK Cabinet Office and 'Detica' (2011) estimates that the total costs of cybercrime in the UK amount to nearly £27 billion per annum. The most damage is caused by IP thefts and espionage, while scareware is the least costly. The data provided by the European Parliament (2019) suggest that the global cost of cybercrime amounts to nearly €530 billion. The cyberattacks are observed to be increasing in terms of number, disruptive potential,

and financial damage, which undermines the capability of national governments to fight against them.

According to Armin et al. (2016), national governments need reliable data on the extent of cybercrime so that they are able to properly distribute the budget revenue, and the target measures are cost-effective; i.e., the funds spent on detection and prevention of cybercrime must be balanced with the losses incurred as a result of these crimes. Al-Dosari (2020) considers establishment of the special police departments, implementation of new investigation methods, implementation of technological innovations, contact management improvement in state institutions, staff training, expansion of cyber-defensive capabilities (e.g. development of the measures that would allow penetrating an attacker's systems and damaging them), and intelligence gathering to be the target measures for the fight against cybercrime. At the EU level, the European Commission launched the cybersecurity package in 2017. Among other measures, this package establishes an EU cybersecurity certification network, initiates the establishment of cyber-research centres in the EU member states, and outlines the measure plans for rapid emergency and law enforcement response as well as the overall political response and deterrence (The European Parliament, 2019). On 17 May 2019, the Council established an autonomous sanctions framework for cyberattacks. This framework allows the EU to impose sanctions on persons or entities that are **responsible for cyberattacks or attempted cyberattacks**, who provide financial, technical, or material **support** for such attacks or who are **involved** in other ways. Sanctions may also be imposed on persons or entities associated with them (The European Council, 2019).

Some authors (Volosovych & Baraniuk, 2018; Modzelewska & Grodzka, 2020; Shestak et al., 2021) state that ***cryptocurrencies*** can generate greater state budget revenue through high tax rates, which are invoked to tax crypto gains (cryptocurrencies could be deemed capital assets if purchased for investment purposes, so the gain arising on the transfer of these assets shall be taxable as capital gains) ('The Economic Times', 2022). For instance, in the UK, cryptocurrency is treated as a capital asset, and the tax rate on crypto capital gains is 10–20 percent, depending on an economic agent's overall taxable income, the size of the gain, and deducted allowances; in Canada, cryptocurrency is treated as a digital asset, the purchase or holding of which does not attract tax, but the sale does (only 50 per cent of the capital gain is subject to tax); in Germany, holding cryptocurrency for less than 1 year is taxed unless the profit is below €600; in India, the 30 per cent tax is charged on income from transfer of virtual digital assets and no set-off is allowed in case of any loss; in the USA, cryptocurrency is taxed as any other assets, and the tax between 10 and 20 per cent is imposed on crypto transactions (Gautam, 2022).

However, the biggest concerns of national governments regarding cryptocurrencies are related to their use for economic and financial crimes, as well as a lack of legal recognition of cryptocurrencies (developed countries, such as the United States, refuse to recognize cryptocurrencies as legal tender). According to Mcwhinney et al. (2022), by using Bitcoins, citizens can bypass capital controls set by the government, and the cases of illegal activities are difficult to identify. It is a fully decentralized currency (Lyocsa et al., 2020). National budgets are balanced

based on 'fiat money' (i.e. the conventional currencies issued by governments that ensure the full faith and credit). Countries rely on their central banks to create money for their economies and regulate money supply. The transaction cycle (i.e. the cycle involving lenders, borrowers, and consumers) is based on trust between transaction parties. In the case of using cryptocurrencies, money is created as if out of thin air; i.e., money supply is not backed by tangible assets, money supply is not created or affected by central banks (Mcwhinney et al., 2022), and no central authority is responsible for the value of cryptocurrency (Lyocsa et al., 2020). For this reason, the amount of money generated by cryptocurrencies can unbalance money supply, which can lead to the formation of asset bubbles that, in their turn, may cause economic crises. Among other negative outcomes, this will have a negative impact on the national budget which will be unbalanced and will require additional funds to manage asset bubbles and economic crises. As noted by Mcwhinney et al. (2022), until the cryptocurrency ecosystem gets mature, public sector institutions will continue to view it with distrust.

Governments and municipalities are rightly expected to provide qualitative public services. It is part of the social contract between society and the state. According to Habibov et al. (2019), citizens support their government if they are satisfied with its performance and the quality of public services. Thus, satisfaction with the quality of public services forms public belief concerning the legitimacy of the state and performance of its democratic institutions (Corral & Orces, 2013).

'Transparency International' (2022b) expresses concern about the globally observed stagnant levels of ***corruption***. Their report suggests that over the past 10 years, 84 per cent of the countries worldwide have either had poor or no progress in reducing corruption. Although Western Europe and the EU remain the highest scoring regions, their progress has slowed down, and in some cases, the worrying signs of backsliding can be observed. The COVID-19 pandemic seems to have become an excuse to assign a secondary role to anti-corruption measures. The most noticeable drops in Corruption Perceptions Index 2021 were recorded in Poland (56) and Hungary (43), where the policies restrict citizens' rights and freedom of expression. Switzerland (84), the Netherlands (82), Belgium (73), Slovenia (57), and Cyprus (53) were at historic lows on Corruption Perceptions Index 2021. Even being among the best performers, Germany (80), the United Kingdom (78), and Austria (74) were shaken by the serious corruption scandals ('Transparency International', 2022b).

In the countries with much higher levels of corruption than the EU (e.g. Russia (136), Pakistan (140), Iran (150), Venezuela (177), and a number of African countries) ('Transparency International', 2022a), citizens have to pay bribes to receive certain public services. Although at first glance it may appear that bribery is an individual-level act, it actually reflects the existence of financial crimes in public institutions. Nguyen et al. (2017) analysed whether corruption correlates with the quality of public services in the context of a transition economy (Vietnam) and found that corruption is statistically significantly negatively related to the quality of public services; i.e., when corruption is increasing, the quality of public services is decreasing and vice versa. The similar results were provided by Habibov et al.

(2017) who revealed that corruption tends to reduce public trust in state institutions and increase tolerance for bribes. Habibov et al.'s (2019) research disclosed a causal relationship between high levels of corruption and low satisfaction with the work of local and national authorities. When satisfaction with the quality of public services is rising, the indicators representing the effects of corruption start changing from negative to positive values for both local and national authorities. Puron-Cid (2021) found that corruption negatively affects the capacity of national governments to meet their financial obligations while simultaneously providing public services and building infrastructure. Montes and Paschoal (2016) researched the impact of corruption on the efficiency of the public sector in both developing and developed countries (the sample of 130 countries). The results of their research show that the countries with a lower level of corruption are characterized by higher quality of public services, more credible policies, higher quality of policy forming and adopting, and greater commitment of national governments to the policies they implement. The impact of corruption on the efficiency of the public sector is greater in developed than in developing countries. The estimates also reveal that an increase in the rule of law can significantly raise the effectiveness of the public sector. In developing countries, it can be increased by promoting democratic regimes. Nguyen et al. (2017) point out that a higher level of transparency, participation, and accountability can reduce corruption and at the same time raise the quality of public services. Barr et al.'s (2009) research shows that public service provision can be improved by monitors elected by service recipients and the higher degree of service provision observability. But their research provides only weak evidence that higher wages improve the performance of service providers.

On the other hand, Habibov et al. (2017) note that corruption may 'grease the wheals' and help to mitigate the ineffective bureaucratic procedures. This approach, which is also noticeable in Leff's (1964) and Huntington's (1968) studies, treats corruption as a way to bypass bureaucratic obstacles, especially in the countries with complex and rapidly changing regulations. Taking a bribe seems to mean a bureaucrat's commitment to work more productively, which can serve as an incentive to distribute scarce resources more efficiently. In this way, shortages of scarce goods and services are reduced; thus, public services are provided with better quality. Holmes (2000) and Green's (2011) empirical results suggest that this is typical of command-style economic systems (e.g. countries under communist regimes) and the states where the provision of public services is not developed (e.g. countries of Asia, Africa). Lavallée et al. (2008) note that the negative impact of corruption on the quality of public services is in any case lower in countries where citizens are satisfied with the services they receive.

Kumar (2012) researched the social, economic, and political impact of ***money laundering***. According to the author, money laundering helps realize the ambitions of drug traffickers, inside dealers, terrorists, and other organized criminals. Deep-rooted money laundering activities weaken public trust in state institutions and reduce the quality of public services. First of all, this is because money launderers seek to acquire wealth and power through their criminal behaviour and then try to infiltrate the legitimate society, thereby distorting its structure. In addition, they try to

deceive and bypass public authorities so that their activities are not detected and that they are not punished. Frauds and bribery often serve this purpose. The inability and/or unwillingness of public authorities to identify and break money laundering chains indicate inefficient performance of the relevant functions and undermine the trust that public institutions can work effectively at all. According to Levi and Reuter (2006), one of the aspects of the damage caused by money laundering is reduced credibility of government and public services. Addressing the situation in a developing country (Nigeria), Okogbule (2007) even treats this damage as evil. Kemal (2014) states that money laundering helps to turn 'dirty' money into 'clean' by evading prosecution and taxes and becoming legitimate. Therefore, money laundering is often associated with lower efficiency of a country's legal system, law enforcement, prosecutor offices, tax inspectorates and business registries, and weaker accountability (Ping, 2010; Kemal, 2014).

Money laundering is a sophisticated crime. Although at first glance it seems to be a victimless crime (i.e. not a crime against a particular individual), in its nature it is a crime against the state, its economic and social structures, and the rule of law (Kumar, 2012). McDowell (2001) note that money laundering reduces the quality of public services because the economic power gained by criminals often manifests itself in the form of corruption—public officials, managers, and employees of state institutions are bribed. Consequently, the economic power gained by criminals has a detrimental effect on all elements of society. If the proceeds of a criminal act can be laundered through public institutions because the managers and/or employees are corrupt and turn a blind eye to the criminal nature of particular funds, the institutions themselves become a part of a criminal network (Kumar, 2012). If criminals can use the proceeds of money laundering and the rule of law principles are not implemented in practice, we cannot talk about the efficiency of public institutions. In extreme cases, this can even lead to a virtual takeover of the legitimate government (McDowell, 2001).

Aljawarneh and Atan (2018) and Alomari (2020) researched the relationship between e-government and money laundering. According to Aljawarneh and Atan (2018), information transmitted by electronic means expands opportunities not only for business, but also for all groups of society and its individual and collective segments; it also accelerates the provision of public services (it allows to exchange information between state institutions and citizens, submit electronic reports, process documents, execute transactions, etc.). E-government is one of the modern concepts, and its impact on the public sector manifests itself as a new basis for providing services to citizens and businesses (Al-Omari et al., 2020). Modern information and communication technologies raise the performance competence of public institutions and help achieve the required efficiency. However, at the same time, information and communication technologies open up more space for money laundering operations. Electronic systems make it easier to register so-called front companies, carry out business takeovers, convert money into other types of assets, repatriate money from host countries home to poorer countries, etc. Tropina (2016) suggests that the relationship between digital technologies and money laundering is noticeable in the areas of money acquisition, transfers, and use. This poses a threat to a

country's stability and security, undermines the rule of law, and raises the pressure from civil society and other actors to take the appropriate action against illicit financial flows.

To prevent money laundering, it is necessary to deter criminals from using public institutions to launder the proceeds of crime and significantly increase the transparency of public institutions so that their representatives are deterred from participating in money laundering chains. Anti-money laundering law enforcement must be designed so as to ensure proportionate punishments for criminals and their money laundering associates (Levi & Reuter, 2006). Alomari's (2020) research proposes that information and communication technologies can also provide national governments with more tools in the fight against money laundering: with the help of cyber-technologies and e-government systems, particular compliance units for the fight against money laundering can be established. The compliance units would enhance customer due diligence, suspicious activity monitoring, case management, and watch-list filtering. In this way, the compliance units would mediate the relationship between e-government and money laundering, thereby ensuring a cohesion between e-government and structural components. Tropina (2016) suggests that digital technologies can serve as a source of empowerment and transparency and contribute to detecting and investigating money laundering cases, although they will never substitute for proper legal frameworks, international cooperation, and public–private collaboration.

Carvalho (2019), Androniceanu et al. (2019), Rashid (2020), Mason et al. (2020) and many other researchers see the negative impact of ***tax evasion*** on the quality of public services. According to Carvalho (2019), since tax revenue is the major source of financing public infrastructure and public services, the lack of the revenue to perform the aforementioned functions and misallocation of resources lead to poor-quality public services. Ineffective collection of tax revenue which limits the resources that state institutions could use for the provision of quality public services is considered the major negative effect of tax evasion (Rashid, 2020). This has the opposite effect: receiving low-quality public services, tax-paying economic agents no longer see a reason to pay taxes honestly, which stimulates even greater tax evasion. According to Alm and Kasper (2020), successful tax evasion may encourage other economic agents to engage in this practice, so the efficiency of state institutions will decrease as a consequence of the public tax non-compliance. In addition, tax evasion has distorting effects on taxation policies: failing to collect the planned tax revenue, the national government can decide to raise the tax level unreasonably (the tax level is considered unreasonable when the added value generated in the country does not grow in proportion to the increase in tax rates), which in subsequent periods may lead to even greater tax evasion. The latter, in its turn, will force governments to devote more resources to detecting and punishing cases of non-compliance. Thus, the activities of public institutions will become ineffective in the sense that resources will be distributed inefficiently. Kesselman (1989) suggests that if public institutions use products and services from tax compliant and noncompliant sectors in the same proportion as households, then higher tax rates will not affect the costs of tax evasion. If public institutions,

however, use more products and services from the tax compliant sector, then it is likely that higher tax rates will reduce the level of tax evasion.

Tax non-compliance also means that income in society will be distributed in an arbitrary, unpredictable and socially unjust way (i.e. part of the income will not be distributed through public institutions), and the accuracy of the macroeconomic statistics will be distorted (Alm & Kasper, 2020). According to Mason et al. (2020), tax evasion and income redistribution carried out arbitrarily, without the mediation of public institutions, indicate that taxpayers perceive the policies of the national government and the public sector as unfair and unfavourable to them. Androniceanu et al. (2019) confirm that the relationship between tax evasion and public policies is basically determined by the socio-economic policies implemented by public authorities.

Islam et al. (2020), who researched the relationship between the public policies and tax evasion in 7 South Asian Association for Regional Cooperation (SAARC) countries over the 1998–2015 period by applying the ordinary least square method, found that the public policies concerning monetary, fiscal, and investment freedom as well as property rights have a negative impact on tax evasion, while the effect of financial freedom is positive. The research also provided the evidence of the negative impact of the stricter governance and religiosity on tax evasion. Considering these and other empirical results presented by other authors, it can be stated that the relationship between the quality of public services and tax evasion is mutual: tax evasion tends to reduce the efficiency of the public sector because public resources are directed to the informal sector of the economy, while adequate monetary, fiscal, and investment policies alongside stricter regulation of the public sector lead to better tax compliance.

Tax evasion is one of the features of ***the shadow economy***, although the impact of the shadow economy on the public sector is not limited to uncollected taxes, reducing the state budget revenue. Fewer resources available to the public sector lead to low public investment, thus downplaying the role of the public sector in creating infrastructure, improving the business environment and complementing private investment (Misati, 2010). Scarcity of resources can also determine insufficiency and stagnation of the legal framework created by public authorities, as well as insufficiently fast adjustment to the changing economic, business, and social situation (for instance, poor protection of investors' interests, inefficient licensing system) (Estevao et al., 2022). The above-mentioned factors reduce the efficiency of the formal sector and may even lead to its collapse. As a result of the poorly performed functions of public institutions, working conditions and occupational safety requirements may not be complied with, or the relevant institutions may not properly monitor how these requirements are complied with in the practice of business enterprises. This will raise the degree of job uncertainty and the rights of workers in both sectors will be violated; i.e., public institutions will not perform their functions well enough to exercise workers' rights (Dell'Anno, 2018). Wallace and Haerpfer (2018) even believe that due to the scarcity of public resources, public servants can be underpaid, and therefore demotivated and demoralized, which may further stimulate circumvention of laws and regulations, improper performance of

work functions or the delay in the performance of these functions, and the aforementioned deviations will originate no longer from the private sector, but from the public sector itself.

On the other hand, as stated by Misati (2010), the large scale of the shadow economy may force public institutions to issue over-burdening regulations, which will undermine entrepreneurial spirit and reduce business efficiency and investment. Over-burdening regulation, in its turn, can stimulate bureaucracy and corruption in the public sector if institutional reforms are not carried out (Mughal & Schneider, 2020). Wallace and Latcheva's (2006) research in transition countries of the Central and Eastern Europe disclosed that greater participation in the shadow economy is linked to the negative attitudes towards legitimacy of the public realm and loss of trust in public institutions. Therefore, it is assumed that the growth of the informal sector can diminish trust in the state itself, although it is noted that significant variations from country to country are possible in this regard.

When assessing the effects of the shadow economy in a broader sense, Sultana et al. (2022) state that the damage of the shadow economy manifests itself through a decentralized model of organizing an economic activity, typical of the informal sector. This informal (decentralized) model undermines the effectiveness of the formal coordination and planning functions attributed to public institutions because by applying the decentralized model, the factors, resources, and market characteristics of the formal sector are distorted. Since the shadow economy operates in parallel with the formal economy, the complex interaction between the two sectors may cause public policy complications (Mughal & Schneider, 2020).

Santos et al. (2021) emphasize the relationship between ***informal entrepreneurship*** and the activities of public institutions: the authors state that a high level of informal entrepreneurship diminishes investors' trust in public institutions and complicates investment decisions, and the greater is incompatibility of the functions of formal and informal institutions, the greater is the probability of informal entrepreneurship. Since for most entrepreneurs the demand for venture capital funding depends on the proper functioning of public institutions, especially in terms of law and regulation, the growth of the level of informal entrepreneurship indicates that the legal and regulatory functions of public institutions are not relied on. Williams and Bezeredi (2018) draw attention to the relationship between informal entrepreneurship and the poor quality of public services, a lax of tax fairness, a wider potential for corruption, and instability in the formal institutions.

Williams and Shahid (2014) suggest that informal entrepreneurship is determined by the asymmetry between formal and informal institutions (codified laws and regulations representing formal institutions, and social norms and codes of conduct representing informal ones). This implies that informal entrepreneurship compromises formal laws and regulations, but activities are still carried out within the boundaries of the social codes of conduct; i.e., informal entrepreneurship does not undermine the power of social norms and codes of conduct, but it undermines the imperative power of formal regulations. Fredstrom et al.'s (2021) research reveals that informal entrepreneurship tends to shape the outcomes of governance and public management improvements, while incompatibility between formal and informal

institutions leads to institutional incongruence. According to the authors, the paradox is that the efforts of public institutions to improve governance and public management at a high level of informal entrepreneurship can make the situation even worse; i.e., if, while trying to control informal entrepreneurship, public authorities will tighten the requirements for conducting business and this decision will not comply with the principles of informal institutions, then the tension between the informal sector and public authorities can only intensify.

Laing et al. (2021) argue that informal entrepreneurship shows inability of public authorities to ensure simple and easy business start-up and high-quality business regulation. In normally functioning systems, national governments treat entrepreneurship as 'good', because it creates jobs and generates value added. Thus, national governments tend to spend the budget revenue on funding business start-up and development. A high level of informal entrepreneurship shows that public authorities do not perform the function of promoting business as an engine of the economy. As stated by Laing et al. (2021), in the short run, national governments can make some institutional framework changes, thus affecting the scale and nature of entrepreneurship, but the structural changes that could determine, for example, the structure of business sectors, can be implemented only in the long run.

The impact of ***fraud*** was analysed by the Commonwealth Fraud Prevention Centre (2020) whose report proposes that the negative effects of fraud on the quality of public services can occur in the following ways:

- Public institutions' failure to deliver the intended services. If finite funds and resources are diverted away from an intended target, services are not provided or the required service standards are not met.
- Failure to meet aims and objectives of the target programmes. Fraudulent programmes usually do not have a clear vision and do not aim at any tangible results.
- Shutting down particular programmes, projects, or services. If the resources intended for a programme, project, or service are diverted away or appropriated, the programme, project, or service can be terminated because of the lack of resources.
- The negative customer/user experience. With the lack of resources, the quality of public services is decreasing, which negatively affects the experience of customers and users.
- Higher opportunity costs. Discontinued or poor-quality programmes, projects, or services can mean lost opportunities for customers/users. These costs may also be incurred by programme, project, and service providers, if they suffer financial losses and additional operational costs.

The Centre for Financial Reporting Reform (CFRR) (2019) notes that frauds can originate from both external and internal sources. This assumption is confirmed by Omidi et al. (2017), Kabiru and Muthinja (2022), etc. External frauds are committed by natural or legal persons against public institutions (e.g. by submitting falsified reports, concealing the true origin of goods/services, and performing accounting manipulations). Internal frauds can be committed by any employee at any level of

the public sector (starting with minor travel, office supply, fuel expenditure abuses, payroll fraud (requesting pay for hours not worked), and ending with large-scale fraud when establishing high-value contracts (e.g. specifying unreasonably high prices of goods/services and misappropriating the difference between the fake and real price of these goods/services). Special attention is paid to fraud during public procurement procedures. In this case, entrusted power is abused for personal gain. Public procurement tenders are illegally won by submitting cash 'under the table' to a public official, so it is very difficult to gather evidence that a crime has occurred (The Centre for Financial Reporting Reform (CFRR), 2019).

Frauds in various public bodies can be related to additional costs and capacity drain: on one hand, productive resources flow from the public sector and public assets are embezzled (Omidi et al., 2017; Agwor & Akani, 2017); on the other hand, the limited resources of public institutions are directed to respond to fraud and deal with its outcomes. Additional resources are needed for fraud identification (identity protection, vetting systems, eligibility, person checks, etc.), investigation (police and law enforcement agencies), prosecution, courts, tribunals and legal aid, prison costs (to upkeep fraudsters that are convicted), fraudsters' welfare (support, assistance, benefits), and document management (The International Public Sector Fraud Forum, 2020).

What is more, frauds can result in faulty infrastructures, the construction of which is the direct responsibility of public authorities: unreliable road, sea, air transport infrastructure, unsafe bridges, and guardrails can even cause a risk to people's lives. For instance, the cause of the Grenfell Tower fire that occurred in Great Britain on 14 June 2017 was the defectively installed electric system; the exterior of the building did not comply with regulations, which was the central reason why the fire spread; i.e., fraud by contractors put people's safety and lives at risk. Frauds in supplying military and law enforcement bodies with necessary safety equipment may mean that faulty or unsafe safety equipment (e.g. bulletproof vests and bomb detectors) will be delivered, which may pose a risk to the lives of the military staff and officers (The International Public Sector Fraud Forum, 2020). In addition, frauds may pose a risk to national security if they are undertaken by actors for the purpose of financing terrorism, if the proceeds of fraud perpetrate other criminal activities, and if border security is compromised by enabling smuggling and trafficking of illicit goods.

Dobie (2020) argues that in the case of fraud, a lack of knowledge alongside the established customs and practices or the absence of the necessary management systems combined with a *laissez-faire* culture can lead to people unknowingly misusing or misdeclaring funds. In the latter case, training and education could help to solve the problem. However, these cases are not common. Deliberate fraud is much more common because where money circulates, there will always be people exploiting the system for personal gain.

Frauds against public institutions are likely to diminish trust in government, public authorities, and social security institutions because individuals who have been impacted by frauds will lose trust in public services and transactions. This is referred to as reputational harm. Erosion of trust in government in terms of

information, a lack of confidence in the government's ability to deliver particular policies, and treating the government as an easy target for frauds can lead to a decrease in legal compliance. In addition, frauds occurring within the public sector or against it can diminish the morale of public servants, which may lead to poorer performance of their functions. In medium and long runs, this fraudulent system may stimulate a culture of non-compliance under which some level of fraud will be treated as acceptable. All the aforementioned forms of public distrust in public authorities can cause tension in terms of the relationship between the public bodies and the citizens. The effects of fraud on the public sector can be mitigated by implementing stronger internal control and auditing, using the latest technologies, especially for data analysis (Agwor & Akani, 2017; The Centre for Financial Reporting Reform (CFRR), 2019).

When researching the issues of ***illicit financial flows***, Brandt (2022) provides the channels through which both natural and legal persons usually conduct illicit financial flows. The channels include hiding of wealth in tax heavens, channelling FDI through multiple tax heavens, and eroding profits in high tax countries, thus significantly raising the profits in low-tax countries. The author provides the estimations indicating that around 10 per cent of global GDP is held in tax heavens, nearly 40 per cent of FDI is channelled through multiple tax heavens, and a 1-percentage-point drop in the average corporate tax rate is associated with a 0.8–1.0 per cent drop in corporate profits.

Addressing the effects of illicit financial flows, Thiao and Read (2021) note that these flows have a number of complex effects on the level of public revenue and resource mobilization; i.e., they complicate public revenue and public resource mobilization due to violation of law and deterioration of effective governance (both in the public and private sectors). Ogunleye and Fashina (2010), Culpeper and Bhusshan (2010), and Brandt (2022) argue that an indispensable strategy for providing high-quality public services requires public resource mobilization and investment. Public resource mobilization rate depends on a number of factors and may vary from country to country. According to the data provided by the Central Bank of West African States (BCEAO) (2013), the public resource mobilization rate in the West African Economic and Monetary Union (8 member states) amounted to 19.1% in 2013, which was lower than in the entire sub-Saharan Africa with the rate equal to 27.5%. It indicates that the funds which could be used by national governments for the investment in public infrastructures are illicitly transferred out of the countries. According to Herkenrath (2014), illicit financial flows deprive a country from the urgently needed resources that could be used for private and public investment. This way, a country's infrastructure building is hampered and state institutions are weakened, especially minding the fact that illicit financial flows tend to go hand in hand with corruption and money laundering. Similar results were provided by Chowla and Falcao (2016), Barasa (2018), Rapanyane and Ngoepe (2020), and many other authors. Brandt (2022) confirms that not having the adequate revenue that could be spent on public needs, public authorities are restricted when providing the crucial public services, such as education, health care, and infrastructure. The author notes that developing countries remain most

vulnerable in this regard, while developed countries place restrictions on the amount of deductible interests, demand the relevant documentation to control the transfer prices, and require tax disclosures from businesses operating in specific industries. In developing countries, such requirements are either missing or not enforced to a degree that is effective. As a consequence, the quality of the public services in low-income countries is lower because these countries are vulnerable to the negative effects of illicit financial flows.

In the report provided by the UK Cabinet Office and 'Detica' (2011), ***cybercrime*** is referred to as a mix between individual and organized criminals with potential involvement of the state. After analysing various aspects of the impact of cybercrime, Lewis (2018) highlights the risk of personal identity data theft (stolen information is offered for sale on the dark web; i.e., the stolen data is monetized). Personal data can be stolen not only from private servers, but also from state institutions. This risk is particularly high when state institutions use internal servers, store the data in their own premises (instead of storing the data on third-party servers or in the cloud) which often do not meet security requirements, and do not care whether the private data centres that are employed or are intended to be employed meet the international TIER standards (the international standards for data centre performance), etc. The above-mentioned factors, above all, harm the prestige of state institutions from the public's point of view (reputational harm). In addition, if the systems are damaged, the transfer of institutional data to state centres as well as provision of public services through the Internet may be disrupted. From the financial perspective, this means additional expenditure on protecting state networks and systems, cybersecurity, cyber-insurance, recovery from cyberattacks, and higher legal and reporting costs. According to Morgan (2020), cybercrime is a channel to transfer the great economic wealth from the sphere of control of state institutions; it poses risks to innovation and investment. Cybercrime costs cover data destruction, intellectual property thefts, embezzlement, fraud, post-attack disruption of the normal execution of functions, forensic investigation, restoration, etc.

Al-Dosari (2020) argues that particular forms of cybercrime can disrupt the performance of state institutions and even pose a threat to the critical national infrastructure and national security. This argument is confirmed in the report provided by the UK Cabinet Office and 'Detica' (2011). For instance, through direct hacking of the servers and websites belonging to the official state institutions and systemically important public companies, sensitive information can be leaked (e.g. the information about military plans, objects, army locations), energy supply can be disrupted, ransomware can hit healthcare and energy service providers, social media can be used to form a radical oppositional opinion, etc.

Bartoletti et al. (2021) define ***cryptocurrency scams*** as unlawful behaviour of an individual or a group of individuals who intentionally conduct fraudulent activities by exploiting the features of blockchain technologies, in particular anonymity and pseudonymity, to have an illegal or unfair gain. The authors also note that anonymity and pseudonymity are the characteristics of blockchain technologies that make cryptocurrency scams hard to detect. Thus, from this point of view, the negative effects on the framework of public services are caused by the latent nature of

cryptocurrency scams which impedes the effective implementation of the law enforcement function that is considered one of the major functions of the state (the monopoly of law enforcement is in the hands of the state, so only the state can implement justice). According to Mackenzie (2022), crime control is almost entirely absent from the new-generation crypto economy.

Navaro's (2019) study proposes that cryptocurrency scams can weaken the financial market supervision and control functions performed by the national central bank because the illicit funds can enter the financial market through cryptocurrency exchange. In addition, cryptocurrencies represent ownership rights in digital goods that are not established and regulated legally (insufficiency of the national legal framework) (Mackenzie, 2022). Mackenzie (2022) notes that online crime demands a fundamentally different method of analysis and investigation compared to traditional offline crimes, which implies that effective analysis and investigation methods have not yet been implemented in state service provision systems, and the staff is insufficiently prepared.

Bartoletti et al.'s (2021) research reveals that cryptocurrency scams are difficult to report by users because the existing systems are not complete; they often provide inconsistent and erroneous information, and the information about the types of scams is limited (Navaro, 2019). This aspect indicates that when trying to deal with cryptocurrency scams, the system of providing and exchanging information both between the public and the state and within public institutions is ineffective, which may cause doubts in the public as to whether the information is worth providing at all. In this way, difficulties may arise in collecting and announcing the reliable public data. Case detection and data collection are also complicated by the complexity of cryptocurrency scams, which makes them difficult to categorize; i.e., public authorities are facing a lack of a standardized, comprehensive taxonomy. For instance, although pump-and-dump schemes are illegal, in many cases it is easy to confuse them with legitimate investment schemes.

3 Conclusions

The conclusions have been summarized as follows:

1. The impact of economic and financial crimes on the government budget is basically manifested in the fact that these crimes significantly reduce budget revenue which could be used to meet the socio-economic and political needs of citizens and to build public infrastructure. A lack of budget revenue leads to inefficient state expenditure and inefficient investment and causes a fiscal deficit, to cover which national governments can either increase tax rates or are forced to borrow funds in international financial markets, which raises the level of public debt and vulnerability of the economy, and diminishes capability of governments to affect the economy through necessary interventions when financial imbalances need to be corrected. The difficulties to measure how much revenue the budget

loses can cause inaccuracies in the national account statistics, which can lead to mistakes in appropriate budget allocation and public policies. The use of digital technologies (artificial intelligence, cloud computing, interactive information sharing methods) at the control-state, control-enterprise, and control-society levels is seen as one of the solutions to reduce the volume of economic and financial crimes and increase the government budget revenue. In any case, the economic and financial crime detection and prevention measures must be cost-effective.

2. By reducing the state budget revenue, economic and financial crimes curtail the major source of financing for the development of public infrastructure and public services and lead to an inefficient distribution of state expenditure. This determines the inefficient performance of the functions assigned to public institutions and thus the low quality of public services. Resource limitation can determine insufficiency and stagnation of the legal framework created by public authorities and its inability to adjust to changing economic, business, and social situations. Excessive regulation caused by high levels of economic and financial crime can promote bureaucracy and provide opportunities for corruption in the public sector if the appropriate institutional reforms are not carried out. The existence of economic and financial crimes also means that part of the income in society is distributed arbitrarily (i.e. not through state institutions), unpredictably, and socially unjustly. This informal model undermines the effectiveness of formal coordination and planning, socially fair distribution of the resources possessed by public institutions and public trust in state institutions (reputational harm). The negative impact of economic and financial crimes on the quality of public services can be mitigated by stronger internal control and auditing, and invoking the latest technologies, especially data analysis. E-government is one of the modern concepts, a new basis for the effective provision of public services to citizens and businesses. Modern ICTs improve the performance competence of public institutions, allow to establish particular compliance units that mediate the relationship between the government and society, and help achieve the required efficiency by ensuring cohesion among the structural components of the public service provision.

References

Aaskoven, L. (2018). Budget institutions and taxation. *Public Choice, 174*(3–4), 335–349.

Abiahu, M.-F. C., Nestor, A., Muo, O. E. C., & Chinyere, O. J. (2016). *Effect of money laundering on Nigerian economy.* Retrieved from https://www.researchgate.net/publication/318508694_Effect_of_Money_Laundering_on_Nigerian_Economy

Abu-Orabi, M. M. A.-M., & Al Abbadi, A. F. A. (2019). The effects of money laundering on monetary markets introduction. *Modern Applied Science, 13*(12), 43–51. https://doi.org/10.5539/mas.v13n12p43

Agwor, T. C., & Akani, F. N. (2017). Internal control system and fraud prevention in public Service of Bayelsa State, Nigeria. *International Journal of Novel Research in Marketing Management and Economics, 4*(3), 170–178.

Al-Dosari, K. N. (2020). Cybercrime: Theoretical determinants, criminal policies, prevention & control mechanisms. *International Journal of Technology & Systems*. Retrieved from https://iprjb.org/journals/index.php/IJTS/article/view/1133/1247

Aljawarneh, N. M. S., & Atan, T. (2018). Linking tolerance to workplace incivility, service innovative, knowledge hiding, and job search behavior: The mediating role of employee cynicism. *Negotiation and Conflict Management Research, 11*(4), 298–320.

Alm, J., & Kasper, M. (2020). *Tax evasion, market adjustments, and income distribution*. Retrieved from https://wol.iza.org/uploads/articles/526/pdfs/tax-evasion-labor-market-effects-and-income-distribution.pdf?v=1

Alomari, K. A. K. (2020). Linking between E-government and money laundering: The mediating role of compliance unit. *International Journal of Academic Research in Business & Social Sciences, 10*(2), 179–194. Retrieved from https://pdfs.semanticscholar.org/69c4/faa3ca15f5684e9de471f23d34a62c015554.pdf

Al-Omari, Z., Alomari, K., & Aljawarneh, N. (2020). The role of empowerment in improving internal process, customer satisfaction, learning and growth. *Management Science Letters, 10*(4), 841–848.

Aluko, A. (2012). *The impact of money laundering on economic, and financial stability and on political development of developing countries*. Financial Regulation and Economic Law (ICGFREL), Institute of Advanced Legal Studies School of Advanced Study University of London. https://doi.org/10.1108/13685201211266024

Anderson, R., Barton, C., Bohme, R., Clayton, R., van Eeten, M. J. G., Levi, M., Moore, T., & Savage, S. (2013). Measuring the cost of cybercrime. In R. Bohme (Ed.), *The economics of information security and privacy*. Springer. https://doi.org/10.1007/978-3-642-39498-0_12

Androniceanu, A., Gherghina, R., & Ciobanasu, M. (2019). The interdependence between fiscal public policies and tax evasion. *Administratie si Management Public*. https://doi.org/10.24818/amp/2019.32-03

Argentiero, A., & Cerqueti, R. (2019). *Public debt management and tax evasion.* Retrieved from https://openresearch.lsbu.ac.uk/download/0ce78896f61445d1ef346a7d4abbcd48dcf19e5cb89173153a3c85df84935a18/344197/Argentiero_Cerqueti_SI_NED_CICSE_2017_TEX_SOURCE_FILE.pdf

Armin, J., Thompson, B., & Kijewski, P. (2016). Cybercrime economic costs: No measure no solution. In B. Akhgar & B. Brewster (Eds.), *Combating cybercrime and cyberterrorism. Advanced sciences and technologies for security applications*. Springer. https://doi.org/10.1007/978-3-319-38930-1_8

Arsic, M., & Krstic, G. (2015). *Effects of formalisation of the shadow economy.* Retrieved from https://library.oapen.org/bitstream/handle/20.500.12657/28087/1001907.pdf?sequence=1#page=107

Barasa, T. (2018). *Illicit financial flows in Kenya: mapping of the literature and synthesis of the evidence*. Retrieved from https://www.africaportal.org/publications/illicit-financial-flows-kenya-mapping-literature-and-synthesis-evidence/

Barr, A., Lindelow, M., & Serneels, P. (2009). Corruption in public service delivery: An experimental analysis. *Journal of Economic Behaviour & Organization, 72*(1), 225–239. https://doi.org/10.1016/j.jebo.2009.07.006

Bartoletti, M., Lande, S., Loddo, A., Pompianu, L., & Serusi, S. (2021). Cryptocurrency scams: Analysis and perspectives. *IEEE Access, 9*, 148353–148373. Retrieved from https://ieeexplore.ieee.org/abstract/document/9591634

Benfratello, L., Monte A. D., & Pennacchio, L. (2015). *Corruption and public debt: An empirical analysis*. University of Naples "Federico II" and CSEF, WP. Retrieved from https://www.siecon.org/sites/siecon.org/files/oldfiles/uploads/2015/10/Pennacchio.pdf

Bierstakers, J., Brody, R., & Pacini, C. (2006). Accountants' perception regarding fraud detection and prevention methods. *Managerial Auditing Journal, 21*(5), 520–535.

Brandt, K. (2022). Illicit financial flows and developing countries: A review of methods and evidence. *Journal of Economic Surveys*. Retrieved from https://onlinelibrary.wiley.com/doi/full/10.1111/joes.12518\

Carvalho, J. L. D. P. (2019). *The effects of tax evasion on economic growth: A stochastic growth model approach.* Retrieved from https://www.locus.ufv.br/bitstream/123456789/26737/1/texto%20completo.pdf

Chowla, P., & Falcao, T. (2016). *Illicit financial flows: Concept and flows*. Retrieved from https://www.un.org/esa/ffd/wp-content/uploads/2017/02/Illicit-financial-flows-conceptual-paper_FfDO-working-paper.pdf

Cobham, A., & Jansky, P. (2017). *Illicit financial flows: An overview*. Retrieved from https://www.tralac.org/images/docs/12398/ige-ffd-unctad-illicit-financial-flows-an-overview-background-paper-november-2017-draft.pdf

Cobham, A., & Jansky, P. (2020). *Estimating illicit financial flows*. Oxford University Press.

Combes, J.-L., Minea, A., & Sawadogo, P. N. (2019). *Assessing the effects of combating illicit financial flows on domestic tax revenue mobilization in developing countries*. Retrieved from https://halshs.archives-ouvertes.fr/halshs-02019073/document

Conyers Dill & Pearman. (2013). *Impact of new Bermuda anti-money laundering regime on investment fund operators and administrators*. Retrieved from https://www.opalesque.com/52058/The_impact_of_the_new_Bermuda058.html

Cooray, A., Dzhumashev, R., & Schneider, F. (2017). How does corruption affect public debt? An empirical analysis. *World Development, 90*, 115–127.

Corral, M., & Orces, D. (2013). *Economic development, corruption and satisfaction with democracy across the Americas: A comparative multilevel analysis*. Salamanca, Instituto de Iberoamérica Universidad de Salamanca, Universidad de Salamanca. Working Paper No. DT 18/2013.

Crivelli, E., de Mooij, R. A., & Keen, M. (2015). *Base erosion, profit shifting and developing countries*. IMF Working Paper 15/118, International Monetary Fund. Retrieved from https://www.imf.org/external/pubs/ft/wp/2015/wp15118.pdf

Culpeper, R., & Bhusshan, A. (2010). Why enhance domestic resource mobilisation in Africa? *Trade Negotiations Insights, 9*(6), 5–7. Retrieved from https://www.ictsd.iisd.org/

Delavallade, C. (2006). Corruption and distribution of public spending in developing countries. *Journal of Economics and Finance, 30*(2), 222–239.

Dell'Anno, R. (2018). Inequality, informality, and credit market imperfections. *Macroeconomic Dynamics, 22*(5), 1184–1206. https://doi.org/10.1017/S1365100516000

Di Porto, E., Elia, L., & Tealdi, C. (2017). Informal work in a flexible labour market. *Oxford Economic Papers, 69*(1), 143–164. https://doi.org/10.1093/oep/gpw010

Dlamini, B., & Dube, G. (2020). Precipitants of tax evasion in the informal sector in Zimbabwe: A case study of Bulawayo Metropolitan Province. *International Journal of Management Studies and Social Science Research, 2*(1), 1–10.

Dobie, L. (2020). *Tackling fraud and financial crime in the global public sector through training and education.* Retrieved from https://www.ifac.org/knowledge-gateway/building-trust-ethics/discussion/tackling-fraud-and-financial-crime-global-public-sector-through-training-and-education

Enste, D. H. (2018). *The shadow economy in industrial countries.* Retrieved from https://wol.iza.org/articles/shadow-economy-in-industrial-countries/long

Estevao, J., Lopes, J. D., & Penela, D. (2022). The importance of the business environment for the informal economy: Evidence from the doing business ranking. *Technological Forecasting and Social Change, 174*, 121288.

European Commission and OECD. (2015). *Policy brief on informal entrepreneurship. Entrepreneurial Activities in Europe*. Publications Office of the European Union, 2015. ISBN 978-92-79-43393-1.

Everhart, S. S., Martinez-Vazquez, J., McNab, M., & R. M. (2009). Corruption, governance, investment and growth in emerging markets. *Applied Economics, 41*(13), 1579–1594.

Fedajev, A., Velickovic, M., Nikolic, R., Cogoljevic, M., & Remeikiene, R. (2022). Factors of the shadow economy in market and transition economies during the post-crisis period: Is there a difference? *Inzinerine Ekonomika-Engineering Economics, 33*(3), 246–263.

Fredstrom, A., Peltonen, J., & Wincent, J. (2021). A country-level institutional perspective on entrepreneurship productivity: The effects of informal economy and regulation. *Journal of Business Venturing, 36*(5), 106002. https://doi.org/10.1016/j.jbusvent.2020.106002

Gallaway, J. H., & Bernasek, A. (2002). Gender and informal sector employment in Indonesia. *Journal of Economic Issues, XXXVI*(2), 314–321.

Gautam, V. (2022). C*ountries where cryptocurrency is taxed.* Retrieved from https://www.indiatimes.com/worth/investment/countries-where-crypto-is-taxed-561760.html

Ghura, D. (1998). *Tax revenue in sub-Saharan Africa: Effects of economic policies and corruption.* International Monetary Fund, working paper no. 1998/135. Retrieved from https://www.imf.org/en/Publications/WP/Issues/2016/12/30/Tax-Revenue-in-Sub-Saharan-Africa-Effects-of-Economic-Policies-and-Corruption-2754

Global Financial Integrity. (2013). *Illicit financial flows and the problem of net resource transfers from Africa: 1980–2009.* Retrieved from https://www.afdb.org/fileadmin/uploads/afdb/Documents/Publications/Illicit_Financial_Flows_and_the_Problem_of_Net_Resource_Transfers_from_Africa_1980-2009_-_Executive_Summary.pdf

Green, A. (2011). Institutions matter, but in surprising ways: New evidence on institutions in Africa. *Kyklos, 64*, 1–105. https://doi.org/10.1111/j.1467-6435.2010.00496.x

Guillamon, M.-D., Faura, J. C., Martinez, U. F., & Benito, B. (2021). Effect of political corruption on municipal tax revenues. *Revista de Contabilidad – Spanish Accounting Review, 24*(2), 231–240.

Gupta, S., Mello, L. D., & Sharan, R. (2001). Corruption and military spending. *European Journal of Political Economy, 17*(4), 749–777.

Habibov, N., Afandi, E., & Cheung, A. (2017). Sand or grease? Corruption–institutional trust nexus in post-Soviet countries. *Journal of Eurasian Studies, 8*. https://doi.org/10.1016/j.euras.2017.05.001

Habibov, N., Fan, L., & Auchynnikava, A. (2019). The effects of corruption on satisfaction with local and national governments. Does corruption 'grease the wheals'? *Europe-Asia Studies, 71*(5), 736–752. https://doi.org/10.1080/09668136.2018.1562044

Haron, R., & Ayojimi, M. S. (2019). The impact of GST implementation on the Malaysian stock market index volatility an empirical approach. *Journal of Asian Business and Economic Studies, 26*(1), 17–33.

Hassan, M. (2017). *The impact of the shadow economy on aid and economic development nexus in Egypt.* Retrieved from https://mpra.ub.uni-muenchen.de/80990/1/MPRA_paper_80990.pdf

Hendriyetty, N., & Grewal, B. S. (2017). Macroeconomics of money laundering: Effects and measurements. *Journal of Financial Crime, 24*(1), 65–82. https://doi.org/10.1108/JFC-01-2016-0004

Herkenrath, M. (2014). *Illicit financial flows and their developmental impacts: An overview*. International Development Policy. Retrieved from https://journals.openedition.org/poldev/1863\

Herranz, M. M., & Turino, F. (2022). *Tax evasion, fiscal policy and public debt: Evidence from Spain.* Retrieved from https://www.researchgate.net/publication/357676939_Tax_Evasion_Fiscal_Policy_and_Public_Debt_Evidence_from_Spain.

Hessami, Z. (2014). Political corruption, public procurement, and budget composition: Theory and evidence from OECD countries. *European Journal of Political Economy, 34*, 372–389.

Highfield, R., Evans, C., & Walpole, M. (2018). The development and testing of a diagnostic tool for assessing VAT compliance costs: Pilot study findings. *eJournal of Tax Research, 16*, 620–654.

Hillman, A. L. (2004). Corruption and public finance: An IMF perspective. *European Journal of Political Economy, 20*(4), 1067–1077.

Holmes, L. (2000). Funktionen und Dysfunktionen der Korruption und ihrer Bekämpfung in Mittel- und Osteuropa. In Zentrum für Europa- und Nordamerika- Studien (Ed.), *Politische Korruption*. Leske & Budrich.

Huntington, S. P. (1968). *Political order in changing societies*. Yale University Press.

Hwang, J. (2002). A note on the relationship between corruption and government revenue. *Journal of Economic Development, 27*(2), 161–178.

Islam, A., Ur Rashid, M. H., Hossain, S. Z., & Hashmi, R. (2020). Public policies and tax evasion: Evidence from SAARC countries. *Heliyon, 6*(11), e05449.

Kabiru, J. W., & Muthinja, M. M. (2022). The link between occupational fraud and public service delivery in Kenya. *African Development Finance Journal, 3*(1), 117–130.

Kassa, E. T. (2021). Factors influencing taxpayers to engage in tax evasion: Evidence from Woldia City administration micro, small, and large enterprise taxpayers. *Journal of Innovation and Entrepreneurship, 10*. Retrieved from https://innovation-entrepreneurship.springeropen.com/articles/10.1186/s13731-020-00142-4

Kemal, M. U. (2014). Anti-money laundering regulations and its effectiveness. *Journal of Money Laundering Control, 17*(4), 416–427.

Kesselman, J. R. (1989). Income tax evasion: An intersectoral analysis. *Journal of Public Economics, 38*(2), 137–182.

Kitsios, E., Jalles, J. T., & Verdier, G. (2022). Tax evasion from cross-border fraud: Does digitalization make a difference? *Applied Economics Letters, 30*, 1400–1406. https://doi.org/10.1080/13504851.2022.2056566

Knight, M., Loayza, N., & Villanueva, D. (1996). *The peace dividend: Military spending cuts and economic growth. Policy Research Working Paper Series, No. 1577*. The World Bank.

Kumar, A. (2012). Money laundering: Concept, significance and its impact. *European Journal of Business and Management, 4*(2), 113–120.

Laing, E., van Stel, A., & Storey, D. J. (2021). Formal and informal entrepreneurship: A cross-country policy perspective. *Small Business Economics*. Retrieved from https://link.springer.com/article/10.1007/s11187-021-00548-8

Lavallée, E., Razafindrakoto, M., & Roubaud, F. (2008). *Corruption and trust in political institutions in sub-Saharan Africa. Working paper no. 18*. Afrobarometer.

Le Billon, P. (2011). *Extractive sectors and illicit financial flows: What role for revenue governance initiatives?* Retrieved from https://www.cmi.no/publications/4248-extractive-sectors-and-illicit-financial-flows

Leff, N. (1964). Economic development through bureaucratic corruption. *American Behavioral Scientist, 8*, 3–14. https://doi.org/10.1177/000276426400800303

Levaggi, R., & Menoncin, F. (2020). *Tax evasion and debt in a dynamic general equilibrium model*. Retrieved from https://tarc.exeter.ac.uk/media/universityofexeter/businessschool/documents/centres/tarc/events/8thannualconference/Rosella_Levaggi__Tax_evasion_and_debt_in_a_dynamic_general_equilibrium_model.pdf

Levi, M., & Reuter, P. (2006). Money laundering. *Crime and Justice, 34*(1), 289–375. Retrieved from https://orca.cardiff.ac.uk/id/eprint/3154/1/Levi%202006.pdf

Lewis, J. A. (2018). *Economic impact of cybercrime – No slowing down.* Retrieved from https://csis-website-prod.s3.amazonaws.com/s3fs-public/publication/economic-impact-cybercrime.pdf

Liu, C., & Mikesell, J. L. (2019). Corruption and tax structure in American states. *American Review of Public Administration, 49*(5), 585–600. https://doi.org/10.1177/0275074018783067

Lyocsa, Š., Molnar, P., Plihal, T., & Širanova, M. (2020). Impact of macroeconomic news, regulation and hacking exchange markets on the volatility of bitcoin. *Journal of Economic Dynamics and Control, 119*, 103980. https://doi.org/10.1016/j.jedc.2020.103980

Mackenzie, S. (2022). Criminology towards the metaverse: Cryptocurrency scams, grey economy and the technosocial. *The British Journal of Criminology, 62*(6), 1537–1552. https://doi.org/10.1093/bjc/azab118

Mason, P. D., Utke, S., & Williams, B. M. (2020). Why pay our fair share? How perceived influence over laws affects tax evasion. *The Journal of the American Taxation Association, 42*(1). https://doi.org/10.2139/ssrn.3030127

Mauro, P. (1996). *The effects of corruption on growth, investment, and government expenditure.* IMF Working Paper No. 96/98, Policy Development and Review Department. Retrieved from SSRN https://ssrn.com/abstract=882994

McDowell, J. (2001). The consequences of money laundering and financial crime. *An Electronic Journal of the U.S. Department of State, 6*(2), 1–8.

McWhinney, J., Brown, R. J., & Reeves, M. (2022). *Why governments are wary of bitcoin*. Retrieved from https://www.investopedia.com/articles/forex/042015/why-governments-are-afraid-bitcoin.asp

Misati, R. N. (2010). The role of the informal sector in investment in sub-Saharan Africa. *International Entrepreneurship and Management Journal, 6*(2), 221–230. https://doi.org/10.1007/s11365-010-0147-y

Mishchuk, H., Bilan, S., Yurchyk, H., Akimova, L., & Navickas, M. (2020). Impact of the shadow economy on social safety: The experience of Ukraine. *Economics and Sociology, 13*(2), 289–303. https://doi.org/10.14254/2071-789X.2020/13-2/19

Modzelewska, A., & Grodzka, P. (2020). Tax fairness and cryptocurrency. *Annual Center Review, 12*(13), 22–27.

Mohasoa, T. (2016). *Know about money laundering.* Retrieved from http://www.centralbank.org.ls/employment/Know_about_Money_laundering.ng.pdf

Montes, G. C., & Paschoal, P. C. (2016). Corruption: What are the effects on government effectiveness? Empirical evidence considering developed and developing countries. *Applied Economics Letters, 23*(2), 146–150. https://doi.org/10.1080/13504851.2015.1058900

Morgan, S. (2020*). Cybercrime to cost the world $10.5 trillion annually by 2025.* Retrieved from https://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016/

Mughal, K. S., & Schneider, F. G. (2020). How informal sector affects the formal economy in Pakistan? A lesson for developing countries. *South Asian Journal of Macroeconomics and Public Finance, 19*(1) Retrieved from https://journals.sagepub.com/doi/full/10.1177/2277978719898975

Mukah, S. T., & Fossung, M. F. (2019). Tax evasion in Cameroon: Causes and remedies. *Research Journal of Finance and Accounting, 10*(14), 79–90. https://doi.org/10.2139/ssrn.3433386

Myint, U. (2000). Corruption: Causes, consequences and cures. *Asia Pacific Development Journal, 7*(2), 33–58.

Navaro, R. R. (2019). Preventative fraud measures for cryptocurrency exchanges: Mitigating the risk of cryptocurrency scams. *Utica College ProQuest Dissertations Publishing, 2019*, 22620714. Retrieved from https://www.proquest.com/openview/0f46c30d16666fd2f74d74a75df440a1/1?pq-origsite=gscholar&cbl=18750&diss=y

Nguyen, T. V., Bach, T. N., Le, T. Q., & Le, C. Q. (2017). Local governance, corruption, and public service quality: Evidence from a national survey in Vietnam. *International Journal of Public Sector Management, 30*(2), 137–153. https://doi.org/10.1108/IJPSM-08-2016-0128

OECD. (2019). *Revenue statistics 2019 tax revenue trends in the OECD*. OECD Publishing. https://doi.org/10.1787/0bbc27da-en

Ogunleye, E. K., & Fashina, A. D. (2010). *The imperatives for domestic resource mobilization for sustained post-crisis recovery and growth in sub-Saharan Africa*. Retrieved from https://www.afdb.org/sites/default/files/documents/publications/session_i.2.3_2._the_imperatives_for_domestic_resource_mobilization_for_sustained_post-crisis_recovery_and_growth_in_ssa.pdf

Okogbule, N. S. (2007). Official corruption and the dynamics of money laundering in Nigeria. *Journal of Financial Crime, 14*(1), 49–63. https://doi.org/10.1108/13590790710721800

Omidi, M., Min, Q., & Omidi, M. (2017). Combined effect of economic variables on fraud, a survey of developing countries. *Economics and Sociology, 19*(2), 267–278. https://doi.org/10.14254/2071-789X.2017/10-2/20

Othman, Z., Nordin, M. F. F., & Sadiq, M. (2020). GST fraud prevention to ensure business sustainability: A Malaysian case study. *Journal of Asian Business and Economic Studies, 27*(3) Retrieved from https://www.emerald.com/insight/content/doi/10.1108/JABES-11-2019-0113/full/html, 245–265.

Ozekicioglu, S. S., & Tulumce, S. Y. (2020). The impacts of corruption on budget balance and public debt. *Journal of Management and Economics Research, 18*(3), 46–60. https://doi.org/10.11611/yead.775529

Ozili, P. K. (2018). *Tax evasion and financial instability*. MPRA Paper. Retrieved from https://mpra.ub.uni-muenchen.de/88661/1/MPRA_paper_88661.pdf

Ping, H. (2010). A typological study on money laundering. *Journal of Money Laundering Control, 13*(1), 15–32.

Puron-Cid, G. (2021). The effects of corruption of public officials on the dimensions of financial sustainability of state governments in Mexico. *Public Budgeting & Finance, 41*(2), 65–88. https://doi.org/10.1111/pbaf.12282

Rachmawati, T. (2014). Informal sector and local government revenue: The contribution of street vendors. *Jurnal Administrasi Publik, 11*(1), 25–35.

Raghunandan, A. (2016). *Government subsidies and corporate fraud.* Retrieved from https://www.uts.edu.au/sites/default/files/Aneesh%20Raghunandan_2016%20Accounting%20Researcher%20Consortium.pdf

Rapanyane, M. B., & Ngoepe, C. C. (2020). The impact of illicit financial flows on the South African political economy under Jacob Zuma, 2009–2018. *Journal of Public Affairs, 20*(2). https://doi.org/10.1002/pa.2020

Rashid, M. H. U. (2020). Taxpayers's attitude towards tax evasion in a developing country: Do the demographic characteristics matter? *International Journal of Applied Behavioral Economics, 9*, 1–19.

Rysin, V., & Antoshchuk, I. (2021). *The impact of informal employment on the formation of state budget revenues in Ukraine.*. Retrieved from http://market-infr.od.ua/journals/2021/53_2021/25.pdf.

Santos, E., Fernandes, C. I., Ferreira, J. J., & Lobo, C. A. (2021). What is the impact of informal entrepreneurship on venture capital flows? *Journal of the Knowledge Economy, 12*, 2032–2049. Retrieved from https://link.springer.com/article/10.1007/s13132-020-00701-w

Schneider, F., Buehn, A., & Montenegro, C. E. (2010). New estimates for the shadow economies all over the world. *International Economic Journal, 24*(4), 443–461.

Schwarz, P. (2011). Money launderers and tax havens: Two sides of the same coin? *International Review of Law and Economics, 31*, 37–47. https://doi.org/10.1016/j.irle.2010.12.001

Shestak, V., Kiseleva, A., & Kolesnikov, Y. (2021). Taxation issues for digital financial assets. *Social Science Computer Review*, 089443932110039. https://doi.org/10.1177/0894439321100391

Shleifer, A., & Vishny, R. W. (1993). Corruption. *The Quarterly Journal of Economics, 108*(3), 599–617.

Slemrod, J. (2007). Cheating ourselves: The economics of tax evasion. *Journal of Economic Perspectives, 21*(1), 25–48.

Sultana, N., Rahman, M. M., & Khanam, R. (2022). The effect of the informal sector on sustainable development: Evidence from developing countries. *Business Strategy and Development, 5*(4), 437–451. Retrieved from https://onlinelibrary.wiley.com/doi/full/10.1002/bsd2.217\

Tanzi, V., & Davoodi, H. R. (1998). Corruption, public investment, and growth. In H. Shibata & T. Ihori (Eds.), *The welfare state, public investment, and growth* (pp. 41–60). Springer.

Tanzi, V., & Shome, P. (1993). *Tax evasion: Causes, estimation methods, and penalties. A focus on Latin America*. Retrieved from https://repositorio.cepal.org/bitstream/handle/11362/9464/S9300142_en.pdf?sequenc

The Central Bank of West African States (BCEAO). (2013). *Base de données économique et financière (Edition en ligne)*. Retrieved from https://www.bceao.int/

The Centre for Financial Reporting Reform (CFRR). (2019). *Public sector internal audit: focus on fraud.* Retrieved from https://cfrr.worldbank.org/sites/default/files/2019-11/public_sector_internal_audit_fraud_pages.pdf

The Commonwealth Fraud Prevention Centre. (2020). *The total impacts of fraud.* Retrieved from https://www.counterfraud.gov.au/total-impacts-fraud

The Economic Times. (2022). *5 tax rules that Budget 2022 could impose on cryptocurrencies.* Retrieved from https://economictimes.indiatimes.com/wealth/personal-finance-news/5-tax-rules-that-budget-2022-could-impose-on-cryptocurrencies/room-for-crypto-in-budget-2022/slideshow/89251590.cms

The European Council. (2019). *Cyber-attacks: Council is now able to impose sanction.* Retrieved from https://www.consilium.europa.eu/en/press/press-releases/2019/05/17/cyber-attacks-council-is-now-able-to-impose-sanctions/

The European Parliament. (2019). *Cyber: How big is the threat?* Retrieved from https://www.europarl.europa.eu/RegData/etudes/ATAG/2019/637980/EPRS_ATA(2019)637980_EN.pdf.

The International Public Sector Fraud Forum. (2020). *Guide to understanding the total impact of fraud.* Retrieved from https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/866608/2377_The_Impact_of_Fraud_AW__4_.pdf

The UK Cabinet Office and 'Detica'. (2011). *The cost of cybercrime. A Detica report in partnership with the Office of Cyber Security and Information Assurance in the Cabinet Office.* Retrieved from https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/60943/the-cost-of-cyber-crime-full-report.pdf

Thiao, A., & Read, R. (2021). The effect of illicit financial flows on government revenues in the west African economic and monetary union countries. *Cogent Social Sciences, 7*(1). https://doi.org/10.1080/23311886.2021.1972558. Retrieved from https://www.tandfonline.com/doi/full/10.1080/23311886.2021.1972558

Transparency International. (2022a). *Corruption Perceptions Index.* Retrieved from https://www.transparency.org/en/cpi/2021/index/sdn

Transparency International. (2022b). *2021 Corruption Perceptions Index reveals a decade of stagnating corruption levels in Western Europe amidst ongoing scandals.* Retrieved from https://www.transparency.org/en/press/2021-corruption-perceptions-index-press-release-regional-western-europe

Tropina, T. (2016). *Do digital technologies facilitate illicit financial flows?* World Development Report. Retrieved from https://thedocs.worldbank.org/en/doc/396751453906608518-0050022016/original/WDR16BPDoDigitalTechnologiesFacilitateIllicitFinancialFlowsTropina.pdf

Ukaj, S. D. (2014). Tax evasion and the impact on economic growth. *Economica, 10*(6) Retrieved from https://journals.univ-danubius.ro/index.php/oeconomica/article/view/2614/2618

Vitvitskiy, S., Kurakin, O. N., Pokataev, P. S., Skriabin, O. M., & Sanakoiev, D. (2021). Formation of a new paradigm of anti-money laundering: The experience of Ukraine. *Problems and Perspectives in Management, 19*(1), 354–363. https://doi.org/10.21511/ppm.19(1).2021.30

Volosovych, S., & Baraniuk, Y. (2018). Tax control of cryptocurrency transactions in Ukraine. *Banks and Bank Systems, 13*(2), 89–106. https://doi.org/10.21511/bbs.13(2).2018.08

Volosovych, S., & Baraniuk, Y. (2019). State financial control in terms of digitalization of the institutional environment. *Baltic Journal of Economic Studies, 5*(4), 82–91. https://doi.org/10.30525/2256-0742/2019-5-4-82-91

Wallace, C., & Haerpfer, C. (2018). Patterns of participation in the informal economy in east-Central Europe, 1991–1998 1. In *The social impact of informal economies in Eastern Europe* (p. 19). Routledge.

Wallace, C., & Latcheva, R. (2006). Economic transformation outside the law: Corruption, trust in public institutions and the informal economy in transition countries of Central and Eastern Europe. *Europe-Asia Studies, 58*(1), 81–102. https://doi.org/10.1080/09668130500401707

Williams, C. C., & Bezeredi, S. (2018). An institutional theory of informal entrepreneurship: Some lessons from FYR Macedonia. *Journal of Developmental Entrepreneurship, 23*(3), 1850019. Retrieved from https://www.worldscientific.com/doi/abs/10.1142/S108494671850019X

Williams, C. C., & Shahid, M. S. (2014). Informal entrepreneurship and institutional theory: Explaining the varying degrees of (in)formalization of entrepreneurs in Pakistan. *Entrepreneurship and Regional Development: An International Journal* 0898–5626. Retrieved from https://eprints.whiterose.ac.uk/89077/8/Williams%20-%20Informal.pdf

Yamamura, E. (2014). Trust in government and its effect on preferences for income redistribution and perceived tax burden. *Economics of Governance, 15*(1), 71–100.

Yikona, S. (2011). *How corruption and tax evasion distort development.* Retrieved from https://blogs.worldbank.org/governance/how-corruption-and-tax-evasion-distort-development

Rita Remeikienė obtained doctoral degree in Economics, Kaunas University of Technology in 2012. Her main areas of scientific research and expertise are shadow economy, corruption, money laundering, green deal, and self-employment. Since 2021, she leads as chief researcher in two important projects, namely 'Protecting work and income in the digital economy: a case study of platform workers' and 'Model of the interaction of labour market and social support policies and development of methodologies for its implementation' (No. 13.1.1-LMT-K-718-05-0008), the last one being co-financed by the European Regional Development Fund. She works as a senior researcher at Vilnius University, Lithuania.

Ligita Gaspareniene is a senior researcher at Vilnius University. She worked as a principal researcher in the 'Welfare society' project titled 'Links between unemployment and shadow economy in Lithuanian regions'. Until now, she is a senior researcher in the project 'Model of the interaction of labour market and social support policies and development of methodologies for its implementation' co-funded from the EU Structural Fund. Professor also works in the project 'Protecting work and income in the digital economy: a case study of platform workers' funded from Lithuanian Research Council. Her interest research fields are corruption, shadow/digital economy, sustainability, and green deal.

Chapter 9
Effects on the Economic and Sustainable Development and on the Poverty and Social Inequality

Rita Remeikienė and Ligita Gaspareniene

Abstract The chapter aims to analyse the effects of the main economic and financial crimes on countries' economies and social inequality/poverty. Economic development and social inequality and poverty are examined together, since socio-economic inequality and poverty is a deep problem that becomes an obstacle to the development of the entire world economy, so the study of the effects of crime on social inequality also affects economic development. The analysis of scientific literature revealed that economic and financial crimes distort market competition, demand, prices of products/services and production factors, diminish business performance, slow down business development due to the difficulties in accessing capital, destroy normal trust-based business relationship, cause reputational damage to legitimate business and discredit legitimate transactions, thereby discouraging investment and innovation. The indirect negative effects appear as fewer opportunities to improve working conditions, business enterprises face difficulties in protecting intellectual property and patents, more funds need to be allocated to cyber security, and the risk of illegal trade in harmful waste is increasing.

The effects of economic and financial crimes on social inequality are both direct (decreasing state budget funds, higher taxes imposed on other economic entities reducing their real income) and indirect (slower economic growth). Economic and financial crimes can deeply damage normal functioning of the economic system when market mechanisms and the principles of fair competition are violated; thus, income inequality increases not only due to insufficient financing of social support, which is determined by a lack of money in the state budget, but also due to violation of the principle of justice when all market participants operating under equal conditions should have the right to a fair return/earnings.

Keywords Corruption · Money laundering · Tax evasion · Cybercrimes · Shadow economy · Illegal money flows · Fraud · Informal business · Economic and sustainable development · The poverty and social inequality

R. Remeikienė (✉) · L. Gaspareniene
Vilnius University, Law Faculty, Vilnius, Lithuania
e-mail: rita.remeikiene@tf.vu.lt; ligita.gaspareniene@tf.vu.lt

M. V. Achim (ed.), *Economic and Financial Crime, Sustainability and Good Governance*, Contributions to Finance and Accounting,
https://doi.org/10.1007/978-3-031-34082-6_9

JEL Classification K42 · H30 · H41 · J46 · J68 · J31

1 Introduction

Actuality of topic. Financial and economic crimes have a negative impact on the country's economic development, poverty and social inequality. Corruption, money laundering, tax evasion, cybercrimes, shadow economy, illegal money flows, fraud and informal business – the main financial and economic crimes that stop economic growth through investments – hinder the absorption of European structural funds. Corruption, together with other types of crime, reduces business competitiveness. Although corruption as a phenomenon does not cause poverty, it has a direct impact on economic and governance factors that in turn cause poverty. By studying the causes and consequences of crime, it would be possible to determine the interactions between the most common crimes and their impact on the country's economic development, poverty and social inequality.

The level of investigation of a scientific problem. The researchers focused their studies on the impact of financial and economic crimes on economic development and social inequality/poverty. Shah and Aish (2022), Berglund and Ekelund (2019) and Gjoni et al. (2015) focused on money laundering schemes. In the age of technology, the use of money laundering schemes and scandals, especially when the information is easily known and accessible, has a negative impact on foreign investment, because the involvement of the public in illegal activities creates distrust and damages the reputation of businesses, as a result of which investments no longer reach not only the country, but also have a negative impact business value. Dirty money distorts the consumer market, as it aims to legalize it in the market by purchasing certain jewelry products, real estate luxury goods and works of art. Paying extra with dirty money does not pay attention to the price, so the real value of these purchases is artificially inflated.

Economic entities that pay less taxes have more income. This is how income inequality is formed, money laundering promotes income inequality because 'laundered' money is reinvested in similar criminal activities, that is, criminals are getting rich and the criminal sector is expanding faster than other sectors.

Other researchers (Alm & Kasper, 2020; Baumann & Friehe, 2010 and others) have analysed tax evasion, which promotes the transfer of production factors from taxed to tax-avoiding sectors of the economy, as a result of which the prices of final products rise. In order to avoid taxes, companies are forced to invest less in order to ensure their future survival. The widespread practice of tax evasion can seriously damage the normal functioning of the economic system, so income inequality tends to increase due to the insufficient financing of social support, which is determined by the lack of money in the state budget (Argentiero et al., 2021).

Researchers of another direction focused on cybercrime (Steinberg, 2019, and others). Businesses suffer from high levels of intellectual property theft and espionage. Computer and financial service providers, as well as companies in the pharmaceutical, biotechnology, electronic and electrical equipment industries, are the

most common victims of cybercrime. Cybercrime is also becoming a means of escaping poverty.

The scientific problem is formulated as a question: What are the consequences for economic development and social inequality and poverty caused by the main economic and financial crimes?

The aim of the chapter is to analyse the effects of the main economic and financial crimes on countries' economies and social inequality/poverty.

In order to achieve the goal, a comparative and systematic analysis of the scientific literature will be performed. Economic development and social inequality and poverty are examined together, since socioeconomic inequality and poverty is a deep problem that becomes an obstacle to the development of the entire world economy, so the study of the effects of crime on social inequality also affects economic development.

2 Literature Review and Research Design

One of the main negative directions of the impact of economic and financial crimes on business is undermining the private business sector. As stated by McDowell (2001), the most detrimental microeconomic effects are felt in the private sector.

Money launderers often use front companies, which co-mingle proceeds from illegal activities with legitimate funds to hide ill-gotten gains. In other words, money laundering tends to discourage or frustrate legitimate business enterprises (Murithi, 2013). Front companies have access to large amounts of illegal funds that allow them to subsidize the production of camouflaged products/services and offer these products/services at significantly lower than market prices. In some cases, camouflaged products/services can even be offered at a lower price than their self-cost (McDowell, 2001). Thus, front companies distort the market competition and hinder the performance of market-efficient business companies (microeconomic effect) that are forced to attract capital funds from the financial markets at a higher price. Business conduct without following the principles of the free market at the same time leads to a negative macroeconomic impact (under the assumption that macroeconomic (in)-efficiency is determined by the (in)efficiency of individual business enterprises). Dobrowolski and Sulkowski (2019) emphasize the negative impact of money laundering on markets and innovation development.

Gjoni et al. (2015) point out that upon a 'dirty' money transfer, a beneficiary tends to acquire assets (real estate, jewellery, works of art and luxury goods), which leads to a distortion of consumption demand. In addition, money launderers are ready to pay more for purchases than the real value of these purchases because they want to spend the illegally obtained money as quickly as possible. With large funds at their disposal, money launderers can pay far more than the true value of the assets. This artificially raises the prices of assets and goods (especially real estate, jewellery, works of art, luxury goods) and creates a price disequilibrium and artificial flows of goods and assets. The empirical study by Shah and Aish (2022) confirms that money

laundering and corruption have a statistically significant positive relationship with inflation.

The negative impact of money laundering on legitimate business also appears as discrediting the legitimate transactions. Suspicions or knowing that part of the market transactions are carried out through money laundering schemes makes legitimate transactions no longer attractive to foreign investors. This is because the involvement of a part of society in illegal activities causes distrust of other economic agents who alienate their investment (Gjoni et al., 2015). The similar conclusions were drawn by Berglund and Ekelund (2019) who state that in the Information Age, when business is more than ever exposed to news and media, money laundering scandals cause reputational damage to business and have a negative impact on the value of business in stock markets.

According to Abdixhiku et al. (2017), ***tax evasion*** in business is mainly affected by the tax burden, distrust in public institutions, the level of corruption, the share of cash in payments (the sectors characterized by a larger number of cash transactions tend to be more evasive) and the size of a company (larger companies are less prone to tax evasion). Having researched the effects of tax evasion, Baumann and Friehe (2010) state that tax evasion can affect activeness of a business enterprise. The authors argue that activeness of a business enterprise in a given period depends on the level of investment, which, in its turn, is determined by the level of tax evasion in this enterprise. The relationship between the level of tax evasion and the level of investment is shaped as follows: Tax evasion tends to raise a company's future payoffs, but at the same time it reduces the level of investment (i.e. by evading taxes, a company needs to invest less to ensure its survival in the future). Similar results were provided by Carvalho (2019) who found that a decision of a business company to evade taxes resembles a decision to form an investment portfolio: Investing in risky assets is associated with a decision to evade taxes, and vice versa – investing in risk-free assets is associated with a decision to pay taxes honestly. Thus, the decision to evade taxes affects business activity in the same way as operation in higher risk conditions.

Alm and Kasper (2020) suggest that tax evasion stimulates the transfer of production factors from tax-compliant to tax-evading economic sectors, which leads to a relative increase in the prices of production factors (labour and capital) and thus of final products. In other words, businesses operating in the formal sector start incurring higher production costs, which forces them to raise prices for consumers. An increase in prices is likely to result in less production being purchased, thus reducing business turnover, that is, tax evasion causes cascading market corrections and general supply and demand equilibrium adjustments. It also tends to change the incentive structure of both businesses and consumers. If the practice of tax evasion in business is successful, the number of tax evaders in the market will be growing. However, the more participants engage in this practice, the less significant is advantage of tax evasion; the advantage is eliminated by the potential of competition and substitution.

By employing the structural equation modelling (SEM), Zhang et al. (2016) researched the relationship between tax evasion and corporate financial performance

(i.e. market value of the Chinese corporations in the research sample). The authors note that business managers use tax evasion as an instrument to engage in rent seeking activities, but this practice diminishes shareholders' value. A statistically significant positive indirect relationship was detected between tax evasion and corporate market value. This relationship is explained in light of the tendency to consider tax evasion as one of the factors of business growth and profitability. According to Swenson (1999), stock exchanges treat low taxes paying companies as the ones effectively controlling costs, so their share prices are higher. Similar results were provided by Handayani (2020). After conducting a quantitative study with a sample of manufacturing companies listed on the Indonesia Stock Exchange between 2016 and 2018, Handayani (2020) found that tax evasion is related to information asymmetry in financial statements of manufacturing companies; nevertheless, return on investment and liquidity indicators remained sufficiently high (an average ROA of 7.9%; the average value of CR of 2.55), share prices did not fall, and the companies did not lose investors' trust because they delivered the attractive financial indicators showing good business performance.

Hanlon and Slemrod's (2009) as well as Chen et al.'s (2014) studies provide opposite results showing that share prices of the companies that engage in tax evasion or sheltering tend to decline. Having researched a sample of Vietnamese listed firms in the period 2010–2016, Khuong et al. (2020) obtained mixed results in terms of the relationship between tax evasion and business performance: Their empirical findings suggest that the effects of tax evasion on business performance can be either positive or negative, depending on how both of the variables are measured.

Thus, the results of some studies imply that tax evasion can be treated as a business value-adding activity on stock exchange, but it should be noted that to be able to successfully exploit this advantage, business companies need to impose the extremely strict internal management and control because any conflicts of interest between business managers and shareholders as well as opportunistic management may lead to a decrease in the company's value (Desai & Dharmapala, 2009).

Having researched the effects of the ***shadow economy***, Hassan (2017) found that the shadow economy intensifies unfair market competition that is especially harmful to formally operating and law-abiding business enterprises which, by paying higher taxes, are able to add lower value both to their products/services and to the general economy. In addition, incurring higher operating costs, law-abiding businesses can devote less funds to improving working conditions for their employees. These factors reduce business competitiveness not only in local but also in international markets and reduce the confidence of international investors (Vinnychuk & Ziukov, 2013). According to Sultana et al. (2022), the production and business activities carried out in the informal sector do not ensure long-term economic efficiency. Business in this sector is characterized by a decentralized model of economic organization; business coordination and planning become a difficult task since production factor, resource and product markets are distorted. Estevao et al. (2022) note that if the level of the shadow economy is high, the general economy will run based on the ineffective tax and licensing systems, which raises the risk of collapse

of the formal sector. Vinnychuk and Ziukov (2013) argue that the shadow economy destroys business relationship, which leads to the decline in production. Mroz (2010) suggests that operating in the informal sector causes a considerably higher risk for business, and the costs incurred to hide informal activities are higher than the costs of formal activities (e.g. part of the VAT tax cannot be reclaimed, the costs of fuel, expenses of business trips, secondments, etc., that reduce the taxable profit cannot be attributed to deductible expenses). The internal level of business is at risk of illegal arbitration and insider trading, while the market share is threatened by an increased risk of fake products and branded piracy, difficulties in protecting intellectual property and patents, and a higher risk of illegal trade in radioactive and other harmful waste.

On the other hand, as stated by Arsic and Krstic (2015), the shadow economy can contribute to the growth of the formal sector: Since the shadow and formal economies are substitutes, the effects of the shadow economy are multiplicative. An economic agent selects between operating in the formal and informal sector; not starting a business (being unemployed) is not considered an option. This view is supported by Estrin and Mickiewicz (2012) who suggest that the shadow economy tends to increase the likelihood of entrepreneurial entry. Djankov et al. (2002) argue that in the countries where the official costs of entry are very high, operating in the informal sector helps businesses to circumvent the impediments. This means that having intentions to try out a business, new entrepreneurs first tend to choose activities in the less binding informal sector, and if the business goes as expected, it is transferred to the formal sector. The authors, however, note that this linear relationship between the shadow economy and entrepreneurial entry is U-shaped: Entrepreneurial entry is least likely when the level of the shadow economy reaches about a quarter of GDP.

Enste (2018) argues that by operating in the informal sector of the economy, entrepreneurs can reduce high costs and administrative burdens and bypass inefficient bureaucracy. Schneider et al. (2010) believe that the shadow economy can become a ‘safe harbour’ for business during the periods of economic crises and turmoil. From this point of view, operation in the informal sector becomes essential for establishing or maintaining a business.

Thus, there are the proponents of a positive effect held by corruption and shadow economy upon economic and sustainable development. This positive effect is also known as ‘grease the wheels’. Supporting this view, there are findings documenting that corruption may actually help firms circumvent government regulation and therefore the firm grows. This is also the case of several countries such as China, Vietnam and Cambodia, which face economic growth in spite of their lack of good governance (Achim & Borlea, 2020; Hoinaru et al., 2020; Beck & Mahler, 1986; Caselli & Michaels, 2013; Jiang & Nie, 2014). In addition, there is evidence that the shadow economy, especially in corrupt countries, represents an important buffer for solving many economic problems (Zaman & Goschin, 2015).

Sultana et al. (2022) note that ***informal entrepreneurship*** is often carried out by individuals who are both workers and business managers (e.g. in the case of self-employment or when an initiator of informal entrepreneurship not only organizes

and coordinates the business, but also performs the functions of an employee). For this reason, management of an informal business is often inefficient because the individuals running this business lack the relevant knowledge and skills. This view is supported by Rothenberg et al. (2016).

Eijdenberg et al. (2019) and Azunre et al. (2021) believe that informal entrepreneurship is characterized by small-scale production and under-capitalization, it does not ensure appropriate distribution of labour and capital, workers who work without employment contracts are socially vulnerable, and the business itself tends to be short term, since it does not have sufficient coverage by formal agreements. Ruzek (2015) adds that the level of business organizing and technology is usually low here, since the major goal is to earn income in the current period, and no investment is made. Due to the impact of the above-mentioned factors, the business is not sustainable.

Estevao et al. (2022) note that informal entrepreneurs find it difficult to get credits and attract investment (in the case of informal operating, investors' interests are not protected). Santos et al. (2021) see the difficulties in attracting venture capital since access to this capital depends on proper functioning of formal institutions.

Piperopoulos et al. (2021) analysed the impact of informal entrepreneurship on small businesses operating in the formal sector. Their empirical analysis included 11,988 observations in 110 emerging economies. The results of the study confirmed that informal entrepreneurship has a negative impact on small businesses operating in the formal sector. Both formal and informal businesses operate in the same markets and, depending on the nature of their activities, target similar consumer groups. Thus, informal entrepreneurship takes market share away from formal business. The OECD's (2010) report proposes that informal entrepreneurship infringes the intellectual property rights of formal business and undermines the incentives to implement innovation. Piperopoulos et al. (2021) found that the effect of informal entrepreneurship on small businesses operating in the formal sector is stronger in an institutional environment characterized by a complex judicial system, but weaker in an institutional environment characterized by complex tax regulations. In the first case, the institutional environment does not protect property rights of the companies operating in the formal sector; the measures to enforce contract terms and resolve business disputes are not effective, so it is difficult for formal companies to effectively protect themselves from the impact of informal entrepreneurship. In the second case, with a complex tax system, even companies operating in the formal sector face the conditions of uncertainty and incur higher transaction costs. From this perspective, the conditions for conducting formal and informal business are similar.

On the other hand, some sources (McGahan, 2012; de Castro et al., 2014) propose that symbiosis between formal and informal entrepreneurship is possible. For example, companies operating in the formal sector may choose to cooperate with informal entrepreneurs by concluding agreements on subcontracting, outsourcing labour-intensive work, selling or reselling low quality products that do not meet market standards, etc. Having analysed the World Bank Enterprise Survey data, representing 127 states, and the determinants of business performance, Williams et al. (2016) found that the companies whose activities are started as informal

entrepreneurship to evade registration costs and get established in the market later (i.e. after registering the business) tend to have higher annual sales, more stable employment and greater productivity growth rates compared to the companies that were formally registered from the beginning of their activities. These findings imply that informal activities at the beginning of a business can help form stronger foundations for further business development and growth.

Corruption, according to Ahmed and Alamdar (2018), who researched the effects of corruption and budget deficit on the investment in the private sector, has a negative impact on business development and performance because a high level of corruption in the country reduces investment in the private sector. This view is supported by Hoinaru et al. (2020) who state that a high level of corruption hinders not only investment, but also absorption of the European Structural Funds. Ahmed and Alamdar (2018) cite the results of Mauro's (1995, 1996) econometric analysis (covering a sample of 67 countries in the period 1960–1985), which showed that corrupt countries tend to have statistically significantly lower investment rates, and economic growth is limited specifically through the investment channel. The mathematical calculations disclosed that a one standard deviation improvement in corruption index (i.e. even a small decrease in the level of corruption) tends to raise investment by 5 percent of GDP. Ahmed and Alamdar (2018) researched the situation in Pakistan over the period 1984 to 2015. To check the cointegration between the variables (corruption and the private sector investment), the authors selected Johansen and Juselius's (1990) method and an Error Correction Model. The results confirmed that corruption has a significant negative impact on investment in the private sector, that is, they confirmed that investment in the private sector is affected not only by purely economic factors, but also by latent social phenomena.

After conducting a study of 11,000 business enterprises in developed and developing countries, De Rosa et al. (2010) found that bribery of public officials practiced by representatives of business companies to bypass bureaucratic obstacles does not help to achieve higher productivity, and corruption has a negative impact on business performance. Similar results were provided by Brzic et al. (2021) who focused on the relationship between corruption and business productivity and researched a sample of 62 European telecommunications companies in the period 2012–2019. The results of their research disclosed that corruption has a negative impact on business productivity. Achim's (2017) study, which examined a sample of 185 countries in the period 2012–2015, confirmed the negative effects of corruption on business development: The author found that corruption negatively affects the factors representing business development, such as ease of doing business, the level of entrepreneurship and market capitalization.

Having surveyed representatives of the private business, Gaviria (2002) found that corruption significantly reduces the growth of sales, and corruption, together with other types of crime, diminishes business competitiveness. Chen and Cheng (2019) provide evidence confirming the detrimental effects of corruption on new business establishments in the USA over the period 1997–2012. Their study also disclosed that the negative impact of corruption on business is enhanced by a high bureaucratic level of business regulation.

On the other hand, after researching the Chinese market in the period 1999–2007, Jiang and Nie (2014) found that corruption has a positive effect on profitability of private companies (by shortening bureaucratic procedures and helping to bypass hindering regulatory provisions). Corruption is treated as a cost of opening up wider opportunities for business. In this respect, corruption helps to allocate resources better, thus increasing business productivity. But according to Hoinaru et al. (2020), it is more characteristic of ineffectively regulated low-income countries, and according to Sahakyan and Stiegert (2012), the nature of the relationship between corruption and business performance may depend on a company's size, age and the number of business competitors (it is stated that corruption can improve business performance for larger, younger and less competitive companies).

Chenguel (2020) analysed the effects of corporate ***financial frauds*** (misappropriation of assets, manipulation of financial results, incomplete or misleading disclosure of financial and accounting information) and found that public information about the cases of fraud makes investors question the competence and vigilance of the market regulators (this is especially true for financial markets), and all business-related agents – auditors, financial analysts, members of the board of directors and credit rating agencies – must assume their responsibility. The companies that are exposed to fraud not only suffer financial losses, but can also lose some employees due to the damaged reputation. Dyck et al. (2017) link the costs of corporate fraud to the deadweight business value destruction, which is capitalized in a company's equity value. Chenguel (2020) states that within a few months after the announcement of fraud and embezzlement, the action is plummeted and the company is sold or declares bankruptcy. Even after a judicial restructuring, stakeholders lose everything.

The report provided by the Commonwealth Fraud Prevention Centre (2020) suggests that fraud pushes business clients/customers into a vulnerable position. Feeling vulnerable, the clients/customers can decide to refrain from having any business with a fraudulent company, which may result in business collapsing. The negative impact of fraud on competition and market functioning is also confirmed: By taking advantage of illegal activities, fraudsters can gain a competitive advantage in the market. Unable to compete fairly, legitimate businesses can be forced to leave the market or become bankrupt. This way, fraudsters can achieve a monopoly over the market. In a monopoly, the goods and services provided to clients/customers may not meet their needs, but they will still have to buy the goods and services on offer having no other choice.

Additional costs are treated as another significant aspect of the negative impact of fraud on business. These costs are significant and extensive, and they cannot be underestimated. The Commonwealth Fraud Prevention Centre (2020) indicates the following additional costs incurred by business because of fraud:

- Assessment costs (sufficient resources must be allocated, and the staff must constantly monitor the situation and assess when to start an investigation)
- Detection costs (implementation of fraud detection, technology tools, data analysis systems)

- Investigation costs (although the pretrial investigation is carried out by public institutions, the detailed analysis of these costs can determine business priorities for prevention; investigation costs also cover the costs incurred by business companies when their personnel must provide evidence, testify in court proceedings, review findings to reveal system and software vulnerabilities, etc.);
- Response costs (if a fraud is identified, this requires additional resources for reversing the damage, further protection and prevention; these costs also include cancelling a service; administrative actions require organizational resources in terms of time and briefing)
- Restitution costs (resources are required to restore normal provision of services, compensating victims for losses, setting up new accounts, restoring lost identities)
- Program/system review and audit costs (costs to pay external consultants and auditors)
- Retrofitting and redesigning programs/systems (if repeated frauds reveal vulnerabilities in business programs/systems, they need to be redesigned and retrofitted, which causes significant costs (e.g. process design, operations, project management and digital costs)

Frauds observed in a certain sector or business lead to increased regulation, so legitimate businesses incur additional costs of checks and processes. On the other hand, if a large number of frauds are recorded in a certain sector, the authorized institutions may not have enough staff to carry out regular inspections. Therefore, the inspections can be incomplete and insufficiently qualified, and the inspectors can be overloaded with work. All this indicates a lower quality of services that the business sector receives from state institutions.

Finally, if systemic frauds are characteristic of an entire economic sector, they can undermine the integrity of this sector (The Commonwealth Fraud Prevention Centre, 2020). Legitimate businesses will still be thought of badly simply because they operate in that sector (reputational damage). From a national perspective, the potential of that sector to provide quality goods and services will be lost.

Gordon (2020), however, states that in the periods of economic hardship, the need to survive can override other motives. Although economic downturns are cyclical, a recession can last longer. A financial crisis, an external trade shock, an adverse supply shock and inflating costs are the factors that increase pressures on business companies to 'make ends meet'. A company may need to downsize, and having fewer people to do all the work is likely to reduce the company's morale. Under these conditions, a business may choose to break the rules in order to survive. In other words, during the periods of economic decline and recession, business companies have motivation, pressure and incentives to engage in fraudulent activities. Financial statement frauds, misappropriations, false asset values and overstatement of revenue are the most common fraud schemes indicated in the article (Gordon, 2020).

According to Bhusal (2016) and Binawa and Ihendinihu (2018), ***illicit financial flows*** refer to the illegal flows of financial funds across borders through misinvoicing

of imports and exports (misrepresentation of price or volumes of goods in invoices), and abusive transfer pricing. It is often related to money laundering and tax evasion. Fumpa-Makano (2019) notes that illicit financial flows help business companies remit their profits as loyalties to their subsidiaries and thus benefit from lower taxes (raise profits at the expense of lower taxes). Herkenrath (2014) emphasizes the goals of concealing illegal activities and tax evasion. The author treats these goals as the reaction of investors or businesses to unfavourable investment conditions (i.e. through illicit financial flows, attempts are made to artificially improve investment conditions). This business decision is considered a utility maximization goal, although the relative level of risk is recognized (Letete & Sarr, 2017). The risk is associated with possible depreciation, liquidity premiums, investment risk, return differentials, etc. (Osman & Salifu, 2022), and the potential of secretly transferring the proceeds from illegal activities abroad tends to raise the risk premium (Moore, 2012). Brandt (2022) argues that when conducting opaque international transactions, illicit financial flows lead to unfair competition in international markets and cause misallocation of resources.

Price and Sun (2017) link involvement in illicit capital flows with corporate social irresponsibility. Their research reveals interesting results showing that the incidents of corporate social irresponsibility have a longer-lasting effect than the initiatives of corporate social responsibility, but regardless of whether businesses are socially responsible or not, the ones that do little social irresponsibility or little social responsibility tend to perform better than those who are extremely actively involved in any of the aforementioned phenomena.

The report by the UK Cabinet Office and 'Detica' (2011) suggests that although ***cybercrime*** has a considerable impact on the government budget, public services and citizens, the biggest damage is caused to the business sector: The calculations show that the costs of cybercrime incurred by businesses in the United Kingdom reach up to £21 billion. Despite the differences in calculation methodologies, underreporting by victims and the paucity of data collection by governments, the global costs of cybercrime amount to nearly $600 billion (CSIS, 2018). Steinberg (2019) indicates that cybercrime costs for a business enterprise (regardless of the size of a business) average about $200,000 and provides the forecasts that cybercrime costs should reach about $5.2 trillion worldwide in the next five years. More than half of small businesses have suffered cybercrime attacks in the last year, and only 14 percent were ready to defend themselves (Steinberg, 2019). Businesses suffer from high levels of intellectual property thefts and espionage. The companies considered most common victims of cybercrime are computer and financial service providers, as well as the companies operating in the pharmaceutical, biotech, electronic and electrical equipment industries (The UK Cabinet Office and 'Detica', 2011).

The CSIS (2018) report, which analyses the economic impact of cybercrime, identifies the negative directions of the cybercrime's impact on business:

- Business loses intellectual property and intellectual information.
- Stolen identities promote further online fraud.

- Business suffers damage when cybercriminals abuse the sensitive business information about possible mergers or the preliminary information about the performance of the companies listed on stock exchange.
- Business incurs opportunity costs when normal production or service provision activities are disrupted. Opportunity costs also cover the costs incurred by business to restore systems after cyberattacks and repair the damage caused by ransomware, which involves payments to redeem encrypted data, business network protection costs, cyberinsurance, etc.
- Business may suffer reputational damage if the trust in its online activities (e.g. online shopping, security of payment systems) is decreasing; there is a risk of legal liability for improperly handled and stored customer personal data, etc.

Smith et al. (2019), who analysed the impact of cybercrime on corporate stock value based on the financial data of the companies that became victims of cybercrime, found that cybercrime had a negative impact on the stock prices of these companies throughout the period under consideration, which damaged business reputation and disappointed investors' expectations. The CSIS (2018) report notes that the indirect costs associated with cybercrime, for instance, the costs of individual decisions when individuals (e.g. consumers of goods and services) choose traditional ways of purchasing goods and services to avoid the risks related to online transactions, are difficult to calculate.

According to Gordon (2020), an even greater risk of cyberattacks is observed in the periods of economic recession, when cyber criminals seek to take advantage of business vulnerabilities: During an economic recession, businesses are forced to reduce their expenditure, which can negatively affect business cyber security and security of the personal data accumulated in business databases. Frauds and intellectual property thefts account for the majority of losses caused by cybercrime, but recovery and opportunity costs, lost income and greater expenditure on cyber security are also significant negative effects. The wide availability of exploit kits, custom malware, botnet rentals and ransomware further increases the threat of cybercrime and business losses. Paradoxically, businesses affected by various forms of cybercrime treat the financial losses as unavoidable costs of doing business online (CSIS, 2018).

A rapidly growing form of cybercrime is the use of ransomware. The common victims of this cybercrime are businesses and individual users. Although a significant proportion of victims do not pay the ransom, a sufficient proportion do, which makes this form of crime is profitable. Recently, commercialization of ransomware has been noticed: In some cases, the median cost of a ransomware package is only $10, which encourages hackers to carry out ransomware attacks (CSIS, 2018).

To protect themselves against the detrimental effects of cyberattacks, businesses are suggested to invest in the physical security of operating systems (e.g. to install 'airgapped' networks, advanced intruder detection hardware) and staff training. This is especially important for the business sectors that use and store a lot of IP data (e.g. pharmaceutical, biotech sectors) (the UK Cabinet Office and 'Detica', 2011).

Trozze et al.'s (2022) study confirmed that the frequency of ***cryptocurrency frauds*** and the losses caused by these frauds are growing rapidly worldwide, and the digital space along with the characteristics cryptocurrencies – decentralization and pseudo-anonymity – provides many unexploited opportunities for crime. Academic literature tends to focus on ransomware, smart Ponzi schemes and (synonymous) high-yield investment programmes (HYIPs), followed by undefined or general fraud and scams (Trozze et al., 2022). The investment in cryptocurrencies can seem modern and efficient, although its returns are often volatile, but the risk of loss is extremely high, especially considering the fact that the cryptocurrency market is poorly regulated (Feinstein & Werbach, 2021). Various Ponzi schemes and ransomware are considered the most profitable and feasible, which shows that this type of scams causes most substantial losses for investors (Trozze et al., 2022). Business companies are even being created to fraudulently offer cryptocurrency mining investments (Povich, 2021). This practice damages the reputation of the investment business, reduces the confidence of investors (both private and institutional) and unbalances the financial markets by distorting the legitimate profits generated by cryptocurrencies. Feinstein and Werbach's (2021) research revealed that even when applying various models of legal regulation of cryptocurrencies, the influence of the regulation is practically not felt (the largest part of the models under consideration yielded almost entirely null results). This leads to the conclusion that even legal regulation is not yet capable of ensuring anti-money laundering and anti-fraud enforcement actions in the area of trading in cryptocurrencies.

As stated by Hillendahl (2022), although the true negative impact of cryptocurrency scams on business is difficult to assess and measure, the main problem area remains the damage caused by thefts of personally identifiable information (PII) that occur during fraudulent cryptocurrency transactions. The stolen funds can be diverted to a legitimate business and converted into some traditional currency that is considered legal tender. In addition, companies that use cryptocurrency payments in their operations may suffer from spoofed apps or websites, which can cause reputational damage if consumers fall victim to a scam.

Economic and financial crimes are associated with significant social costs. In a general sense, these crimes shift the economic power from the market, national government and citizens into the hands of criminals (Safdari et al., 2015). The need for additional resources for identification and prevention of economic and financial crimes means that budget funds that can be allocated to the development of social services (e.g. health care, education) and social support, necessary to socially vulnerable population groups, are decreasing. Kumar (2012) points out that economic and financial crimes have a particularly harmful social impact since the number of victims of these crimes is significantly higher than the number of victims of other crimes. Due to their negative social impact, economic and financial crimes harm people who *prima-facie* do not appear to be direct victims of these crimes.

Okunlola (2014) argues that ***money laundering*** tends to raise pressure on social stratum: It undermines the existing ethical standards and creates the illusion that it is worth engaging in criminal activities. The state's expenditure on the fight against

crime inevitably grows, while social needs of the population remain in the background.

Ogbodo and Miesheigha (2013) note that money laundering and the predicate offenses (drug trafficking, arms trafficking, corruption, tax evasion, terrorism, etc.) cause the tax gap, that is, money launderers pay less taxes than the economic agents who declare their income. The authors present the statistical data showing that this tax gap in Africa is estimated to amount to over 40 percent. Economic agents who pay less taxes have more income at their disposal. This is how income inequality is formed.

Gjoni et al. (2015), who focused on the economic and social impact of money laundering, draw attention to the increase in social inequality caused by formation of criminal organizations. Having gained economic power through money laundering activities, criminal organizations can establish and expand businesses, and their welfare is increasing; in the meantime, not being able to compete with criminal organizations, legitimate entrepreneurs do not earn potential income, so their well-being is decreasing, while income inequality is increasing. This view is supported by Safdari et al. (2015). Okunlola (2014) argues that money laundering stimulates income inequality, as the 'laundered' money is reinvested in similar criminal activities, that is, criminals are getting richer, and the criminal sector is expanding faster than other sectors.

McDowell (2001) suggests that additional costs, though not so clearly visible, include treatment of drug addicts, if drug trafficking is widespread in a particular country. The similar argument is expressed in Okunlola's (2014) study (drug trafficking often results in negative health consequences and leads to higher healthcare costs). The need to divert state budget funds for other purposes damages population's economic and social security and stimulates the spread of poverty (Safdari et al., 2015). By building a general equilibrium model, Araujo (2006) provides the evidence the money laundering has a negative impact on per capita consumption, which confirms the assumption that money laundering is related to the decrease in the purchasing power of society.

McDevitt's (2009) study, however, shows that there is no clearly visible connection between money laundering and poverty, as well as between anti-money laundering initiatives and poverty reduction. It is stated that anti-money laundering initiatives are expensive to implement, so developing countries incur soaring opportunity costs by diverting funds from social development programs to implementation of anti-money laundering initiatives.

The early theoretical propositions concerning the relationship between ***corruption*** and income inequality arise from Krueger's (1974) and Rose-Ackerman's (1978) studies which suggest that corruption allows certain groups of society (mostly public officials and public servants) to profit, and this eventually leads to a growing level of income inequality.

Chetwynd et al. (2003) argue that corruption as a phenomenon does not cause poverty, but it has a direct effect on economic and governance factors that, in their turn, produce poverty. Regarding the impact of corruption on economic factors, it is noted that corruption distorts markets, reduces investment and leads to economic

inefficiency due to higher costs of doing business. The above-mentioned factors, in their turn, lead to income inequality, thus deepening poverty. The analysis of the impact of corruption on governance factors reveals that corruption erodes the institutional capacity of a country's government to provide qualitative public services; due to corruption, investment is diverted from the public sector to capital projects, corruption is associated with noncompliance with safety and health requirements and greater budgetary pressure on the national government. These factors stimulate poverty. It is concluded that the overall negative distributional effects of corruption are more severe with a higher level of corruption.

By applying the dynamic panel system GMM estimators to research 97 countries during the 1997–2006 period, Negin (2010) finds the bidirectional causality between corruption and poverty; the effect of corruption on poverty is recognized to be both direct and indirect (through slower economic growth). Negin et al. (2010) support this view and note that corruption aggravates living conditions of the poor because it distorts the decision-making process at the institutional level and hinders the development of productive social programs (e.g. in the areas of education and healthcare) due to channelling of monetary funds to large capital-intensive projects. Ardigo (2020) states that the phenomenon of corruption rooted in society, especially characteristic of developing countries (the author examines the case of Guatemala), impoverishes its victims and is sometimes even the only way for a discriminated population to meet their basic needs.

The empirical evidence that corruption exacerbates social inequality and causes degradation of living standards in the long run was also provided by Justesen and Bjornskov (2014), Habibov and Cheung (2016), Dimant and Tosato (2018) and other researchers. Negin (2010) states that in low-income economies, corruption even threats the global fight against poverty.

Carvalho (2019), who researched the economic effects of ***tax evasion***, states that tax evasion has a negative impact on the well-being of economic agents and households: The author argues that tax evasion that determines insufficiency of the government budget revenue for public needs (e.g. the development of public infrastructure, education, social and health protection, national security) can force the national government to raise tax rates, which will reduce the real income available to economic agents and households, and thus can deepen their social exclusion. The similar view is provided Kumar (2012) who states that the lack of money in the state budget, caused by tax evasion, does not allow to implement targeted social support and development schemes, thus negatively affecting the part of the population that could benefit from implementation of the target schemes. Matsaganis and Flevotomou's (2010) estimates indicate that income under-reporting of 10 percent tends to result in a 26 percent shortfall in tax collection; thus, this proportion reduces the share of the state budget that could be allocated to implementation of the targeted social support and development schemes. The authors confirm that tax evasion causes lower progressivity of the income tax system and leads to income inequality and poverty. Similar results concerning both lower progressivity of the income tax system and income inequality caused by tax evasion were provided by Vousinas (2017).

Koyuncu and Unal (2018) add that if a part of society cannot effectively use social assistance, society's standards of living are decreasing and human development is deteriorated. Having researched 36 OECD countries over the 1999–2010 period, the authors found that tax evasion has a particularly strong negative effect on human development in the long run, and poverty is a side effect of the relationship between tax evasion and deteriorated human development.

Alstadsaeter et al.'s (2019) study proposes that tax evasion can stimulate inequality since the potential to evade taxes tends to expand with income, that is, economic agents (both individuals and legal entities) earning much income tend to look for and find more opportunities compared to economic agents earning little income to use the advantages provided by so-called tax haven regions, to disguise and hide part of their income and assets. The authors state that economic agents at the top of wealth distribution evade nearly 30 percent of taxes, while the average of tax evasion amounts to approximately 3 percent.

Thus, the relationship between tax evasion and inequality is recognized in many previous studies. However, Argentiero et al. (2021), who studied the relationship between tax evasion and inequality through the lens of behavioural economics and the empirical data analysis, note that it is difficult to determine the direction of the relationship between these two variables, that is, it is difficult to determine whether inequality is a consequence of tax evasion or vice versa. Nevertheless, it is recognized that the widespread practice of tax evasion can deeply damage normal functioning of the economic system, when market mechanisms and the principles of fair competition are violated; thus, income inequality tends to increase not only due to insufficient financing of social support, which is determined by the lack of money in the state budget, but also due to violation of the principle of justice which stipulates that market participants operating under equal conditions shall receive a fair return/earnings.

Sultana et al. (2022) analysed the relationship between the ***shadow economy*** and working poverty in 50 developing countries over the 2010–2019 period. They suggest that the informal economy links two interrelated vicious cycles – poverty and development. On one hand, poverty is associated with low income, low productivity, labour rights abuses, unfair competition and environmental degradation, while development is associated with higher income and improved well-being of the population. Therefore, when trying to achieve economic and social efficiency, one of the main goals to be pursued is transforming informal activities into formal ones.

Mishchuk et al.'s (2020) research revealed the negative impact of the shadow economy on the major components of social safety in Ukraine: the spread of poverty, a high share of food expenditure, lower living standards and limited household opportunities. The correlation coefficients confirmed the existence of the relationship between the shadow economy and economic safety, and the shadow economy and social safety ($-$ 0.865 and -0.560, respectively). According to Bilan et al. (2020), by reducing the government budget revenue, the shadow economy not only causes objective social consequences, but also impedes a country's socio-economic development, primarily in terms of preservation of human capital.

Enste's (2018) study, however, proposes that the shadow economy can improve the socio-economic situation of economic agents since this phenomenon is usually formed as a response to the increasing tax burden and more stringent governmental regulation in industrial countries. Thus, by not paying all or part of taxes and social security contributions, economic agents can raise their real income, which will later be spent on consumption in the official economy (Hassan, 2017). The study by Arsic and Krstic (2015) implies that the shadow economy has a greater impact on household income than on consumption. In addition, operating in the informal economy can provide income for subjects who are unable to find permanent employment and/or receive no other income. The positive effects of the shadow economy in terms of providing conditions for alternative employment, especially in emerging economies, were confirmed by Mishchuk et al. (2020). The authors note that operation in the informal sector helps less competitive part of the population earn a living. In this respect, the shadow economy is treated as the option 'exit' or 'survive', selected by subjects who feel overburdened or neglected by the state (Arsic & Krstic, 2015). It is, however, emphasized that in the long run, the shadow economy poses a threat to economic development and raises social risks, especially in relation to that part of society whose income depends to a significant extent on redistribution of tax revenue collected in the state budget.

When analysing the relationship between ***informal employment*** and social issues, it is argued that the relationship between informal employment and poverty is bidirectional: On one hand, it is believed that informal entrepreneurship tends to raise the level of poverty because workers in this sector usually work for low wages and are socially vulnerable without receiving social guarantees (Larsson & Svensson, 2018; Mishchuk et al., 2020, Sultana et al., 2022, etc.); on the other hand, poverty is considered one of the reasons for the individual decision to operate in the informal sector, the last hope of the poor (often unskilled, low-paid workers) to earn at least some income (Basu & Chau, 2015; Ghose, 2017, etc.). The statistical data of the International Labour Organisation (2020) proposes that informal entrepreneurship provides opportunities to earn income for nearly 2 billion workers worldwide. Chrenekova et al.'s (Chrenekova et al., 2016) survey of economic agents operating in the informal sector of Ukraine showed that the majority of the respondents perceive the situation of their households as poor (i.e. they have low income) and claim that they cannot buy even the products included in the consumer basket. Nygaard and Dreyer (2020) argue that twice as many economic agents from poor households choose to work in the informal sector compared to the number of representatives of poor households who choose to work in the formal sector of the economy. This trend is believed to become even stronger in the post-COVID-19 period since the income of 1.6 billion economic agents acting in the informal sector worldwide is likely to decrease on average by 60 percent after the COVID-19 pandemic (Nygaard and Dreyer (2020) provide the statistical estimates delivered by the International Labour Organization).

Nevertheless, informal entrepreneurship is not always associated with poverty and low standards of living. Having conducted the research in the Netherlands, Heitink et al. (2017) state that operation in the informal sector provides opportunities

for economic agents to increase their income and enjoy work. The results of the research revealed that the informal sector has both full-time and part-time workers, and informal tasks are performed by every sixth employee simultaneously doing a formal job. By selecting informal entrepreneurship, economic agents get rid of the burden of responsibility and gain more independence, which makes them feel better psychologically. The empirical evidence that informal entrepreneurship can help economic agents raise their income and work potential is also provided by Marcelli et al. (2010) who argue that similar trends are observed in both developed and developing economies. Thus, as summarized by Huang et al. (2020), informal employment can help reduce poverty and contributes to socio-economic stability. Nevertheless, when the level of social security is changing (social security is perceived as both a sense of security and the availability of social benefits and compensations), the behaviour of economic agents in the labour market may change as well (Grishnova et al., 2019). In addition, the benefits obtained from informal entrepreneurship may not be so great that an economic entity makes a decision to engage in it. For instance, Rojas (2013) found that the difference between subjective well-being in the formal and informal sectors of the economy can be so small that it will not be associated with a better or worse quality of life from the point of view of economic agents. Mishchuk et al. (2020) see the negative effects of informal entrepreneurship on a country's social security system, which experiences significant shortages of budgetary resources that could be used to finance social benefit programs and make social transfers to most vulnerable population groups.

According to Idolor (2010), ***fraud*** requires theft and manipulation of records. Through frauds, stolen assets and/or resources are converted into personal property and resources. Based on these observations, it can be stated that frauds, on one hand, are likely to raise the income of those involved in them (e.g. when individuals commit frauds pushed by poverty (Ahmad et al., 2021), or when corporate funds are directed to chief executive officers for personal use (Zahra et al., 2007)), but on the other hand, they tend to reduce the general revenue of business companies, institutions and the state budget, which could be used for meeting social needs. Ahmad et al. (2021) present the estimates showing that a rise of poverty by unit leads to a 27 percent increase in the level of fraud, while Agarwal and Medury (2014) directly state that frauds, committed by politicians, bureaucrats, industrialists and representatives of the business sector, should be treated as a major cause of poverty.

Having researched various aspects of the effects of fraud, The Commonwealth Fraud Prevention Centre (2020) notes that despite the fact that every crime of this type means direct losses suffered by public bodies, it is also important to realize that every fraud affects an individual, a family or a community that encounter the negative consequences. The report by The Commonwealth Fraud Prevention Centre (2020) proposes that the damage caused by fraud can be financial, physical or psychological (mental). Fraud undermines functionality of the social programs intended to help the most vulnerable social groups. Fraud disrupts the supply of the standard services or products by target programs; the support intended for vulnerable social groups (e.g. food products, school supplies for children) is stolen, embezzled, the funds intended for support are diverted out of target payment and

programs, that is, they are not used for their intended purposes. Thus, socially vulnerable population groups become indirect victims of fraud, which can further worsen their difficult socio-economic situation and limit availability of the adequate help. In the worst cases, when the funds intended for the provision of medical services are misdirected or appropriated, this may even mean a risk to the physical health of individuals: People can have unnecessary or unsafe medical procedures, they may not have access to the vital treatment or treatment procedures can be provided without compliance with standards, people can be exposed to hazardous substances or environments, etc. Zahra et al. (2007) believe that although corporate frauds can bring benefits to an individual perpetrator or a company (e.g. by reducing costs, profit tax, concluding a desired contract), other members of society should be treated as victims of this crime. Frauds negatively affect not only victims and their domestic surroundings, but also fraudsters and their close environment. Due to frequent contact with the criminal justice system, fraudsters are likely to be ostracized by their communities, unwanted at work (in fact, it can be extremely difficult for them to find a job), which can significantly reduce their income and worsen the level of well-being. If corporate frauds are committed by chief executive officers who hold a high social status, it can create the impression that representatives of the upper class are not punished and thus deepen the feeling of social inequality (Zahra et al., 2007).

The Commonwealth Fraud Prevention Centre (2020) also notes that victims of fraud often encounter various psychological and emotional problems (they feel shame, embarrassment, distress, sadness and anger). Having faced the cases of fraud in public institutions, victims are likely to encounter such problems as loss of reputation, feelings of vulnerability, isolation and exposure. The above-mentioned problems not only deepen social exclusion of the victims of fraud, but can also lead to suicide. The indirect social costs of fraud refer to the additional unforeseen costs that fraud victims may incur due to the necessity to seek a lawyer's consultation, to contact law enforcement authorities, deal with banks, insurance companies, etc. What is more, frauds can have far-reaching impacts beyond the individual. For instance, they can cause disruption to families and carriers when trying to resolve the situation. Losing a family and/or a career may push a person into social isolation.

Herkenrath (2014), who researched the economic effects of ***illicit financial flows***, notes that the scarcity of public investment, which hampers infrastructure building, limits the scope of measures that could be used by the state for alleviating poverty; thus, illicit financial flows deepen poverty and raise social inequality. Cobham and Jansky (2017) note that illicit financial flows are not always related to illegality, but represent a broad group of cross-border economic and financial transactions that are made in financial secrecy. Based on Baker's (2005) estimations, over 60 percent of total illicit financial flows are created through legal commercial activities, while the remaining 40 percent are the result of economic and financial crimes.

Herkenrath (2014) cites the African Development Report 2012, which proposes that investment is one of the major channels that contributes to human development. If capital flows are preserved in the country of origin and reinvested, they are likely

to raise income per capita, so the population is less poor. Nevertheless, the attention is drawn to the fact that the relationship between illicit capital flows and investment losses is not one-sided (Herkenrath, 2014), especially given the difficulties in identifying the elements related to illicit financial flows, such as the country of origin, channels and ultimate destinations (Jansky, 2015).

A positive result can be obtained when capital flows that leave the country return to the country as foreign direct investment. Blankenburg and Khan (2012) argue that in some cases, illicit capital flows can facilitate labour migration, which is likely to increase inflows of remittances and raise the income disposed by the emigrants' family members remaining in the home country, though the flow of remittances is likely to be markedly less than income, which these family members could earn in the formal labour market.

Alstadsaeter et al. (2019) emphasize the negative effect of illicit capital flows: The authors state that illicit capital flows help to disguise wealth and thus raise social inequality. This view is supported by Nkurunziza (2012) who treats illicit financial flows as a major obstacle to poverty reduction. The author provides arguments that although illicit financial flows are driven by portfolio considerations of earning higher returns on assets, from a broader perspective, illicit capital outflows mean the illicit appropriation of resources, which can be related to corruption and trade mispricing. In this regard, illicit financial flows raise the degree of risk and uncertainty in the local economy, which, in its turn, discourages investment that could be used to promote employment and public welfare and reduce poverty. Although acknowledging that illicit financial flows are not always bad (investment components and portfolio investments), and the benefits of foreign direct investment for poor countries are not as great as commonly thought, Jansky (2015) confirms that the restriction of illicit financial flows would provide additional development opportunities for poor countries: The author provides Gurria's (2008) estimations showing that due to illicit financial flows, poor countries lose three times more than the value of foreign aid they receive. The major social risk factors determined by illicit financial flows are the loss of resources for public expenditure, lower benefits of social support, weakened governance, reduced state capacity to redistribute resources pursuing for curtailing inequality and a higher degree of state fragility (Cobham & Jansky, 2017).

Adesina (2017), who analysed the impact of ***cybercrime*** on poverty in Nigeria, argues that technological progress always has niches that can be exploited for criminal purposes. The author sees a connection between human security and cybercrime and between human security and poverty. Human security refers to prioritizing citizens' security, in particular their welfare, rather than security of a state (Agir, 2015). The United Nations Development Program (UNDP) (1994) proposes that one of the ways to provide human security is promotion of unhindered access to the economy, health and education. Leaning on literature analysis, comparative analysis and synthesis methods, Ilievski and Bernik (2016) draw the conclusion that cybercrime is related to such socio-economic factors as GDP per capita, unemployment and education. This implies that cybercrime is one of the

determinants of poor economic development, leading to low social welfare and inequality.

Cybercrime has a negative impact on developing economies due to frauds on e-payment platforms in the banking sector (direct costs) and damaged reputation (business transactions and financial instruments in these economies are viewed with suspicion) (indirect costs). According to Shola (2021), cybercrime is very damaging to a country's image and reputation. The prevalence of cybercrime not only undermines the efforts to grant national security (using the methods of literature analysis and statistical data analysis, the author researched the case of Nigeria), but also creates the impression that all activities in the country are dishonest, and its citizens are fraudsters. As a result, the countries with high levels of cybercrime are viewed with suspicion in virtually every area of life, including education, business, relationships and travel. All forms of interactions across cyberspace are viewed with distrust. In this way, the country not only loses income from tourism and foreign investment; its financial instruments (e.g. bank drafts, checks) become not viable. Treated as financially unreliable, these countries experience discrimination and isolation, which limits funds for the development of anti-poverty programs and implementation of the relevant social programs.

If in the case of cybercrime an individual identity or personal data is stolen, this can negatively affect a person's eligibility for benefits or services this person is reliant on. Cybercrimes committed against a person can pose financial or credit availability problems and can have a detrimental long-term effect on a person's financial health and ongoing credit ratings (The Commonwealth Fraud Prevention Centre, 2020). The above-mentioned circumstances can push a person into poverty and social risk.

Literature reveals another direction of the relationship between cybercrime and poverty: Some cybercriminals start the so-called 'yahoo yahoo' business trying to escape poverty (Adesina, 2017). Hence, the relationship between cybercrime and poverty is bidirectional: On one hand, cybercrime deepens poverty through the negative impact on the national economy and the damage to its international reputation; on the other hand, poverty can push individuals into cybercrime as a means to escape poverty. According to Adesina (2017), the fight against cybercrime is always a joint responsibility of individuals, businesses and national governments. This means that only joint efforts and information sharing can produce positive results.

When analysing the impact of ***cryptocurrencies*** on poverty chains in the Global South, Kshetri (2017) notes that cryptocurrencies have the potential to cause significant economic and social transformations. The study emphasizes that one of the characteristics of blockchain is transparency, which, in its turn, can help ensure the transparency and efficiency of transactions in developing countries. With the increase in the number of effective transactions, faster economic and social development in these countries is expected. A similar approach is supported by Marwa et al. (2018) who state that with the help of blockchain technologies and cryptocurrencies, the number of business transactions can increase, business could be conducted more simply and efficiently, and the development projects could be

executed in a more effective manner. All of this could serve the growth of the economy and therefore, the increase in the public income.

Golumbia (2020), however, contradicts this point of view, stating that cryptocurrency trading markets are dominated by scams and fraud and being poorly controlled, eliminate democratic oversight, that is, many transactions are made by agents that see no value in adherence to the rules provided by regulated systems. This causes great damage to the development of society. Bartoletti et al. (2021) express concern about the instability of the cryptocurrency market and suspected price bubbles. Although the use of cryptocurrencies promises to produce currency, create 'safe heaven' currencies for the countries undergoing financial troubles, replace the functions of the central banking, provide permanent records of property ownership, secure digital interactions and provide cheap remittance services, which is extremely important for developing countries, in fact, cryptocurrency scams are associated with a flawed financial system that is difficult to defraud (Golumbia, 2020). Bartoletti et al. (2021) extensively describe Ponzi schemes that lure investors with large and quick profits. According to the authors, participation in these schemes is associated with financial losses and discourages investors from investing in the future. This means that due to the negative impact of Ponzi schemes, investment in developing countries can decrease, which will slow down the economic progress and will not allow effective fighting against poverty. Fake crypto services, such as fake exchange, fake wallets, fake mixing, fake mining pools and fake donations, have a similar negative effect.

The arguments explicated above lead to the conclusion that cryptocurrency scams can have a detrimental effect on the financial and central banking systems of developing countries, which is likely to increase the level of economic and social uncertainty. Quadir and Ahmad (2021) even treat the impact of cryptocurrency scams as the currency danger to a state that is just beginning its development because they can kill the national currency and cause financial instability, which will complicate the state's economic and social development processes.

3 Conclusions

The following conclusions on this chapter can be made:

1. Although acting in the informal sector can in some cases help to reduce high entrepreneurial entry and operating costs and allow business to survive in the conditions of an economic recession (literature mostly indicates the cases of inefficiently regulated low-income countries), the destructive effects of economic and financial crimes are most pronounced in the private sector. Economic and financial crimes distort market competition, demand, prices of products/services and production factors, diminish business performance, slow down business development due to the difficulties in accessing capital, destroy normal trust-based business relationship, cause reputational damage to legitimate business and

discredit legitimate transactions, thereby discouraging investment and innovation. The indirect negative effects appear as fewer opportunities to improve working conditions, business enterprises face difficulties in protecting intellectual property and patents, more funds need to be allocated to cyber security, and the risk of illegal trade in harmful waste is increasing. If systematic economic and financial crimes are characteristic of the entire economic sector, they can undermine the overall integrity of the economy.

2. Economic and financial crimes reduce state budget funds that can be allocated to the development of social services and the support of socially vulnerable population groups when trying to reduce poverty and social inequality. In this respect, the number of victims of these crimes is significantly higher than the number of victims of other crimes, since the harm is done to people who prima facie do not appear to be direct victims of crimes. The effects of economic and financial crimes on social inequality are both direct (decreasing state budget funds, higher taxes imposed on other economic entities reducing their real income) and indirect (slower economic growth). Literature recognizes that economic and financial crimes can deeply damage normal functioning of the economic system when market mechanisms and the principles of fair competition are violated; thus, income inequality increases not only due to insufficient financing of social support, which is determined by a lack of money in the state budget (disruption of services or products provided in accordance with the targeted provision of social programs), but also due to violation of the principle of justice when all market participants operating under equal conditions should have the right to a fair return/earnings. The prevalence of economic and financial crimes has a strong impact on a country's image and reputation: Countries with high crime rates are viewed with suspicion in virtually all areas of life, including education, business, relationships and travel, and transactions are treated as unreliable. In this way, countries lose foreign investment, their financial instruments (e.g. bank drafts, checks) become not viable, and these countries experience discrimination and isolation, which limits the funds for the development of anti-poverty programs and social programs.

References

Abdixhiku, L., Krasniqi, B., Pugh, G., & Hashi, I. (2017). Firm-level determinants of tax evasion in transition economies. *Economic Systems, 41*(3), 354–366. https://doi.org/10.1016/j.ecosys.2016.12.004

Achim, M. V. (2017). Corruption, income and business development. *Journal for International Business and Entrepreneurship Development, 10*, 85–100.

Achim, M. V., & Borlea, N. S. (2020). Effects of economic and financial crimes. Ways of fighting against. In M. V. Achim & N. S. Borlea (Eds.), *Economic and financial crime. Corruption, shadow economy, and money laundering* (pp. 245–271). Springer Nature Switzerland AG.

Adesina, O. S. (2017). Cybercrime and poverty in Nigeria. *Canadian Social Science, 13*(4), 19–29.

Agarwal, G. K., & Medury, Y. (2014). Internal auditor as accounting fraud buster. *IUP Journal of Accounting Research & Audit Practices, 13*(1), 7–29.

Agir, B. S. (2015). European perspective of human security: From a conception to the reality? In I. Dordevic, M. Glamotchak, S. Stanarevic, & Gacic (Eds.), *Twenty years of human security: Theoretical foundations and practical applications* (pp. 365–374). University of Belgrade and Institut Français de Geopolitique—Universite.

Ahmad, B., Ciupac-Ulici, M., & Beju, D.-G. (2021). Economic and non-economic variables affecting fraud in European countries. *Risks, 9*(6), 119. https://doi.org/10.3390/risks9060119

Ahmed, M., & Alamdar, A. (2018). Effects of corruption and budget deficit on private investment: Evidences from Pakistan. *International Journal of Development and Sustainability, 7*(6), 1898–1913.

Alm, J., & Kasper, M. (2020). *Tax evasion, market adjustments, and income distribution*. Retrieved from https://wol.iza.org/uploads/articles/526/pdfs/tax-evasion-labor-market-effects-and-income-distribution.pdf?v=1

Alstadsaeter, A., Johannesen, N., & Zucman, G. (2019). Tax evasion and inequality. *The American Economic Review, 109*(6), 2073–2103.

Araujo, A. R. (2006). The effects of money laundering and terrorism on capital accumulation and consumption. *Journal of Money Laundering Control, 9*(3), 265–271. https://doi.org/10.1108/13685200610681788

Ardigo, I. A. (2020). *The impact of corruption on the poor: The case of Guatemala.* Retrieved from https://www.u4.no/publications/the-impact-of-corruption-on-the-poor-the-case-of-guatemala

Argentiero, A., Casal, S., Mittone, L., & Morreale, A. (2021). Tax evasion and inequality: Some theoretical and empirical insights. *Economics of Governance, 22*, 309–320.

Arsic, M., & Krstic, G. (2015). *Effects of formalisation of the shadow economy.* Retrieved from https://library.oapen.org/bitstream/handle/20.500.12657/28087/1001907.pdf?sequence=1#page=107

Azunre, G. A., Amponsah, O., Takyi, S. A., & Mensah, H. (2021). Informality-sustainable city nexus: The place of informality in advancing sustainable Ghanaian cities. *Sustainable Cities and Society, 67*, 102707. https://doi.org/10.1016/j.scs.2021.102707

Baker, R. W. (2005). *Capitalism's Achilles heel: Dirty money and how to renew the free-market system.* Retrieved from http://iffoadatabase.trustafrica.org/iff/capitalism_achilles_heel_dirty_money_and_how_to_free_market_system.pdf

Bartoletti, M., Lande, S., Loddo, A., Pompianu, L., & Serusi, S. (2021). Cryptocurrency scams: Analysis and perspectives. *IEEE Access, 9*, 148353–148373. Retrieved from https://ieeexplore.ieee.org/abstract/document/9591634

Basu, A. K., & Chau, N. H. (2015). Informal work in developing countries. In *International Encyclopedia of the social & behavioral sciences* (2nd ed.). Elsevier. https://doi.org/10.1016/B978-0-08-097086-8.94028-5

Baumann, F., & Friehe, T. (2010). Tax evasion, investment, and firm activity. *Public Finance Analysis, 66*(1), 1–14.

Beck, P., & Mahler, M. (1986). A comparison of bribery and bidding in thin markets. *Economics Letters, 20*, 1–5.

Berglund, C., & Ekelund, B. (2019). *Corporate scandal: The reputational impact on the financial performance*. Retrieved from https://www.diva-portal.org/smash/get/diva2:1320243/FULLTEXT01.pdf.

Bhusal, T. P. (2016). Corruption and illicit financial flows in Nepal. *Tribhuvan University Journal, 30*(2), 211–224. https://doi.org/10.3126/tuj.v30i2.25565

Bilan, Y., Mishchuk, H., Samoliuk, N., & Yurchyk, H. (2020). Impact of income distribution on social and economic Well-being of the state. *Sustainability, 12*(1), 429. https://doi.org/10.3390/su12010429

Binawa, M. J., & Ihendinihu, J. U. (2018). Effect of risk assets management on the post consolidation financial performance of commercial banks in Nigeria. In *The 8th AFRA international conference, University of Calabar International Conference Centre, Calabar* (p. 610).

Blankenburg, S., & Khan, M. (2012). Governance and illicit flows. In P. Reuter (Ed.), *Draining development? Controlling flows of illicit funds from developing countries* (pp. 21–68). World Bank.

Brandt, K. (2022). Illicit financial flows and developing countries: A review of methods and evidence. *Journal of Economic Surveys*. Retrieved from https://onlinelibrary.wiley.com/doi/full/10.1111/joes.12518\

Brzic, B., Dabic, M., Kukura, F., & Podobnik, B. (2021). The effects of corruption and the fraction of private ownership on the productivity of telecommunication companies. *Technology in Society, 65, No. 101532*, 101532. https://doi.org/10.1016/j.techsoc.2021.101532

Carvalho, J. L. D. P. (2019). *The effects of tax evasion on economic growth: A stochastic growth model approach.* Retrieved from https://www.locus.ufv.br/bitstream/123456789/26737/1/texto%20completo.pdf

Caselli, F., & Michaels, G. (2013). Do oil windfalls improve living standards? Evidence from Brazil. *American Economic Journal: Applied Economics, 5*, 208–238.

Chen, C., & Cheng, S. (2019). The effects of corruption and regulation on business entrepreneurship: Evidence from American states. *Public Performance and Management Review, 42*(6), 1481–1506. https://doi.org/10.1080/15309576.2019.1574593

Chen, X., Hu, N., Wang, X., & Tang, X. (2014). Tax avoidance and firm performance: Evidence from China. *Nankai Business Review International, 5*(1), 25–42. https://doi.org/10.1108/NBRI-10-2013-0037

Chenguel, M. B. (2020). *Financial fraud and managers, causes and effects.* Retrieved from https://www.intechopen.com/chapters/74186.

Chetwynd, E., Chetwynd, F., & Spector, B. (2003). *Corruption and poverty: A review of recent literature*. Retrieved from https://pdf.usaid.gov/pdf_docs/PNACW645.pdf

Chrenekova, M., Melichova, K., Marišova, E., & Moroz, S. (2016). Informal employment and quality of life in rural areas of Ukraine. *European Countryside, Sciendo, 8*(2), 135–146.

Cobham, A., & Jansky, P. (2017). *Illicit financial flows: An overview.* Retrieved from https://www.tralac.org/images/docs/12398/ige-ffd-unctad-illicit-financial-flows-an-overview-background-paper-november-2017-draft.pdf

CSIS. (2018). *Economic impact of cybercrime – No slowing down.* Retrieved from https://csis-website-prod.s3.amazonaws.com/s3fs-public/publication/economic-impact-cybercrime.pdf

de Castro, J. O., Khavul, S., & Bruton, G. D. (2014). Shades of Grey: How do informal firms navigate between the macros and meso institutional environments? *Strategic Entrepreneurship Journal, 8*, 75–94.

De Rosa, D., Gooroochurn, N., & Gorg, H. (2010). *Corruption and productivity: Firm-level. Evidence from the BEEPS survey. Kiel Working Paper No. 1632*. World Bank.

Desai, M. A., & Dharmapala, D. (2009). Corporate tax avoidance and firm value. *The Review of Economics and Statistics, 91*(3), 537–546.

Dimant, E., & Tosato, G. (2018). Causes and effects of corruption: What has past decade's empirical research taught us? A survey. *Journal of Economic Surveys, 32*(2), 335–356. https://doi.org/10.1111/joes.12198

Djankov, S., La Porta, R., Lopez-de-Silanes, F., & Shleifer, A. (2002). The regulation of entry. *The Quarterly Journal of Economics, 117*, 1–37.

Dobrowolski, Z., & Sulkowski, L. (2019). *Implementing a sustainable model for anti-money laundering in the United Nations development goals.* Retrieved from https://www.mdpi.com/2071-1050/12/1/244/htm

Dyck, A., Morse, A., & Zingales, L. (2017). *How pervasive is corporate fraud?* Retrieved from https://www.law.nyu.edu/sites/default/files/upload_documents/Adair%20Morse%20How%20Pervasive%20is%20Corporate%20Fraud.pdf

Eijdenberg, E. L., Sabokwigina, D., & Masurel, E. (2019). Performance and environmental sustainability orientations in the informal economy of a least developed country. *International Journal of Entrepreneurial Behavior & Research, 25*(1), 129–149. https://doi.org/10.1108/IJEBR-01-2018-0040

Enste, D. H. (2018). *The shadow economy in industrial countries.* Retrieved from https://wol.iza.org/articles/shadow-economy-in-industrial-countries/long

Estevao, J., Lopes, J. D., & Penela, D. (2022). The importance of the business environment for the informal economy: Evidence from the doing business ranking. *Technological Forecasting and Social Change, 174*, 121288.

Estrin, S., & Mickiewicz, T. (2012). Shadow economy and entrepreneurial entry. *Review of Development Economics, 16*(4), 559–578. https://doi.org/10.1111/rode.12004

Feinstein, B. D., & Werbach, K. (2021). The impact of cryptocurrency regulation on trading markets. *Journal of Financial Regulation, 7*(1), 48–99. https://doi.org/10.1093/jfr/fjab003

Fumpa-Makano, R. (2019). *Tax exemptions and tax expenditures.* Corporate Taxation in Zambia. Retrieved from https://taxjustice-and-poverty.org/fileadmin/Dateien/Taxjustice_and_Poverty/AwarenessJoint/NairobiConference/MakanoBackground.pdf

Gaviria, A. (2002). Assessing the effects of corruption and crime on firm performance: Evidence from Latin America. *Emerging Markets Review, 3*(3), 245–268. https://doi.org/10.1016/S1566-0141(02)00024-9

Ghose, A. K. (2017). Informality and development. *Indian Journal of Labour Economics, 60*(1), 109–126. https://doi.org/10.1007/s41027-017-0080-5

Gjoni, M., Gjoni, A., Kora, H. B. (2015, November). Money laundering effects. University of Business and Technology in Kosovo. In *International Conference on Management, Business and Economics*. Retrieved from https://www.researchgate.net/publication/330630840_Money_Laundering_Effects

Golumbia, D. (2020, February 14). *Blockchain: The white Man's burden.* Transcript of talk delivered at The White West: Automating Apartheid III, Kunsthalle Wien.

Gordon, L. M. (2020). *Understanding fraud in economic downturns and recessions.* Retrieved from https://www.mnp.ca/en/insights/directory/understanding-fraud-in-economic-downturns-and-recessions

Grishnova, O., Cherkasov, A., & Brintseva, O. (2019). Transition to a new economy: Transformation trends in the field of income and salary functions. *Problems and Perspectives in Management, 1*(2), 18–31.

Gurria, A. (2008). *The global dodgers.* Retrieved from https://www.theguardian.com/commentisfree/2008/nov/27/comment-aid-development-tax-havens

Habibov, N., & Cheung, A. (2016). The impact of unofficial out-of-pocket payments on satisfaction with education in post-soviet countries. *International Journal of Educational Development, 49*, 70–79. https://doi.org/10.1016/j.ijedudev.2016.02.002

Handayani, R. (2020). *Effects of tax avoidance and financial performance on firm value.* Retrieved from https://www.ijmsssr.org/paper/IJMSSSR00203.pdf

Hanlon, M., & Slemrod, J. (2009). What does tax aggressiveness signal? Evidence from stock price reactions to news about tax shelter involvement. *Journal of Public Economics, 93*(1), 126–141. https://doi.org/10.1016/j.jpubeco.2008.09.004

Hassan, M. (2017). *The impact of the shadow economy on aid and economic development nexus in Egypt.* Retrieved from https://mpra.ub.uni-muenchen.de/80990/1/MPRA_paper_80990.pdf

Heitink, E., Heerkens, Y., & Engels, J. (2017). Informal care, employment and quality of life: Barriers and facilitators to combining informal care and work participation for healthcare professionals. *Work, 58*(2), 215–231. https://doi.org/10.3233/WOR-172607

Herkenrath, M. (2014). *Illicit financial flows and their developmental impacts: An overview*. International Development Policy. Retrieved from https://journals.openedition.org/poldev/1863\

Hillendahl, A. (2022). *Beware of cryptocurrency scams.* Retrieved from https://www.experian.com/blogs/insights/2022/05/beware-of-cryptocurrency-scams/

Hoinaru, R., Buda, D., Borlea, S. N., Vaidean, V. L., & Achim, M. V. (2020). The impact of corruption and shadow economy on the economic and sustainable development. Do they "sand the wheels" or "grease the wheels"? *Sustainability, 12*(2), 481. https://doi.org/10.3390/su12020481

Huang, G., Xue, D., & Wang, B. (2020). Integrating theories on informal economies: An examination of causes of urban informal economies in China. *Sustainability, 12*(7), 2738. https://doi.org/10.3390/su12072738

Idolor, E. J. (2010). Bank frauds in Nigeria: Underlying causes, effects and possible remedies. *African Journal of Accounting, Economics, Finance and Banking Research, 6*(6), 62–80.

Ilievski, A., & Bernik, I. (2016). Social-economic aspects of cybercrime. *Innovative Issues and Approaches in Social Sciences, 9*(3), 8–22. Retrieved from http://www.iiass.com/pdf/IIASS-volume9-number3-2016.pdf#page=8

International Labour Organisation. (2020). COVID-19 crisis and the informal economy. *ILO Brief, 204*, 1–8. Retrieved from https://www.ilo.org/global/topics/employment-promotion/informal-economy/publications/WCMS_743623/lang%2D%2Den/index.htm

Jansky, P. (2015). Updating the rich countries' commitment to development index: How they help poorer ones through curbing illicit financial flows. *Social Indicators Research, 124*, 43–65.

Jiang, T., & Nie, H. (2014). The stained China miracle: Corruption, regulation, and firm performance. *Economics Letters, 123*, 366–369.

Johansen, S., & Juselius, K. (1990). The maximum likelihood estimation and inference on co-integration with applications to the demand for money. *Oxford Bulletin of Economics and Statistics, 52*(2), 169–210.

Justesen, M., & Bjornskov, C. (2014). Exploiting the poor: Bureaucratic corruption and poverty in Africa. *World Development, 58*, 106–115. https://doi.org/10.1016/j.worlddev.2014.01.002

Khuong, N. V., Liem, N. T., Thu, P. A., Khanh, T. H. T., & Ntim, C. G. (2020). Does corporate tax avoidance explain firm performance? Evidence from an emerging economy. *Cogent Business & Management, 7*(1), 1780101. Retrieved from https://www.tandfonline.com/doi/full/10.1080/23311975.2020.1780101

Koyuncu, J. Y., & Unal, H. S. (2018). Is there any long-term association between tax evasion and human development? Evidence from OECD countries. *Social Sciences Research Journal, 7*(3), 92–101.

Krueger, A. O. (1974). The political economy of the rent-seeking society. *American Economic Review, 64*, 291–303.

Kshetri, N. (2017). Will blockchain emerge as a tool to break the poverty chain in the global south? *Third World Quarterly, 38*(8), 1710–1732. https://doi.org/10.1080/01436597.2017.1298438

Kumar, A. (2012). Money laundering: Concept, significance and its impact. *European Journal of Business and Management, 4*(2), 113–120.

Larsson, C. W., & Svensson, J. (2018). Mobile phones in the transformation of the informal economy: Stories from market women in Kampala, Uganda. *Journal of Eastern African Studies, 12*(3), 533–551. https://doi.org/10.1080/17531055.2018.1436247

Letete, E., & Sarr, M. (2017). *Illicit financial flows and political institutions in Kenya. Working paper series no. 275*. African Development Bank Group. Retrieved from https://www.tralac.org/images/docs/11965/illicit-financial-flows-and-political-institutions-in-kenya-afdb-working-paper-july-2017.pdf

Marcelli, E., Williams, C. C., & Joassart, P. (2010). *Informal work in developed nations*. Routledge.

Marwa, S., Westgard, E., Khan, F., Kamara, B., & Ogeto, J. (2018). *Can a FinTech combination of blockchain, M-PESA and smart contracts improve development project execution in sub-Saharan Africa?* Retrieved from https://www.academia.edu/40778586/CAN_A_FINTECH_COMBINATION_OF_BLOCKCHAIN_M_PESA_AND_SMART_CONTRACTS_IMPROVE_DEVELOPMENT_PROJECT_EXECUTION_IN_SUB_SAHARAN_AFRICA_A_Literature_Review.

Matsaganis, M., & Flevotomou, M. (2010). *Distributional implications of tax evasion in Greece.* Hellenic observatory papers on Greece and Southeast Europe (GreeSE paper No. 31). Hellenic Observatory, London School of Economics and Political Science.

Mauro, P. (1995). Corruption and growth. *The Quarterly Journal of Economics, 110*(3), 681–712.

Mauro, P. (1996). *The effects of corruption on growth, investment, and government expenditure.* IMF working paper no. 96/98, policy development and review department. Retrieved from SSRN https://ssrn.com/abstract=882994

McDevitt, A. (2009). *Money laundering and poverty reduction*. GSDRP Publications. Retrieved from https://gsdrc.org/publications/money-laundering-and-poverty-reduction/

McDowell, J. (2001). The consequences of money laundering and financial crime. *An Electronic Journal of the U.S. Department of State, 6*(2), 1–8.

McGahan, A. M. (2012). Challenges of the informal economy for the field of management. *Academy of Management Perspectives, 26*(3), 12–21.

Mishchuk, H., Bilan, S., Yurchyk, H., Akimova, L., & Navickas, M. (2020). Impact of the shadow economy on social safety: The experience of Ukraine. *Economics and Sociology, 13*(2), 289–303. https://doi.org/10.14254/2071-789X.2020/13-2/19

Moore, M. (2012). The practical political economy of illicit flows. In P. Reuter (Ed.), *Draining development? Controlling flows of illicit funds from developing countries* (pp. 457–482). Washington, D.C.

Mroz, B. (2010). The shadow economy in Poland: Causes, manifestations, economic and social effects. *Journal of Management and Financial Sciences, III*(3), 96–118.

Murithi, R. R. (2013). The effect of anti-money laundering regulation implementation on the financial performance of commercial banks in Kenya. Retrieved from http://erepository.uonbi.ac.ke/bitstream/handle/11295/62905/Muriithi_The%20effect%20of%20anti-money%20laundering%20regulation.pdf?sequence=3&isAllowed=y

Negin, V. (2010). *Effects of corruption on poverty and economic growth.* Retrieved from https://core.ac.uk/download/pdf/153803034.pdf

Negin, V., Abd Rashid, Z., & Nikopour, H. (2010). *The causal relationship between corruption and poverty: A panel data analysis*. Retrieved from https://mpra.ub.uni-muenchen.de/24871/1/MPRA_paper_24871.pdf

Nkurunziza, J. D. (2012). *Illicit financial flows: A constraint on poverty reduction in Africa.* Association of Concerned Africa Scholars, Bulletin No. 87, Fall. Retrieved from http://iffoadatabase.trustafrica.org/iff/illicit_financial_flows_a_constraint_on_poverty_reduction_in_africa.pdf

Nygaard, K., & Dreyer, M. (2020). *Countries provide support to workers in the informal economy*. Retrieved from https://som.yale.edu/blog/countries-provide-support-to-workers-in-the-informal-economy

OECD. (2010). *Policy roundtable: Competition policy and the informal economy 2009.* Retrieved from https://www.oecd.org/daf/competition/44547855.pdf

Ogbodo, U. K., & Miesheigha, E. G. (2013). The economic implications of money laundering in Nigeria. *International Journal of Academic Research in Accounting, Finance and Management Sciences, 3*(4), 170–184.

Okunlola, O. C. (2014). Money laundering: A threat to sustainable democracy in Nigeria. *Journal of Economics and Sustainable Development, 5*(2), 85–98.

Osman, A., & Salifu, M. (2022). Effects of illicit financial flows on economic growth and development in sub-Saharan Africa. *Universal Journal of Finance and Economics, 2*(1), 31–41. https://doi.org/10.31586/ujfe.2022.436

Piperopoulos, P., Kafouros, M., Aliyev, M., Liu, E. Y., & Au, A. (2021). How does informal entrepreneurship influence the performance of small formal firms? A cross-country institutional perspective. *Entrepreneurship and Regional Development, 33*(7–8), 668–687. https://doi.org/10.1080/08985626.2021.1887371

Povich, E. S. (2021). *Cryptocurrency fraud soars, spurring state action.* Retrieved from https://www.pewtrusts.org/en/research-and-analysis/blogs/stateline/2021/11/17/cryptocurrency-fraud-soars-spurring-state-action

Price, J. M., & Sun, W. (2017). Doing good and doing bad: The impact of corporate social responsibility and irresponsibility on firm performance. *Journal of Business Research, 80*, 82–97. https://doi.org/10.1016/j.jbusres.2017.07.007

Qadir, A. M. A., & Ahmad, R. M. (2021). One coin-scam cryptocurrency impact on financial market. *Technium Social Sciences Journal, 16*, 274–282. Retrieved from https://heinonline.org/HOL/LandingPage?handle=hein.journals/techssj16&div=23&id=&page=

Rojas, M. (2013). The subjective well-being of people in informal employment: Empirical evidence from Mexico. *Evidence-based HRM, 1*(2), 169–186. https://doi.org/10.1108/EBHRM-04-2013-0006

Rose-Ackerman, S. (1978). *Corruption: A study in political economy*. Academic.

Rothenberg, A. D., Gaduh, A., Burger, N. E., Chazali, C., Tjandraningsih, I., Radikun, R., Sutera, C., & Weilant, S. (2016). Rethinking Indonesia's informal sector. *World Development, 80*, 99–113.

Ruzek, W. (2015). The informal economy as a catalyst for sustainability. *Sustainability (Switzerland), 7*(1), 23–34. https://doi.org/10.3390/su7010023

Safdari, A., Nurani, M. S., Aghajani, K., & Abdollahian, F. (2015). Social impact of money laundering. *Asian Journal of Research in Social Sciences and Humanities, 5*(1), 1–16.

Sahakyan, N., & Stiegert, K. W. (2012). Corruption and firm performance. *Eastern European Economics, 50*, 5–27.

Santos, E., Fernandes, C. I., Ferreira, J. J., & Lobo, C. A. (2021). What is the impact of informal entrepreneurship on venture capital flows? *Journal of the Knowledge Economy, 12*, 2032–2049. Retrieved from https://link.springer.com/article/10.1007/s13132-020-00701-w

Schneider, F., Buehn, A., & Montenegro, C. E. (2010). New estimates for the shadow economies all over the world. *International Economic Journal, 24*(4), 443–461.

Shah, I. H., & Aish, K. (2022). A nexus between corruption, money laundering (ML) and inflation: Evidence from south Asian countries. *Journal of Money Laundering Control, 25*(4), 730–741. https://doi.org/10.1108/JMLC-09-2021-0096

Shola, A. T. (2021). Poverty, cybercrime and national security in Nigeria. *Journal of Contemporary Sociological Issues, 1*(2), 1–23. https://doi.org/10.19184/csi.v1i2.24188

Smith, K. T., Jones, A., Johnson, L., & Smith, L. M. (2019). Examination of cybercrime and its effects on corporate stock value. *Journal of Information, Communication and Ethics in Society, 17*(1), 42–60. https://doi.org/10.1108/JICES-02-2018-0010

Steinberg, S. (2019). *Cyberattacks now cost companies $200,000 on average, putting many out of business*. Retrieved from https://www.cnbc.com/2019/10/13/cyberattacks-cost-small-companies-200k-putting-many-out-of-business.html

Sultana, N., Rahman, M. M., & Khanam, R. (2022). The effect of the informal sector on sustainable development: Evidence from developing countries. *Business Strategy and Development, 5*(4), 437–451. Retrieved from https://onlinelibrary.wiley.com/doi/full/10.1002/bsd2.217\

Swenson, C. (1999). Increasing stock market value by reducing effective tax rates. *Tax Notes, 83*, 1503–1505.

The Commonwealth Fraud Prevention Centre. (2020). *The total impacts of fraud.* Retrieved from https://www.counterfraud.gov.au/total-impacts-fraud

The UK Cabinet Office and 'Detica'. (2011). *The cost of cybercrime. A Detica report in partnership with the Office of Cyber Security and Information Assurance in the Cabinet Office.* Retrieved from https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/60943/the-cost-of-cyber-crime-full-report.pdf

The United Nations Development Programme. (1994). *Human development report.* Retrieved from https://hdr.undp.org/content/human-development-report-1994?utm_source=EN&utm_medium=GSR&utm_content=US_UNDP_PaidSearch_Brand_English&utm_campaign=CENTRAL&c_src=CENTRAL&c_src2=GSR&gclid=CjwKCAiAzKqdBhAnEiwAePEjkijRQM4iXkisRF-lFTugGuqaiRdANxeP2xNZx7nFbusUANV8itAq2hoCZxwQAvD_BwE

Trozze, A., Kamps, J., Akartuna, E. A., Hetzel, F. J., Kleinberg, B., Davies, T., & Johnson, S. D. (2022). Cryptocurrencies and future financial crime. *Crime Science*, 1. Retrieved from https://crimesciencejournal.biomedcentral.com/articles/10.1186/s40163-021-00163-8

Vinnychuk, I., & Ziukov, S. (2013). Shadow economy in Ukraine: Modelling and analysis. *Business Systems and Economics, 2*(3), 141–152.

Vousinas, G. L. (2017). Shadow economy and tax evasion. The Achilles heel of Greek economy. Determinants, effects and policy proposals. *Journal of Money Laundering Control, 20*(4), 386–404. https://doi.org/10.1108/JMLC-11-2016-0047

Williams, C. C., Perez, A. M., & Kedir, A. (2016). Informal entrepreneurship in developing economies: The impacts of starting up unregistered on firm performance. *Entrepreneurship: Theory and Practice, 41*(5), 1–28. https://doi.org/10.1111/etap.12238

Zahra, S. A., Priem, R. L., & Rasheed, A. A. (2007). Understanding the causes and effects of top management fraud. *Organizational Dynamics, 36*(2), 122–139.

Zaman, G., & Goschin, Z. (2015). Shadow economy and economic growth in Romania. Cons and pros. *Procedia Economics and Finance, 22*, 80–87.

Zhang, C., Cheong, K. C., & Rasiah, R. (2016). Corporate tax avoidance and performance: Evidence from China's listed companies. *Institutions and Economies, 8*(3), 61–83.

Rita Remeikienė obtained Doctoral degree in Economics, Kaunas University of Technology on 2012. Her main areas of scientific research and expertise are Shadow Economy, Corruption, Money Laundering, Green Deal, Self-employment. Since 2021 she leads as Chief researcher in two important projects namely, 'Protecting work and income in the digital economy: a case study of platform workers' and 'Model of the interaction of labour market and social support policies and development of methodologies for its implementation' (No. 13.1.1-LMT-K-718-05-0008), the last one being co-financed by the European Regional Development Fund. She works as a senior researcher at Vilnius University, Lithuania.

Prof. Dr. Ligita Gaspareniene is a senior researcher at Vilnius university. She worked as a principal researcher in the 'Welfare society' project titled 'Links between unemployment and shadow economy in Lithuanian regions'. Until now she is a senior researcher in the project 'Model of the interaction of labour market and social support policies and development of methodologies for its implementation' co-funded from the EU Structural Fund. Professor also works in the project 'Protecting work and income in the digital economy: a case study of platform workers' funded from Lithuanian Research council. Her interest research fields are corruption, shadow/digital economy, sustainability, Green deal.

Chapter 10
Effects on the Soundness of Financial-Banking Institutions and on the Business Development

Rita Remeikienė and Ligita Gaspareniene

Abstract The aim of the chapter is to carry out an analysis of the effects of the main economic and financial crimes on business development and the activity and reputation of financial and banking institutions. Business development and the activities of financial-banking institutions are examined together, since business financing is inseparable from bank/financial institution funds. The analysis of scientific literature revealed that economic and financial crimes undermine the functions of financial-banking institutions to accumulate capital from local savings and foreign funds and to act as a stimulating factor for investment and efficient distribution of resources, thus creating an environment favourable to economic growth. Financial institutions with flows and deposits of proceeds of crime face additional challenges in properly managing their assets, liabilities and operations. Although acting in the informal sector can in some cases help to reduce high entrepreneurial entry and operating costs and allow business to survive in the conditions of an economic recession (literature mostly indicates the cases of inefficiently regulated low-income countries), the destructive effects of economic and financial crimes are most pronounced in the private sector. Economic and financial crimes distort market competition, demand, prices of products/services and production factors, diminish business performance, slow down business development due to the difficulties in accessing capital, destroy normal trust-based business relationship, cause reputational damage to legitimate business and discredit legitimate transactions, thereby discouraging investment and innovation.

Keywords Corruption · Money laundering · Tax evasion · Cybercrimes · Shadow economy · Illegal money flows · Fraud · Informal business · Financial-banking institutions · Business development

JEL Classification K42 · E44 · G28 · M21 · M48

R. Remeikienė (✉) · L. Gaspareniene
Vilnius University, Law faculty, Vilnius, Lithuania
e-mail: rita.remeikiene@tf.vu.lt; ligita.gaspareniene@tf.vu.lt

M. V. Achim (ed.), *Economic and Financial Crime, Sustainability and Good Governance*, Contributions to Finance and Accounting,
https://doi.org/10.1007/978-3-031-34082-6_10

1 Introduction

Actuality of the topic. Financial crimes such as money laundering can cause liquidity problems for financial institutions due to the unexpected outflow of large sums of money. Abuse of the financial system, dubious transactions and opaque capital flows through money laundering schemes harm the reputation of financial institutions and can lead to their bankruptcy, which can weaken the entire financial system. Money laundering from high integration of capital markets can also negatively affect exchange rates and interest rates, as launderers seek to hide their income rather than maximize returns. Money laundering channels can also distort a country's imports and exports. Imports that do not stimulate domestic economic activity and employment will artificially reduce the prices of domestic products and services, thereby reducing the profitability of local business enterprises. In terms of exports, offenders may manipulate export prices to launder funds from illicit activities.

Corruption diverts money intended for business development into private pockets, it also discourages direct foreign investment, as a result of which capital flows, tax revenues are lost, additional jobs are not created, and the benefits of technology and knowledge dissemination are not obtained. Corruption is a fatal disease of the development of any society because it violates the principles of justice, where prosperity is guaranteed only to those in authority. The shadow economy, cybercrime, illegal money flows and tax evasion contribute to both the suspension of banking institutions and the failure of businesses to gain a foothold in the market.

The level of investigation of a scientific problem. The impact of money laundering on financial institutions and business development is examined by Ferwerda (2010), Slutzky et al. (2020), McDowell (2001), Kemal (2014), Kumar (2012), Abu-Orabi and Al Abbadi (2019); Toan (2022), Walker and Unger (2009) and others. The impact of corruption on financial institutions and business development was investigated by Chitakunye et al. (2015), Habibov et al. (2019), Venard (2013), Yu et al. (2022) and others. The influence of the shadow economy, cybercrime, illegal entrepreneurship on financial institutions and business development has also been analysed by many researchers, such as Ruggiero (2020), Schia and Willers (2021), McWhinney et al. (2022), Kang and Lee's (2019), Shin and Rice (2022) and others.

The scientific problem is formulated in the following question: What are the consequences of the main economic and financial crimes for the development of business and the activity of financial and banking institutions?

The aim of the chapter is to carry out an analysis of the effects of the main economic and financial crimes on business development and the activity and reputation of financial and banking institutions.

In order to achieve the goal, a comparative and systematic analysis of the scientific literature will be performed. Business development and the activities of financial-banking institutions are examined together, since business financing is inseparable from bank/financial institution funds.

2 Literature Review and Research Design

Economic and financial crimes can damage the integrity of financial and banking institutions. Direct and indirect negative effects will be felt in banking and non-banking financial institutions, as well as equity, loan and currency markets. Since the aforementioned institutions perform the function of capital accumulation from local savings and foreign funds, they act as a stimulating factor for investment and efficient allocation of resources and create an environment favourable to economic growth (Kumar, 2012). Economic and financial crimes undermine the performance of these functions.

Money laundering can harm the activities of financial and banking institutions in several ways. First, financial institutions with flows and deposits generated from proceeds of crime face additional challenges in properly managing their assets, liabilities and operations. Large amounts of laundered money can inflow a certain financial institution, but they can unexpectedly disappear through wire transfers, which will be driven not by market factors, but, for example, by visits of law enforcement and control authorities to economic agents who try to disguise the origin of their income. Unexpected outflows of large sums of money can cause liquidity problems for financial institutions (McDowell, 2001). On the other hand, as stated by Ferwerda (2010) and Slutzky et al. (2020), money laundering can increase liquidity within the financial system when offenders keep the ill-gotten gains in their bank accounts.

The second negative aspect of the impact of money laundering on financial systems, according to Kumar (2012), is that there exists a correlation between money laundering and fraudulent activities undertaken by the staff in financial-banking institutions. The development of common financial services and instruments, such as insurance, issuance of credit cards, automated teller machines, contribute to money laundering – these instruments make money laundering activities more sophisticated and diversified (Kemal, 2014), and financial institutions become vulnerable to crime. This strengthens the development of parallel money laundering systems, allows elimination of weaker competitors and gives the rise to monopoly (Kumar, 2012).

Third, the development of financial institutions and financial markets can be hampered by a decline in public confidence. The efficient functioning of financial markets largely depends on the extremely high professional, legal and ethical standards set for them – compliance with these standards is strictly monitored by authorized supervisory institutions. Operational transparency, compliance with standards, codes and legal norms are the main conditions for trust in financial institutions, as emphasized in the Basel Core Principles for Effective Supervision and in the Code of Good Practices on Transparency in Monetary and Financial Policies (IMF, 2001). Violations of the aforementioned norms, abuse of the financial system, conclusion of dubious transactions and non-transparent capital flows undermine the reputation of financial institutions and can lead to their bankruptcy, which can weaken the entire financial system (IMF, 2001; Kumar, 2012).

Fourth, due to the high integration of capital markets, money laundering can also negatively affect exchange and interest rates because launderers seek to conceal their income rather than maximize returns (McDowell, 2001). According to Sagastume et al. (2016), large capital flows or local outflows mean that money laundering has a negative impact on exchange rates and interest rates since these capital flows are not predictable. Abu-Orabi and Al Abbadi (2019) argue that fluctuations in exchange rates and interest rates may increase due to unexpected large-scale fund transfers across borders. In addition, money laundering can raise the risk of monetary instability through resource misallocation, as well as asset structure and commodity price distortions (McDowell, 2001; Abu-Orabi & Al Abbadi, 2019).

Fifth, the financial system sector is used by the money laundering offenders as a mean of laundering the money coming from illegal transactions, through the financial-banking services offered; therefore, money laundering crimes through financial-banking systems erode the performance of financial institutions and therefore the trust in them (Achim & Borlea, 2020, p. 249).

The main internal money laundering prevention measures that can be undertaken by financial and banking institutions are careful monitoring of account opening, accepting money on deposit and issuing loans (Alomari, 2020). Lester and Roth (2007) recommend strengthening the internal policy, risk management, customer identification and validation, procedure and control compliance, monitoring the operations and transactions, collection and analysis of documents and information, and cooperation with authorities and audit.

Ali et al. (2020), who formed the sample of 38 countries to research the direct and indirect effects of ***corruption*** on banking institutions over the period 2000–2017, conclude that corruption increases the likelihood of banking crises, especially in developing countries, although the corruption-banking stability relationship is non-linear in both developing and developed countries. The authors distinguish between endogenous and exogenous factors of corruption in the banking sector: The endogenous factor represents bribery of bank employees, while the exogenous factor represents corruption in political, judiciary and legal institutions. According to Ali et al. (2020), the indirect effect of corruption on banks lies in the excessive risk of bank lending, though the negative impact on bank profitability is less pronounced. The elements of the negative impact of corruption on bank lending are as follows: hindering the efficient intermediation of capital, granting higher default rates, easier access to funding based not on assessment of an applicant's financial condition or business plan, but on receiving a bribe, etc.

Asteriou et al. (2021) argue that corruption stimulates allocation of bank funds to inefficient projects at the expense of efficient projects, which undermines the soundness of banking institutions. When assessing the consequences of diverting funds from efficient to inefficient projects, Chen et al. (2015) observe that this practice is not only flawed in terms of the efficiency of capital allocation, but also detrimental in terms of bank susceptibility risks.

Evidence of the negative effects of corruption on bank profitability is provided by Arshad and Rizvi (2013), who investigated the Islamic bank profitability over the period 2000–2010, Abuzayed et al. (2019), who researched the sample of 7235

banks in 160 countries in the period 2000–2016, Asteriou et al. (2021), whose research sample included 326 banks operating in 19 euro area countries in the period 2005–2018, and Hasan and Ashfaq (2021), who investigated the situation in 178 countries in the period 2000–2017. After examining the relationship between corruption and bank profitability in 38 countries over the period 2011–2017, Bolanriwa and Soetan (2019) found that corruption is a significant factor affecting bank profitability in both developing and developed economies, but in highly corrupt economies, the impact of corruption on bank profitability can be both positive and negative.

According to Liu et al. (2020), corruption not only stimulates uncertainty in terms of inability of banks to meet their obligations, but also raises the risk of borrowers' defaulting. This problem was also noted by Bahoo (2020). Toader et al.'s (2018) findings propose that a lower level of corruption has a positive impact on bank stability and is associated with lower losses incurred because of financially unsound credits. Liu et al. (2020) provide the results showing that there is an inverted U-shaped relationship between corruption and business access to bank loans: The lower is the level of corruption, the higher is the access to loans, and vice versa. This relationship is partly explained by government guarantees conducive to business access to financing.

Interestingly, Eksi and Dogan's (2020) study of 19 Eastern European and Central Asian countries in the period 2012–2017 disclosed that perception of corruption is not a stimulator of financial development in the countries under consideration. According to Liu et al. (2020), corruption-induced risks to the solvency of banks and borrowers can be reduced by better institutional quality. Hasan and Ashfaq (2021) advocate stronger governance mechanisms.

Elsherif (2019), who researched the relationship between ***the shadow economy***, financial inclusion and the financial system stability in 20 emerging economies over the period 2004–2014 by applying two-stage linear regression, found that the size of the shadow economy has a significant impact on the relationship between financial inclusion and financial stability, and the shadow economy can significantly improve the level of financial instability. Credit to government and state-owned enterprises were found to have a statistically significant positive relationship with the shadow economy. Safuan et al.'s (2021) research disclosed an inverted U-shaped non-linear relationship between the shadow economy and financial sector development (the authors analysed the Indonesian economy over the 1980–2020 period). Their study also proposes that the shadow economy tends to expand at the early stages of the financial sector development, but in the further stages, the size of the shadow economy tends to decrease, which implies that a large scale of the shadow economy hinders faster development of the financial sector; but if the financial sector is sufficiently developed, the impact of the shadow economy is insignificant, because the financial sector itself restricts the shadow economy. Similar results were provided by Canh and Thanh (2020), who researched the sample of 114 economies over the 2002–2015 period. In this research, the development of the financial sectors was represented by three dimensions – financial depth, financial access and financial efficiency; the research covered two sub-sectors – financial institutions and financial

markets. The research confirmed that the relationship between the shadow economy and financial development is U-shaped non-linear. The authors also provide evidence that financial depth and financial access have a positive effect on the shadow economy in the short run, while financial institutions tend to reduce the size of the shadow economy in the long run. It is noted that financial development may have the negative effects on the shadow economy in low- and lower-middle-income economies as well as in upper-middle-income economies, but in high-income economies the negative effects are dominant and the non-linear relationship is consistent.

Bayar and Aytemiz's (2017) study of the situation in Turkey proposes that the causality running from financial development to the shadow economy is unidirectional (i.e. financial development tends to reduce the size of the shadow economy), but having researched the sample of 161 countries over the period 1960–2009, Berdiev and Saunoris (2016) found that the reverse causality between the variables (financial development and the shadow economy) is also possible because a shock to the shadow economy can hinder financial development. However, Elgin and Uras's (2013) study of 152 countries in the period 1999–2007 shows that informal entrepreneurship can prompt the development of the financial sector by reducing capacity limitations.

In Gharleghi and Jahanshagi's (2020) study, the development of the financial sector is represented by three indicators – liquid liabilities, private credit to deposit money banks and capitalization of the stock market. The research sample covered 29 developed and developing economies over the 1975–2015 period. This study basically confirmed the results provided by Safuan et al. (2021) and Canh and Thanh (2020), but additionally revealed that the development of the financial sector starts to significantly contribute to reducing the size of the shadow economy in the countries where the value of GDP per capital exceeds US$33,600, while it does not have a significant impact in the countries where this threshold is lower.

Considering the fact that the developed financial sector seems to acquire immunity to the harmful effects of the shadow economy and tends to reduce the size of the shadow economy, researchers recommend ensuring smooth development of the financial sector and its capacity through expanding credit markets for micro, small and medium businesses (Safuan et al., 2021) and granting access to financial markets for the widest possible range of business entities (Gharleghi & Jahanshagi, 2020).

Gang et al.'s (2022) study implies that the relationship between ***informal entrepreneurship*** and the financial sector is bidirectional: On one hand, operating in the informal sector limits access to external financing (i.e. a business is financed through an entrepreneur's personal or household funds), which impedes business development, growing into a company (i.e. expanding a business beyond family and household units) and transferring into the formal sector of the economy; on the other hand, the lack of involvement of economic entities, even operating informally, can become the cause of the credit market instability, especially in developing economies. These findings are supported by Bruhn and Love's (2009) results which indicate that informal entrepreneurs in developing economies largely are low-income individuals who tend to apply for loans from microfinance providers (often also operating informally). This practice distorts credit markets, and even

opening of new bank branches does not lead to a shift towards formal business. In contrast, the level of informal business tends to increase by 7.6 percent (Bruhn & Love, 2009).

Capasso et al. (2022) agree that informal entrepreneurs often have limited access to credits and credit markets, which hampers aggregate productivity. Growth of the aggregate level of informality can have a negative impact on the profitability of banks and the smooth operation of financial markets. At the same time, it is noted that when conditions in the financial markets are improving, opportunity costs of informality are increasing, which acts as a stimulus to transfer activities to the formal sector. Thus, it is concluded that the relationship between the development of financial markets and informal entrepreneurship is inverse, non-monotonic, but the direction of causality is thought to depend on the institutional environment and policy interventions.

By applying the Generalized Method of Moments, Omri (2020) provides the results that indicate that informal entrepreneurship is negatively affected by financial development, that is, the causal relationship will not run from informal entrepreneurship to financial development, but vice versa. It is also recognized that if the net influence of financial development is weak, it can be strengthened by the interaction between financial development and governance quality. The latter, however, may not be possible if the economy is at an early stage of its development (Thai & Turkina, 2014).

Elgin and Uras (2013) note that competition in the informal sector leads to inefficient allocation of resources in the economy where resources are misdirected from the financial sector. Since the state budget is supplemented by collecting taxes from different sectors, including the financial sector, the reduction of funds in the budget limits the ability of national governments to promote the development of the financial sector through creating the necessary infrastructure, issuing adequate regulations, etc. In this aspect, informal entrepreneurship has a detrimental effect on the development of the financial sector though uncollected taxes. These findings were confirmed by Gobbi and Zizza (2007) in their research of the Italian debt market over the 1997–2003 period. Raj et al.'s (2014) study of the Indian market, however, shows that the expanding scale of informal entrepreneurship can be associated with greater availability of local banks.

Artavanis et al. (2016) measure income ***tax evasion*** by using bank credits. Basing their research on the analysis of the microdata representing household credits from a Greek bank, the authors document that banks tend to lend tax-evading individuals after assessing their reported income. This implies that tax evasion may raise bank lending risks because the assessment of a debtor's solvency will be based on incomplete information (e.g. if the case of tax evasion were detected and a debtor-offender were forced to pay hidden taxes and late interest, this could have a significant impact on the debtor's real income and ability to meet financial obligations on time).

According to Gallemore and Jacob (2018), tax enforcement via auditing is often in the focus of politicians and academics because it helps to identify tax-related external factors that affect the banking sector as a sector that promotes economic

growth through provision of capital to business. Having researched the data of the Internal Revenue Service (USA) in the period 1992 and 2000, the authors provide the evidence showing that corporate tax enforcement has a positive impact on lending activities of commercial banks. When assessing the solvency and creditworthiness of a potential borrower, banks rely on both hard and soft information. Corporate tax returns and financial statements are the major sources of hard information. With greater tax enforcement, the quality of financial statements is increasing, corporate tax returns and financial statements contain less inaccurate and fraudulent information. As a result, tax enforcement can improve the quality of the information on the basis of which banks make their lending decisions, that is, tax enforcement can lead to more rational lending decisions and at the same time improve stability of the banking sector, which is less likely to be shaken by the so-called 'bad loans' crisis.

Ozili (2020) links tax evasion with financial instability in the sense that tax evasion reduces the government budget revenue, which could be used to promote stability of the financial sector, and pressures national governments to debts. In this aspect, tax evasion has a detrimental effect on the government's capability of intervening the financial system when it needs to be restored or stimulated. Ozili (2018) states that tax evasion and financial instability are not mutually exclusive. For example, tax evasion can prolong disruptions in financial systems. The author proposes that in general, the effects of tax evasion on financial (in)stability are rather complex, but to understand the full impact, it is important to look at tax evasion from two perspectives: the national government's perspective (limitation of the funds under disposition) and a tax evader's perspective (stability of the personal finance).

Alm et al. (2019) use the data from the Business Environment and Enterprise Performance Survey to investigate the relationship between corporate tax evasion and financial constraints. Their results show that financial constraints affect business corporations through the banking system. Financially constrained corporations tend to have greater cash holdings, that is, they tend to shift their business into cash transactions, thus avoiding dealing with the financial sector. In this way, circulation of money in the banking sector is decreasing, which reduces banks' working capital and the ability to provide loans.

Chaikin (2017) and Vo et al. (2020) provide the evidence showing that the causality between tax evasion and the banking sector can run not only from tax evasion to higher risks in the banking sector, but also from the banking sector to tax evasion. Chaikin (2017) suggests that the banking sector is a systemic offender that facilitates financial crimes, primarily money laundering and tax evasion. The role of bank secrecy in stimulating tax evasion is emphasized. Vo et al.'s (2020) study covered the sample of 112 emerging markets, was based on the Tobit model and considered the period 2006–2017. Their results revealed that bank penetration (physical outreach by banks and other lending institutions) along with information sharing (the exchange of data, in particular, credit information, among financial institutions) negatively affects the degree of tax evasion in emerging markets by promoting market transparency. Similar results were provided by Safuan et al. (2022) who focus on the problems of tax evasion in Indonesia in the period

1980–2019. Their results reveal that there exists a non-linear long-run relationship between financial development and tax evasion, and a lower/higher level of financial development corresponds to a higher/lower level of tax evasion. By employing a variety of estimators, the authors prove that financial development can contribute to solving the problem of tax evasion.

Bonini and Boraschi-Diaz (2013) investigated the causes and financial consequences of ***corporate frauds*** applying the methods of literature analysis, statistical data analysis and critical insight. They note that earnings management, which is one of the constituents of corporate fraud that refers to a variety of legitimate and illegitimate actions undertaken by business managers to affect earnings of their corporations, is linked to abnormal accruals, stock offerings and post-offering stock returns. This proposes that opportunistic manipulation of earnings can unreasonably increase corporate income, profit, stock value and return. According to Skousen et al. (2009), manipulations of earnings and revenue are likely to be practiced by the corporations with high debt ratios, while others do it so that their performance can impress shareholders. Dorminey et al. (2010) indicate that this is characteristic of corporations with low liquidity. In any case, when cases of fraud are revealed, lawsuits damage reputation of a corporation. The financial institutions and financial markets where the disreputable corporation used to cooperate and operate also suffer reputational damage. In addition, financial markets may experience negative effects due to insider trading.

Kurant (2014) examined the consequences of fraudulent misreporting in the US market in the period 2006–2012 using value-weighted index and raw returns CARs. The research revealed that when the returns of the corporations committing frauds are not adjusted to the market returns, their stock price tends to increase by an average of 1.63 percent. These findings are in line with Bonini and Boraschi-Diaz's (2013) results, though the calculated stock price increase is not so abnormal. In any case, the real financial consequences of misreporting can be seen not only as reputational damage to the fraudulent corporation itself, but also to the financial sector (for instance, banks) because the fraudulent corporation's loan costs are increasing. With high costs, loans become more difficult to serve, and banks may face the problems of insolvency of the fraudulent corporations.

Having analysed the stock price response to the announcement of frauds in Indian banking sector by applying the Event Study Methodology, Sharma and Verma (2020) found that the announcement of frauds affects stock prices of the banks that suffered a fraud. For instance, the results showed that the Punjab National Bank experienced the biggest fall in their share prices, equal to 8.74 percent. Osei-Assibei et al. (2018) researched the effects of corporate fraud on financial institutions in Ghana. They distinguish between internal (fraudulent acts committed within financial institutions) and external (fraud committed by external individuals or stakeholders who are directly related to financial institutions) fraud. The latter category is wider and includes stolen checks, fraudulent loans, forged documents and e-fraud. By applying a cross-sectional model, the authors found that fraud in general (i.e. the aggregate of internal and external fraud) has a statistically significant negative

impact on financial performance, represented by Return on Assets, of financial institutions.

By applying the method of regression analysis, Achmad and Pamungkas (2018) researched a sample of 87 banking companies listed on the Indonesian Stock Exchange in the period 2011–2016. Their research revealed that fraudulent financial reporting, first of all, has a detrimental effect on the entire financial market due to the damage suffered by investors. When analysing the situation in the banking sector, the authors note that this sector is regulated stricter than other private business sectors. Therefore, when banks suffer fraud-caused damage or fraud cases occur in the banking sector itself (e.g. issuing fictitious guarantees, withdrawing funds, etc.), the reputational damage suffered by banks is greater than that of companies operating in other private business sectors. Sharma and Verma (2020) note that the increasing number of fraud cases not only brings direct financial losses to banks, but also reduces investor confidence, which may negatively affect the performance of other banks operating in the sector. To reduce the number of cases of fraudulent financial reporting, researchers recommend improving stability of the financial system (which would help to solve corporate liquidity problems), ensuring a rational audit and increasing the percentage of independent commissioners in business corporations (Achmad & Pamungkas, 2018).

Netshisaulu et al. (2022) focus on the issue of ***illicit financial flows*** (i.e. illegal movement of money and capital across country borders) and state that due to invoking complex transactions, illicit financial flows create financial opacity, which, in its turn, can harm good financial practices. Although the practices of illicit financial flows often do not conflict with official regulations, their implementation takes advantage of regulatory loopholes and ambiguity, which creates the impression that most transactions in the financial system are characterized by ambiguity. The effects of financial opacity and secrecy in creating an environment conducive to illicit financial flows are also emphasized by Mwita et al. (2019) who focus on financial accounting information transparency in Tanzania. Netshisaulu et al. (2022) propose that the relationship between illicit financial flows and financial systems is bidirectional: On one hand, illicit financial flows lead to instability and unreliability of financial systems; on the other hand, opacity of the financial system and non-compliance with international financial reporting standards, characteristic of developing countries, create conditions favourable to illicit financial flows.

By employing the method of the secondary data (e.g. the Swiss leaks data for HSBC, the Permanent Sub Committee Report on HBUS in the USA, and others) analysis, Naheem (2018) investigates how illicit financial flows occur in the banking and financial services sectors. The research results show that illicit financial flows in many cases occur because banks do not identify the source and purpose of fund transfers and do not verify the beneficial ownership of recipients. This implies that conditions favourable to illicit financial flows are created in the banking system itself, which is in line with Netshisaulu et al.'s (2022) findings. The performance of deficient banks in this respect harms their reputation and creates the impression of unreliability of the entire banking system. Rahman et al. (2019), who analysed illicit financial outflows from 60 developing countries in the period 2004–2013 by

applying Pedroni's heterogeneous panel data methodology, even call it endemic weakness of the banking system.

When analysing how illicit financial flows are absorbed in developing economies (the period under consideration covered 2002 to 2006), Kar et al. (2010) indicate that banks in developed economies (Australia, Japan, the United Kingdom, the USA, the European countries) and offshore financial centres (mainly in Switzerland) are the major points absorbing illicit financial. These findings were confirmed by Chowla and Falcao (2016) who find that in the cases of illicit financial flows, money is transferred to international accounts through multi-layered schemes and jurisdictional structures. Ayogu and Gbadebo-Smith (2015) note that although a substantial part of illicit funds (e.g. in the case of smuggling) are in the form of cash, they sooner or later they end up in the banking system as deposits or funds in the accounts of agents. Kar et al. (2010) provide the estimates that offshore financial centres hold 24–44 percent of the total absorption, while banks hold the balance. Illicit funds often 'settle' in the aforementioned financial institutions as private sector deposits. In the absence of detailed reporting, which would reveal the deposit data by sector, deposit maturity and the country of residence of deposit holders, large data gaps leading to a lack of transaction transparency are created. The results also indicate that absorption of illicit financial flows by banks and offshore financial centres is facilitated by international banks. These results imply that illicit financial flows harm the reputation of financial institutions and reduce the transparency of transactions not only in developing but also in developed countries, and participation of international banks requires introduction of the relevant economic and governance policies to make absorption of illicit financial flows more difficult. Rahman et al. (2019) remind the effects of globalization, macroeconomic vulnerability and gross domestic savings and propose the measure of political stability.

Financial institutions remain one of the main targets of ***cybercrime***, and the expanding potential of online payments, online banking and digital money also expands the opportunities to commit financial crimes. CSIS's (2018) report proposes that banks spend three times more on their cyber security than non-financial institutions. With major international financial institutions investing in defence, better fraud prevention and transaction authentication, organized crime groups have begun to target the 'seams' of well-defended networks by exploiting weak points in the global financial network for mass financial theft, even from the SWIFT system.

Ogunwale (2020) states that banks suffer from malware infections that affect the entire IT infrastructure and take control of processing services and automated teller machines (ATMs). The most common cybercrime techniques are phishing, hacking and malware and identity thefts and ATM spoofing. Based on literature analysis, statistical data analysis (the case of Nigeria) and critical insight, the author notes that cybercrime leads to large losses of commercial banks, which are often hidden from the public not to lose investor confidence and not to cause anxiety among customers regarding possible insecurity, that is, banks try to preserve their reputation.

Akinbowale et al.'s (2020) research, based on the methods of literature analysis and the balanced scorecard analysis, confirms an increasing negative effect of cybercrime on financial institutions. This negative effect manifests both indirectly –

through the loss of public trust in the digital infrastructure – and directly – through fraud and extortion. The tendencies are similar in both developing and developed economies. By employing the methods of the Analytical Hierarchy Process (AHP) and Pareto analysis (PA), Akinbowale et al. (2022) ranked various aspects of the impact of cybercrime on the financial sector. The primary data was collected by surveying 17 licensed South African bank representatives responsible for administration and management operations. The results of the research revealed that cybercrime has the greatest negative impact on the profitability and goodwill of financial institutions (as indicated by 100 percent of the respondents). The second significant aspect of the impact is reduction of the level of consumer satisfaction (as noted by 95.23 percent of the respondents). The impact on the risk management processes was recognized the least significant (as noted by only 7.15 percent of the respondents).

After surveying the banking sector employees and analysing the general public discussion on the issue under consideration in the region of Gulf Countries Council, Ali (2019) emphasizes the negative impact of cybercrime on online banking security and integrity of financial institutions. Malik and Islam (2019) conducted a survey of 302 bank employees in Pakistan and confirmed the negative impact of cybercrime on bank performance. The authors also note that information security awareness tends to reduce the negative impact of cybercrime. After interviewing 123 employees from 12 commercial banks in Malaysia, Ibrahim (2021) invoked the cross-sectional research approach to confirm the latter finding of Malik and Islam (2019). Ibrahim (2021) also confirmed the hypotheses proposing that the fight against cybercrime in the banking sector is significantly affected by public financial literacy, public awareness, education/training, the ICT and technical tools, and law enforcement.

Lagazio et al. (2014) analysed the impact of cybercrime on the financial sector by applying a multi-level model and a system dynamics methodology. Their results disclosed a strong dynamic relationship between tangible and intangible factors affecting cybercrime at the value network. The authors argue that the costs of cybercrime incurred by financial institutions are not determined solely by the number of cybercrime cases; the methods chosen by financial institutions to protect their business interests and carry out market positioning have a significant impact on these costs. Responding to cybercrime, financial institutions should review their strategic behaviour, focus on customer trust and loyalty as a key goal and avoid chronic under-reporting, which may have negative consequences not only for a specific financial institution, but also for the entire sector. Akinbowale et al. (2020) suggest integrating big data technologies into banking systems.

Mcwhinney et al. (2022) examined the potentially negative impact of ***cryptocurrencies*** (specifically Bitcoin) on national financial systems. According to the authors, national governments distribute and regulate money flows in the economy through financial intermediaries (banks and other financial institutions). Acting through financial intermediaries allows to monitor how money is transferred, to which sectors the largest/smallest cash flows go, and to assess how usefully the money is used. In a decentralized cryptocurrency system, peer-to-peer transfers in cryptocurrency networks are made directly between transaction parties, so financial

intermediaries are no longer needed. The chain of trust that underpins the traditional financial system becomes nothing more than an algorithmic construct. In this system, central banks lose their functions since every user with the right computer and hardware can create a cryptocurrency. Thus, governments in developed countries are wary of Bitcoin's progress, as there are fears that the excessive use of cryptocurrencies can turn the traditional financial system upside down, destabilize it and undermine the role of the government, which can lead to the risk of the financial system spiralling out of control (Mcwhinney et al., 2022).

By applying the multivariate GARCH (1,1) methodology, Corbet et al. (2020) *found that* cryptocurrency scams negatively affect the financial market through raising price volatility of a specific cryptocurrency as well as broad cross-cryptocurrency correlations. Abnormal returns, which are generated before a cryptocurrency scam, turn into zero, which unbalances the financial market. This was also confirmed by Corbet et al. (2019) in the study based on a systematic review of empirical literature. The latter study also notes that cryptocurrency-related cybercrimes tend to cause pricing bubbles because of the interaction among regulatory oversight, the potential for the illicit use of cryptocurrencies through anonymity and infrastructural breaches.

Floyd's (2019) review article reminds that Bank of Amerika together with the Securities and Exchange Commission in their briefing treat cryptocurrencies as a risk factor that can negatively affect banks' competitiveness, revenue and profits. The briefing indicates three directions in which cryptocurrencies pose a threat to the banking system. First, it is difficult to trace the movement of funds. Second, consumers may be lured by financial products and services that are speculative and risky. Third, cryptocurrencies can negatively affect the competitive environment of traditional banks: Since transactions are carried out without intermediaries, an increase in the variety of financial products offered by non-depository institutions is likely to increase (some of these products and services will be offered for fraudulent purposes). This is expected to reduce bank income from fee-based products and services, as well as net interest margin. In addition, it is feared that traditional payment processing can be disrupted by cryptocurrency scams (no supervision, no intermediation, no responsibility).

Hermans et al. (2022) note that crypto assets threaten the stability of the entire financial system given that they lack intrinsic economic value. Cryptocurrencies are often used as an instrument for speculation and financing illicit activities. Therefore, there is a reasonable concern about the threat posed by the manipulation of cryptocurrencies to the integrity of the financial market and consumer protection; the lack of intrinsic economic value reduces the value of investment instruments offered by traditional financial institutions. In Europe, the aforementioned risk is increasing due to strengthening interconnections between crypto-assets and the euro area banking sector.

The IMF (2001) report notes that economic and financial crimes have a negative macroeconomic impact, lead to a lower level of population's well-being and can have a negative external impact on cross-border cooperation and international trade.

Kumar (2012) argues that ***money laundering*** can distort international trade and capital flows, which will be detrimental to long-term economic development. The excessive outflows of illegal capital can be facilitated by both domestic and foreign financial institutions. These outflows of capital drain scarce resources possessed by a country. Losing resources makes economic development difficult. Money laundering channels can also distort a country's imports and exports. On the import side, money launderers can buy imported luxury goods for laundered funds or in the process of laundering funds. The imports that do not stimulate domestic economic activities and employment will artificially lower domestic product and service prices, thereby reducing the profitability of local business enterprises (Kumar, 2012). On the export side, offenders can manipulate export prices to launder funds from illicit activities (Walker & Unger, 2009) and invoke export under-invoicing, especially when trading with low- and middle-income countries (Toan, 2022).

The strategy of developing countries to establish offshore financial centres as a means of promoting economic development can be weakened by significant levels of money laundering (money will be laundered through established offshore financial centres) (Kumar, 2012). Young (2013) emphasizes that money laundering through offshore financial centres is stimulated by banking confidentiality. Having conducted the secondary data analysis and 'grey' literature material analysis, Gilmour (2022) points out that innovative trading hubs (so-called freeports) that help to obscure beneficial ownership are used for money laundering.

Abuse of the financial system, financial crimes and money laundering can distort the efficient allocation of resources and wealth (IMF, 2001). For example, money laundering hinders the development of cost-effective investment. Money launderers are interested in protecting their proceeds rather than generating profits from investment. Therefore, they tend to invest funds not necessarily in those activities or sectors that are economically beneficial. They prefer 'sterile' investment in real estate, works of art, antiques and luxury goods, as well as investment in the sectors characterized by marginal productivity (the most common sectors are bars, restaurants, hotels, construction and prostitution). In the above-mentioned sectors, the value of goods or services is difficult to estimate, and they are characterized by sudden increases in value (Kumar, 2012). Gjoni et al. (2015) note that in the case of money laundering, funds are diverted from healthy and successful business areas and transferred to dangerous areas, thus turning illegally obtained funds into criminal sterile investment. Money launderers have no motive to earn income. They have already earned it illegally, so the aim is only to disguise the origin of the income. Low-quality investment simply ensures circulation of money, which slows down economic growth (Ayodeji & Mahmood, 2012). McDowell (2001) provides the example that certain sectors of the economy (e.g. construction, accommodation services) generate income not because of the actual level of demand, but because of the short-term interests of money launderers. When these sectors are no longer needed by money launderers, they are simply abandoned, which causes heavy losses to businesses and can even lead to a crisis in the sectors under consideration and reduce the overall macroeconomic stability.

Dobrowolski and Sulkowski (2019), who analysed the potential to implement the United Nations Sustainable Development Goals (SDGs) adopted in 2015 (the study was based on interviewing 15 representatives of 11 supreme audit institutions), indicate that money laundering hinders sustainable development: From the economic side, it distorts the results of efficient economic activity and creates public distrust of markets and innovations; from the governance side, it reduces accountability, transparency and integrity; from the social side, it catalyses other types of crimes, for instance, corruption, fraud, drug trafficking, terrorism.

Gjoni et al. (2015) argue that money laundering can hinder a country's sustainable development by destabilizing political institutions. The authors point out that after gaining significant economic power, money launderers seek to increase their political control through corruption, bribes and falsification of voting results. Kumar (2012) states that the latter factors can have devastating social consequences by providing fuel for all types of criminals to expand their activities. The economic and political influence of criminal organizations can weaken the state's social structure, collective ethical standards and, finally, democratic public institutions and the foundations of democratic processes, which undoubtedly complicates the course of sustainable economic and social development.

The detrimental effects of money laundering on sustainable development determine the requirement specified by the United Nations – to reduce the volumes of money laundering that destabilizes national economies. The anti-money laundering and auditing model, developed by Dobrowolski and Sulkowski (2019), proposes that this can be done by involving obligated organizations (any financial institutions, electronic money institutions, payment institutions, investment companies, custodian banks, legal entities carrying out brokerage activities), cooperating units (prosecution offices, internal security agencies, tax authorities, customs authorities), financial intelligence units, foreign financial intelligence units and law enforcement agencies in national anti-money laundering systems.

Chitakunye et al.'s (2015) research, based on the critical secondary data review, showed that ***corruption*** has a particularly negative impact on socio-economic development of the Southern African Development Community (SADC), and this is characteristic of both political and bureaucratic corruption (so-called 'big' and 'petty' corruption, respectively): Due to corruption, money intended for sustainable development is dispersed into private pockets. There is also a negative correlation between corruption and FDI. Thus, capital flows and tax revenue are lost, additional jobs are not created, and the benefits from technology and knowledge spillover are not received. Corruption deepens the problems of informal economic activities, creates obstacles to economic and political reforms and reduces investment, and all this hinders economic growth (Habibov et al., 2019).

By using the Structural Equation Modelling Technique, Venard (2013) confirms that corruption negatively affects economic development (the sand-in-the-wheel view). According to the author, the defective institutional framework (economic and political) promotes corruption; this framework cannot ensure human welfare, so sustainable development is not possible. By employing disaggregated data for time series data analysis and previous empirical findings for cross-reference, Hope (2022)

provides evidence that corruption in Africa negatively affects the region's sustainable development through damaging national economies, and this effect is particularly severe. This refutes the assumption that corruption can 'grease the wheels' at least slightly promoting economic development. Yu et al.'s (2022) research of developing economies in the period 2000–2019, based on the framework of the difference generalized method of moments (GMM), concluded that corruption impedes sustainable development through diminishing the effects of foreign aid.

Having analysed the elasticity of socio-economic and environmental development indicators in relation to corruption in 47 countries across Asia, Africa and Latin America and the Caribbean (LAC) over the period 2000 to 2015, Murshed and Mredula (2018) conclude that the causality between corruption and socio-economic development is short-run bidirectional. The authors also find that corruption has a negative effect on environmental development in Asia and Africa, though this result was not confirmed for the LAC region (for identifying the relationship between corruption and environmental development, the Environmental Kuznets's Curve hypothesis was tested).

Marchini et al. (2019) analysed the relationship between corruption and sustainable development in terms of income shifting between subsidiaries and parental companies. The authors considered the sample of the European International Groups having parental companies in France, Germany, Italy, Spain and the UK. Basing their findings on the linear regression and anomie theory, the authors treat corruption as a symptom of instability that affects corporate decision making. They provide evidence that business managers tend to shift income to less corrupt countries, while high levels of corruption reduce incentives to attract foreign income. Thus, corruption impedes sustainable development not only through slower social and environmental development, as revealed by the results of the above-discussed studies, but also through the shift of business income, since a corrupt environment has a negative impact on business attractiveness.

Absalyamova et al. (2016) researched the impact of corruption on sustainable development from the perspective of human capital, which is treated as the potential for generating income in the future. Using the econometric analysis method for the Russian case study, the authors find that a 1 percent increase in the level of corruption in a country's socio-economic system leads to a greater than 1 percent decrease in the Human Capital Sustainable Development Index (HCSDI), that is, corruption has a negative multiplier effect on sustainable development through gradually degrading human capital as a generative power.

Hoinaru et al. (2020) propose that corruption can provide economic efficiency by helping circumvent the restrictive law and bureaucratic barriers, and thus to a certain degree promotes economic development, but at the same time the authors admit that this tendency is more characteristic of developing countries. Meanwhile, in developed high-income countries, economic and sustainable development tends to be negatively affected by corruption. This is supported by Venard (2013) who states that corruption can promote economic growth only when public institutions are of low quality, which is not compatible with the principles of sustainable development. According to Yu et al. (2022), corruption is a deadly disease of any society's

development because it violates the principles of justice when welfare is guaranteed only to persons who have authority. Welfare in such societies is not efficient, and societies cannot be stable.

High levels of ***tax evasion*** create an unstable and unreliable economic environment (Litina & Palivos, 2016). From an economic point of view, the problem of tax evasion arises because the tax base does not take into account the real level of the major taxation variables, such as sales, income of private individuals, profits of business enterprises, population's wealth. In this case, there is a risk that unreasonably high tax rates will be set, and economic agents will not realize the real value of an individual/a corporate tax base (Carvalho, 2019). Dobrovič et al. (2017), who focus on combating tax evasion in Slovakia, note that the additional tax burden is placed on the shoulders of a citizen/consumer. This indicates not only decreasing real income of the latter, but also violation of the principle of equality, without which sustainable development is impossible. In addition, tax evasion hinders normal functioning of the state due to drained resources and creates the illusion that citizens may not pay taxes at all, which can fundamentally undermine the state's foundations.

An unreliable economic environment can also be formed in the presence of imperfect information about taxes (e.g. if tax provisions are constantly changing) and inefficient tax administration. According to Siqueira and Ramos (2005), in the latter case, an audit can improve the situation, and this will mean that the tax base is verifiable at a certain cost. Celimene et al. (2016) note that tax evasion has a negative impact on the amount of per capita spending and therefore on the amount of the income that can be earned from production. Volatile production fluctuations will have the negative effects on the average economic growth rate. Darnihamedani et al. (2018) emphasize that tax evasion has detrimental effects on innovative entrepreneurship and sharply raises start-up cost.

Umanah et al.'s (2021) literature analysis suggests that the taxation framework is significant to sustainable development not only as a major source of the government revenue, but also as a stimulator of economic areas that can potentially generate revenue and promote economic growth. The authors also link high rates of tax evasion to stagnation and unemployment (tax evading economic entities are not capable of ensuring sustainable growth and creating more jobs), which impede both purely economic and sustainable development.

The negative effects of tax evasion can be mitigated by allowing economic agents to invest their illegal benefits in stock markets, by reducing tax rates and increasing productivity of public spending. In addition, reasonable governmental policies can help to form a better attitude of taxpayers towards their fiscal obligations: Knowing exactly the tax rates and being sure that the tax base is reasonable and stable, taxpayers will find it easier to calculate the costs and benefits of the economic activities they are involved in (Barone & Mocetti, 2011). A sound and stable tax base is the major source of financing sustainable development available to national governments. This is confirmed by Kononova et al. (2016), according to whom, the taxation framework is one of the most important institutions that affects the behaviour of citizens (tax awareness, tax compliance) and helps to shape their well-being (social services and economic growth). Bird and Davis-Nozemack (2018), who

researched tax evasion as a sustainability problem, suggest that an approach to tax evasion from a sustainability perspective provides are more holistic understanding of what societal consequences tax frauds can lead to.

The effects of the ***shadow economy*** on the sustainability and growth in 50 developing countries over the 2010–2019 period were researched by Sultana et al. (2022). The results of their study imply that the shadow economy detrimentally affects sustainable development in the sample countries, while the contribution of economic growth and economic freedom is positive. The authors highlight the need not to destroy the shadow economy, but to take interventions that would allow the transfer of business and other economic activities to the formal sector because this can help expand opportunities for economic growth.

Enste's (2018) analysis of the positive and negative effects of the shadow economy revealed that the shadow economy tends to impede welfare and economic growth by worsening fiscal deficits and reducing infrastructure investment. According to Hassan (2017), the shadow economy includes all unregistered economic (market-based) activities. If these activities were registered, they would increase officially registered national income (i.e. they would serve to an increase in GDP). Schneider et al. (2010) argue that the informal economy draws effective resources from the formal economy – it primarily absorbs labour and capital resources, but these resources are used inefficiently, thus generating only minimal value to the overall economy. What is more, the shadow economy distorts the official macroeconomic statistics, based on which policy makers can implement ineffective macroeconomic policies (Schneider & Enste, 2000).

Another negative aspect of the impact of the shadow economy is that the shadow economy undermines functioning of state institutions, which ultimately threatens economic and political development (Enste, 2018). Mishchuk et al. (2020) found that a large size of the shadow economy has a negative impact on GDP (the estimated correlation coefficient was equal to −0.729) and determines the low level of a country's competitiveness as per the world rankings. Mazhar and Jafri (2017) argue that the shadow economy affects monetary policy because it is associated with a larger demand for currency. They also propose that the shadow economy undermines returns to political stability, which is necessary for economic reforms, especially those aimed at making a country's tax system more efficient. Nevertheless, the relationship between the shadow economy and political stability is not confirmed either in Cukierman et al.'s (1992a, b) or Huang and Wei's (2006) studies.

Considering all three aspects of sustainable development (not only economic, but also social and environmental), it is noticeable that the shadow economy from a social point of view leads to distortion in social norms by determining corruption, the weak rule of law and disrespect towards public authorities (Hassan, 2017). From an environmental point of view, it is associated with greater land, water and air pollution when economic entities operating in the informal sector ignore the established environmental regulations (Biswas et al., 2012; Sultana et al., 2022), although it is recognized that the ability of these entities to re-use waste materials leaked from the formal sector can have a positive impact on the environment (Chirisa

& Bobo, 2018; Koksal et al., 2020). In an economic sense, the shadow economy can contribute to productivity since resources that remain unused in the official economy can be used through the shadow economy to increase the overall supply of goods and services (Enste, 2018).

Summarizing the effects of the shadow economy on development and sustainability, Sultana et al. (2022) conclude that although this sector can generate benefits and has the potential to meet the social needs of the population, in the long run it hinders economic and sustainable development because business activities and production in this sector do not ensure long-term economic efficiency and well-being.

Santos et al. (2021) focused on the impact of ***informal entrepreneurship*** on venture capital and financial flows as contributors of economic growth. Their research is based on the multiple regression models for panel data representing the situation in 23 European countries between 2006 and 2015 (total of 230 observations). Their literature analysis shows that venture capital can promote growth in the economies with strong institutional protection of investors, and investors themselves are well-educated and technically oriented. The economies with high levels of informal entrepreneurship can, however, encounter serious challenges posed by venture capital markets. Operating in the economies with high levels of informal entrepreneurship, investors can feel insufficiently secure, not believing that the legal and regulatory framework is strong enough to protect their initial investment contracts from opportunistic renegotiation risks. Thus, informal entrepreneurship can inhibit financial and venture capital flows. The empirical results confirm the theoretical findings: The authors observe the negative moderating effect of informal entrepreneurship on venture capital flows and GDP. Webb et al. (2013) emphasize the negative impact of informal entrepreneurship on business competitiveness as a contributor to macroeconomic development. Maseko et al. (2012) point out that in the case of informal employment, economic development is limited by the fact that informal employment cannot ensure the quality of activities, it does not introduce the latest methods of production, marketing, financial management or the latest technologies. Although it is recognized that informal employment can act as a measure for mitigating labour market volatility (Loayza & Rigolini, 2011), can have a short-term mitigating effect on unemployment (Mishchuk et al., 2020) and helps residents in developing countries earn income (Basu & Chau, 2015; Chrenekova et al., 2016; Ghose, 2017), Ndiweni and Verhoeven (2013) admit that it cannot ensure long-term economic growth and is an expression of a lack of accountability, resource plunder and the failure of the government economic policies. According to Mughal and Schneider (2020), informal employment undermines the long-term foundations of macroeconomic planning and income distribution, simultaneously undermining the foundations of sustainable development.

When assessing the effects of informal employment on the dimension of social development, researchers tend to analyse how strongly it affects living standards, social security and the quality of life (Mishchuk et al., 2020). Gonzalez-Baltazar et al. (2019) surveyed 507 informal workers in Mexico and found that the workers have relatively good economic benefits, but are characterized by a low level of

satisfaction with the quality of labour life; they report a lack of occupational and health safety, and many of them work in unhealthy conditions and are exposed to risks in the workplace. Similar results were provided by Forastieri (1999) who note that informal workers lack sufficient technical means and resources to comply with appropriate health and safety regulations; in addition, they often lack an understanding of the necessity for protection. Having analysed the 2012 Cambodia Labour Force Survey, Dike (2019) found that informal employment is associated with a significant increase in the probability of work injury/illness.

Nakabayashi (2019), who analysed the opposing models representing the relationship between a country's political structure and recognition of human rights, proved that sustainable development depends on the citizens' welfare, which is closely related to family security. Thus, sustainable development from the perspective of social welfare depends on the precedent of family security. Nakabayashi (2019) also links family security to small and medium business development by providing evidence that family security positively affects small, medium business and self-employment. This relationship was confirmed by Čepel (2019), who researched the impact of social and cultural factors on the development of small- and medium-sized businesses in the Czech and Slovak Republics (the research sample covered 312 companies in the Czech and 320 companies in the Slovak Republics; representatives of the companies participated in the questionnaire survey), and found that a favourable family environment motivates doing business and helps with entrepreneurial activities. Given the fact that, as discussed before, informal employment has characteristics that do not provide social security to individuals and households, it can be stated that informal employment limits sustainable development through the dimension of complicated social development.

Brown and McGranahan (2016) argue that informal entrepreneurs tend to operate neglecting or inadequately meeting sustainability requirements in terms of environmental and social protection: They assume no responsibility for pollution of the environment, waste management and recycling, use urban public space in an unauthorized manner and exploit human rights. The features of poor environmental sustainability in the sector of informal entrepreneurship were also observed by Webb et al. (2014), Chen et al. (2018) (environmental pollution) and Burcea (2015) (waste management and recycling).

Formalization of informal economic activities is one of the sustainable development goals declared by the United Nations (ILO, 2015) and, according to Huang et al. (2020), is one of the most serious challenges of the twenty-first century in terms of sustainable economic, social and environmental development. Adeola et al. (2019) confirm that sustainable development is rooted in a deep and adequate understanding of the informal economy. Nevertheless, as noted by Sultana et al. (2022), the impact of the informal economy on sustainable development is difficult to assess objectively, since this economic sector is not regulated and controlled by formal institutions.

Ruggiero (2022) treats financial crime as an inadequate prioritization of immediate goals, manifested on the part of the business and financial sector. According to the author, since ***corporate frauds*** only allow to achieve short-term goals, they

stimulate economic volatility, turmoil and instability, which, in their turn, discourage long-term initiatives and lead to investors' reluctance to get involved in sustainable projects. Kumar (2012) treats corporate fraud not only as deception of the investors who have decided to invest in a certain company, but also as a decrease in the general investor confidence in business transparency. In any case, the decline in investment (both foreign and domestic) limits the potential for business development, thus slowing down the national economic growth.

Jan (2021) argues that corporate fraud (with the major focus on financial statement fraud) can cause financial distress or bankruptcy of an enterprise and can have a great negative impact on the general macroeconomic and business environment. The research, based on the analysis of the financial and non-financial data of TWSE/TEPx listed companies in the period 2001–2019 (the sample covered 153 companies, 51 of which reported financial statement fraud while others did not), revealed that corporate frauds lead to information asymmetry, which can seriously jeopardize sustainability of corporate operations, corporate health and proper functioning of capital markets. The fact that information asymmetry, determined by corporate fraud, undermines public confidence in the financial system and capital markets was confirmed by Cunha et al. (2013) and Martins and Junior (2020). According to Jan (2021), this is incompatible with the principles of sustainable development of the global capital market. Mendes de Oliveira et al. (2022) state that falsification of accounting information impedes the analysis of business risks and scenarios and does not allow taking the necessary damage prevention measures, thus negatively affecting sustainable business development and hampering sustainable development of the economy and corporate social responsibility. According to Harjoto (2017), to achieve sustainable development, business ethical values, which are reflected in corporate social responsibility, should be developed as a means to prevent corporate fraud and have less severe socio-economic effects of fraud.

The Commonwealth Fraud Prevention Centre (2020) notes that frauds can also cause damage to a country's economic and international reputation: Widespread frauds can become a deterrent when assessing whether a country is safe for doing business, international trade, etc. What is more, frauds can damage a country's reputation if they threaten the systems of other countries. For example, if fraudulently obtained information, material or documentation (e.g. obtaining false passports, transferring fraud methodologies to target programs in foreign countries) are used through international entities.

Ruggiero's (2022) research implies that corporate frauds may mean the use of finance for environmentally degrading operations, that is, frauds are treated as a contributor to environmental crime. Ruggiero (2020) draws attention to the manifestations of this phenomenon in the economic sectors of oil, gas and mineral extraction and exportation. The report provided by the Commonwealth Fraud Prevention Centre (2020) proposes that frauds can have a detrimental effect on the environment, which is an important component of sustainable development alongside economic and social development. Fraud cases can lead to direct environmental damage through pollution, loss of biodiversity and disruption of the ecological balance. This damage can be irreversible. The indirect damage will manifest itself

through higher costs of environmental management and conservation and reduced effectiveness of the 'green measures'. The report implies that environmental sustainability tends to decrease in the countries characterized by a high level of corruption and fraud.

Focused on the issues of ***illicit capital flows*** and fraud, Shaxson (2019) argues that the secret financial flows as well as the financial flows created when fleeing taxes tend to increase inequality, lead to a country's vulnerability to crises and bring hard-to-measure political damage when the capital transferred from developing countries is infiltrated into Western political systems. The author also notes that the flows of financial capital running from developing countries to tax haven countries are followed by the phenomenon of labour migration.

Abu-Orabi and Al Abbadi (2019) discuss the illicit capital flows that are created when laundering money. The authors point out that these flows cause exchange rate inflation in developing countries, which, in its turn, reduces the competitiveness of traditional exports in relation to imports. Capital outflows put pressure on national monetary bases, which leads to a domestic price increase and undermines the real purchasing power of the population. To control this situation, national governments can be forced to introduce restrictive financial policies and create a budget surplus, which would help to deal with the financial consequences of capital outflows. According to Mwita et al. (2019), illicit financial flows increase opacity, which hinders economic growth, discourages investment, raises transaction costs and leads to financial uncertainty. Thus, illicit capital flows negatively affect financial and money markets, unbalance the investment sector and also undermine the capability of national governments of implementing the adequate monetary policies. Netshisaulu et al. (2022) note that since illicit capital flows are channelled through commerce, corruption and criminal activities, it is precisely these channels that hinder sustainable development.

Ndikumana and Boyce (2012), who researched the illicit capital flows in four North African countries – Algeria, Egypt, Morocco and Tunisia – in the period 1970–2010, found that the economic model of the countries under consideration is unstable, mainly due to inequality of the distribution of wealth and power. This is because large illicit financial flows fuel accumulation of private wealth by the political and business elites. The estimations showed the capital stock in the sample countries would increase by 60 percent if illicit financial outflows were stopped; under the same condition, GDP per capita would increase by 15 percent. These results imply that illicit capital flows stimulate income and social inequality and impede national economic growth, which destroys the basis for sustainable development of emerging countries.

When researching the situation in 39 developing African economies in the period 2000–2010, Ndikumana (2014) focused on the issue of how much additional growth the countries could have achieved without having illicit financial outflows. The results revealed that the sample countries could have achieved 3 percent higher economic growth if they had not faced the problem of illicit financial outflows. In oil-exporting countries that are particularly sensitive to illicit financial flows, economic growth could have been higher by as much as 3.9 percent.

In the context of social development, the studies by Maton and Daniel (2012) and the OECD (2012) revealed that illicit financial flows negatively affect social development and hinder social cohesion. Cobham and Jansky (2020) emphasize the negative impact on social security, that is, the ability of states to prevent insecurity at the personal, community, environmental and political levels: Illicit financial flows raise the risk of violence against a person, the risk of tension between interest groups, the risk of environmental degradation and the risk of neglecting political rights and duties. The increasing role of criminal activities, including trafficking in drugs, human beings and illegal goods, can increasingly harm the state because implementation of these activities may require the support of state institutions (e.g. the military, customs, police officers). The risk of crimes (e.g. bribery) directly against the state is also increasing because of seeking private benefits, looting state's property and instigating internal conflicts, which cannot in any way serve the sustainable development of the state.

Some studies hint at possible positive effects of economic and financial crimes. For instance, Gjoni et al. (2015) note that illicit monetary flows can have a positive impact on the national economic growth when a country is a platform for the transfer of illegally obtained money (e.g. fiscal, tax haven). If the proceeds of a criminal offense are received in another country and transferred to the host country for the purpose of laundering, then the illegal origin of these proceeds does not have a negative impact on the economy of the host country. Although some sources (IMF, 2001) propose that countries can receive additional income through their lax legal system and faulty tax practices (attracting offshore businesses, making investment in certain sectors of the economy funded through illegal capital flows), the general view prevails that a country's negative reputation reduces its potential in global markets and inhibits sustainable growth. On the contrary, a damaged reputation attracts international criminal organizations driven by short-term goals. The state must devote additional resources to identification and prevention of economic and financial crimes.

Focused on the impact of ***cybercrime*** on economic and sustainable development, the report of the UK Cabinet Office and 'Detica' (2011) emphasizes that the effects of cybercrime are interdependent. If individuals, having suffered losses due to cybercrime, have less funds at their disposal, their spending on goods and services will decrease, which means a loss of revenue for businesses. In the macroeconomic context, a high level of cybercrime tends to reduce the confidence of foreign investors in a country's business environment and government, which means that the country is likely to face stronger international business competition. Attracting less investment can hurt economic growth. One of the biggest long-term threats is the possible development of the underground economy: Motivated individual cybercriminals with sufficient skills and expertise are drawn away from the official economy in both cases – if they conduct cybercrime as co-workers, and if they see cybercrime as a high-income generating activity, an attractive alternative to formal work. When cybercrime activities carried out by individuals are expanding, organized crime groups are being created. Their money laundering and offshoring activities lead to business disruption, extortion and service denial. With expanding

criminal networks, the reputational and financial damage/losses of businesses and state institutions are increasing, and security costs are growing. Instability of the financial system caused by cybercrime can have negative macroeconomic consequences. For instance, a lack of trust in banks can lead to potentially large fiscal liabilities, reduce a country's ability to attract foreign investment and increase the volatility of international capital flows and exchange rates (IMF, 2001). The above-mentioned factors hinder a country's sustainable development.

Olivia's (2022) research emphasizes the following directions of the negative impact of cybercrime on Nigeria's sustainable development: reduction in competitive edge, productivity losses and rising costs (inflation), monetary losses, destroyed image of the country and slowed financial inclusion. Reduction in competitive edge means that businesses lose their competitive advantage and suffer losses when confidential information stolen by hackers is sold to competitors. Losses also include the time costs that businesses have to incur when rectifying cybercrime damage instead of spending this time on generating profits. Productivity losses and rising cost are linked to the necessity to implement the measures allowing to secure the network and reduced profit margins. Monetary losses represent the financial costs incurred by businesses and the economy due to the loss of intellectual property, financial fraud, damage to reputation and third party liability. A country's image destroyed by cybercrime not only scares away potential investors, but also discourages citizens from actively using ICTs, which leads to a negative impact on the welfare of the citizenry. Finally, proliferation of cybercrime retards financial inclusion, and the lack of confidence in the banking sector can earn the country an economic pariah status when financial transactions with the country's citizens are avoided.

Having analysed the links between digital vulnerabilities and sustainable development in developing economies, Schia and Willers (2021) emphasize that the negative effect of cybercrime on sustainable development is stronger in the countries characterized by poor governance and poverty. This is because these countries implement digital technologies with so-called 'technological leapfrogging', so unprecedented societal vulnerabilities can remain sufficiently underestimated. The risk of vulnerability is increasing with the formation of a gap between the rapid digitalization process and the society's readiness and ability to manage modern technologies. The society's readiness to manage technology, first of all, does not mean citizens' skills, but inadequate or weak institutions, legal frameworks, policies and strategies, a lack of standards, poor organizational and individual protection systems. Sustainable development is impossible without solving these problems. Fernandez (2019) notes that economic crimes, including cybercrime, breach a country's economic system, distort economic goals and policies, cause damage to both the private and public sectors and violate the social interests of the citizens.

McWhinney et al. (2022) note that ***cryptocurrency scams*** can undermine a country's authorities and their ability to use traditional economic and fiscal policy measures because they allow bypassing government-imposed capital controls. According to the authors, capital control is established to prevent currency outflows since the value of the currency can decrease due to exports. Cryptocurrency scams

allow bypassing capital controls and provide the conditions for exporting assets. There is a risk that the value of a country's currency will decrease, and the government will lose the leverage of its fiscal policy.

Also, the use of cryptocurrencies is associated with a high degree of anonymity – users in Bitcoin networks are identified only by their addresses on the network, and the algorithms eliminate the need for contract reliability verification. The above-mentioned factors pave the way for illegal transactions and help criminals to avoid detection of fraudulent activities, thus increasing the overall crime rate. One of the most prominent examples of criminal activities with the use of Bitcoins is the case of Silk Road. The digital market platform Silk Road was launched in 2011. By employing privacy techniques (e.g. the Tor network, based on anonymized user data) and cryptocurrency transactions, the participants of this platform were able to anonymously transact in illegal data, hacked passwords, drugs, conduct money laundering activities, etc. Only in 2013 Silk Road was eventually shut down by FBI with seizure of more than 144,000 bitcoins, the total value of which at that time was about $34 million (Frankenfield et al., 2021). Reid and Harrigan (2011) confirm that incomplete identification can stimulate money laundering through cryptocurrency, which can especially spread under the conditions of political instability, volatility of the foreign exchange market and economic shocks (e.g. the COVID-19 pandemic).

Kang and Lee's (2019) quantitative analysis reveals that the level of welfare in an economy where both money and bitcoins are used is lower compared to the level of welfare in an economy where only money is used, and this gap tends to increase with the increase in inflation.

As noted by Shin and Rice (2022), security is one of the keys of sustainable development. Despite the progressive initiatives provided by cryptocurrencies, their growing potential has posed many challenges, such as trust, cyber security and scalability. This has led to questions of how to manage the crypto economy and how to create a sustainable crypto ecosystem. The examples of the digital black markets, where cryptocurrencies are used as the main means of payment, show that the cryptocurrency ecosystem still lacks transparency; this ecosystem is still associated with scandals and criminal activities, which contradicts the principles of sustainable economic and social development.

3 Conclusions

Economic and financial crimes undermine the functions of financial-banking institutions to accumulate capital from local savings and foreign funds and to act as a stimulating factor for investment and efficient distribution of resources, thus creating an environment favourable to economic growth. Financial institutions with flows and deposits of proceeds of crime face additional challenges in properly managing their assets, liabilities and operations. An unexpected outflow of large sums can cause liquidity problems. In this way, the circulation of money in the banking sector

is decreasing, which reduces banks' working capital and the ability to provide loans. Economic and financial crimes may pose a threat to monetary stability due to improper asset structure and artificial distortion of asset and commodity prices. Exchange rate and interest rate fluctuations can increase due to the unexpected transfer of relatively large funds across borders. Financial-banking institutions associated with economic and financial crimes lose public trust (reputational damage), and the probability of banking crises is increasing. All of this hinders the development of financial institutions and financial markets. Direct and indirect negative effects of economic and financial crimes are felt in banking and non-banking financial institutions, as well as equity, loan and currency markets. The main internal control measures that can be undertaken by banking and financial institutions to protect themselves against the negative effects of economic and financial crimes are careful monitoring of account opening, accepting money on deposit and issuing loans. Improving the institutional environment and policy interventions are recommended as external measures.

Economic and financial crimes have a negative impact on sustainable development. In the economic sense, they can lead to distorted international trade and capital flows as well as excessive capital outflows, which drain scarce resources possessed by a country. Losing resources makes economic development difficult. Abuse of the financial system can distort the efficient distribution of resources and assets and hinders the development of economically efficient investment. Economic and financial crimes distort the results of efficient economic activities, create public distrust of markets and innovation and reduce accountability, transparency and integrity. This creates an unstable and unreliable economic environment and a low level of a country's competitiveness and harms its international reputation. In the social sense, economic and financial crimes provide fuel for all types of criminals to expand their activities. The economic and political influence of criminal organizations can weaken the state's social structure, collective ethical standards, democratic public institutions and the foundations of democratic processes. They lead to family insecurity and a lack of occupational and health safety. Human welfare cannot be ensured in a flawed institutional framework. All this undoubtedly complicates the course of sustainable development. In the environmental sense, economic and financial crimes can lead to direct damage to the environment, which will manifest itself through pollution, loss of biodiversity and disruption of the ecological balance. This damage may be irreversible. The indirect damage will mean higher costs for environmental management and conservation as well as reduced effectiveness of the 'green measures'.

References

Absalyamova, S., Absalyamov, T., Khusnullova, A., & Mukhametgalieva, C. (2016). The impact of corruption on the sustainable development of human capital. *Journal of Physics: Conference Series, 738*, 012009. https://doi.org/10.1088/1742-6596/738/1/012009

Abu-Orabi, M. M. A.-M., & Al Abbadi, A. F. A. (2019). The effects of money laundering on monetary markets introduction. *Modern Applied Science, 13*(12), 43–51. https://doi.org/10.5539/mas.v13n12p43

Abuzayed, B., Ammar, M. B., Molyneux, P., & Al-Fayoumi, N. (2019). *Corruption, lending and bank performance*. Retrieved from https://dspace.aus.edu/xmlui/bitstream/handle/11073/16535/SBAWPS%2003-11-2019_Corruption%20Lending%20and%20Bank%20Performance.pdf?sequence=1&isAllowed=y

Achim, M. V., & Borlea, N. S. (2020). Effects of economic and financial crimes. Ways of fighting against. In M. V. Achim & N. S. Borlea (Eds.), *Economic and financial crime. Corruption, shadow economy, and money laundering* (pp. 245–271). Springer Nature Switzerland AG.

Achmad, T., & Pamungkas, I. D. (2018). Fraudulent financial reporting based of fraud diamond theory: A study of the banking sector in Indonesia. *JIAFE (Jurnal Ilmiah Akuntansi Fakultas Ekonomi), 4*(2), 135–150.

Adeola, O., Eigbe, O., & Muritala, O. (2019). The informal economy: CSR and sustainable development. In O. Osuji, F. Ngwu, & D. Jamali (Eds.), *Corporate social responsibility in developing and emerging markets: Institutions, actors and sustainable development* (pp. 85–97). Cambridge University Press.

Akinbowale, O. E., Klingelhofer, H. E., & Zerihun, M. F. (2020). Analysis of cyber-crime effects on the banking sector using the balanced score card: A survey of literature. *Journal of Financial Crime, 27*(3), 945–958. https://doi.org/10.1108/JFC-03-2020-0037

Akinbowale, O. E., Klingelhofer, H. E., & Zerihun, M. F. (2022). Analytical hierarchy processes and Pareto analysis for mitigating cybercrime in the financial sector. *Journal of Financial Crime, 29*(3), 984–1008. https://doi.org/10.1108/JFC-04-2021-0086

Ali, L. (2019). Cyber crimes-A constant threat for the business sectors and its growth (a study of the online banking sectors in GCC). *The Journal of Developing Areas, 51*(3), 267–279. https://doi.org/10.1353/jda.2019.0016

Ali, M. S. B., Fhima, F., & Nouira, R. (2020). How does corruption undermine banking stability? A threshold nonlinear framework. *Journal of Behavioral and Expremental Finance, 27*, 100365. https://doi.org/10.1016/j.jbef.2020.100365

Alm, J., Liu, Y., & Zhang, K. (2019). Financial constraints and firm tax evasion. *International Tax and Public Finance, 26*, 71–102.

Alomari, K. A. K. (2020). Linking between E-government and money laundering: The mediating role of compliance unit. *International Journal of Academic Research in Business & Social Sciences, 10*(2), 179–194. Retrieved from https://pdfs.semanticscholar.org/69c4/faa3ca15f5684e9de471f23d34a62c015554.pdf

Arshad, S., & Rizvi, S. A. R. (2013). Impact of corruption on bank profitability: An analysis of Islamic banks. *International Journal of Business Governance and Ethics, 8*(3), 195–209. https://doi.org/10.1504/IJBGE.2013.057375

Artavanis, N., Morse, A., & Tsoutsoura, M. (2016). Measuring income tax evasion using bank credit. *The Quarterly Journal of Economics, 131*(2), 739–798. Retrieved from https://www.jstor.org/stable/26372652

Asteriou, D., Pilbeam, K., & Tomuleasa, I. (2021). The impact of corruption, economic freedom, regulation and transparency on bank profitability and bank stability: Evidence from the Eurozone area. *Organization, 184*, 150–177. https://doi.org/10.1016/j.jebo.2020.08.023

Ayodeji, A., & Mahmood, B. (2012). The impact of money laundering on economic and financial stability and on political development in developing countries: The case of Nigeria. *Journal of Money Laundering Control, 15*(4), 442–457. https://doi.org/10.1108/13685201211266024

Ayogu, M. D., & Gbadebo-Smith, F. (2015). Governance of illicit financial flows. In S. I. Ajayi & L. Ndikumana (Eds.), *Capital flight from Africa. Causes, effects, and policy issues* (pp. 277–300). Oxford University Press.

Bahoo, S. (2020). Corruption in banks: A bibliometric review and agenda. *Finance Research Letters, 35*, 101499. https://doi.org/10.1016/j.frl.2020.101499

Barone, G., & Mocetti, S. (2011). Tax morale and public spending inefficiency. *International Tax and Public Finance, 18*(6), 724–749.

Basu, A. K., & Chau, N. H. (2015). Informal work in developing countries. In *International Encyclopedia of the Social & Behavioral Sciences* (2nd ed.). Elsevier. https://doi.org/10.1016/B978-0-08-097086-8.94028-5

Bayar, Y., & Aytemiz, L. (2017). Financial development and shadow economy in Turkey. In S. Koc, A. Orhan, & M. C. Gozen (Eds.), *Unregistered employment* (pp. 170–175). IJOPEC Publication.

Berdiev, A. N., & Saunoris, j. W. (2016). Financial development and the shadow economy: A panel VAR analysis. *Economic Modelling, 57*, 197–207. https://doi.org/10.1016/j.econmod.2016.03.028

Bird, R., & Davis-Nozemack, K. (2018). Tax avoidance as a sustainability problem. *Journal of Business Ethics, 151*, 1009–1025.

Biswas, A., Farzanegan, M. R., & Thum, M. (2012). Pollution, shadow economy and corruption: Theory and evidence. *Ecological Economics, 75*, 114–125.

Bolanriwa, S. T., & Soetan, F. (2019). The effect of corruption on bank profitability. *Journal of Financial Crime, 26*(3), 753–773. https://doi.org/10.1108/JFC-09-2018-0102

Bonini, S., & Boraschi-Diaz, D. (2013). The causes and financial consequences of corporate frauds. In *Entrepreneurship, finance, governance and ethics* (pp. 1–35). https://doi.org/10.1007/978-94-007-3867-6_13

Brown, D., & McGranahan, G. (2016). The urban informal economy, local inclusion and achieving a global green transformation. *Habitat International, 53*(4), 97–105.

Bruhn, L., & Love, I. (2009). The economic impact of banking the unbanked. *The World Bank Development Research Group, Policy Research Working Paper No., 4981*, 1–30.

Burcea, S. G. (2015). The economical, social and environmental implications of informal waste collection and recycling. *Theoretical and Empirical Researches in Urban Management, 10*(3), 14–24.

Canh, N. P., & Thanh, S. D. (2020). Financial development and the shadow economy: A multi-dimensional analysis. *Economic Analysis and Policy, 67*, 37–54. https://doi.org/10.1016/j.eap.2020.05.002

Capasso, S., Ohnsorge, F., & Yu, S. (2022). Informality and financial development: A literature review. *The Manchester School, 90*(5), 587–608. https://doi.org/10.1111/manc.12417

Carvalho, J. L. D. P. (2019). *The effects of tax evasion on economic growth: A stochastic growth model approach.* Retrieved from https://www.locus.ufv.br/bitstream/123456789/26737/1/texto%20completo.pdf

Celimene, F., Dufrenot, G., Mophou, G., & N'Guerekata, G. (2016). Tax evasion, tax corruption and stochastic growth. *Economic Modelling, 52*(A), 251–258.

Čepel, M. (2019). Social and cultural factors and their impact on the quality of business environment in the SME segment. *International Journal of Entrepreneurial Knowledge, 7*(1), 65–73. https://doi.org/10.2478/ijek-2019-0005

Chaikin, D. (2017). Money laundering and tax evasionEThe assisting of the banking sector. In M. S. Aßländer & S. Hudson (Eds.), *The handbook of business and corruption* (pp. 237–254). Emerald Publishing. https://doi.org/10.1108/978-1-78635-445-720161012

Chen, M., Jeon, B. N., Wang, R., & Wu, J. (2015). Corruption and bank risk-taking: Evidence from emerging economies. *Emerging Markets Review, 24*, 122–148. https://doi.org/10.1016/j.ememar.2015.05.009

Chen, H., Hao, Y., Li, J., & Song, X. (2018). The impact of environmental regulation, shadow economy, and corruption on environmental quality: Theory and empirical evidence from China. *Journal of Cleaner Production, 195*(9), 200–214.

Chirisa, I., & Bobo, T. (2018). Informal sector operations and the environment: Reconnoitering the African urban space for sustainable urban stewardship. In *Informal sector operations and the environment* (pp. 361–376). IGI Global.

Chitakunye, P., Ojochenemi, D., Derera, E., & Tarkhar, A. (2015). Transnational analysis of the impact of corruption on development in Africa: A review of literature. *Journal of Social Science, 42*(1–2), 129–142. https://doi.org/10.1080/09718923.2015.11893402

Chowla, P., & Falcao, T. (2016). *Illicit financial flows: Concept and flows*. Retrieved from https://www.un.org/esa/ffd/wp-content/uploads/2017/02/Illicit-financial-flows-conceptual-paper_FfDO-working-paper.pdf

Chrenekova, M., Melichova, K., Marišova, E., & Moroz, S. (2016). Informal employment and quality of life in rural areas of Ukraine. *European Countryside, Sciendo, 8*(2), 135–146.

Cobham, A., & Jansky, P. (2020). *Estimating illicit financial flows*. Oxford University Press.

Corbet, S., Lucey, B., Urquhart, A., & Yarovaya, L. (2019). Cryptocurrencies as a financial asset: A systematic analysis. *International Review of Financial Analysis, 62*, 182–199. https://doi.org/10.1016/j.irfa.2018.09.003

Corbet, S., Cumming, D. J., Lucey, B. M., Peat, M., & Vigne, S. A. (2020). The destabilising effects of cryptocurrency cybercriminality. *Economics Letters, 191*, 108741. https://doi.org/10.1016/j.econlet.2019.108741

CSIS. (2018). *Economic impact of cybercrime – No slowing down.* Retrieved from https://csis-website-prod.s3.amazonaws.com/s3fs-public/publication/economic-impact-cybercrime.pdf

Cukierman, A., Edwards, S., & Tabellini, G. (1992a). Seigniorage and political instability. *American Economic Review, 82*, 537–555.

Cukierman, A., Webb, S. B., & Neyapti, B. (1992b). Measuring the independence of central banks and its effect on policy outcomes. *The World Bank Economic Review, 6*, 353–398.

Cunha, P. R., Silva, J. O. D., & Fernandes, F. C. (2013). Pesquisas sobre a lei Sarbanes-Oxley: Uma análise dos journals em língua inglesa. *Enfoque Reflexão Contábil, 32*, 37–51.

Darnihamedani, P., Block, J. H., Hessels, J., & Simonyan, A. (2018). Taxes, start-up cost, and innovative entrepreneurship. *Small Business Economics, 51*(2), 355–369.

Dike, O. (2019). *Informal employment and work health risks: Evidence from Cambodia.* MPRA paper no. 92943. Retrieved from https://mpra.ub.uni-muenchen.de/92943/1/MPRA_paper_92943.pdf

Dobrovič, J., Gombár, M., & Benková, E. (2017). Sustainable development activities aimed at combating tax evasion in Slovakia. *Journal of Security and Sustainability Issues, 6*(4), 761–772. https://doi.org/10.9770/jssi.2017.6.4(19)

Dobrowolski, Z., & Sulkowski, L. (2019). *Implementing a sustainable model for anti-money laundering in the United Nations Development Goals.* Retrieved from https://www.mdpi.com/2071-1050/12/1/244/htm

Dorminey, J., Fleming, S., Kranacher, M.-J., & Riley, R. A. (2010). *The evaluation of fraud theory*. American Accounting Association Annual Meeting.

Eksi, I. H., & Dogan, B. (2020). Corruption and financial development. *Public Finance Quarterly, 2*, 196–209. Retrieved from http://real.mtak.hu/120553/1/A_Eksi-Dogan_20_2.pdf

Elgin, C., & Uras, B. R. (2013). Is informality a barrier to financial development? *SERIEs, 4*(3), 309–331.

Elsherif, N. (2019). *Financial inclusion, shadow economy and financial stability: Evidence from emerging economies*. Master's thesis, the American University in Cairo. AUC Knowledge Fountain. Retrieved from https://fount.aucegypt.edu/etds/520

Enste, D. H. (2018). *The shadow economy in industrial countries.* Retrieved from https://wol.iza.org/articles/shadow-economy-in-industrial-countries/long

Fernandez, R. M. (2019). Effects of economic crimes on sustainable development. *Peace, Justice and Strong Institutions, 2019*, 1–9.

Ferwerda, J. (2010). *Criminals saved our banks: The effects of money laundering during the financial crisis.* Retrieved from http://www.inclusionexclusion.eu/site/wp-content/uploads/2010/03/Paper-Joras-Ferwerda.pdf

Floyd, D. (2019). *Bank of America, JPMorgan call cryptocurrencies a threat.* Retrieved from https://www.investopedia.com/news/bank-america-calls-cryptocurrencies-risk-its-business/

Forastieri, V. (1999). *Improvement of working conditions and environment in the informal sector through safety and health measures*. Retrieved from http://www.ilo.int/wcmsp5/groups/public/%2D%2D-ed_protect/%2D%2D-protrav/%2D%2D-safework/documents/publication/wcms_110306.pdf

Frankenfield, J., Rasure, E., & Li, T. (2021). *Silk road (website).* Retrieved from https://www.investopedia.com/terms/s/silk-road.asp

Gallemore, J., & Jacob, M. (2018). *Tax enforcement externalities and the banking sector.* Retrieved from https://business.gwu.edu/sites/g/files/zaxdzs1611/f/downloads/2018-04-05%20Gallemore%20Jacob.pdf

Gang, I. N., Raj, S. N., & Sen, K. (2022). *Can access to finance spur entrepreneurship in Indian informal sector?* Retrieved from https://www.wider.unu.edu/publication/can-access-finance-spur-entrepreneurship-indian-informal-sector

Gharleghi, B., & Jahanshagi, A. A. (2020). The shadow economy and sustainable development: The role of financial development. *Journal of Public Affairs, 20*(3), e2099. https://doi.org/10.1002/pa.2099

Ghose, A. K. (2017). Informality and development. *Indian Journal of Labour Economics, 60*(1), 109–126. https://doi.org/10.1007/s41027-017-0080-5

Gilmour, P. M. (2022). Freeports: Innovative trading hubs or centres for money laundering and tax evasion? *Journal of Money Laundering Control, 25*(1), 63–71. https://doi.org/10.1108/JMLC-01-2021-0002

Gjoni, M., Gjoni, A., & Kora, H. B. (2015, November). *Money laundering effects.* University of Business and Technology in Kosovo. International Conference on Management, Business and Economics. Retrieved from https://www.researchgate.net/publication/330630840_Money_Laundering_Effects

Gobbi, G., & Zizza, R. (2007). *Does the shadow economy hold back financial deepening? Evidence from the Italian credit market*. Retrieved from https://conference.iza.org/conference_files/worldb2007/zizza_r3406.pdf

Gonzalez-Baltazar, R., Contreras-Estrada, M. I., Leon-Cortes, S. G., Hidalgo-Gonzalez, B. J., & Hidalgo-Santacruz, G. (2019, July 24–28). *Quality of labor life in workers of the informal economy in Guadalajara, Mexico.* Advances in social and occupational ergonomics, proceedings of the AHFE 2019 international conference on social and occupational ergonomics, pp. 266–276. https://doi.org/10.1007/978-3-030-20145-6_26

Habibov, N., Fan, L., & Auchynnikava, A. (2019). The effects of corruption on satisfaction with local and national governments. Does corruption 'grease the wheals'? *Europe-Asia Studies, 71*(5), 736–752. https://doi.org/10.1080/09668136.2018.1562044

Harjoto, M. A. (2017). Corporate social responsibility and corporate fraud. *Social Responsibility Journal, 13*(4), 762–779. https://doi.org/10.1108/SRJ-09-2016-0166

Hasan, R., & Ashfaq, M. (2021). Corruption and its diverse effect on credit risk: Global evidence. *Future Business Journal, 7*. No. 18.

Hassan, M. (2017). *The impact of the shadow economy on aid and economic development nexus in Egypt.* Retrieved from https://mpra.ub.uni-muenchen.de/80990/1/MPRA_paper_80990.pdf

Hermans, L. Ianiro, A., Kochanska, U., Tormalehto, V.-M., van der Kraaij, A., & Simon, J. M. V. (2022). *Decrypting financial stability risks in crypto-asset markets*. European Central Bank. Retrieved from https://www.ecb.europa.eu/pub/financial-stability/fsr/special/html/ecb.fsrart202205_02~1cc6b111b4.en.html\

Hoinaru, R., Buda, D., Borlea, S. N., Vaidean, V. L., & Achim, M. V. (2020). The impact of corruption and shadow economy on the economic and sustainable development. Do they "sand the wheels" or "grease the wheels"? *Sustainability, 12*(2), 481. https://doi.org/10.3390/su12020481

Hope, K. R., Sr. (2022). *The corruption and sustainable development nexus in Africa: A contemporary review and analysis*. Journal of Financial Crime. https://doi.org/10.1108/JFC-10-2022-0257

Huang, H., & Wei, S.-J. (2006). Monetary policies for developing countries: The role of institutional quality. *Journal of International Economics, 70*, 239–252.

Huang, G., Xue, D., & Wang, B. (2020). Integrating theories on informal economies: An examination of causes of urban informal economies in China. *Sustainability, 12*(7) No. 2738. https://doi.org/10.3390/su12072738

Ibrahim, W. N. W. (2021*). an empirical study on cybercrime: The emerging threat to banking sectors in Malaysia.* Retrieved from https://kmc.unirazak.edu.my/wp-content/uploads/2022/06/Master-Thesis-Wan-Nora.pdf

IMF. (2001). *Financial system abuse, financial crime and money laundering – Background paper.* Retrieved from https://www.imf.org/external/np/ml/2001/eng/021201.pdf

International Labour Organisation. (2015). *Formalization of the informal economy: Area of critical importance.* Retrieved from https://www.ilo.org/wcmsp5/groups/public/%2D%2D-ed_norm/%2D%2D-relconf/documents/meetingdocument/wcms_412833.pdf

Jan, C.-L. (2021). Detection of financial statement fraud using deep learning for sustainable development of capital markets under information asymmetry. *Sustainability, 13*(17), 9879. https://doi.org/10.3390/su13179879

Kang, K.-Y., & Lee, S. (2019). *Money, bitcoin, and monetary policy*. Retrieved from SSRN https://ssrn.com/abstract=3303595 or https://doi.org/10.2139/ssrn.3303595\

Kar, D., Cartwright-Smith, D., & Hollingshead, A. (2010). *The absorption of illicit financial flows from developing countries: 2002-2006. Research project*. Retrieved from https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2335028

Kemal, M. U. (2014). Anti-money laundering regulations and its effectiveness. *Journal of Money Laundering Control, 17*(4), 416–427.

Koksal, C., Isik, M., & Katircioglu, S. (2020). The role of shadow economies in ecological footprint quality: Empirical evidence from Turkey. *Environmental Science and Pollution Research, 27*(12), 13457–13466.

Kononova, K., Bitkova, T., & Merkulova, T. (2016). Tax factors of sustainable development: System dynamics approach towards tax evasion analyses. *Rivista di study sulla sostenibilita, VI*(1), 35–47. https://doi.org/10.3280/RISS2016-001005

Kumar, A. (2012). Money laundering: Concept, significance and its impact. *European Journal of Business and Management, 4*(2), 113–120.

Kurant, P. (2014). *Corporate fraud and its consequences: An empirical study.* Master Dissertation. Retrieved from https://core.ac.uk/download/pdf/143409413.pdf

Lagazio, M., Sherif, N., & Cushman, M. (2014). *A multi-level approach to understanding the impact of cyber crime on the financial sector.* Retrieved from https://core.ac.uk/download/pdf/20543077.pdf

Lester, J., & Roth, J. (2007). Criminal prosecution of banks under the Bank secrecy act. *United States Attorney's Bulletin*, pp. 54–71.

Litina, A., & Palivos, T. (2016). Corruption, tax evasion and social values. *Journal of Economic Behavior and Organization, 124*, 164–177.

Liu, P., Li, H., & Guo, H. (2020). The impact of corruption on firms' access to bank loans: Evidence from China. *Economic Research-Ekonomska Istraživanja, 33*(1), 1963–1984. https://doi.org/10.1080/1331677X.2020.1768427

Loayza, N. V., & Rigolini, J. (2011). Informal employment: Safety net or growth engine? *World Development, 39*(9), 1503–1515.

Malik, M. S., & Islam, U. (2019). Cybercrime: An emerging threat to the banking sector of Pakistan. *Journal of Financial Crime, 26*(1), 50–60. https://doi.org/10.1108/JFC-11-2017-0118

Marchini, P. L., Mazza, T., & Medioli, A. (2019). Corruption and sustainable development: The impact on income shifting in European international groups. *Corporate Social Responsibility and Environmental Management, 27*(2), 717–730. https://doi.org/10.1002/csr.1839

Martins, O. S., & Junior, R. V. (2020). The influence of corporate governance on the mitigation of fraudulent financial reporting. *Review of Business Management, 22*, 65–84.

Maseko, N., Manyanin, O., Chiriseri, L., Tsekea, M. P. C., Chazuza, T., & Mutengezanwa, M. (2012). An analysis of the impact of targeted government support on the SMEs growth

and development in Zimbabwe: A survey of Mashonaland Central Province. *Journal of Research in International Business Management, 2*(2), 51–59.

Maton, J., & Daniel, T. (2012). The Kleptocrat's portfolio decisions. In P. Reuter (Ed.), *Draining development? Controlling flows of illicit funds from developing countries* (pp. 415–454). World Bank.

Mazhar, U., & Jafri, J. (2017). Can the shadow economy undermine the effect of political stability on inflation? Empirical evidence. *Journal of Applied Economics, 20*(2), 395–420. https://doi.org/10.1016/S1514-0326(17)30018-1

McDowell, J. (2001). The consequences of money laundering and financial crime. *An Electronic Journal of the U.S. Department of State, 6*(2), 1–8.

McWhinney, J., Brown, R. J., & Reeves, M. (2022). *Why governments are wary of Bitcoin.* Retrieved from https://www.investopedia.com/articles/forex/042015/why-governments-are-afraid-bitcoin.asp

Mendes de Oliveira, D. K., Imoniana, J. O., Slomski, V., Reginato, L., & Slomski, V. G. (2022). How do internal control environments connect to sustainable development to curb fraud in Brazil? *Sustainability, 14*(9), 5593. https://doi.org/10.3390/su14095593

Mishchuk, H., Bilan, S., Yurchyk, H., Akimova, L., & Navickas, M. (2020). Impact of the shadow economy on social safety: The experience of Ukraine. *Economics and Sociology, 13*(2), 289–303. https://doi.org/10.14254/2071-789X.2020/13-2/19

Mughal, K. S., & Schneider, F. G. (2020). How informal sector affects the formal economy in Pakistan? A lesson for developing countries. *South Asian Journal of Macroeconomics and Public Finance, 19*(1) Retrieved from https://journals.sagepub.com/doi/full/10.1177/2277978719898975, 7–21.

Murshed, M., & Mredula, F. (2018). Impacts of corruption on sustainable development: A simultaneous equations model estimation approach. *Journal of Accounting, Finance and Economics, 8*(1), 109–133.

Mwita, R. M., Chachage, B., Mashenene, R. G., & Msese, L. R. (2019). The role of financial accounting information transparency in combating corruption in Tanzanian SACCOS. *African Journal of Applied Research, 5*, 108–119. Retrieved from http://dspace.cbe.ac.tz:8080/xmlui/handle/123456789/214

Naheem, M. A. (2018). Illicit financial flows: HSBC case study. *Journal of Money Laundering Control, 21*(2), 231–246. https://doi.org/10.1108/JMLC-08-2015-0036

Nakabayashi, M. (2019). From family security to the welfare state: Path dependency of social security on the difference in legal origins. *Economic Modelling, 82*, 280–293.

Ndikumana, L. (2014). Capital flight and tax havens: Impact on investment and growth in Africa. *Revue d'économie du développement, 22*, 99–124. Retrieved from https://www.cairn.info/revue-d-economie-du-developpement-2014-HS02-page-99.html

Ndikumana, L., Boyce, J. K. (2012). *Capital flight from North African countries.* Retrieved from http://students.aiu.edu/submissions/profiles/resources/onlineBook/h9f2H2_NAfrica%20capital%20flight%20africa.pdf

Ndiweni, E., Verhoeven, H. (2013). *The rise of informal entrepreneurs in Zimbabwe: Evidence of economic growth or failure of economic policies?* Retrieved from https://core.ac.uk/download/pdf/287533551.pdf

Netshisaulu, N. N., Van der Poll, H. M., & Van der Poll, J. A. (2022). A conceptual framework to analyse illicit financial flows (IFFs). *Risks, 10*(9), 172. https://doi.org/10.3390/risks10090172

OECD. (2012). *International drivers of corruption: A tool for analysis*. Retrieved from https://read.oecd-ilibrary.org/development/international-drivers-of-corruption_9789264167513-en

Ogunwale, H. (2020). *The impact of cybercrime on Nigeria's commercial banking system.* Retrieved from https://www.researchgate.net/profile/Hezekiah-Ogunwale/publication/347388290_THE_IMPACT_OF_CYBERCRIME_ON_NIGERIA'S_COMMERCIAL_BANKING_SYSTEM/links/5fda6c7392851c13fe90a613/THE-IMPACT-OF-CYBERCRIME-ON-NIGERIAS-COMMERCIAL-BANKING-SYSTEM.pdf

Olivia, O. E. (2022). Examining the effect of the elevated rate of cybercrime on the growth and sustainable development of Nigeria's economy. *Journal of Commercial and Property Law, 9*(1), 32–43.

Omri, A. (2020). Formal versus informal entrepreneurship in emerging economies: The roles of governance and the financial sector. *Journal of Business Research, 108*, 277–290. https://doi.org/10.1016/j.jbusres.2019.11.027

Osei-Assibei, M. B., Dui, L. K., Muyun, Z., Asare, E. K., & Amankwaa, I. A. (2018). Corporate fraud: Causes, effects, and deterrence on financial institutions in Ghana. *European Scientific Journal, 14*(28), 315–335. https://doi.org/10.19044/esj.2018.v14n28p315

Ozili, P. K. (2018). *Tax evasion and financial instability. MPRA Paper*. Retrieved from https://mpra.ub.uni-muenchen.de/88661/1/MPRA_paper_88661.pdf

Ozili, P. K. (2020). Tax evasion and financial instability. Journal of Financial Crime, 27(2), pp. 531–539. doi: https://doi.org/10.1108/JFC-04-2019-0051.

Rahman, M., Mustafa, M., & Turpin, L. (2019). Determining illicit financial outflows from sixty developing countries. *Journal of Financial Economic Policy, 11*(1), 62–81. https://doi.org/10.1108/JFEP-12-2017-0120

Raj, S. N. R., Sen, K., & Kathuria, V. (2014). Does banking development matter for new firm creation in the informal sector? Evidence from India. *Review of Development Finance, 4*(1), 38–49.

Reid, F., & Harrigan, M. (2011). *An analysis of anonymity in the bitcoin system.* Retrieved from https://www.researchgate.net/publication/51918209_An_Analysis_of_Anonymity_in_the_Bitcoin_System

Ruggiero, V. (2020). Killing environmental campaigners. *Criminological Encounters, 3*(1), 92–105.

Ruggiero, V. (2022). Sustainability and financial crime. *International Criminology, 2*, 143–151.

Safuan, S., Habibullah, M. S., & Sugandi, E. A. (2021). Mitigating the shadow economy through financial sector development in Indonesia: Some empirical results. *Heliyon, 7*(12), e08633. https://doi.org/10.1016/j.heliyon.2021.e08633

Safuan, S., Habibullah, M. S., & Sugandi, E. A. (2022). Eradicating tax evasion in Indonesia through financial sector development. *Cogent Economics & Finance, 10*(1). https://doi.org/10.1080/23322039.2022.2114167

Sagastume, W. Z., Moreno-Brid, J. C., & Garry, S. (2016). Money laundering and financial risk Management in Latin America, with special reference to Mexico. *Economía: Teoría y Práctica, Nueva Época, 44*, 9–50. http://www.izt.uam.mx/economiatyp/ojs

Santos, E., Fernandes, C. I., Ferreira, J. J., & Lobo, C. A. (2021). What is the impact of informal entrepreneurship on venture capital flows? *Journal of the Knowledge Economy, 12*, 2032–2049. Retrieved from https://link.springer.com/article/10.1007/s13132-020-00701-w

Schia, N. N., & Willers, O. J. (2021). *Digital vulnerabilities and the sustainable development goals in developing countries.* Retrieved from https://nupi.brage.unit.no/nupi-xmlui/bitstream/handle/11250/3007756/Schia-Willers2021_First%2bSubmission%2bDraft.pdf?sequence=1&isAllowed=y

Schneider, F., & Enste, H. (2000). Shadow economies: Size, causes and consequences. *Journal of Economic Literature, 38*, 77–114.

Schneider, F., Buehn, A., & Montenegro, C. E. (2010). New estimates for the shadow economies all over the world. *International Economic Journal, 24*(4), 443–461.

Sharma, D., & Verma, R. (2020). Reaction of stock Price to frauds' announcements: Evidence from Indian banking sector. *Asia-Pacific Journal of Management Research and Innovation, 16*(2), 157–166. https://doi.org/10.1177/2319510X209308

Shaxson, N. (2019). *Tackling tax havens.* Retrieved from https://www.imf.org/en/Publications/fandd/issues/2019/09/tackling-global-tax-havens-shaxon

Shin, D., & Rice, J. (2022). Cryptocurrency: A panacea for economic growth and sustainability? *A critical review of crypto innovation. Telematics and Informatics, 71*, 101830. https://doi.org/10.1016/j.tele.2022.101830

Siqueira, M. L., & Ramos, F. S. (2005). A economia da sonegação: teorias e evidências empíricas. *Revista de Economia Contemporânea, 9*(3), 555–581.

Skousen, C. J., Smith, K. R., & Wright, C. J. (2009). Detecting and predicting financial statement fraud: The effectiveness of the fraud triangle and SAS no. 99. In M. Hirschey, K. John, & A. K. Makhija (Eds.), *Corporate governance and firm performance (advances in financial economics)* (Vol. 13, pp. 53–81). Emerald Group. https://doi.org/10.1108/S1569-3732(2009)0000013005

Slutzky, P., Villamizar-Villegas, M., & Williams, T. (2020). *Drug money and bank lending: The unintended consequences of anti-money laundering policies.* Retrieved from http://tomas-williams.com/wp-content/uploads/2020/06/Drug-Money-and-Bank-Lending-05-28-2020.pdf

Sultana, N., Rahman, M. M., & Khanam, R. (2022). The effect of the informal sector on sustainable development: Evidence from developing countries. *Business Strategy and Development, 5*(4), 437–451. Retrieved from https://onlinelibrary.wiley.com/doi/full/10.1002/bsd2.217\

Thai, M. T. T., & Turkina, E. (2014). *Entrepreneurship in the informal economy*. Routledge. https://doi.org/10.4324/9780203066775

The Commonwealth Fraud Prevention Centre. (2020). *The total impacts of fraud.* Retrieved from https://www.counterfraud.gov.au/total-impacts-fraud

The UK Cabinet Office and 'Detica'. (2011). *The cost of cybercrime. A Detica report in partnership with the Office of Cyber Security and Information Assurance in the Cabinet Office.* Retrieved from https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/60943/the-cost-of-cyber-crime-full-report.pdf

Toader, T., Onofrei, M., Popescu, A., & Andrieș, A. M. (2018). Corruption and banking stability: Evidence from emerging economies. *Emerging Markets Finance and Trade, 54*, 591–617. https://doi.org/10.1080/1540496X.2017.1411257\

Toan, B. H. (2022). Effects of foreign direct investment on trade-based money laundering: The case of Vietnam. *Cogent Social Sciences, 8*(1). https://doi.org/10.1080/23311886.2022.2132672

Umanah, S., Sadom, T. E., & Oyedokun, G. (2021). Tax evasion, avoidance and sustainable development: A literature review. In *Proceedings of the 3rd annual international academic conference of the chartered Institute of Taxation in Nigeria*, pp. 121–137. ISBN 978-978-989-469-7.

Venard, B. (2013). Institutions, corruption and sustainable development. *Economics Bulletin, 33*(4), 2545–2562.

Vo, D. H., Nguyen, H. M., Vo, T. M., & McAleer, M. (2020). Information sharing, Bank penetration and tax evasion in emerging markets. *Risks, 8*(2), 38. https://doi.org/10.3390/risks8020038

Walker, J., & Unger, B. (2009). Measuring global money laundering: "The Walker gravity model". *Review of Law and Economics, 5*(2), 821–853. https://doi.org/10.2202/1555-5879.1418

Webb, J. W., Bruton, G. D., Tihanyi, L., & Ireland, R. D. (2013). Research on entrepreneurship in the informal economy: Framing a research agenda. *Journal of Business Venturing, 28*(5), 598–614. https://doi.org/10.1016/j.jbusvent.2012.05.003

Webb, J. W., Ireland, R. D., & Ketchen, D. J., Jr. (2014). Toward a greater understanding of entrepreneurship and strategy in the informal economy. *Strategic Entrepreneurship Journal, 8*(1), 1–15.

Young, M. A. (2013). The exploitation of offshore financial centres: Banking confidentiality and money laundering. *Journal of Money Laundering Control, 16*(3), 198–208. https://doi.org/10.1108/JMLC-01-2013-0004

Yu, Y., Lihong, H., Mouneer, S., Ali, H., & Munir, A. (2022). Foreign assistance, sustainable development, and commercial law: A comparative analysis of the impact of corruption on developing economies. *Frontiers in Environmental Science, 08*. Retrieved from https://www.frontiersin.org/articles/10.3389/fenvs.2022.959563/full

Rita Remeikienė obtained Doctoral degree in Economics, Kaunas University of Technology on 2012. Her main areas of scientific research and expertise are Shadow Economy, Corruption, Money Laundering, Green Deal, Self-employment. Since 2021 she leads as Chief researcher in two important projects namely, 'Protecting work and income in the digital economy: a case study of platform workers' and 'Model of the interaction of labour market and social support policies and development of methodologies for its implementation' (No. 13.1.1-LMT-K-718-05-0008), the last one being co-financed by the European Regional Development Fund. She works as a senior researcher at Vilnius University, Lithuania.

Ligita Gaspareniene is a senior researcher at Vilnius university. She worked as a principal researcher in the 'Welfare society' project titled 'Links between unemployment and shadow economy in Lithuanian regions'. Until now she is a senior researcher in the project 'Model of the interaction of labour market and social support policies and development of methodologies for its implementation' co-funded from the EU Structural Fund. Professor also works in the project 'Protecting work and income in the digital economy: a case study of platform workers' funded from Lithuanian Research Council. Her interest research fields are corruption, shadow /digital economy, sustainability, Green deal.

Part IV
Fighting Financial Crimes Strengthens the Sustainable Economy

Chapter 11
Policy and Regulatory Framework on Fighting Financial Crime for Developing Sustainable Economy Models

Laura Elly Naghi, Raluca Anica Onufreiciuc, Lorena-Elena Stanescu, and Raul Felix Hodoș

Abstract This study undertakes a critical review of European policies and regulatory frameworks aimed at mitigating financial crime, intending to provide recommendations on their effective implementation towards the development of sustainable economic models. By employing a qualitative research methodology, the authors examine existing literature on policies and regulatory frameworks for addressing financial crime in the context of achieving a sustainable economy. The findings highlight the importance of an all-encompassing policy and regulatory blueprint that includes the use of state-of-the-art technology, global cooperation, exchange of intelligence, and unified oversight on disclosure obligations on sustainability. The authors emphasise the imperative for policymakers, regulators, financial institutions, and other stakeholders to embrace environmental, social, and governance (ESG) criteria and a consistent and harmonised framework of sustainability requirements and disclosure obligations to attain a sustainable economy model.

L. E. Naghi (✉)
Faculty of Finance and Banking, Department of Finance, Bucharest University of Economic Studies, Bucharest, Romania
e-mail: laura.naghi@fin.ase.ro

R. A. Onufreiciuc
Faculty of Law and Administrative Sciences, "Stefan cel Mare" University of Suceava, Suceava, Romania

Nicolae Titulescu University of Bucharest, Bucharest, Romania

Faculty of Law, Paris-Panthéon-Assas University, Paris, France

L.-E. Stanescu
"Al. I. Cuza" University, Iași, Romania

R. F. Hodoș
Faculty of Finance and Banking, Department of Finance, Bucharest University of Economic Studies, Bucharest, Romania

Faculty of Law and Social Studies, University "1 Decembrie 1918" of Alba Iulia, Alba Iulia, Romania

M. V. Achim (ed.), *Economic and Financial Crime, Sustainability and Good Governance*, Contributions to Finance and Accounting,
https://doi.org/10.1007/978-3-031-34082-6_11

Keywords Financial crime · Sustainable economy model · ESG · Policy · Regulations · ESA · Financial system

JEL Classification K42 · E44 · D53

1 Introduction

In this paper, we delve into the critical analysis of policies and regulatory frameworks designed to combat financial crime and their consequential role in facilitating sustainable economic models. With the escalation of financial crimes threatening the stability and integrity of global economies, it is important to devise efficacious policies and regulatory strategies such as detecting, preventing, and curbing these unlawful activities. Through this investigation, we aim to enrich the current academic discourse by scrutinising the multifaceted dimensions of policy application and regulatory enforcement, while exploring their potential ramifications on sustainable economic paradigms.

In this exploration, a qualitative research methodology is employed, delving into the existing literature surrounding the policy and regulatory framework for combating financial crime and fostering sustainable economic models. The data collection method encompasses an assessment of academic articles, reports, and policy documents sourced from international organisations, regulatory authorities, and governmental entities.

The findings of this analysis reveal an escalating awareness regarding the necessity for an all-encompassing policy and regulatory blueprint to address financial malfeasance and foster resilient economic paradigms. In this context, the research highlights pivotal policy and regulatory strategies, encompassing the employment of cutting-edge technology to augment financial offence detection, risk appraisal, and transaction scrutiny. Moreover, the study delves into the crucial role of global collaboration and intelligence exchange in the ceaseless crusade against financial misdeeds.

Based on the correlation between illicit financial flow, corruption, bribery, and money laundering, on the one hand, and a sustainable economy, on the other hand, the paper reveals the need for a robust policy and regulatory framework to combat financial crime and promote sustainable economic models. The findings of the study have important implications for policymakers, regulators, financial institutions, and other stakeholders in their efforts to combat financial crime and promote sustainable economic growth by stressing the importance of international cooperation and coordination, the integration of technology in the preventive crime measures, the need for adopting environmental, social, and governance (ESG) criteria in a larger sphere, as well as the adoption of a unified oversight on disclosure obligations concerning sustainability at the European level. As a result, the European legislators' efforts to integrate and harmonise the treatment of financial and economic crime within the new legislative and regulatory framework meant to achieve a sustainable economy are greatly welcomed.

The purpose of this chapter is to provide information on these issues by examining the current sustainable policies and regulatory developments in connection with the specific abilities of the financial crime system to increase economic sustainability.

2 Understanding Financial Crime and Its Impact on a Sustainable Economy

2.1 Literature Review

The reviewed scholarship highlights the need for effective, coherent policies and regulatory frameworks at the European level to combat financial crime and promote sustainable economic models. While our analysis focuses primarily on research on the European Union legal framework, we also considered studies that are relevant to other regions.

Some of the studies indicate that financial crime is a serious threat to the economy and society, and various measures need to be implemented to tackle it. For example, Teivāns-Treinovskis and Amosova (2016) and Achim et al. (2021) provide evidence that sustainable development is positively correlated with reducing corruption, the shadow economy, and cybercrime. Also, the paper by Pickett and Pickett (2002) emphasises the importance of whistleblowing and detection in fraud response plan investigations. Similarly, Laura L. Hansen (2009) argues that corporate structures need to be critically scrutinised, and changes must be implemented to prevent financial crime. In contrast, the study by Gerasimova Ksenia (2008) suggests that the criminal law enforcement approach chosen by the main international organisations—UN, World Bank, and EU—is not effective in controlling corruption and economic crime in developing countries. However, Ruggiero and South (2013) argue the need for a new approach to tackle financial crime in the context of sustainable development. The review also includes studies that propose specific measures to investigate and prevent financial crime. For example, the paper by Petter Gottschalk (2010) suggests that the prevention strategy of corporate social responsibility is an information technology strategy. Concerning the effects of the new technological advancements on financial activities, Brici (2022), Johnstone (1999), and Merlonghi (2010) explore the impact of digitalisation on financial crime. While traditional methods of financial crime remain as prevalent as ever as Mwenda (2006) identifies financial assistance in the acquisition of a company's shares as a form of financial crime, the spread of financial services throughout the global electronic environment may help mitigate technological challenges. Furthermore, as Merlonghi (2010) highlights the vulnerabilities created by innovative payment instruments that can be exploited for financial crime, Bowron and Shaw (2007) discuss the limitations of traditional control methods in curbing the rise of fraud and money laundering offences.

Ryder et al. (2015) highlight the increase in financial crime as a trigger event for the credit crunch, and Picard (2008) emphasises the increasing sophistication employed by organised crime and criminal businessmen. Chatain et al. (2011) caution against overly restrictive identification and verification processes in know-your-customer policies, which may drive users back to the informal financial system. Ryder (2011) recommends the confiscation and forfeiture of illicit proceeds of crime, while Rider (2016) notes that a significant proportion of serious crime is economically motivated.

Finally, the studies we reviewed highlight the complexities of combating financial crime and the need for a systemic approach that includes collaboration between law enforcement agencies and financial institutions, robust AML and anti-corruption programs, effective regulatory frameworks, European oversight, and consistent international standards. While sustainable development may support the prevention of financial crime, in the future it may necessitate a new tech-oriented approach to combating financial crime and promoting sustainable economic models.

2.2 How Financial Crime Undermines Sustainable Economic Models

The realm of financial crime has assumed an entirely novel dimension, concomitant with the swift progressions in digital technology, and the adroitly devised social engineering schemes in the contemporary era. Interpol posits that notwithstanding the persistent concerns over bribery, corruption, and money laundering, the misappropriation of digital assets, cryptocurrencies, CEO fraud, and ransomware incursions have attained considerable maturation in recent times and emerged as a widespread *modus operandi* for the perpetration of illicit activities. These developments have not eluded the Nordic countries, wherein law enforcement agencies are encountering analogous patterns (Financial Crime, n.d.).

Financial crime is a term that pertains to a category of financial abuse and encompasses a range of non-violent criminal activities that typically lead to monetary losses, including but not limited to financial fraud (International Monetary Fund, 2001, p. 3). Economic crime, on the other hand, constitutes a subcategory of financial crime and encompasses a broader scope of illegal actions, such as money laundering, market abuse, and terrorist financing, which are commonly referred to as "white-collar crimes" (Palmer, 2018, p. 2).

Financial crime, including economic crime, money laundering, and illicit financial flows, has significant negative impacts on the achievement of the Sustainable Development Goals (SDGs), as it was widely recognised (Dohlman & Neylan, n.d.; Martini, 2014, p. 2; World Bank, 2017; UNODC, 2016; Malan et al., 2021). Financial crimes drain resources away from public services and hinder access to affordable and quality healthcare, which are essential for achieving Goal 3. Financial crimes also undermine the integrity of financial systems, leading to reduced

economic growth and employment opportunities, and hindering progress towards Goal 8. Developing countries have lost an estimated US$5.9 (Martini, 2014) trillion over the last decade due to corruption, criminal activities, and tax evasion, which significantly hampers economic and social development, affecting public institutions' ability to access resources and provide goods and services, thus impeding progress towards Goal 1. Also, the literature (Achim et al., 2021) holds up that all these crimes bring along many negative effects upon people on many channels: the decrease of the revenues collected by the national budgets [Goal 5]; the diminishing of the level of economic and sustainable development [Goals 7, 8, 9, 10]; the reduction of the level of investments, or the increase of social inequalities and poverty [Goal 14] (Aidt, 2003).

Specifically, money laundering (Sanction Scanner, 2023) and corruption harm economic growth and development. Corruption reduces the efficiency of public spending, distorts the allocation of resources, increases uncertainty, reduces investment, and leads to a misallocation of talent. However, the impact of corruption on economic growth is uncertain according to theoretical predictions. There are two opposing hypotheses: the "grease the wheels" hypothesis that claims corruption increases growth, and the "sand the wheels" hypothesis that argues corruption reduces growth (Hoinaru et al., 2020, p. 479). Empirical evidence leans towards the latter, indicating that corruption harms economic growth (Gründler & Potrafke, 2019, p. 16).

2.3 *Bridging the Gap Between Financial Crime Prevention and Sustainable Economic Models: Towards Interconnectivity in the EU Regulatory Frameworks*

The entire economic and social growth is strongly connected to crime prevention and strengthening criminal justice. While the current European legislative framework leads the way to sustainable economies, it lacks robustness because it is not clear where policies and regulations fighting financial crime lie within the holistic approach to regulating sustainable finance. This raises some concerns regarding the financial crime regulatory system's present ability to achieve sustainable economic outcomes.

The activities taken to prevent financial crime and the objective of developing sustainable economic models are synergistic (Aidt, 2010, p. 42; Anoruo & Braha, 2005, p. 44; Hoinaru et al., 2020, p. 481). It is worth noting that they are both related in the sense that criminal activities significantly impede sustainable development goals achievement by driving out a legitimate economic activity (Europol, 2021), yet their regulatory and governance systems tend to be rather divergent across the world. Therefore, the first question that comes up is what actions are needed to bridge the gap between policies in fighting financial and economic crime to achieve sustainable economic models.

The Roadmap for Financing the 2030 Agenda for Sustainable Development 2019–2021 outlines a series of initiatives to curb illicit financial flows related to proceeds of crime (United Nations, 2021): global, regional, and national analysis and advocacy programs designed to curb illicit financial flows; regional and national capacity to fight illicit financial flows and corruption (Achim, 2017, p. 85), strengthen the collaboration with financial institutions and centres to curb illicit financial flows, and recovery and return of stolen assets to support sustainable development. Also, it is mentioned achieving the increase in the domestic resource mobilisation and enhancement of the composition, effectiveness and efficiency of public spending, the need for tax transparency and curbing tax avoidance and tax crime.

Therefore, when, where, and how unlawful practices intersect and correlate to one another affecting the creation of sustainable economic models are all important for the efforts of building a sustainable financial system and, more broadly, a sustainable world.

Since the sustainable economy's momentum is expected to continue, international organisations and governments have increased their joint efforts to promote the development of sustainable finance (Malcoci & Hodos, 2009, p. 886). A vast number of countries are setting up the appropriate frameworks, industry best practices, and laws, which will provide more legitimacy (Lazar, 2010) and transparency to the market and support creating a healthy economic ecosystem (i.e., Basel Accords, Financial Action Task Force's recommendations, European Supervisory Authorities' guidelines and opinions). In addition to these efforts, an European recent initiative, the Platform on Sustainable Finance, has been appointed to ensure the development of regulatory standards for sustainable finance across all stakeholder groups. Therefore, the interconnectivity of regulatory frameworks may be an approach to achieving financial and sustainability goals across the world.

Therefore, though it is still too early in the development of sustainable finance infrastructure (*i.e.*, metrics and targets, disclosure requirements, standards, and ratings), ESG integration and sustainability reporting will play a significant role in combating financial and economic crime.

3 Designing a Sustainable Economic Model: Challenges and Opportunities in a Changing World

During the past decade, as opposed to only focusing on the "market" economy, the concept of the economy has been discussed as contributing to real, sustainable, human well-being (Rockström et al., 2009, p. 472). Currently, economic policies (Naghi et al., 2018, p. 359) do not improve well-being or happiness, according to economist Richard Layard (2005), who proposed that "happiness should become the goal of policy, and the progress of national happiness should be measured and analysed as closely as the growth of GNP (gross national product)". Therefore, in

the search for a new economic model, the scholars argue for one "consistent with our new full-world context" that should be based clearly on "the goal of sustainable human well-being" (Costanza et al., 2014, p. 284). A sustainable economic model could be the answer. The real challenge, however, is figuring out how to get there.

Dedicated to serving in the transition to a more sustainable economy, which represents one of the pillars of sustainable development (UN General Assembly, 2015), the European legislator has designed a new normative architecture which balances the economic, social, and environmental dimensions. Since the EUROPE 2020—A European strategy for smart, sustainable, and inclusive growth, the European Commission (2010) has worked to integrate sustainable development into its policies, laying the groundwork for the next generation of sustainable regulatory frameworks:

Furthermore, as it is stated in the *Action Plan: Financing Sustainable Growth*, the European Commission's (2018) approach to transitioning to a sustainable economy includes: (1) redirect capital flows towards sustainable investment to promote equitable and sustainable growth; (2) manage financial risks associated with climate change, resource depletion, environmental deterioration, and societal concerns; (3) encourage transparency and long-term thinking in financial and economic activities.

While acknowledging the taxonomy complexities, we refer to the concept of sustainable economy as the alignment of the activities of production, distribution and consumption of goods and services, and the financial market outcomes with environmental principles, particularly, and fundamentally with human values. Or, in corporate terms, the sustainable economy is about ESG values embedded into the economy. In practice, it is difficult to balance all these almost invisible and hard-to-track factors, but we may rely on the matrix, proposed by the United Nations (UN DESA's World Economic Situation and Prospects Monthly Briefing, 2018).

As we draw parallels between financial ecosystems and white-collar crime policies, the challenge for regulators is to respond with an innovative, harmonised, and efficient legal framework that addresses these new realities. Thus, the second question would be how can the system for preventing financial crime be restructured to be efficient and coherent enough for sustainability.

In light of the above call to action, worldwide financial criminal regulations need to align with the transition to a sustainable economy. To this end, our review of the literature comes up with four categories of measures that can be taken to prevent and combat financial crime (Achim & Borlea, 2020, pp. 257–263) preventive measures, punitive measures, international cooperation measures, and asset recovery measures.

Based on these measures, a promising environment for preventing and fighting economic and financial crime is developing. To augment the benefits of these measures, we propose by relating to the sustainable economy matrix (Fig. 11.1) that the new environment should resort to principle-based system conditions: ensure full compliance with EU values, principles, and fundamental rights; enhance transparency, accountability, and democracy in societies; improve the effectiveness and efficiency of the EU law; provide a cross-sector collaboration and stakeholders engagement; promote global integration and harmonised implementation; support

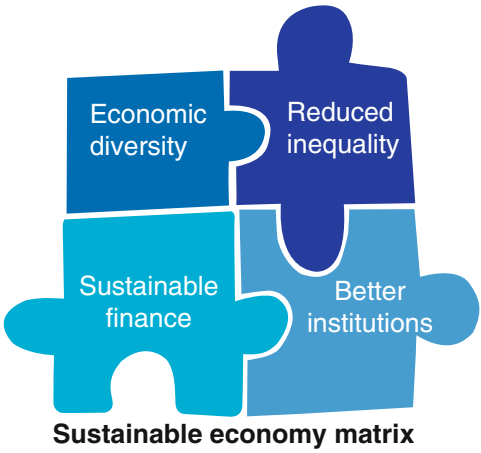


Fig. 11.1 Sustainable economy matrix (author's source)

international law enforcement and judicial cooperation; build up a sustainable culture within the entire ecosystem through research, education, and funding.

To summarise, the fight against economic and financial crime for developing sustainable economic models has been more of a concern in academics than in industry and public policy, and it should be treated more seriously.

4 Policy Coherence and Preventive Measures in Sustainable Finance: Bridging the Gap Between Regulation and Implementation

Sustainability is a process, not a moment. In this spirit, the works of the Platform on Sustainable Finance are towards promoting (1) policy coherence and efficiency across regimes for consistent implementation of the Taxonomy Regulation, the proposal (European Parliament, 2021) for the Corporate Sustainable Reporting Directive (CSRD), Sustainable Finance Disclosure Regulation (SFDR) (European Parliament, 2019a), Benchmark Regulation (BMR) (European Parliament, 2016a), Sustainability preferences in Markets in Financial Instruments Directive (2004/39/EC) (MiFID II) (European Parliament, 2014) and Insurance Distribution Directive (IDD) (European Parliament, 2016a), and (2) a collaborative approach of Platform 2.0, EFRAG, and the ESAs to support the sustainable finance policy implementation (Platform on Sustainable Finance, 2022a, p. 129).

The fight against economic and financial crime for developing sustainable economic models has been more of a concern in academics than in public policy. Therefore, policymakers should give the issue of economic and financial crime in building sustainable economic models the attention it deserves. Besides relying mostly on the European sustainable finance new legal framework and the emerging criminal strategies, implementing evidence-based strategies, principle-based system

conditions, and adopting a comprehensive and collaborative approach are needed towards building a sustainable economy.

4.1 The Emergence of a Modern Regulatory Regime for Sustainable Finance in Europe

The emergence of sustainable finance as a key pillar of a sustainable economy has led to the development of a modern regulatory regime for new emerging financial systems. In Europe, sustainability is considered a principle under Article 3 para. (3) and (5) of the Treaty on European Union (European Union, 1992). Traditionally, financial regulation for sustainable economies has taken a "hands-off" approach, leaving the industry to regulate itself and develop its standards and practices on its own. The lack of specific regulations and guidelines for stakeholders has limited the mandatory integration of financial and non-financial information in the NFRD (European Parliament. 2014), and sustainability policies were considered "nice-to-have". As an example, the Guidelines on reporting climate-related information under Directive 2014/95/EU provide only guidance on key non-financial performance indicators relevant to particular activities. A further limitation is the lack of a mandatory integration of financial and non-financial information in the European Non-Financial Reporting Directive (European Parliament, 2014).

Sustainable finance, a pillar of a sustainable economy, "generally refers to the process of taking due account of environmental and social considerations in investment decision-making, leading to increased investments in longer-term and sustainable activities" (European Commission, 2018). Consequently, sustainable finance is envisioned as an instrument that supports long-term economic growth through the implementation of environmental, social, and governance (ESG) strategies into financial activities.

As the literature holds up, sustainable finance is essentially challenged by forming corporate governance cultures as well as advances in financial analytics, environmental pricing, instrument structuring, security selection that is sustainability-aware, and risk management that monitor and manage the impact of the corporate on society and the environment (Bose et al., 2019, p. 76). To address these limitations, a shift in regulatory paradigms has occurred in Europe, with the "smart" approach (Zetzsche & Anker-Sørensen, 2022, pp. 87–113)) becoming a normative framework for developing sustainable finance policies and regulations. The appointment of an EU High-Level Expert Group in 2017 and the release of the EU's Action Plan: Financing Sustainable Growth in March 2018 (European Commission, 2018) have marked this shift, with the ESG no longer just a desirable add-on to policies. Instead, the European legislator has adopted a "resulting legislation" approach based on actual objectives, targets, sanctions, and timeframes. In this pursuit, the European regime is under review to improve the comparability of information, enforce the disclosure requirements, and provide incentives for the implementation costs.

Based on the enacted policies and legislation, we have identified a tripartite approach to create a sustainable financial system consisting of setting up a sustainable finance policy and regulatory framework; integration of ESG criteria into mainstream corporate governance; and shaping a system of financial monitoring and supervision.

Looking at this approach aimed at achieving a sustainable financial system alongside regulatory developments in combating financial and economic crime, we will explore possibilities of enabling policy coherence between a sustainable economy and crime fighting.

4.1.1 Setting Up of a Sustainable Finance Policy and Regulatory Framework

As part of the global effort towards a more sustainable economy, the new European regulatory framework on sustainable finance reflects commitments to the 2016 Paris Agreement on climate change and the United Nations 2030 Agenda for Sustainable Development (Busch et al., 2018, p. 23). Also art. 2 para. (24) of Regulation on sustainability-related disclosures in the financial services sector (SFDR) provides that "sustainability factors" are "defined as environmental, social and employee matters, respect for human rights, anti-corruption and anti-bribery matters" (European Parliament, 2019a). The shift from principle-based environmental legislation to rules-based regulation has some impact on the criminal system as well for at least three reasons: companies will try to prevent breaches of applicable rules that will result in criminal liability and incur the associated penalties and costs; new bodies for the enforcement of EU environmental criminal law are being established and the existing enforcement institutions are adopting new environmental priorities; and an important institutional change involves the European Supervisory Authorities' increased responsibility for sustainable finance regulation and supervision, as well as enhanced anti-money laundering capabilities.

Several normative acts support the set-up of a sustainable finance policy and regulatory framework, such as the European Green Deal, European Green Deal Investment Plan, European Climate Law (European Parliament, 2021b), EU Sustainability Taxonomy Regulation, EU Ecolabel (European Parliament, 2011), Green Bonds Standard (European Parliament, 2021c), Climate Benchmarks Regulation (European Parliament, 2019b). The laws provide the necessary guidelines and standards for sustainable investments to guarantee that financial operations stay in line with environmental and social objectives. With more attention being paid to sustainability and global warming, these laws are essential for advancing green finance and developing a sustainable economy. Moreover, this legal structure guarantees transparency and accountability when it comes to financial decision-making which is essential for generating trust between stakeholders and organisations.

The enactment of this legal framework for sustainable finance has a wide range of effects on corporate governance such as (1) strengthening traditional corporate governance's sustainability aspects with sub-objectives such as

sustainability-assessment skills in the highest governance body and transparency on sustainability objectives and targets, and (2) strengthening corporate governance aspects independent significance for sustainability sub-objectives as *anti-bribery and anti-corruption measurements, responsible lobbying and political engagement, transparent and non-aggressive tax planning, diversity of board members, and the option for employee representation on supervisory boards*, as detailed by the Platform on Sustainable Finance in the "Final Report on Social Taxonomy" (Platform on Sustainable Finance, 2022b). Scholars (Pacces, 2021, p. 172) provide examples such as index investors who seek to improve their sustainability ratings will have to interact with companies on ESG issues because they cannot simply avoid companies that do not meet the Taxonomy Regulation's definition of sustainability. It is worth considering the potential unintended consequences of sustainable finance regulations, particularly the impact on small and medium-sized enterprises. Therefore, further research could be used to investigate the measures that can be taken to ensure that these regulations do not disproportionately harm smaller businesses and the actual potential of these regulations to foster corporate conduct that aligns with responsible and ethical norms.

Furthermore, the sustainable finance policy and regulation frameworks lay out the framework for discussions on how to enforce the European Green Deal and the 2030 Climate target plan (European Commission, 2020). The third-largest crime in the world, behind illegal drug trafficking and counterfeiting crimes (Nellemann et al., 2018), environmental crime is currently one of the most lucrative global criminal enterprises, bringing in up to USD300 billion a year (Nature Finance, 2022). In light of the growing nature and cross-border aspect of this type of crime, several law enforcement agencies have made this issue a mission and converged on a pan-European action (Eurojust, 2022). Europol, Eurojust through the EU Agency for Criminal Justice Cooperation (2022), the European Network of Prosecutors for the Environment (ENPE), and the European Anti-Fraud Office (OLAF) are some of the bodies for which preventing and fighting environmental crime are high priority. Nevertheless, the sustainable finance policy and regulation framework serve also as a foundation for advancing the consultations (Faure et al., 2016, p. 23) on the revised Environmental Crime Directive (European Parliament, 2021d), the extension of the European Public Prosecutors Office's jurisdiction over environmental crimes with known links to organised crime, and the potential establishment of a European Green Prosecutor Office.

Integrated discussions on the sustainable economy and the fight against economic, financial, and environmental crime are beneficial for setting up a harmonised EU criminal system that will ensure legal certainty and fundamental rights protection alongside standardised penalties and sanctions and coordinated enforcement.

4.1.2 Integration of ESG Criteria into Mainstream Corporate Governance

The integration of ESG criteria into mainstream corporate governance is a highly intricate challenge, necessitating a comprehensive approach. The European regulatory framework contains references to values (Art. 2 of TEU) and principles that are relevant to EU values, similar to the Common Good Matrix, a model for evaluating corporate social responsibility, designed to help organisations develop and evaluate entrepreneurial and charitable activities related to the common good. This assessment process, embedding ESG practices in organisational compliance, is also reflected in the EU (non-) financial reporting policies. Scholars have embraced the common good approach concerning the banks' reporting obligations proposing the concept of "common good disclosure" (Fiondella et al., 2016, p. 499), using the example of Banca di Credito Cooperativo del Garda, an Italian mutual credit cooperative bank that has succeeded in contributing not only to the common welfare of the local community but also to the expansion of the communal credit cooperative banking system. Therefore, incorporating ESG standards should not be seen as a mere exercise in compliance, but rather a long-term commitment to responsible investment strategies.

Legal instruments such as the Shareholder Rights Directive II (European Parliament, 2017), Pension Funds Directive II/IORP II (European Parliament, 2016b), Low Carbon Benchmarks Regulation (European Parliament, 2016c), Solvency II (European Parliament, 2009), UCITS (European Parliament, 2009b), AIFMD (European Parliament, 2011), Corporate Sustainability Due Diligence (CSDDD) (European Parliament, 2022), MiFID II (European Parliament, 2014b), MiFIR (European Parliament, 2014c), and IDD (European Parliament, 2016a) provide a framework of policies and regulations to nurture responsible investment approaches and sustainable corporate governance. However, the effectiveness of such measures relies on several factors, including investors' knowledge and understanding of ESG, businesses' ability to implement sustainable practices, and states' resources to supervise.

There is a growing need for companies to provide transparent and standardised ESG disclosures to meet the demands of investors, regulators, and other stakeholders. As an "umbrella term", the concept of ESG is aimed to incorporate many options for business sustainability and governance metrics. Reviewing this legal framework reveals the three key components of ESG at the investor level identified in the literature as "(i) ESG as a set of investment criteria; (ii) ESG as a commitment; and (iii) ESG as a method" (Câmara, 2022, p.13). As a result of its in-depth analysis and extensive coverage, ESG governance has been branded as having a "cascade effect" (Câmara, 2022, p.18), that encourages organisations to participate in ESG-based decisions and to systematically encourage others to do likewise.

However, given the concerns regarding the ambiguity of the ESG definitions and ratings (Pollman, 2022, p.16; Avramov et al., 2021, p. 3), developing reliable and comparable ESG metrics and sustainability disclosure standards are complex tasks

that require the involvement of various stakeholders, including investors, regulators, and academics. In this context, an idea would be to examine the role of technology in promoting ESG integration and monitoring. Innovations such as blockchain, artificial intelligence, and big data analytics have the potential to enhance ESG reporting, monitoring, and compliance (Ahmed et al., 2022, p. 6495). For example, blockchain technology (Europol, 2022) can provide a tamper-proof and transparent system for tracking ESG data throughout the supply chain.

Moreover, in the context of the new European legal framework on sustainable finance and ESG mainstream adoption and the academic debate, if there is a positive or a negative relationship between ESG performance and financial performance, further research is needed to explore the link between ESG performance and financial performance and to identify the mechanisms through which ESG practices create value for companies and their stakeholders.

Legislative intervention and increased disclosure under existing legislation are seen as necessary to ensure that companies providing ESG information do so in a meaningful, accurate, and regulatory-compliant way. Otherwise, entities that make inaccurate ESG statements expose themselves to significant litigation and reputational risks.

4.1.3 Shaping of a System of Financial Monitoring and Supervision

As a result of transformations focused on the European financial system, a new structure for financial supervision and monitoring of sustainable finance has been established. This legal framework is designed to ensure that all stakeholders in the financial value chain have access to consistent and coherent sustainability information.

The Corporate Sustainability Reporting Directive (CSRD), Sustainable Finance Disclosure Regulation (SFDR), Non-financial Reporting Directive (NFRD) (European Parliament, 2014d), Second EU Capital Requirement Regulation (CRR II) (European Parliament, 2019a), Capital Requirements Directive (CRD V) (European Parliament, 2019a), EU Taxonomy Regulation, and the European Single Access Point for financial and non-financial information publicly disclosed by companies (ESAP) (European Parliament, 2021e) are a key legal instrument that reflects an acknowledgement of the potentially significant relationship between ESG practices, financial performance, and market stability.

The successful execution and enforcement of these regulations are paramount and entail the need for the disclosure of precise, trustworthy, and comparable information across different jurisdictions and elements thereof. Moreover, companies, and especially SMEs, must be conscious of the fact that, for the meaningful implementation of these regulations, a proactive approach should be taken. The NFRD, SFDR, and Taxonomy Regulation are key components of EU sustainability reporting requirements (European Commission, 2021, p. 3). Under NFRD, large companies should disclose information related to environmental matters, social matters and treatment of employees, respect for human rights, anti-corruption and bribery, and

diversity on company boards (in terms of age, gender, educational, and professional background). SFDR establishes harmonised rules for financial market participants and financial advisers regarding transparency in the implementation of sustainability risks and the consideration of adverse sustainability impacts in their processes, as well as the provision of sustainability-related information concerning financial products.

According to scholarship (Barth et al., 2012, p. 3), increasing capital requirements or supervisory powers has no beneficial influence on the financial industry, and enhanced supervision is found to be positively connected to banking corruption. They argue, however, that increased private monitoring does not provide increased financial stability, but can be connected with deeper, more efficient, and less corrupt financial institutions. The CSRD, the NFRD, and other relevant proposed EU legislation have been aimed at enhancing corporate transparency and accountability, promoting sustainable economic growth, and combating financial crime.

However, the effectiveness of these measures depends on their proper implementation and enforcement. The lack of a unified oversight mechanism and coordinated approach across various institutions involved in the financial system and those with activities in combating crime could undermine the intended outcomes of these initiatives. Therefore, a unified oversight mechanism would entail the establishment of a single authority or regulatory body responsible for overseeing the implementation and enforcement of sustainability disclosure obligations. Effective communication and coordination between financial institutions and authorities involved in crime-fighting activities such as ESA and FIU would enhance the existing system of preventing financial crime while safeguarding sustainable economic models. Information exchange between FIUs would also effectively support the detection and prevention of financial crimes.

Additionally, the function of education and public awareness should be examined in the advancement of sustainable economic models. Educating the public on the significance of sustainability and the consequences of economic practices can cultivate the desire for more sustainable products and services. For example, the role of investors in promoting sustainable finance should be further considered given that institutional investors, such as pension funds and asset managers, have significant influence over the allocation of capital and can use their leverage to push for more sustainable investment practices. Therefore, promoting financial literacy and enabling easy access to financial education can support people to make knowledgeable decisions that correspond with their principles and advance sustainable development.

4.2 *Establishing a Preventive System for Combating Financial and Economic Crime Through a Sustainable Finance Legal Framework*

In the pursuit of establishing a sustainable financial system, the EU has apparently developed a preventive system *per se* to combat financial and economic crime through promoting ESG mainstream adoption and sustainability disclosure requirements. Considering the extensive regulatory area of sustainability, the numerous legislative proposals, and the embryonic state of implementation, it is difficult for the actions taken in this phase to be integrated due to resistance to change and a lack of holistic knowledge. Under these circumstances, the Platform on Sustainable Finance aims to promote policy coherence and efficiency across regimes and a collaborative approach to supporting sustainable finance policy implementation.

In terms of establishing a preventive system for combating financial and economic crime through sustainable finance legal tools, based on Article 18 Minimum safeguards of the Taxonomy Regulation regarding the alignment with the OECD Guidelines for Multinational Enterprises (MNE) (OECD, 2011), United Nations Guiding Principles on Business and Human Rights (UNGPs) (United Nations, 2011) the eight ILO conventions on fundamental principles and rights at work, and the international bill of human rights, four core topics, respectively, (1) human rights, including workers' rights, (2) bribery/corruption, (3) taxation, and (4) fair competition, were identified in the Platform on Sustainable Finance's Final Report on Minimum Safeguards (2022).

The CSRD contains several explicit comments regarding these subjects, including the extent of necessary disclosure on human rights, anti-bribery, and corruption. Additionally, the Draft ESRS Exposure Drafts on the current European Sustainability Reporting Standard (ESRS) G3 (EFRAG, 2022) include in its metrics anti-competitive behaviour, although taxation is not explicitly included.

Given the role of the Platform on Sustainable Finance in building a European sustainable economy, we suggest the adoption of a system-based methodology to assess the impact of the Platform on Sustainable Finance related to financial sustainability. Furthermore, integrating the objectives listed within the Sustainable Finance Action Plan into European Commission Anti-Fraud Strategy (2019) and future legislation could also bridge the gaps between fighting economic crime and developing a sustainable financial system (Hotca, 2022, p. 10).

4.3 *Institutional Change in Financial Regulation for a Sustainable Economy*

Under Article 20 of the Taxonomy Regulation, the European Commission has established the Platform on sustainable finance, a permanent expert group, which will assist the Commission with its sustainable finance policies.

A new configuration with greater horizontal integration: the Platform on sustainable finance includes sustainability experts across all stakeholder groups, such as private stakeholders from financial, non-financial and business sectors, NGOs and civil society, and academia, as well as public and international institutions. In particular, for this research, we note next to the European Environment Agency, the European Investment Bank, the European Investment Fund, and the European Agency for Fundamental Rights, the presence of the three European supervisory authorities ("*ESAs*"): the European Banking Authority ("*EBA*"), the European Securities and Markets Authority ("*ESMA*"), and the European Insurance and Occupational Pensions Authority ("*EIOPA*").

The integration strategy could lower coordination costs and ensure effective communication channels between the involved stakeholders, as well as build the right infrastructure for developing the sustainable finance model. However, it also raises serious concerns about the adequate implementation of the new legal framework (Ignatescu & Onufreiciuc, 2021, p. 74).

Due to ESAs competencies to regulate and supervise financial markets, including the work in strengthening the fight against financial crime, their participation in the Platform on Sustainable Finance signifies an innovative juncture between the redesign of institutional financial supervisory architecture and the enactment of substantive rules in sustainable finance. For instance, the supervisory authorities also will play a crucial role in preventing effective greenwashing. Nevertheless, since ESAs are assigned a wide range of duties and tasks by the EU financial services reform and the Sustainable Finance Action Plan, companies that seek to engage with EU-based clients or partners should be able to disclose any date with environmental, social, and governance factors. This adds an extra layer to the complexity of sustainable governance and financial supervisory within the European business environment (Fig. 11.2).

The provided data in the table indicates the priorities of European authorities regarding policy approaches that enable sustainable finance and confront financial criminal activity. These priorities signify the varied roles and responsibilities of distinct authorities when they promote financial stability and sustainable finance, simultaneously addressing the potential threats, challenges, and risks connected to financial crime, digitalisation, and consumer protection.

The collaboration of the ESAs in the Platform on Sustainable Finance symbolises a revolutionary point between the development of institutional financial oversight architecture and the implementation of substantive rules when it comes to sustainable finance. Considering that the ESAs are in charge of regulating and controlling financial markets, their participation in the Platform can aid in avoiding greenwashing, which is a method wherein companies overestimate the environmental advantages of their products and services.

The integration of sustainable finance as a priority in the majority of the authorities also underlines the significance of this theme in the European financial sector. The data highlights the intricate and incorporated nature of financial leadership, simultaneously stressing the need for communication among distinct national and

	ESAs	ESMA	EBA	EIOPA	ECB	SRB	ESM	EDIS	SSM	NRAs	DGSs	NCAs
Financial stability	•	•	•	•	•	•	•	•	•	•	•	•
Sustainable finance	•	•	•	•	•	•	•	•		•		
AML/CFT	•	•	•	•	•						•	•
Whistle-blowing		•										
Information Exchange System	•	•	•	•		•	•				•	•
Financial Digitalisation	•	•	•	•		•	•				•	•
Supervision/	•	•	•	•	•		•				•	•
Risk monitoring												
Single Rulebook	•	•	•	•		•	•	•				
Consumer Protection			•		•	•					•	

ESAs - European Supervisory Authorities
ESMA - *European Securities and Markets Authority*
EBA - European Banking Authority
EIOPA- European Insurance and Occupational Pensions Authority
ECB – European Central Bank
SRB – Single Resolution Board
ESM – European Stability Mechanism
EDIS - European Deposit Insurance Scheme
SSM – Single Supervisory Mechanism
NRAs – National Resolution Authorities
DGSs – Guarantee Scheme Designated Authorities
NCAs - National Competent Authorities

Fig. 11.2 Policy approaches enabling sustainable finance and fighting financial crime. Source: Authors' source-adapted by Simmons & Simmons LLP (2022)

European authorities to efficiently counter financial crime and promote sustainable finance.

5 Summary and Conclusions

This chapter describes the European policy and regulatory framework for combating financial crime in the development of sustainable economic models.

To contribute to the theoretical approach on how combating economic and financial crime strengthens the sustainable economy, this chapter examines the EU legislative efforts to create a sustainable financial system. The proposed EU sustainable finance policy and legal framework reinforce the function of governance in controlling the transition to corporate sustainability. Thus, this new regulatory approach functions also as a preventive system *per se* for fighting financial and economic crime by supporting ESG mainstream implementation and disclosure standards.

It is interesting to note that the transition from principle-based environmental law to rules-based regulation affects the criminal system for at least three reasons. First, the organisations will want to avoid breaches of applicable regulations, which will result in criminal responsibility and related fines and expenses. Second, new entities are being formed to implement EU environmental criminal legislation, while existing enforcement agencies are embracing new environmental goals. Third, a significant institutional reform includes the European Supervisory Authorities taking on greater responsibility for sustainable finance legislation and supervision, as well as expanded anti-money laundering capabilities. Therefore, companies seeking to work with EU-based clients or partners should be able to share any information about environmental, social, and governance aspects. This adds to the complexities of sustainable governance and financial oversight in the European corporate environment.

Furthermore, we observe that the pursuit of corporate transparency and accountability will not be simple when we examine the corporate transparency standards, in particular, the anti-money laundering regulatory framework and the most recent jurisprudential rulings. However, by integrating data protection into corporate sustainability due diligence guidelines, this balance exercise between corporate accountability and the protection of personal data may help decide the best course of action to comply with both regimes.

In conclusion, the EU strives to provide research, outreach, and engagement for governments, investors, policymakers, and other stakeholders in fighting unlawful practices and illicit financial flows for developing sustainable economic models. By integrating economic and financial crime into overall sustainable economic development, including sustainable finance regulations, coherence between sustainable finance and criminal law, digitalisation, industry and other policies may be ensured.

References

Achim, M. V. (2017). Corruption, income and business development. *Journal for International Business and Entrepreneurship Development, 10*(1), 85–100.

Achim, M. V., & Borlea, N. S. (2020). Economic and financial crime. Corruption, shadow economy, and money laundering. In *Studies of Organized Crime (SOOC)* (Vol. 20). Springer.

Achim, M., Borlea, N. S., Văidean, L., Remus, V., Florescu, D., Mara, E., & Cuceu, I. (2021). Economic and financial crimes and the development of society. *Improving Quality of Life*

- *Exploring Standard of Living, Wellbeing, and Community Development.* https://doi.org/10.5772/intechopen.96269

Ahmed, I., Zhang, Y., Jeon, G., Lin, W., Khosravi, M. R., & Qi, L. (2022). A blockchain- and artificial intelligence-enabled smart IoT framework for sustainable city. *International Journal of Intelligence Systems, 37*, 6493–6507. https://doi.org/10.1002/int.22852

Aidt, T. S. (2003). Economic analysis of corruption: A survey. *The Economic Journal, 113*(491), F632–F652. Retrieved from http://www.jstor.org/stable/3590256

Aidt, T. S. (2010). *Corruption and sustainable development*; no. CWPE 1061. Retrieved December 13, 2022, from https://www.repository.cam.ac.uk/bitstream/handle/1810/242086/cwpe1061.pdf;jsessionid533A12327621029A0EF0B686DD27C5E5C?sequence51

Anoruo, E., & Braha, H. (2005). Corruption and economic growth: The African experience. *Journal of Sustainable Development, 7*(1), 43–55.

Avramov, D., Cheng, S., Lioui, A., & Tarelli, A. (2021). Sustainable investing with ESG rating uncertainty. *Journal of Financial Economics (JFE), 145*(2). https://doi.org/10.2139/ssrn.3711218

Barth, J. R., Caprio, G., Jr., & Levine, R. (2012). The evolution and impact of bank regulations. *Policy Research Working Paper* 6288. The World Bank. Retrieved from https://openknowledge.worldbank.org/bitstream/handle/10986/12183/wps6288.pdf?sequence=1&isAllowed=y

Bose, S., Dong, G. & Simpson, A. (2019). Governing the corporation. Palgrave studies in impact finance. In *The financial ecosystem* (pp. 47–81). Palgrave Macmillan.

Bowron, M., & Shaw, O. (2007). Fighting financial crime: A UK perspective. *Economic Affairs, 27*, 6–9. https://doi.org/10.1111/j.1468-0270.2007.00701.x

Brici, I. (2022). *New tendency of economic and financial crime in the context of digital age. A literature review*. Retrieved from https://hrcak.srce.hr/file/393864

Busch, D., Guido, F., & Hurk, A. (2018). *The European Commission's sustainable finance action plan*. Retrieved from SSRN https://ssrn.com/abstract=3263690 or https://doi.org/10.2139/ssrn.3263690

Câmara, P. (2022). The systemic interaction between corporate governance and ESG. In P. Câmara & F. Morais (Eds.), *The Palgrave handbook of ESG and corporate governance* (pp. 3–40). Springer.

Chatain, P., Zerzan, A., Noor, W., Dannaoui, N., & Koker, L. (2011). *Protecting mobile money against financial crimes. Global policy challenges and solutions*. Retrieved from https://elibrary.worldbank.org/action/showCitFormats?doi=10.1596%2F978-0-8213-8669-9

Costanza, R., Kubiszewski, I., Giovannini, E., Lovins, H., Mcglade, J., Pickett, K. E., Ragnarsdottir, K. V., Roberts, D., De Vogli, R., & Wilkinson, R. (2014). Time to leave GDP behind. *Nature, 505*, 283–285.

Dohlman, E., & Neylan, T.(n.d.). *Policy coherence in combating illicit financial flows: PCSD thematic module DRAFT*. OECD. Retrieved from https://www.oecd.org/gov/pcsd/IFFs%20thematic%20module%20v12cl_for%20web.pdf

EFRAG. (2022).*[Draft] European sustainability reporting standards (ESRS) G1 business conduct*. Retrieved from https://www.efrag.org/Assets/Download?assetUrl=%2Fsites%2Fwebpublishing%2FSiteAssets%2F17%2520Draft%2520ESRS%2520G1%2520Business%2520Conduct%2520November%25202022.pdf

EuroJust. (2022). *EU and US prosecutors stepping up cooperation in fight against environmental crime*. European Union Agency for Criminal Justice Cooperation. Retrieved from https://www.eurojust.europa.eu/news/eu-and-us-prosecutors-stepping-cooperation-fight-against-environmental-crime

European Commission. (2010). *Europe 2020: A strategy for smart, sustainable and inclusive growth*. COM(2010) 2020 final. Retrieved from https://ec.europa.eu/eu2020/pdf/COMPLET%20EN%20BARROSO%20%20%20007%20-%20Europe%202020%20-%20EN%20version.pdf

European Commission. (2018). *Communication action plan: Financing sustainable*. COM(2018) 97. Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52018DC0097

European Commission. (2020). *2030 climate target plan. Stepping up Europe's 2030 climate ambition investing in a climate-neutral future for the benefit of our people*. Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions COM/2020/562 final. Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52020DC0562

European Commission. (2021). *Strategy for financing the transition to a sustainable economy*. Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions. COM/2021/390 final. Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52021DC0390

European Parliament. (2009a). *Directive 2009/138/EC of the European Parliament and of the Council of 25 November 2009 on the taking-up and pursuit of the business of Insurance and Reinsurance (solvency II) (recast)*.

European Parliament. (2009b). *Directive 2009/65/EC of the European Parliament and of the Council of 13 July 2009 on the coordination of laws, regulations and administrative provisions relating to undertakings for collective investment in transferable securities (UCITS)*.

European Parliament. (2011). *Directive 2011/61/EU of the European Parliament and of the Council of 8 June 2011 on Alternative Investment Fund Managers and amending Directives 2003/41/EC and 2009/65/EC and Regulations (EC) No 1060/2009 and (EU) No 1095/2010*.

European Parliament. (2014a). *Directive 2014/95/EU of the European Parliament and of the Council of 22 October 2014 amending Directive 2013/34/EU as regards disclosure of non-financial and diversity information by certain large undertakings and groups text with EEA relevance*. Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32014L0095

European Parliament. (2014b). *Directive 2014/65/EU of the European Parliament and of the Council of 15 May 2014 on markets in financial instruments and amending Directive 2002/92/EC and Directive 2011/61/EU (recast)*. Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32014L0065

European Parliament. (2014c). *Regulation (EU) No 600/2014 of the European Parliament and of the Council of 15 May 2014 on markets in financial instruments and amending Regulation (EU) No 648/2012*. Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32014R0600

European Parliament. (2014d). *Directive 2014/95/EU of the European Parliament and of the Council of 22 October 2014 amending Directive 2013/34/EU as regards disclosure of non-financial and diversity information by certain large undertakings and groups*.

European Parliament. (2016a). *Directive (EU) 2016/97 of the European Parliament and of the Council of 20 January 2016 on insurance distribution (recast)Text with EEA relevance*. Retrieved from https://eur-lex.europa.eu/legal-content/en/ALL/?uri=CELEX:32016L0097

European Parliament. (2016b). *Directive (EU) 2016/2341 of the European Parliament and of the Council of 14 December 2016 on the activities and supervision of institutions for occupational retirement provision (IORPs) (recast)*.

European Parliament. (2016c). *Regulation (EU) 2016/1011 of the European Parliament and of the Council of 8 June 2016 on indices used as benchmarks in financial instruments and financial contracts or to measure the performance of investment funds and amending Directives 2008/48/EC and 2014/17/EU and Regulation (EU) No 596/2014*.

European Parliament. (2017). *Directive (EU) 2017/828 of the European Parliament and of the Council of 17 May 2017 amending Directive 2007/36/EC as regards the encouragement of long-term shareholder engagement*. Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32017L0828

European Parliament. (2019a). *Directive (EU) 2019/878 of the European Parliament and of the Council of 20 May 2019 amending Directive 2013/36/EU as regards exempted entities,*

financial holding companies, mixed financial holding companies, remuneration, supervisory measures and powers and capital conservation measures.

European Parliament. (2019b). *Regulation (EU) 2019/2089 of the European Parliament and of the Council of 27 November 2019 amending Regulation (EU) 2016/1011 as regards EU Climate Transition Benchmarks, EU Paris-aligned Benchmarks and sustainability-related disclosures for benchmarks*.

European Parliament. (2021a). *Proposal for a Regulation of the European Parliament and of the Council establishing the Authority for Anti-Money Laundering and Countering the Financing of Terrorism and amending Regulations (EU) No 1093/2010, (EU) 1094/2010, (EU) 1095/2010*. Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52021PC0421

European Parliament. (2021b). *Regulation (EU) 2021/1119 of the European Parliament and of the Council of 30 June 2021 establishing the framework for achieving climate*. Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32021R1119

European Parliament. (2021c). *Proposal for a Regulation of the European Parliament and of the Council on European green bonds, COM/2021/391 final*. Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52021PC0391

European Parliament. (2021d). *Proposal for a Directive of the European Parliament and of the Council on the protection of the environment through criminal law and replacing Directive 2008/99/EC COM(2021) 851 final 2021/0422 (COD)*. Retrieved from https://commission.europa.eu/system/files/2021-12/1_1_179760_prop_dir_env_en.pdf

European Parliament. (2021e). *Proposal for a Regulation of the European Parliament and of the Council establishing a European single access point providing centralised access to publicly available information of relevance to financial services, capital markets and sustainability. COM/2021/723 final*.

European Parliament. (2022). Proposal for a directive of the European parliament and of the council on corporate sustainability due diligence and amending directive (EU) 2019/1937. COM(2022) 71 final.

European Union. (1992). *Treaty on European Union (Consolidated Version), Treaty of Maastricht, 7 February 1992, Official Journal of the European Communities C 325/5; 24 December 2002*. Retrieved December 19, 2022, from https://www.refworld.org/docid/3ae6b39218.html

Europol. (2021). *European Union serious and organised crime threat assessment (SOCTA) 2021: A corrupting influence: The infiltration and undermining of Europe's economy and society by organised crime*. Publications Office of the European Union. Retrieved from https://data.europa.eu/doi/10.2813/346806

Europol. (2022). *One of the darkweb's largest cryptocurrency laundromats washed out*. Retrieved from https://www.europol.europa.eu/media-press/newsroom/news/one-of-darkwebs-largest-cryptocurrency-laundromats-washed-out

Faure, M., Philipsen, N., del Castillo, T. F., et al. (2016). *Conclusions and recommendations. Study in the framework of the EFFACE research project.*

Financial Crime. (n.d.). *A sustainable future is less corrupt*. Retrieved from https://transcendentgroup.com/trends/financial-crime-a-sustainable-future-is-less-corrupt/

Fiondella, C., Marco, M., Spanò, R., & Zagaria, C. (2016). Common good disclosure. In O. M. Lehner (Ed.), *Routledge handbook of social and sustainable finance*. Routledge. Retrieved December 18, 2022.

Gerasimova, K. (2008). Can corruption and economic crime be controlled in developing countries and if so, is it cost-effective? *Journal of Financial Crime, 15*(2), 223–233. https://doi.org/10.1108/13590790810866917

Gottschalk, P. (2010). *Investigation and prevention of financial crime: Knowledge management, intelligence strategy and executive leadership*. Routledge.

Gründler, K., & Potrafke, N. (2019). *Corruption and economic growth: New empirical evidence, ifo Working Paper, No. 309*. ifo Institute - Leibniz Institute for Economic Research at the University of Munich.

Hansen, L. (2009). Corporate financial crime: social diagnosis and treatment. *Journal of Financial Crime, 16*(1), 28–40. https://doi.org/10.1108/13590790910924948

Hoinaru, R., Buda, D., Borlea, N. S., Vaidean, V. L., & Achim, M. V. (2020). The impact of corruption and shadow economy on the economic and sustainable development. Do they "sand the wheels" or "grease the wheels"? *Sustainability, 2020*(12), 481. https://doi.org/10.3390/su12020481

Hotca, M. (2022). *Manual de drept penal. Partea generala*. Universul Juridic.

Ignatescu, C., & Onufreiciuc, R. (2021). Digital euro: A (digital) symbol of Progress and integration in Europe. *Logos Universality Mentality Education Novelty: Law., 9*, 74–82. https://doi.org/10.18662/lumenlaw/9.1/58

International Monetary Fund. (2001). *Financial system abuse, financial crime and money laundering – Background paper*. Retrieved from https://www.imf.org/external/np/ml/2001/eng/021201.pdf

Johnstone, P. (1999). Financial Crime: Prevention and regulation in the intangible environment. *Journal of Money Laundering Control, 2*(3), 253–263. https://doi.org/10.1108/eb027191

Layard, R. (2005). *Happiness: Lessons from a new science*. Allen Lane.

Lazar, I. (2010, November 5–6). The impact of the Lisbon Treaty on the public finances of the European Union. In *Procedinngs of the International Workshop "Advanced Resarch and Trends in Acountig Audit and Finance", Alba-Iulia, Faculty of Sience, University "1 Decembrie 1918" Alba-Iulia*, ISBN 978-973-1890-76-0, coauthor.

Malan, J., Bosch Chen, I. et al. (2021, July). *Impact of organised crime on the EU's financial interests*. Retrieved from https://www.europarl.europa.eu/RegData/etudes/STUD/2021/697019/IPOL_STU(2021)697019_EN.pdf

Malcoci, C., & Hodos, R. (2009). The limits of sustainability in e-commerce framework. *Revista de Management Comparat Internațional, 52*, 886–893. Retrieved from https://www.ceeol.com/search/article-detail?id=736977

Martini, M. (2014). *Combating illicit financial flows: The role of the international community*. Transparency International: Anti-corruption Resource Center. Retrieved from https://knowledgehub.transparency.org/assets/uploads/helpdesk/Combating_illicit_financial_flows_the_role_of_the_international_community_2014.pdf

Merlonghi, G. (2010). Fighting financial crime in the age of electronic money: Opportunities and limitations. *Journal of Money Laundering Control, 13*(3), 202–214. https://doi.org/10.1108/13685201011057118

Mwenda, K. (2006). *Combating financial crime: The legal, regulatory, and institutional frameworks*. Mellen Press.

Naghi, L. E., Glon, O. & Darmaz-Guzun, A. (2018). The influence of foreign direct investments on economic policies in Romania. In *Proceedings of the international conference on economics and social sciences* (Vol. 1, pp. 359–364). Bucharest University of Economic Studies, Romania. Retrieved from https://ideas.repec.org/e/pno107.html

Nature Finance. (2022). Retrieved from https://www.naturefinance.net/breaking-the-connection-between-environmental-crimes-and-finance/

Nellemann, C., Henriksen, R., Pravettoni, R., Stewart, D., Kotsovou, M., Schlingemann, M. A. J, Shaw, M., & Reitano, T. (Eds). (2018). *World atlas of illicit flows. A RHIPTO-INTERPOL-GI assessment*. RHIPTO-Norwegian Center for Global Analyses, INTERPOL and the Global Initiative Against Transnational Organized Crime. Retrieved from https://globalinitiative.net/wp-content/uploads/2018/09/Atlas-Illicit-Flows-FINAL-WEB-VERSION-copia-compressed.pdf

OECD. (2011). *OECD guidelines for multinational enterprises*. OECD. https://doi.org/10.1787/9789264115415-en.

Pacces, A. (2021). Sustainable corporate governance: The role of the law. In D. Busch, G. Ferrarini, & S. Grünewald (Eds.), *Sustainable finance in Europe. Corporate governance, financial stability and financial markets*. Palgrave Macmillan.

Palmer, A. (2018). *Countering economic crime: A comparative analysis*. Routledge.

Picard, M. (2008). Financial crimes: The constant challenge of seeking effective prevention solutions. *Journal of Financial Crime, 15*(4), 383–397. https://doi.org/10.1108/13590790810907227

Pickett, K., & Pickett, J. (2002). *Financial Crime investigation and control*. Wiley.

Platform on Sustainable Finance. (2022a). *Final report on minimum safeguards*. Retrieved from https://finance.ec.europa.eu/system/files/2022-10/221011-sustainable-finance-platform-finance-report-minimum-safeguards_en.pdf

Platform on Sustainable Finance. (2022b). *Final report on social taxonomy*. Retrieved from https://commission.europa.eu/system/files/2022-03/280222-sustainable-finance-platform-finance-report-social-taxonomy.pdf

Pollman, E. (2022). *The making and meaning of ESG*. University of Pennsylvania Carey Law School, Law & Economics Research Paper No. 22-23. European Corporate Governance Institute - Law Working Paper No. 659/2022. Retrieved from SSRN https://ssrn.com/abstract=4219857

Rider, B. (2016). *Research handbook on international financial crime*. Edward Elgar.

Rockström, J., Steffen, W., W., Noone, K., et al. (2009). A safe operating space for humanity. *Nature, 461*, 472–475.

Ruggiero, V., & South, N. (2013). Green criminology and crimes of the economy: Theory, research and praxis. *Critical Criminology*. https://doi.org/10.1007/s10612-013-9191-6

Ryder, N. (2011). *Financial Crime in the 21st century: Law and policy*. Edward Elgar Publishing.

Ryder, N., Turksen, U., & Hassler, S. (2015). *Fighting financial crime in the global economic crisis: Policy, trends and sanctions*. Routledge.

Sanction Scanner. (2023). *Negative effects of money laundering on the economy*. Retrieved from https://sanctionscanner.com/blog/negative-effects-of-money-laundering-on-the-economy-132

Simmons & Simmons LLP. (2022). *Summary table of 2023 financial regulatory priorities*. Retrieved from https://www.simmons-simmons.com/en/publications/cl94ag2bb6ixg0b79606apajp/eu-institutions-financial-regulatory-priorities-for-2023

Teivāns-Treinovskis, J., & Amosova, J. (2016). Some aspects of criminal environment impact on sustainable entrepreneurship activities. *Entrepreneurship and Sustainability Issues, VsI Entrepreneurship and Sustainability Center, 4*(1), 17–24.

UN DESA's World Economic Situation and Prospects Monthly Briefing. (2018). *Four steps towards a more sustainable global economy*. Retrieved from https://www.un.org/en/desa/four-steps-towards-more-sustainable-global-economy

UN General Assembly. (2015). *Transforming our world: The 2030 Agenda for Sustainable Development, 21 October 2015, A/RES/70/1*. Retrieved December 13, 2022, from https://www.refworld.org/docid/57b6e3e44.html

United Nations. (2011). *Guiding principles on business and human rights: Implementing the United Nations "protect respect and remedy" framework*. United Nations Office of the High Commissioner for Human Rights.

United Nations. (2021). *Our common agenda - Report of the Secretary-General*. Retrieved from https://documents-dds-ny.un.org/doc/UNDOC/GEN/N21/217/01/PDF/N2121701.pdf?OpenElement

United Nations Office on Drugs and Crime (UNODC). (2016, July). *Coherent policies for combatting illicit financial flows*. OECD. Retrieved from https://www.un.org/esa/ffd/wp-content/uploads/2016/01/Coherent-policies-for-combatting-Illicit-Financial-Flows_UNODC-OECD_IATF-Issue-Brief.pdf

World Bank. (2017). *Illicit Financial Flows (IFFs)*. Retrieved from https://www.worldbank.org/en/topic/financialsector/brief/illicit-financial-flows-iffs

Zetzsche, D. A., & Anker-Sørensen, L. (2022). Towards a smart regulation of sustainable finance. In P. Câmara & F. Morais (Eds.), *The Palgrave handbook of ESG and corporate governance* (pp. 87–113). Springer.

Laura Elly Naghi , PhD is Associate Professor of Finance at Bucharest University of Economic Studies, Department of Finance. With postdoctoral studies in insurance, her work experience derives from and includes: teaching financial professional training, academic courses and seminaries; research activities; participating in scientific conferences as a researcher, reviewer of papers or Chairperson of session. As Head of the Financial Literacy Department at the Institute of Financial Studies, she develops and coordinates the implementation of financial literacy programs at national levels for teachers, students, and population in general. Her focus in research is on financial markets, fundamental prudential supervisory framework, ethics, and corporate governance.

Raluca Anica Onufreiciuc is Associate Assistant in Law at "Stefan cel Mare" University, Suceava, and PhD Candidate at Nicolae Titulescu University of Bucharest and Paris-Panthéon-Assas University. Her current research focus is on good governance, competition rules and administrative jurisdictions, financial transparency and the impact AI can have on its enforcement raising novel and important issues at the intersection between private/public use of personal data for purposes of safeguarding security and public order.

Lorena-Elena Stanescu , Ph.D. in Law ("Al. I. Cuza" University, Iasi, Romania) is a lawyer, particularly interested in the intersection of law, technology, and sustainability, with a particular emphasis on creating a robust and inclusive ecosystem for sustainable financial digitalisation.

Raul Felix Hodoș , PhD is Associate Professor in Law at "1 Decembrie 1918" University, Alba Iulia, and PhD Student in Finance at University of Economic Studies, Bucharest. His research interests are mainly in commercial and new technology law and data protection.

Chapter 12
Strengthening the EU Fight Against Money Laundering to Promote Sustainable Economic Models

Laura Elly Naghi, Raluca Anica Onufreiciuc, Lorena-Elena Stanescu, and Raul Felix Hodoș

Abstract This chapter examines the effects of money laundering on economies and highlights the pressing need for a coherent legal framework that supports anti-money laundering (AML) and sustainable economic practices. Using a theoretical approach and qualitative research, the chapter analyses the effectiveness of existing EU AML regulations and identifies measures to improve them. It also explores the intersection of AML and environmental, social, and governance (ESG) efforts and the need for increased cooperation and stricter disclosure requirements for companies in a sustainable economy. Ultimately, the chapter provides valuable insights for the EU to address emerging technological challenges while combatting money laundering and promoting sustainable economic models.

Keywords Anti-money laundering · ESG · Sustainable economy · EU AML single rulebook · Financial crime · Cybercrime · Blockchain

L. E. Naghi (✉)
Faculty of Finance and Banking, Department of Finance, Bucharest University of Economic Studies, Bucharest, Romania
e-mail: laura.naghi@fin.ase.ro

R. A. Onufreiciuc
Faculty of Law and Administrative Sciences, Stefan cel Mare" University of Suceava, Suceava, Romania

Nicolae Titulescu University of Bucharest, Bucharest, Romania

Faculty of Law, Paris-Panthéon-Assas University, Paris, France

L.-E. Stanescu
"Al. I. Cuza" University, Iași, Romania

R. F. Hodoș
Faculty of Finance and Banking, Department of Finance, Bucharest University of Economic Studies, Bucharest, Romania

Faculty of Law and Social Studies, University "1 Decembrie 1918" of Alba Iulia, Alba Iulia, Romania

M. V. Achim (ed.), *Economic and Financial Crime, Sustainability and Good Governance*, Contributions to Finance and Accounting,
https://doi.org/10.1007/978-3-031-34082-6_12

JEL Classification Q56 · G15

1 Introduction

Money laundering is a critical global concern, with a detrimental impact on the sustainability of economies worldwide. The imperative to combat money laundering cannot be overstated, after all, money laundering can be considered a sophisticated form of stealing. This illegal activity compromises the integrity of financial systems and poses a significant threat to the stability and growth of economies. Perpetrators employ money laundering to disguise the proceeds of their unlawful activities, which may include corruption, tax evasion, drug and human trafficking, and terrorism. By concealing these profits, offenders may elude taxes, finance further criminal enterprises, and subvert public officials. Although the European Union (EU) has taken considerable strides in combatting money laundering and terrorist financing, there remains much work to be done.

This chapter adopts a theoretical approach and employs a qualitative research methodology to investigate the problem of how the EU can enhance its fight against money laundering to foster sustainable economic models. In particular, this study aims to provide a comprehensive analysis of the current state of the effectiveness of the EU anti-money laundering (AML) regulations, their level of transposition across member states, and measures that can be implemented to enhance the EU's fight against money laundering. Additionally, the study explores the potential impact of AML and environmental, social and governance (ESG) convergence, the need for sustainable economic models, and the potential inclusion of cybersecurity within the ESG risks. Through this inquiry, this chapter endeavours to contribute to the ongoing discourse on how the EU can combat money laundering more effectively and promote sustainable economic models resilient to financial crimes.

In this chapter, we explore the multi-layered legal framework that the EU has implemented to counteract money laundering and terrorist financing. Despite this, the framework has significant shortcomings, including weak enforcement mechanisms and fragmented regulations and enforcement practices among member states. We discuss the need for the EU to adapt to the latest technological advancements and adjust its AML/CFT rules accordingly through the upcoming EU single rulebook on AML/CFT to address challenges related to new risks arising from technology and innovation, such as digital economy, crypto-economy and tokenisation, and artificial intelligence changes.

Furthermore, we examine the convergence of AML and ESG and its positive impact on the financial industry, which reflects a growing recognition of the interdependence between financial activities and environmental and social factors. However, we also highlight the need for the EU to enhance cooperation between AML and ESG authorities, establish a centralised body responsible for supervising and enforcing both AML and ESG requirements, and introduce stricter AML and ESG disclosure requirements for companies operating in the sustainable economy to strengthen its efforts in the fight against money laundering. Also, we propose the

extension of ESG concerns by including cybercrime risks. Ultimately, these measures can ensure the stability and transparency of the EU's financial markets and promote the legitimate use of funds flowing into a sustainable economy.

2 Overview of the EU's Anti-Money Laundering Legislative Efforts

The EU has provided a multifaceted regulatory framework to combat money laundering and terrorist financing. Since 1990, the EU recognised the need to prevent the misuse of the financial system for money laundering by adopting its first AML directive. Afterwards, the legislation has been revised constantly to mitigate the new risks associated with money laundering and terrorist financing.

In 2015, the EU introduced a modernised regulatory framework which included the fourth anti-money laundering directive (AMLD4) (European Parliament, 2015) and the regulation on information on the payer accompanying transfers of funds. These instruments aimed to promote the highest standards for the AML/CFT fight, considering the 2012 recommendations of the Financial Action Task Force (FATF, 2012). Following this, the EU published the fifth AML Directive in 2018 (AMLD5) (European Parliament, 2018), which amended the fourth directive.

The current AML framework aims to set minimum standards for customer due diligence, introduce enhanced due diligence measures, and increase corporative transparency by introducing reporting requirements and establishing central registers of beneficial owners. The regulatory framework acknowledges the impact of technological advancements, such as virtual currencies and anonymous prepaid cards, which are included in AMLD5.

However, the current AML framework suffers from several deficiencies, including inadequate coverage, enforcement measures, and fragmentation (FATF Report, 2010; FATF, 2022). The lack of a clear definition of beneficial ownership makes it difficult to identify the true beneficiaries of financial transactions. The enforcement measures are not severe enough to deter money laundering (Heinäluoma et al., 2021, p. 4), and supervisory authorities are often understaffed or under-resourced, hindering their ability to carry out their duties effectively (Cacciatore, 2019, p. 502). Additionally, the fragmentation of regulations and enforcement practices across member states creates inconsistencies and gaps that can be exploited by money launderers operating across multiple jurisdictions (Hanley-Giersch, 2019).

Further on, the need for a robust and harmonised anti-money laundering regulatory framework was reinforced by high-profile money laundering scandals that have shaken the world in recent years and convinced the legislator to prioritise the protection of the financial interests of Europeans. The LuxLeaks (Le Monde, 2016), the Panama Papers (The Guardian, 2016), the Paradise Papers (The Guardian, 2017) and the Football Leaks (Knight, 2023) have exposed the vulnerabilities of the financial system. Moreover, the recent revelations about the involvement of several

European banks in the "Troika Laundromat" (The Guardian, 2019) money laundering operation in Russia are deeply concerning.

These high-profile financial scandals triggered a wave of regulatory reforms within the banking and finance sector regarding AML/CFT rules, spanning from establishing new institutions, for example, the European Supervisory Authorities (ESAs), European Financial Intelligence Units (FIUs), European Banking Authority (EBA), and the European Central Bank (ECB) to more prescriptive measures, such as initiating the single rulebook on AML/CFT.

In July 2021, the European Commission presented a package of legislative proposals (European Commission, 2021) to strengthen the EU's AML/CFT rules. This package included a proposal for a new EU authority to fight money laundering, improve the detection of suspicious transactions and activities, and close loopholes used by criminals to launder illicit proceeds or finance terrorist activities through the financial system. Furthermore, in 2022, co-legislators reached an agreement on the Commission's proposal to amend the transfer of funds regulation (Kanko & Urtasun, 2021). The agreement requires all crypto-assets service providers participating in crypto transfers to obtain information about the customers and beneficiaries of the crypto-assets transfers they operate and conduct customer due diligence compliance procedures comparable to those already used in the financial system.

The EU's commitment and efforts to countering money laundering demonstrate its unwavering dedication to preserving the integrity of the financial system and ensuring a level playing field for all market participants. The forthcoming EU single AML rulebook represents a significant development in this effort, as it will establish a unified framework for AML/CFT measures across all EU member states. By improving regulatory coverage and enforcement measures, this new legal framework has the potential to strengthen the fight against financial crime and better protect the financial interests of EU citizens.

3 A Perspective on the Transposition of the EU AML Legislation Across Member States

Despite the EU's efforts to tackle money laundering and terrorist financing, there are still significant challenges to inadequate implementation and fragmentation of the EU's AML/CFT legal framework, lack of a coordinated EU-level supervision mechanism, deficiencies in supervision and enforcement measures, emerging risks related to new technologies, digital business models, and new digital currencies (stablecoins, cryptocurrencies) (Kanko & Urtasun, 2021; European Commission, 2022a).

Firstly, significant deficiencies in the national AML regimes of many EU member states were identified, as per the 2019 report (European Commission, 2019), which called for greater efforts to ensure effective transposition and implementation of the EU AML framework by member states.

In particular, the report emphasises the importance of strengthening cooperation and information sharing between national authorities, as well as enhancing supervision and enforcement measures. Secondly, some member states have not fully transposed the Fifth EU Anti-Money Laundering Directive (AMLD5), which raises concerns about the effectiveness of the EU's AML/CFT framework, according to the 2022 report (European Commission, 2022a). It emphasises the need for greater coordination and cooperation between national authorities and the EU level. The report notes that some EU countries have been identified as "high-risk" jurisdictions due to deficiencies in their AML regimes, including inadequate supervision and enforcement measures. Thirdly, the 2022 report emphasises the growing significance of technology and innovation, particularly in the context of the blurring lines between the virtual and real worlds. The need to keep pace with developments in technology and financial innovation, including the use of cryptocurrencies, is crucial to ensure that AML measures are adapted to address new and emerging risks. Also, the increasing use of cryptocurrencies and other virtual assets for money laundering and terrorist financing purposes leads to more means to manage and supervise the digital economy market.

Fourth place, the 2022 report notes that the real estate sector continues to be a high-risk area for money laundering. Criminals can invest their illegal funds in countries where real estate prices have risen sharply in recent years, creating opportunities to integrate them into the legitimate economy. Fifth place, the effective implementation and consistent enforcement of the EU's AML rules are crucial in combatting financial crime and maintaining the integrity of the financial system. To this end, the EU has relied heavily on directives to prevent money laundering, requiring member states to implement them into their national legislation. However, recent reports (European Court of Auditors, 2021, pp. 12–15) suggest that consistent implementation of AML regulations across all member states remains a challenge.

The transposition of AML directives into national laws has been problematic, leading to infringement proceedings and court proceedings against certain member states. For instance, all member states were required to implement the rules of AMLD4 by June 2017, but none of them had notified complete transposition (European Commission, 2020a), indicating a lack of urgency and commitment to implementing AML regulations. The European Commission has taken steps to address inadequate implementation, including sending letters of formal notice and reasoned opinions to several member states. For example, the European Commission has sent letters of formal notice to Germany, Portugal, and Romania for incorrectly transposing AMLD4. This issue has persisted, with the EU formally threatening Cyprus, the Netherlands, and Spain, in 2020, and referring Greece, Ireland, and Romania to the Court of Justice of the EU for failing to implement the AMLD4 (European Commission, 2018) into their national law, while Spain, Latvia, and Malta have been sent reasoned opinions for incomplete implementation.

Despite these efforts, some member states have still not completely implemented AMLD4, highlighting the complexity of AML regulations and the need for consistent enforcement across all member states. By March 2019, only six member states had completed transposition, seven had partially transposed, and 15 had not notified

any measures. However, some member states had overstated the extent to which they had taken transposition measures, resulting in the uneven implementation of AML law across the EU (European Court of Auditors, 2021, p. 25).

The European Commission has continued to address inadequate implementation, sending letters of formal notice to eight member states—Cyprus, Hungary, the Netherlands, Portugal, Romania, Slovakia, Slovenia, and Spain—in February 2020 for failing to notify any implementation measures for the AMLD5 (Wahl, 2020). Relying on directives led to slow and uneven implementation of EU AML/CFT law (European Court of Auditors, 2021, p. 31). Failure of member states to completely implement AML directives is a cause for concern, as financial crime can have serious consequences, such as funding terrorist activities and undermining economic stability. However, this also shows that different member states face different challenges when it comes to implementing AML directives such as the complexity of the legislation, uneven action taken by member states, and a lack of resources dedicated to AML tasks at the Commission (European Court of Auditors, 2021, p. 30). Further on, in January 2023, the European Commission sent letters of formal notice to Spain and Italy, accusing them of incorrect application of the AMLD4, as amended by AMLD5. The two countries had previously notified the Commission of their complete transposition of the directive, but the Commission identified several instances of incorrect application, specifically regarding the setting up of the central beneficial ownership registers, a key part of the directive (European Commission, 2023). Sixth place, the need to enhance international cooperation in the fight against money laundering and terrorist financing also should be acknowledged. Criminals do not respect national borders, and therefore, for the global financial system not to be used for illicit purposes a collective effort should be made.

In summary, the EU has implemented a multi-layered legal framework to counteract the illegal activities of money laundering and terrorist financing. Despite these efforts, however, the existing framework has significant shortcomings, including insufficient regulatory coverage, weak enforcement mechanisms, and fragmented regulations and enforcement practices among member states. Recent high-profile money laundering cases have underscored the urgent need for a strong and unified anti-money laundering regulatory framework. While the EU has made significant strides in addressing these issues, it continues to face challenges related to the inadequate transposition of AML directives at the national level, as well as new risks arising from technology and innovation. To effectively combat money laundering and terrorist financing, the EU tries to stay abreast of the latest technological advancements and adjust its AML/CFT rules accordingly through the upcoming EU single rulebook on AML/CFT.

4 The EU Single Rulebook on AML/CFT

In the past years, several international organisations with activities in combating anti-money laundering and the financing of terrorism and proliferation (AML/CFT), such as the Financial Action Task Force ("***FATF***") or the organisation for anti-financial crime professionals ("***ACAMS***"), have reoriented on incorporating ESG concerns within the AML/CFT framework (FATF, 2022, p. 3).

Moving ahead in this direction, on 7 May 2020, the European Commission presented an Action Plan for a comprehensive Union policy on preventing money laundering and terrorist financing, which builds on six pillars, as shown in the figure (Regulatory framework on preventing money laundering and terrorist financing). On 20 July 2021, the European Commission presented the package of regulatory proposals designed to harmonise and strengthen the AML/CFT rules across the EU and which contributes to the efforts towards a sustainable economy.

- Regulation on establishing the Authority for Anti-Money Laundering and Countering the Financing of Terrorism ("***AMLA***") (European Parliament, 2021f), which will serve as the primary body coordinating national authorities to guarantee that EU regulations are appropriately and consistently implemented by the private sector (Stănescu, 2022a, b)
- Regulation on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing ("***AMLR***") (European Parliament, 2021f), which contains rules directly applicable to the member states, especially regarding customer due diligence and beneficial ownership
- "**6AMLD**" (European Parliament, 2021a), which strengthens the cooperation between the national supervisory authorities and the financial intelligence units (FIU) of the member states
- Regulation on Transfers of Funds (recast) (European Parliament, 2021b), which will allow for the tracking of cryptocurrency asset transactions (Săvescu, 2022)

As shown in Table 12.1, regulating environmental crime through the 6AMLD is another measure intended by the legislator to enable better prosecution for this type of crime with a cross-border element. Therefore, another key driver of this convergence is the recognition that environmental and social risks can pose significant AML risks. Financial institutions can unwittingly be used as vehicles for money laundering or terrorist financing when they provide financing to entities engaged in environmentally or socially harmful activities. For example, the financing of illegal logging or human trafficking can be used to launder money or finance terrorism. This means that ESG factors need to be incorporated into AML risk assessments, and AML requirements need to be integrated into ESG reporting frameworks. Similarly, the US Financial Crimes Enforcement Network (FinCEN) has highlighted the potential AML risks associated with environmental and social activities (FinCEN, 2021).

Despite the inclusion of virtual currencies and anonymous prepaid cards in AMLD5, there remains an opportunity for further analysis (Min-Yuh, 2022;

Table 12.1 Authors' Source: Adapted after the table from "VIII. The way forward: a Roadmap" from the Communication from the Commission on an Action Plan for a comprehensive Union policy on preventing money laundering and terrorist financing 2020/C 164/06 (European Commission, 2020b)

Regulatory framework on preventing money laundering and terrorist financing		
Pillars	Legal framework	Actions
Effective implementation of the EU AML/CFT rules	AMLA	– Establishing AMLA – Interconnecting the beneficial ownership registers – Creating an AML/CFT database of information collected from supervisors and supervisory authorities – Issuance of the third supranational risk assessment (SNRA) – Monitoring the capacity of member states to prevent and fight money laundering and terrorist financing through the Structural Reform Support Programme – Infringement/legal proceedings.
An EU single rulebook on AML/CFT	AMLR, transfer of funds regulation, 6AMLD	– Provides requirements for beneficial ownership, customer due diligence, and the roles and responsibilities of supervisors and FIUs
EU-level AML/CFT supervision	AMLA, AMLR	– Establishing AMLA as the centrepiece of the AML/CFT integrated supervisory system, consisting of AMLA and the national authorities with an AML/CFT supervisory mandate – The three European supervisory authorities (EBA, EIOPA and ESMA) which supervise and provide regulatory guidance
A support and cooperation mechanism for FIUs	6AMLD	– Transfer of technical management of FIU.net to the Commission 6AMLD regulates 22 predicate offences, **with environmental and cybercrime being the two that stand out the most**
Enforcing criminal law rules at the union level and exchanging information	Proposal for a Directive on criminal penalties for the violation of Union restrictive measures (European Commission, 2022b), proposal for a regulation of the as regards Europol's cooperation	– Establishment of the EFECC – Enhance domestic and cross-border information exchange among all competent authorities

(continued)

Table 12.1 (continued)

Regulatory framework on preventing money laundering and terrorist financing		
Pillars	Legal framework	Actions
	with private parties, the processing of personal data by Europol in support of criminal investigations (European Parliament, 2020c), proposal for a Directive on information exchange between law enforcement authorities of Member States (European Parliament, 2021c) Proposal for a Regulation on automated data exchange for police cooperation ("Prüm II") (European Parliament, 2021d)	
A stronger EU in the world	EU legal framework	– Developing a methodology for the identification of high-risk third countries

Karasek-Wojciechowicz, 2021; Thommandru & Chakka, 2023; Alarab et al., 2020) of how technology can be leveraged to enhance AML/CFT efforts. Therefore, a deeper understanding of emerging technologies such as blockchain, artificial intelligence (AI), and big data analytics can aid in improving the EU's AML/CFT efforts. In the context of legislating the EU single rulebook on AML/CFT and creating sustainable economic models, the potential trade-offs between financial regulation and financial inclusion should be acknowledged. AML/CFT regulations are basically conceived to prevent financial crime, but unintended consequences may arise, such as limiting access to financial services for certain individuals or businesses. This issue is particularly acute in developing countries, where stringent AML/CFT regulations can pose challenges for small and medium-sized enterprises seeking to access banking services. Therefore, European policymakers should carefully consider the board consequences of AML/CFT regulations on financial inclusion and ensure that marginalised groups are not unduly affected.

5 The Need for Sustainable Economic Models: AML and ESG Convergence

5.1 Literature Review

The concept of sustainable economic models is gaining significant traction due to global risks such as the cost-of-living crisis, natural disasters and extreme weather events, geoeconomic confrontation (global risks ranked by severity over 2 years) or failure to mitigate climate change, failure of climate-change adaptation, and natural

disasters and extreme weather events (global risks ranked by severity over 10 years) (WEF, 2023, p. 14).

While the literature on the relationship between money laundering and SDG is mainly focused on developing countries, limited research has been conducted on the EU. One study that addresses this gap is the 2019 research by Zbysław and Sułkowski (2020). They proposed a sustainable model for AML to enhance the audit capacity and investigative functions of parliamentary watchdogs. Their model aims to achieve all SDGs, create a generally accepted approach to auditing AML outcomes, and strengthen risk management.

Moreover, the literature review indicates that the focus of the research is mainly on developing countries highlighting the importance of addressing money laundering issues to achieve sustainable development goals globally (Razzak & Khan, 2022; Mackey et al., 2018; Hope, 2022; Bartlett, 2002). However, this may limit the generalisability of the findings to the EU context.

However, we note the limited literature available to measure the impact of ESG adoption on preventing money laundering activities in the EU. This lack of research presents a limitation in understanding the effectiveness of ESG measures in preventing money laundering activities. Therefore, for the purpose of this chapter, we have extended our review by including studies that do not directly address the relationship between money laundering and sustainable economic models in the EU.

Given that the new EU AML/CFT regulatory framework has important connections to the new sustainable finance framework, at which heart are ESG concerns, financial institutions are increasingly expected to incorporate sustainability factors into their decision-making processes and investments, and this includes considerations related to AML compliance. For example, sustainable finance initiatives may require enhanced ESG due diligence as part of AML programs or may require AML programs to consider the impact of money laundering on environmental and social factors. Having these two-fold connections between AML and sustainable finance frameworks, there is a need for further research to investigate the effectiveness of the new EU AML/CFT rules and the relationship between them and ESG adoption in preventing money laundering activities. Further research could examine the impact of ESG factors on AML compliance, as well as the impact of AML programs on ESG considerations. By understanding these connections, policymakers, financial institutions, and other stakeholders can work to ensure that the regulatory framework promotes both financial stability and sustainability.

5.2 AML and ESG Convergence Within the EU Regulatory Framework

While recognising the intricacies of the taxonomy (European Economic and Social Committee, 2017), the concept of a sustainable economy is anchored in the principles of environmental responsibility and human values and endeavours to align

economic activities with sustainable development objectives. Based on this understanding, one factor that contributes to sustainable economic models is the adoption of ESG criteria by organisations.

In the view of the EU legislator, building a sustainable financial system requires integrating ESG considerations into decision-making processes while also ensuring compliance with AML regulations to prevent illicit exploitation of the system. While AML and ESG convergence has challenges such as conflicting priorities and interests, EU regulatory initiatives such as SDFR, NFRD, CSRD, CSDDD, CRR II, CRD V, EU Taxonomy Regulation, and ESAP highlight the synergies between AML and ESG. They promote the development of new financial products and services that incorporate sustainability principles and emphasise integrating ESG factors into financial decision-making processes. Therefore, the convergence of AML concerns and ESG risks, increasingly apparent in the contemporary business environment and regulatory landscape, is driven by various factors such as a heightened awareness of the social and environmental impacts of business activities, enhanced financial transparency and accountability, and the implementation of EU regulatory frameworks designed to promote sustainable finance and mitigate money laundering and terrorist financing risks. The modern AML framework's three main pillars are criminalisation, confiscation, and secrecy offensive (Gallant, 2017, p. 126), and the ESG disclosure legal framework supporting sustainable finance advances AML/CFT procedures through sustainable corporate governance obligations, legal reporting on sustainability factors, enhanced customer due diligence requirements, and supervisory authorities' responsibilities in the AML/CFT domain. Additional examples demonstrate the importance of money laundering practices in the EU sustainability reporting regulations and the systems that institutions are putting in place to avoid financial crime, such as harmonised disclosure standards, automated screening, risk management, and continuous monitoring.

From another perspective, the EU is addressing financial institutions, unwittingly trapped in the "vortex of money laundering" (Gallant, 2017, p. 130), to reduce AML risks and complicity in evading legal restrictions. As stated in the *Final draft implementing technical standards on prudential disclosures on ESG risks in accordance with Article 449a CRR* by EBA (2022), the quantitative disclosures in the ITS on Pillar 3 disclosures should include risks on money laundering and financing terrorism. The EBA stresses that these risks are directly related to environmental risks and thus necessary for developing a comprehensive framework for ESG disclosures, as well as providing greater policy coherence within the EU and greater consistency, reliability, and comparability. Also, in the *Final Report Joint EBA and ESMA Guidelines on common procedures and methodologies for the supervisory review and evaluation process (SREP) under Directive (EU) 2019/2034* (Joint EBA & ESMA, 2022), it is highlighted that investment firms should address money laundering and terrorist financing (ML/TF) risks to maintain their financial strength, internal market integrity, and overall financial stability. In another example, EBA (2021b) links the poor code of conduct or a lack of action on anti-money laundering in a given company to a potential institution's negative balance sheet and increased credit risk. The rationale is that if that code of conduct becomes public, customers

and investors may lose confidence in the company, which can attract financial sanctions and affect its ability to conduct long-term economic activities. Therefore, concerns for maintaining a good reputation (and a good ESG risk score) can represent sufficient motivation for the implementation of preventive and coercive measures to reduce money laundering and terrorist financing risks. These aspects are also important from the perspective of stakeholder engagement in AML and ESG convergence. Given the complexity of the regulatory landscape and the competing interests of different parties, stakeholder engagement is essential for ensuring effective AML and ESG convergence in the EU. In this respect, financial institutions, investors, civil society organisations, and regulators should develop a shared understanding of the risks and opportunities associated with sustainable finance and AML/CFT, as well as collaboration on the development and implementation of regulatory frameworks and standards.

Finally, there are also growing calls for financial institutions to include ESG considerations in their AML policies and procedures. For example, the Principles for Responsible Banking, developed by the United Nations Environment Programme Finance Initiative (2023) call for banks to "*start by running a thorough impact analysis across their portfolio of activities to understand the greatest positive and negative impacts the bank has on society and the environment*".

5.3 Convergence and Conflict: Balancing Corporate Transparency and Personal Data Protection in the EU's AML/CFT and ESG Regulatory Frameworks

On 22 November 2022, in the joined cases WM (C-37/20) and Sovim SA (C-601/20) *v* Luxembourg Business Registers—Request for a preliminary ruling from the *Tribunal d'arrondissement* (Luxembourg), based on the Article 7–8 of the Charter of Fundamental Rights of the European Union as well as for breaching the principle of proportionality as established out, in particular, in Article 5(4) of Treaty on European Union, the European Union's Court of Justice (CJEU) (Joint Committee of the Supervisory Committee, 2022) ruled that the provision of the 5AMLD requiring the Member States to ensure that information on the beneficial ownership of corporate and other legal entities incorporated within their territory is accessible in all cases to any member of the general public is invalid. As we hold up from the Conclusions of Advocate General Mr. Giovanni Pitruzzella (Wahl, 2022), this case came to be about the fair balance between, on the one hand, the requirement for transparency regarding the beneficial owners and the control structure of corporate entities, which have a fundamental role in preventing money laundering and terrorist financing, and, on the other hand, respecting the fundamental rights of the persons concerned, namely the beneficial owners, and in particular their rights to respect for private life and the protection of personal data.

Taking a closer look at what this decision means for AML/CFT policy will be interesting. As an immediate response following this judgment, public access to UBO registers was suspended, and the mechanism established by the AMLD4 was restored. Aside from Luxembourg, other governments, such as the Dutch government, promptly required appropriate registers to prohibit public access. As part of the discussion, the debate extends to whether AML/CFT objectives should be recognised as objectives of general interest by the EU, which are capable of justifying restrictions on rights and freedoms under human rights law.

This ruling clearly has ramifications for the entire corporate crime and compliance regulatory and legislative system. For instance, the case may affect the implementation of the disclosure of income tax information by certain companies under Directive 2021/2101/EU (European Parliament, 2021e) regarding the reporting of information based on Article 48c which allows companies to refrain from disclosing "deferred taxes or provisions for uncertain tax liabilities" without any clear definition.

Given the important EU AML/CFT pieces of legislation such as interconnecting beneficial ownership registers, creating a database of information gathered from supervisors and supervisory authorities for AML/CFT, increasing the requirements for beneficial ownership, extending the due diligence process for customers, defining supervisory and financial intelligence units (FIUs) roles and responsibilities, and enhancing the domestic and international exchange of information among all competent authorities, ultimately, financial institutions are expected to develop more rigorous customer due diligence (also referred to under the concept of "know your customer"—KYC), transaction monitoring, and sanctions screening for identifying and mitigating illicit activity related to the ESG. In these activities, leveraging sustainability reporting can be valuable in mitigating money laundering and terrorist financing risks. For example, FIUs can use this information to assess the risk profile of sectors or industries and identify those with elevated risks of money laundering and terrorist financing. Additionally, FIUs can monitor transactions to identify activities conducted through illegal financial means and take appropriate actions. Lastly, sustainability information can be used to develop strategies to prevent money laundering and terrorist financing risks.

However, following the Judgment of the Court in joined Cases C-37/20 and C-601/20: Luxembourg Business Registers and Sovim, it will be interesting to examine how international AML/CFT standards and best practices will develop over time. This balance exercise between corporate transparency and the protection of personal data may be useful in determining appropriate measures to comply with both regimes, with the embedding of data protection in corporate sustainability due diligence rules; however, further investigations may inquire about the effectiveness of these new regulations and the relationship between them and the ESG adoption on AML activities.

6 The Intersection of Cybersecurity, AML Rules, and Sustainable Economic Models: Proposal for Cybercrime in the ESG Risks

As we look ahead, the convergence of the physical and virtual worlds becomes difficult to differentiate because of the increasing digitalisation of the physical world, the emergence of new digital economies, such as crypto-economy, and the prevalence of tokenisation, to name a few trends. With the advent of cutting-edge tools like blockchain, distributed ledger technology, artificial intelligence, and the internet of things, we are witnessing a fundamental transformation in the creation and management of digital assets and future virtual economies. These breakthroughs offer promising new prospects for digitising the physical realm, generating fresh value, and ushering in a wave of innovation that could potentially reshape our world. However, alongside these developments come fresh challenges, including the need to adhere to AML/CFT regulations, guard against cybersecurity threats, and manage the risks that come with illicit and illegal activities. A key worry (Coelho et al., 2021; EBA, 2021a, p. 39; FATF, 2021) is that these new technologies could facilitate criminal activities such as money laundering, terrorist financing, identity theft, and cybercrime. As digital assets become more mainstream and valuable, the risks of financial crimes and fraud loom larger. Moreover, the rise of these technologies has spawned new cybersecurity challenges. With an ever-increasing amount of data being stored and transferred digitally, the danger of cyber-attacks and data breaches has risen to unprecedented levels transforming into concern for the actual sustainable economy achievement.

For instance, each year, about $600 billion, or nearly one per cent of the global GDP, is lost to cybercrime, making it one of the most serious threats to the financial system (Lewis, 2018). In response to such risks, the European Commission (EC) introduced "The Cybersecurity Strategy" (**Joint Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions,** 2013**)** by seeking to improve resilience to cyber threats while also ensuring that individuals and companies benefit from reliable digital technologies (**Joint Communication to the European Parliament and the Council,** 2020**).**

Since cybersecurity is "no longer a technological 'option', but a societal need," the EU has intensified the legislative efforts to provide "coherent and coordinated cyber secure policies by design" (Baldini et al., 2020). As a result, the most recent proposal for a Cyber Resilience Act will support the EU cybersecurity framework, which includes the EU *Cybercrime Directive* (European Parliament, 2013), the Directive on the security of Network and Information Systems (NIS Directive) (European Parliament, 2016), the Directive on measures for a high common level of cybersecurity across the Union (NIS 2 Directive) (European Parliament, 2020a), which was agreed by the European Parliament and the Council, and the EU Cybersecurity Act (European Parliament, 2019). Nonetheless, the interaction between the money laundering framework and cybercrime legislation remains enigmatic.

On the map of digital finance, particularly, the EC proposes to establish wide laws to guarantee the operational resilience of the financial services industry through "DORA" (Proposal for a Regulation of the European Parliament and of the Council on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014 and (EU) No 909/2014). DORA (European Parliament, 2020b) is intended to ensure that EU financial sector operations can resist operational disruption and cyber-attacks. It provides a regulatory framework for digital operational resilience, requiring all businesses to prepare for, respond to, and recover from all sorts of information and communication technology-related interruptions and threats.

Moreover, in the context of geopolitical tensions, the risk of cyberattacks and their repercussions continue to be a major vulnerability for the financial industry in the EU, underscoring the need to improve cyber resilience (EBA, 2022). In this context, it is recommended to accelerate the implementation of the Recommendation of the European Systemic Risk Board on a pan-European systemic cyber incident coordination framework for relevant authorities of designing an effective coordinated Union-level response in the case of a significant, cross-border information and communication technologies incident or threat that has a systemic effect on the whole financial sector of the Union. This operation resulting in the establishment of the EU-SCICF for appropriate authorities will contribute to the financial sector's long-term stability and economic growth.

From another point of view, adopting in the financial industry the new legal framework for cryptocurrencies, such as the Proposal for a Regulation of the European Parliament and of the Council on a pilot regime for market infrastructures based on distributed ledger technology (DLT Pilot regime) and the Proposal for a Regulation of the European Parliament and of the Council on Markets in Crypto-assets, and amending Directive (EU) 2019/1937 (MiCA), is a genuinely ambitious and disruptive leap (Stănescu & Onufreiciuc, 2020). Moreover, access to decentralised finance (DeFi) services is seen as fulfilling the promise of democratising finance by enabling borrowers to access very competitive financing instantly. But achieving the potential of DeFi to reshape the real-world economy is primarily contingent on the tokenisation of real-world assets, harmonising regulatory frameworks, and integrating compliance rules, such as adopting a digital identification system or implementing AML/CFT procedures (Stănescu, 2022a, b, p. 54). A transition from virtual worlds to real economies is likely to reduce transaction costs, improve asset control, stimulate competition, and promote financial inclusion. However, the potential associated challenges should also be considered, with cyber and operational risks and reputational risks (in the event of scams, cyber-attacks, crypto crashes, and contagion) being some of the most important along with legal and financial risks. As a result, the prevalence of cybercrime grows exponentially.

Advanced technologies, such as artificial intelligence and blockchain, have the potential to enhance AML/CFT sector (Doppalapudi et al., 2022; BIS Innovation Hub, n.d.).

By employing machine learning algorithms, financial institutions can efficiently detect suspicious activities and monitor transactions. Additionally, blockchain

technology, specifically through the implementation of smart contracts and distributed ledger technology, aids in securing and streamlining AML/CFT compliance, ultimately contributing to a more stable, transparent, and secure global financial system, thus supporting sustainable economic models.

However, the new EU sustainable finance framework is largely silent on cybercrime. To take further precautions to avoid and identify economic crime, cybercrime now necessitates a particular set of instruments. Organisations and policymakers could better recognise and manage cyber risk as part of their ESG strategy (Sarnek & Dolan, 2022) with the guidance of an industry-standard framework for assessing it. To ensure a sustainable financial system, systemic cyber risk must be addressed, and a standardised framework for cybercrime analysis could contribute to effective governance. Establishing, developing, and promoting corporate cyberculture at each company level should be part of an organisation's commitment to becoming a sustainable entity.

7 Conclusions

The challenge of building a sustainable economic model while fortifying the EU's fight against money laundering is a complex one, requiring a multi-dimensional approach that addresses the deficiencies in coherence and consistency within legal frameworks. To achieve this, legislators must take bold steps to improve transparency, ensure financial stability, and strengthen financial interconnectivity through the integration of AML/CFT rules and ESG tools.

As we move forward, collaboration between authorities overseeing AML and ESG disclosures is essential, and a centralised body for supervising and enforcing AML and ESG requirements could be a key component of this effort. The implementation of standardised disclosure rules for companies operating within the sustainable economy and the use of state-of-art technology to enhance the AML/CFT effectiveness and sustainability disclosure requirements would also be a crucial step in promoting transparency and legitimacy within the financial markets.

These measures can support to the creation sustainable economic models that ensure that funds allocated to the sustainable economy serve legitimate purposes. Such an approach contributes to greater financial market stability and integrity, sustaining the transition to a more sustainable future. However, continued research is necessary to investigate the effectiveness of the new EU AML/CFT rules and the impact of the new EU ESG criteria and sustainability disclosure standards on preventing money laundering activities, as well as to explore new avenues for addressing the evolving challenges of financial crime and sustainability.

References

Alarab, I., Prakoonwit, S., & Nacer, M. (2020). Comparative analysis using supervised learning methods for anti-money laundering in bitcoin. In *Proceedings of the 2020 5th international conference on machine learning technologies (ICMLT 2020)* (pp. 11–17). Association for Computing Machinery. https://doi.org/10.1145/3409073.3409078

Baldini, G., et al. (2020). Cybersecurity, our digital anchor. In I. Nai Fovino et al. (Eds.), *EUR 30276 EN*. Publications Office of the European Union. https://doi.org/10.2760/352218

Bartlett, B. (2002). The negative effects of money laundering on economic development. *Platypus Magazine, 77*, 18–23. Retrieved from https://search.informit.org/doi/10.3316/agispt.20030578

BIS Innovation Hub. (n.d.). *Project Aurora: Using data to combat money laundering across firms and borders*. Retrieved from https://www.bis.org/about/bisih/topics/fmis/aurora.htm

Cacciatore, F. (2019). Patterns of networked enforcement in the European system of financial supervision: What is the new role for the national competent authorities? *European Journal of Risk Regulation, 10*(3), 502–521. https://doi.org/10.1017/err.2019.25

Coelho, R., Fishman, J., & Ocampo, D. (2021). *Supervising cryptoassets for anti-money laundering. FSI Insights on policy implementation 31*. Retrieved from https://www.bis.org/fsi/publ/insights31.pdf

Doppalapudi, et al. (2022). *The fight against money laundering: Machine learning is a game changer*. McKinsey & Company. Retrieved from https://www.mckinsey.com/capabilities/risk-and-resilience/our-insights/the-fight-against-money-laundering-machine-learning-is-a-game-changer

EBA. (2021a). *Opinion of the European Banking Authority on the risks of money laundering and terrorist financing affecting the European Union's financial sector*. EBA/Op/2021/04. Retrieved from https://www.eba.europa.eu/sites/default/documents/files/document_library/Publications/Opinions/2021/963685/Opinion%20on%20MLTF%20risks.pdf

EBA. (2021b). *Report on management and supervision of esg risks for credit institutions and investment firms EBA/rep/2021/18*. Retrieved from https://www.eba.europa.eu/sites/default/documents/files/document_library/Publications/Reports/2021/1015656/EBA%20Report%20on%20ESG%20risks%20management%20and%20supervision.pdf

EBA. (2022). *Joint Committee report on risks and vulnerabilities in the EU Financial System, JC 2022 09*. Retrieved from https://www.eba.europa.eu/sites/default/documents/files/document_library/Risk%20Analysis%20and%20Data/Risk%20reports%20and%20other%20thematic%20work/2022/1030546/Joint%20Report%20on%20Risks%20and%20Vulnerabilities%20-%20Spring%202022.pdf

European Commission. (2018). *July infringements package: Key decisions (Press Release)*. Retrieved from https://ec.europa.eu/commission/presscorner/detail/en/MEMO_18_4486

European Commission. (2019). *Report from the Commission to the European Parliament and the Council on the assessment of the risk of money laundering and terrorist financing affecting the internal market and relating to cross-border activities. COM(2019) 370 final*.

European Commission. (2020a). *Anti-money laundering: Commission decides to refer Austria, Belgium and the Netherlands to the Court of Justice of the EU for failing to fully implement EU anti-money laundering rules (Press release)*. Retrieved from https://ec.europa.eu/commission/presscorner/detail/en/IP_20_1228

European Commission. (2020b). *Communication from the Commission on an action plan for a comprehensive Union policy on preventing money laundering and terrorist financing (2020/C 164/06)*. Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52020XC0513(03)&from=EN

European Commission. (2021). *Proposal for a directive: Anti-money laundering and countering the financing of terrorism legislative package*. Retrieved from https://finance.ec.europa.eu/publications/anti-money-laundering-and-countering-financing-terrorism-legislative-package_en

European Commission. (2022a). *Report from the Commission to the European Parliament and the Council on the assessment of the risk of money laundering and terrorist financing affecting the internal market and relating to cross-border activities. COM(2022) 554 final*.

European Commission. (2022b). *Annex to the Communication from the Commission to the European Parliament and the Council Towards a Directive on criminal penalties for the violation of Union restrictive measures. COM(2022) 249 final*.

European Commission. (2023). *January Infringements package: Key decisions (Press release)*. Retrieved from https://ec.europa.eu/commission/presscorner/detail/en/inf_23_142

European Court of Auditors. (2021). *EU efforts to fight money laundering in the banking sector are fragmented and implementation is insufficient (special report)*. Retrieved from https://www.eca.europa.eu/Lists/ECADocuments/SR21_13/SR_AML_EN.pdf

European Economic and Social Committee. (2017). *New sustainable economic models (Exploratory opinion)*. Retrieved from https://webcache.googleusercontent.com/search?q=cache:iC8q2wG9pykJ:https://webapi2016.eesc.europa.eu/v1/documents/EESC-2017-01690-00-00-AC-TRA-EN.docx/content&cd=2&hl=ro&ct=clnk&gl=ro%20,%20https://www.weforum.org/agenda/2019/09/how-to-make-markets-more-sustainable/

European Parliament. (2013). *Directive 2013/40/EU of the European Parliament and of the Council of 12 August 2013 on attacks against information systems and replacing Council Framework Decision 2005/222/JHA*.

European Parliament. (2015). *Directive (EU) 2015/849 of the European Parliament and of the Council of 20 May 2015 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, amending Regulation (EU) No 648/2012 of the European Parliament and of the Council, and repealing Directive 2005/60/EC of the European Parliament and of the Council and Commission Directive 2006/70/EC*. Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32015L0849

European Parliament. (2016). *Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union*.

European Parliament. (2018). *Directive (EU) 2018/843 of the European Parliament and of the Council of 30 May 2018 amending Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, and amending Directives 2009/138/EC and 2013/36/EU*. Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32018L0843

European Parliament. (2019). *Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act) (Text with EEA relevance)*.

European Parliament.. (2020a). *Proposal for a Directive of the European Parliament and of the Council on measures for a high common level of cybersecurity across the Union, repealing Directive (EU) 2016/1148*. Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2020%3A823%3AFIN

European Parliament. (2020b). *Proposal for a Regulation of the European Parliament and of the Council on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014 and (EU) No 909/2014. COM/2020/595 final*. Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020PC0595

European Parliament. (2020c). *Proposal for a Regulation of the European Parliament and of the Council amending Regulation (EU) 2016/794, as regards Europol's cooperation with private parties, the processing of personal data by Europol in support of criminal investigations, and Europol's role on research and innovation*. Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020PC0796

European Parliament. (2021a). *Proposal for a Directive of the European Parliament and of the Council on the mechanisms to be put in place by the Member States for the prevention of the use*

of the financial system for the purposes of money laundering or terrorist financing and repealing Directive (EU) 2015/849. Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52021PC0423

European Parliament. (2021b). *Proposal for a Regulation of the European Parliament and of the Council on information accompanying transfers of funds and certain crypto-assets (recast)*. Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52021PC0422

European Parliament. (2021c). *Proposal for a Directive of the European Parliament and of the Council on information exchange between law enforcement authorities of Member States, repealing Council Framework Decision 2006/960/JHA*. Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52021PC0782

European Parliament. (2021d). *Proposal for a Regulation of the European Parliament and of the Council on automated data exchange for police cooperation ("Prüm II"), amending Council Decisions 2008/615/JHA and 2008/616/JHA and Regulations (EU) 2018/1726, 2019/817 and 2019/818 of the European Parliament and of the Council*. Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2021%3A784%3AFIN

European Parliament. (2021e). *Directive (EU) 2021/2101 of the European Parliament and of the Council of 24 November 2021 amending Directive 2013/34/EU as regards disclosure of income tax information by certain undertakings and branches*. Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32021L2101

European Parliament. (2021f). *Proposal for a Regulation of the European Parliament and of the Council on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing*. Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52021PC0420

FATF. (2012). *International standards on combating money laundering and the financing of terrorism & proliferation*. Retrieved from www.fatf-gafi.org/recommendations.html

FATF. (2021). *Opportunities and challenges of new technologies for AML/CFT*. FATF. Retrieved from https://www.fatf-gafi.org/publications/fatfrecommendations/documents/opportunities-challenges-newtechnologies-aml-cft.html

FATF. (2022). *Guidance for a risk-based approach to the real estate sector*. FATF. Retrieved from www.fatf-gafi.org/publications/documents/Guidance-RBA-Real-Estate-Sector.html

FATF Report. (2010). *Money laundering vulnerabilities of Free Trade Zones*. Retrieved from https://www.fatf-gafi.org/en/publications/Methodsandtrends/Moneylaunderingvulnerabilitiesoffreetradezones.html

Financial Crimes Enforcement Network (FinCEN). (2021). *FinCEN Calls attention to environmental crimes and related financial activity*. FIN-2021-NTC4. Retrieved from https://www.fincen.gov/sites/default/files/2021-11/FinCEN%20Environmental%20Crimes%20Notice%20508%20FINAL.pdf

Gallant, M. (2017). Tackling the risks of money laundering. In Nic (Ed.), *White collar crime and risk: Financial crime, corruption and the financial crisis (Palgrave studies in risk, crime and society)*. Palgrave Macmillan.

Hanley-Giersch, J. (2019). *Status of the European AML framework.* Retrieved from https://www.acamstoday.org/status-of-the-european-aml-framework/

Heinäluoma, E. et al. (2021). Retrieved from https://www.ceps.eu/wp-content/uploads/2021/01/TFR_Anti-Money-Laundering-in-the-EU.pdf

Hope, K. (2022). Reducing corruption and bribery in Africa as a target of the sustainable development goals: Applying indicators for assessing performance. *Journal of Money Laundering Control, 25*(2), 313–329. https://doi.org/10.1108/JMLC-03-2021-0018

Joint Committee of the Supervisory Committee. (2022). *Joint committee Report on risks and vulnerabilities in the EU financial system*. Retrieved from https://www.eba.europa.eu/sites/default/documents/files/document_library/Risk%20Analysis%20and%20Data/Risk%20reports%20and%20other%20thematic%20work/2022/1030546/Joint%20Report%20on%20Risks%20and%20Vulnerabilities%20-%20Spring%202022.pdf

Joint Communication to the European Parliament and the Council. (2020). *The EU's Cybersecurity Strategy for the Digital Decade The EU's Cybersecurity Strategy for the Digital Decade JOIN/2020/18 final*. Retrieved from https://eur-lex.europa.eu/legal-content/ga/TXT/?uri=CELEX:52020JC0018

Joint Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions. (2013). *Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace/*JOIN/2013/01final**. Retrieved from https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-strategy

Joint EBA and ESMA. (2022). *Guidelines on common procedures and methodologies for the supervisory review and evaluation process (SREP) under directive (EU) 2019/2034*. Retrieved from https://www.eba.europa.eu/sites/default/documents/files/document_library/Publications/Guidelines/2022/EBA-GL-2022-09%20GL%20on%20SREP%20for%20IF/1037290/Final%20report%20on%20SREP%20guidelines%20under%20IFD.pdf

Kanko, A., & Urtasun, E. (2021). *Proposal for a regulation on information accompanying transfers of funds and certain crypto-assets (recast). Legislative train schedule – European Parliament*. Retrieved from https://www.europarl.europa.eu/legislative-train/theme-an-economy-that-works-for-people/file-revision-of-the-regulation-on-transfers-of-funds

Karasek-Wojciechowicz, I. (2021). Reconciliation of anti-money laundering instruments and European data protection requirements in permissionless blockchain spaces. *Journal of Cybersecurity, 2021*, 1–28. https://doi.org/10.1093/cybsec/tyab004

Knight, S. (2023). *Will football leaks finally blow up the premier league?. The New Yorker*. Retrieved from https://www.newyorker.com/news/letter-from-the-uk/will-football-leaks-finally-blow-up-the-premier-league

Le Monde. (39th of June, 2016). *LuxLeaks: suspended sentence for French whistleblowers*. Retrieved from http://www.lemonde.fr/europe/article/2016/06/29/luxleaks-au-luxembourg-verdict-attendu-pour-les-trois-lanceurs-d-alerte-francais_4960591_3214.html

Lewis, A. J. (2018). *Economic impact of cybercrime*. Center for Strategic & International Studies. Retrieved from https://www.csis.org/analysis/economic-impact-cybercrime

Mackey, T., et al. (2018). The sustainable development goals as a framework to combat health-sector corruption. *Bulletin of the World Health Organization, 96*(9), 634–643. https://doi.org/10.2471/BLT.18.209502

Min-Yuh, D. (2022). Artificial intelligence for knowledge graphs of cryptocurrency anti-money laundering in fintech. In *Proceedings of the 2021 IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining (ASONAM'21)* (pp. 439–446). Association for Computing Machinery. https://doi.org/10.1145/3487351.3488415

Razzak, J., & Khan, S. (2022). Nexus between money laundering and sustainable development goals: A threat to developing countries. In Information Resources Management Association (Ed.), *Research anthology on measuring and achieving sustainable development goals* (pp 686–703). IGI Global. https://doi.org/10.4018/978-1-6684-3885-5.ch036.

Sarnek, A., & Dolan, C. (2022). *Cybersecurity is an environmental, social and governance issue. Here's why*. Retrieved from https://www.weforum.org/agenda/2022/03/three-reasons-why-cybersecurity-is-a-critical-component-of-esg/

Săvescu, A. (2022). *Incrementa atque decrementa aulae Cryptocurrency*. Retrieved from https://www.juridice.ro/771346/incrementa-atque-decrementa-aulae-cryptocurrency.html

Stănescu, L-E. (2022a). *AMLA: noua autoritate europeană pentru combaterea spălării banilor și a finanțării terorismului*. Retrieved from https://www.juridice.ro/776038/amla-noua-autoritate-europeana-pentru-combaterea-spalarii-banilor-si-a-finantarii-terorismului.html

Stănescu, L. E. (2022b). Regulation of the obligations of cryptoactive service providers in the framework of the proposed regulation on AML/CFT. *Revista Română de drept penal al afacerilor, 1*, 53–80.

Stănescu, L. E., & Onufreiciuc, R. (2020). *Viitoare reglementări privind piața criptoactivelor*. Retrieved from https://www.juridice.ro/708752/viitoare-reglementari-privind-piata-criptoactivelor.html

The Guardian. (5th of April, 2016). *What are the Panama Papers? A guide to history's biggest data leak*. Retrieved from https://www.theguardian.com/news/2016/apr/03/what-you-need-to-know-about-the-panama-papers

The Guardian. (5th of November, 2017). *Paradise Papers leak reveals secrets of the world elite's hidden wealth*. Retrieved from https://www.theguardian.com/news/2017/nov/05/paradise-papers-leak-reveals-secrets-of-world-elites-hidden-wealth

The Guardian. (4th of March, 2019). *Q&A: What is the 'Troika Laundromat' and how did it work?*. Retrieved from https://www.theguardian.com/world/2019/mar/04/qa-what-is-the-troika-laundromat-and-how-did-it-work#:~:text=The%20network%20operated%20like%20a,belonging%20to%20a%20single%20company

Thommandru, A., & Chakka, B. (2023). Recalibrating the banking sector with Blockchain Technology for Effective Anti-Money Laundering Compliances. *Banks, Sustainable Futures, 5*. Retrieved from https://www.sciencedirect.com/science/article/pii/S2666188823000035

United Nations Environment Programme Finance Initiative. (2023). *Principles for responsible banking. Shaping the future of banking*. Retrieved from https://www.unepfi.org/banking/bankingprinciples/

Wahl, T. (2020). *Infringement procedures for non-transposition of 5th AML directive. Eucrim*. Retrieved from https://eucrim.eu/news/infringement-procedures-non-transposition-5th-aml-directive/

Wahl, T. (2022). *AG opinion on public access to information on beneficial owners. Eucrim*. Retrieved from https://eucrim.eu/news/ag-opinion-on-public-access-to-information-on-beneficial-owners/

World Economic Forum (WEF). (2023). *The global risks report 2023 (18th Edition Insight Report)*. Retrieved from https://www3.weforum.org/docs/WEF_Global_Risks_Report_2023.pdf?_gl=1*1urrqse*_up*MQ..&gclid=Cj0KCQjwk7ugBhDIARIsAGuvgPYxNXIA3bC7HhsbmLxFb5AIcb38u6QtxtmQfwpka8bQ1KrwVQZZd5saAkqyEALw_wcB

Zbysław, D., & Sułkowski, L. (2020). Implementing a sustainable model for anti-money laundering in the United Nations Development Goals. *Sustainability, 12*(1), 244. https://doi.org/10.3390/su12010244

Laura Elly Naghi , PhD is Associate Professor of Finance at Bucharest University of Economic Studies, Department of Finance. With postdoctoral studies in insurance, her work experience derives from and includes: teaching financial professional training, academic courses, and seminaries; research activities; participating in scientific conferences as a researcher, reviewer of papers or Chairperson of session. As Head of the Financial Literacy Department at the Institute of Financial Studies, she develops and coordinates the implementation of financial literacy programs at national levels for teachers, students, and population in general. Her focus in research is financial markets, fundamental prudential supervisory framework, ethics, and corporate governance.

Raluca Anica Onufreiciuc is Associate Assistant in Law at "Stefan cel Mare" University, Suceava, and PhD Candidate at Nicolae Titulescu University of Bucharest and Paris-Panthéon-Assas University. Her current research focus is on good governance, competition rules and administrative jurisdictions, financial transparency and the impact AI can have on its enforcement raising novel and important issues at the intersection between private/public use of personal data for purposes of safeguarding security and public order.

Lorena-Elena Stanescu , PhD in Law ("Al. I. Cuza" University, Iasi, Romania) is a lawyer, particularly interested in the intersection of law, technology, and sustainability, with a particular emphasis on creating a robust and inclusive ecosystem for sustainable financial digitalisation

Raul Felix Hodoş , PhD is Associate Professor in Law at "1 Decembrie 1918" University, Alba Iulia, and PhD Student in Finance at University of Economic Studies, Bucharest. His research interests are mainly in commercial and new technology law and data protection.

Chapter 13
An Overview of Forensic Accounting and Its Effectiveness in the Detection and Prevention of Fraud

Isabella Lucuț Capraș and Monica Violeta Achim

Abstract The main purpose of this study is to determine whether forensic accounting is an effective tool for preventing fraud. To conduct a comprehensive analysis, the research examines three aspects: the skills and attributes of a forensic accountant, the techniques used in forensic accounting, and the challenges and opportunities in the development of the forensic accounting profession. The study's sample includes 30 articles that were critically reviewed using a combination of systematic and traditional literature review methods. The main findings of the study suggest that the abilities and skills, as well as the techniques used in forensic accounting, make this function an effective tool in detecting and preventing fraud; however, they require more attention from academic institutions and specialized bodies that train accounting experts. Moreover, forensic accounting must be recognized as an independent profession. This study can assist businesses and policymakers in improving fraud detection and prevention methods. Furthermore, it can be used in schools to enhance accounting and audit curricula. The study has a social implication because it helps in the prevention and detection of fraud and discusses the forensic accounting profession.

Keywords Forensic accounting · Fraud · Techniques · Skills

JEL Classification G32 · K13 · M42 · M48

I. L. Capraș (✉) · M. V. Achim
Faculty of Economics and Business Administration, Babeș-Bolyai University, Cluj-Napoca, Romania
e-mail: isabella.lucutcapras@econ.ubbcluj.ro

M. V. Achim (ed.), *Economic and Financial Crime, Sustainability and Good Governance*, Contributions to Finance and Accounting,
https://doi.org/10.1007/978-3-031-34082-6_13

1 Introduction

Financial scandals such as Enron, WorldCom and other well-known companies have highlighted the importance of improving fraud detection and prevention techniques as frauds are becoming more complex (Petra & Spieler, 2020; Achim & Borlea, 2020).

The main cause of these scandals is the manipulation of financial statements. As public understanding of the phenomenon has grown, fraud has emerged as a growing focus of research in a variety of disciplines, including accounting and finance (Free & Murphy, 2015). Forensic accounting and anti-corruption practices are critical for reducing the risk of financial crime and detecting frauds. Furthermore, forensic accounting services affect the levels of suspicious activity in companies, and forensic accountants improve fraud management and detection (Okpako & Atube, 2013; Ehioghiren & Atu, 2016). As a result, the subject of fraud is becoming increasingly important for academies, researchers, and legislators (Selimoğlu & Altunel, 2020). Consequently, accurate mechanisms for the detection and prevention of financial crimes must be established, and related sanctions must be applied when fraud is detected.

Fraudulent activities committed by employees at all levels of an organization can harm its reputation, credibility, and, in some cases, survival (Zahra et al., 2007). The International Federation of Accountants (IFAC) has developed the Action Plan for Fighting Corruption and Economic Crime in order to address the growing complexity of the fraud challenge. This plan is crucial in the development of the forensic accounting profession because it indicates that the accounting profession is part of the anti-corruption ecosystem and is viewed as a key driver of sustainable government, contributing to economic development and poverty reduction (International Federation of Accountants, 2022); however, in order to do so, professionals must be well trained and acquire specific skills found in forensic accountants.

Therefore, the field of forensic accounting is a topical and active field that requires investigation, and this study differs from other literature reviews in this field because it combines systematic and traditional literature review and provides a classification for the previous studies considered.

The main objective of this study is to determine whether forensic accounting tools are contributing for preventing financial fraud. In order to conduct a comprehensive analysis, we investigated the most relevant literature searching to find if the following three aspects are meaningful: the skills and attributes of a forensic accountant, the techniques used in forensic accounting, and the challenges and opportunities in the development of the forensic accountancy profession. To achieve this, 30 studies were considered and critically examined.

From the literature investigated, it appears that the abilities and skills, as well as the techniques used in forensic accounting, make this function an effective tool in detecting and preventing fraud; however, they require more attention from universities and specialized bodies that train accounting experts in order to be used and applied throughout investigations. Furthermore, in order to be an effective tool in

fraud prevention, forensic accounting should be recognized as an independent profession; consequently, this profession requires the development of standards and guidelines.

As a result, this study can assist businesses and decision-makers in improving fraud prevention and detection methods. By analysing the skills, knowledge, and techniques used in forensic accounting, this research can also be used in schools to improve accounting and audit curricula. It has a social impact because it aids in the prevention and detection of fraud and outlines the social implications of the forensic accounting profession.

As for the structure of the study, it began with the introductory part. Section 2 explains some theoretical aspects relevant to this study. Section 3 presents the main objective and research Questions. The research methodology is described in Sect. 4. The findings are presented in Sect. 5. Section 6 contains the discussions, and Sect. 7 concludes this chapter.

2 Theoretical Aspects

2.1 Forensic Accounting

Forensic accounting, also known as forensic auditing or financial forensics, is a subset of accounting that denotes activities resulting from actual or anticipated inconsistencies for legal purposes, because forensic accountants are responsible for using fact-finding and analytical abilities to address financial irregularities in a way that meets the standards required by the legal system (Afriyie et al., 2022).

PricewaterhouseCoopers (2019) defines forensic accounting as the work of accountants who conduct investigations, assist in disputes and provide litigation support, and solve other issues that may end up in a court of law.

Another definition is provided by Bologna and Lindquist (1995), which define forensic accounting as "the application of financial skills, and an investigative mentality to unresolved issues, conducted within the context of rules of evidence. As an emerging discipline, it encompasses financial expertise, fraud knowledge, and a sound knowledge and understanding of business reality and the working of the legal system."

Forensic accounting includes two areas: investigative accounting and legal support (Afriyie et al., 2022). Professionals conduct investigations to determine whether or not a financial crime has occurred. They can assess the level of the investigated financial crime if requested, and if the fraud occurs within a company, they investigate at all levels. In terms of legal assistance, financial forensics can help resolve disputes before they reach the courts, so they offer a consulting service. On the other hand, in the court of law, specialists can assess the damages suffered by parties involved in a legal battle and testify for or against as an expert witness.

In order to identify the person or persons responsible for the crime, they investigate financial inconsistencies, analyse evidence, interview potential suspects, and

prepare expert reports. Furthermore, it is part of their job to be able to profile a suspicious person, which may require a basic understanding of the manner in which the criminal mind works, what stimulated a suspect to commit criminal acts, and the way the crime has been conducted (Van Akkeren & Buckby, 2017).

Forensic accounting specialists can be found in companies' compliance departments, law firms, banks, and governmental organizations, in addition to law enforcement agencies (Vidas et al., 2014). A forensic accountant uncovers various types of fraud that can occur in different kinds of organizations, such as medical services, real estate, marketing, hedge funds, and securities trading. These investigators can also look into contract disputes, money laundering, bribery, and embezzlement (Utama & Basuki, 2022).

2.2 Fraud

According to the Institute of Internal Auditors (2022), fraud is an act in which the perpetrator deliberately deceives and harms others for his or her own personal gain.

The Fraud Triangle Theory (Cressey, 1953) can explain how fraud is committed and it is the most frequent taught framework in fraud examination and forensic accounting courses in the United States, United Kingdom, Australia, Hong Kong, and Lebanon (Smith & Crumbley, 2009). According to this theory, there are three elements required for fraud to occur (Cressey, 1953; Albrecht, 1991):

- Pressure/motivation: a non-shareable problem that represents a driving force or motivation to commit fraud;
- Rationalization: explanations for why a particular behaviour is appropriate in a given situation;
- Opportunity: chance for a trust violation, such as weak internal control system that can be misused.

As a result, we can say that the decision to commit fraud is influenced by a number of interconnected factors.

Fraud has numerous negative consequences, including (Honigsberg, 2020):

- Monetary harm: once financial misconduct is revealed, firms lose approximately 29\% of their equity value, and in most cases, some employees end up losing their jobs (Karpoff et al., 2008);
- Psychological negative impact: victims of frauds are more likely to experience broken relationships, health problems, and reputational damage. From a psychological standpoint, even individuals who are not directly involved can be affected by fraud because they lose trust in the system after seeing the harms done to those close to them, and when they lack faith, investors are more reluctant to participate in financial markets (Giannetti & Wang, 2016; Gurun et al., 2018);

- Broad economic repercussions: companies employ and invest excessively during periods of financial misconduct, distorting the allocation of economic resources in the economy (Kedia & Philippon, 2009).

3 Objective and Research Questions

The primary objective of this study is to determine whether forensic accounting tools help to prevent financial fraud. The following research questions are proposed to achieve this goal:

1. Do the skills and characteristics associated with forensic accounting help in the prevention and detection of fraud?
2. Which forensic accounting techniques are reported by the literature as being effective in detecting fraud?
3. What are the benefits and potential problems with the development of the forensic accountant profession according to the literature?

4 Methodology

The main objective of this study is to provide a detailed analysis of the role of forensic accounting in fraud prevention. To achieve this aim, the study employs a combination of systematic literature review (Puntillo et al., 2021) and narrative, critical literature review (Lilienthal & Ayub, 2021) methods, by critically analysing published papers on the subject. The information was also structured and presented in the form of tables and figures.

The search procedure for the articles is illustrated in Table 13.1. The Clarivate Analytics Web of Science (WoS) and Scopus websites were used to search for relevant articles using the search terms "forensic accounting" and "fraud." The results were then refined by applying the inclusion/exclusion criteria. More specifically, in this phase, only the document types article and article reviews were chosen, excluding others such as conference papers, and English was chosen as the language. After that, the resulting sample of articles was manually refined by reading the abstracts and excluding papers that were irrelevant to the research. The articles were then grouped into three topics: skills and abilities of forensic accountants and their suitability in fraud prevention, techniques used in financial forensics and their efficiency in detecting fraud, and difficulties and opportunities in the development of the forensic accounting profession. Articles that did not fit the grouping procedure were removed. The resulting sample was then refined depending on the journal in order to provide a relevant contribution to the existing literature. The resulting sample includes 30 articles.

Table 13.1 The search procedure

Stage in the search process	Procedure description	Database	No. of remaining articles
Search for the articles	String used: "forensic accounting" and "fraud"	Scopus	166
		Web of Science	96
Selecting and applying inclusion/exclusion criteria	Only articles and review articles and only English language	Scopus	119
		Web of Science	66
The merging of the samples	The samples were analysed and duplicate items were removed	Scopus + Web of Science	135
Manual refinement through abstract reading	Abstracts were read, and articles that were not relevant to the research were excluded.	Scopus + Web of Science	87
Grouping of the articles by category and exclusion of non-relevant papers	The articles were grouped into 3 categories related to characteristics and skills, technics and professional development. Articles that were not categorized into any of the groups were excluded.	Scopus + Web of Science	50
Refinement depending on the journal (exclusion of possible untrustworthy journals/publishers)	The articles for the final sample were chosen based on the journal.	Scopus + Web of Science	30

Source: created by the authors

As stated previously, in order to better understand the topic and identify the answer to the research questions, it is considered necessary to divide the literature in order to address the following issues:

- Identification of forensic accountants' *skills and abilities:* By identifying competencies related to forensic accounting according to the literature, their compatibility and applicability in reducing and combating fraud can be analysed.
- Effectiveness of forensic accounting *techniques* in fraud prevention: This category includes articles that investigate whether forensic accountants' techniques are effective in preventing fraud.
- *Difficulties and benefits* in the development of the forensic accounting profession: For a complete analysis, the investigation of difficulties and opportunities in the development of the forensic accounting profession is considered relevant. The applicability and concrete utility of the forensic accounting field can influence the forensic accounting function's effectiveness in preventing fraud.

Therefore, the final sample consists of 30 articles divided into the following three categories:

- Skills and abilities
- Techniques
- Challenges and opportunities

Figure 13.1 shows the composition of the sample based on the categories.

Figure 13.2 illustrates the evolution of articles based on the year of publication. The time period under analysis ranges from 1997 to 2022, but the majority of articles (21 in total) were published in recent years, because of the novelty of the subject.

Figures 13.3 and 13.4 present the sample based on the publisher and the journal, respectively. As can be seen, the most influential publishers in the field of forensic accounting are Emerald and Routledge. However, there is no dominant journal, the articles being published in a variety of journals.

5 Results

5.1 Regarding the Skills and Abilities of Forensic Accountants and their Suitability in Fraud Prevention

Forensic accounting requires a broad variety of skills and knowledge in areas such as accounting, psychology, auditing, and law. Table 13.2 presents previous studies considered in analysing the skills of forensic accountants and their influence on fraud detection classified by author(s), year of publication, source title, methodology, and main findings.

At its most basic, to conduct an examination of a company's financial statements or to resolve financial issues suitable for court, investigative accounting employs four types of skills: accounting, auditing, legal, and investigative (Afriyie et al., 2022; Digabriele, 2009). Accounting expertise is required for forensic professionals, or else time and resources will be wasted. For example, forensic accountants must be well-versed in the country's accounting conventions, relevant accounting standards,

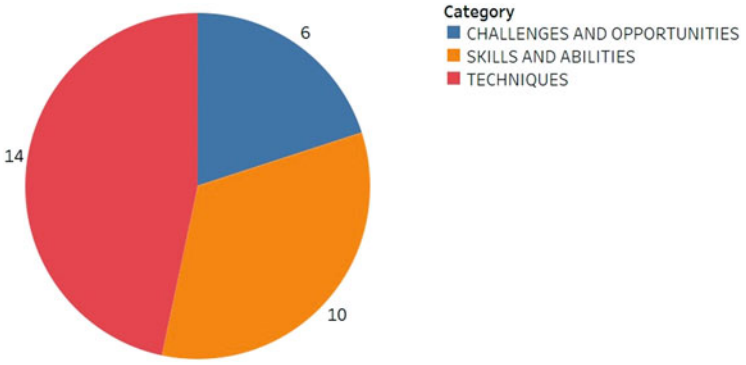


Fig. 13.1 The sample divided into categories. Source: created by the author

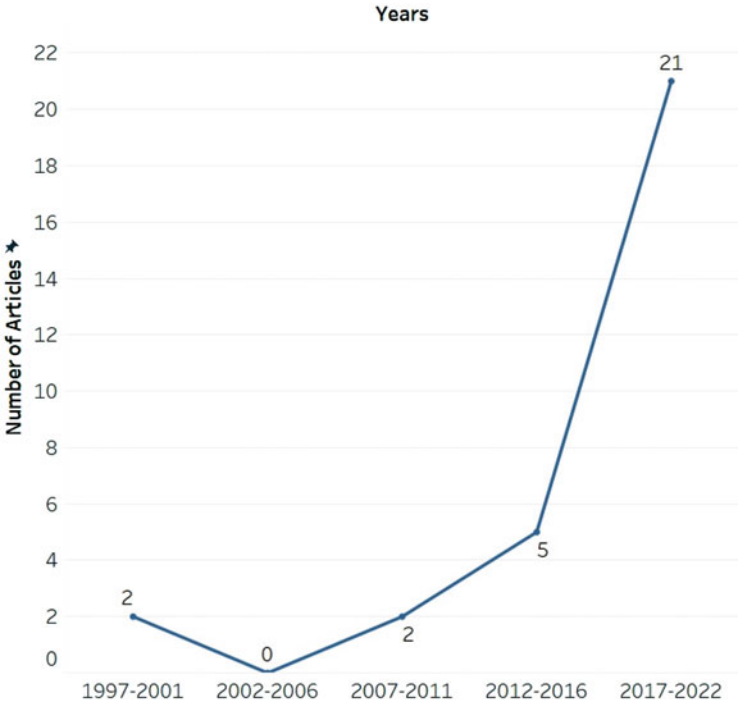


Fig. 13.2 The evolution of articles based on the year of publication. Source: created by the author

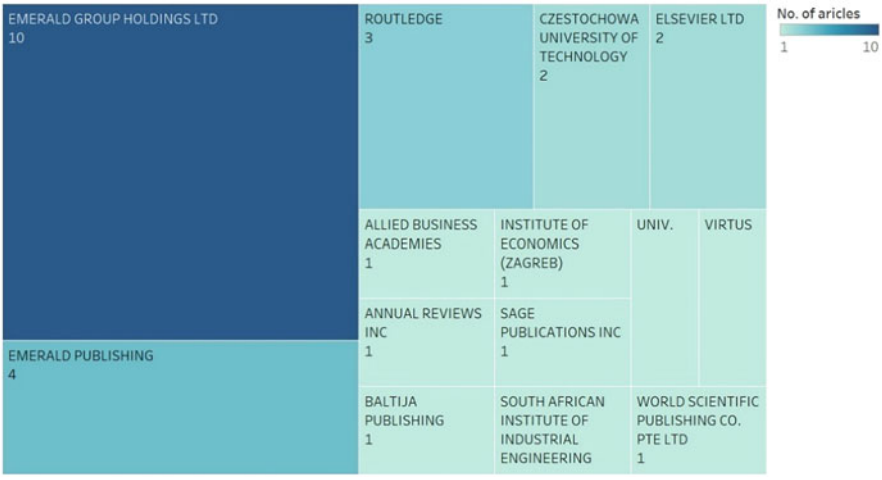


Fig. 13.3 Sample division by publisher. Source: created by the author

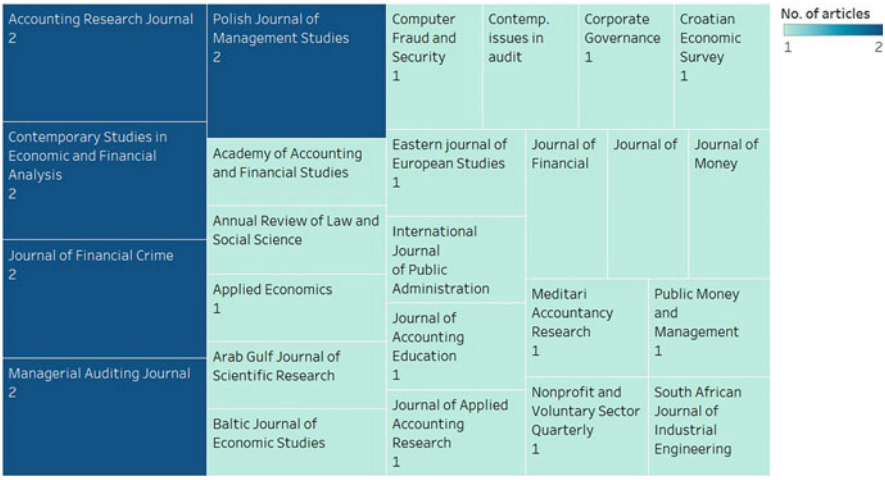


Fig. 13.4 Sample division by journal. Source: created by the author

and assumptions in order to correctly detect fraud because a record that appears to be a fraud in the first place may turn out to be a normal practice under the local accounting conventions of the country in which the investigation takes place. A forensic investigation requires auditing knowledge, but the work of the forensic accountant goes farther than auditing because it includes the examination of both financial and non-financial records and leads to the resolution of all doubts and suspicions about fraud in the organization (Tiwari & Debnath, 2017). Because a crime is unearthed through information gathering dexterity, critical thinking, and in-depth careful examination, investigative skills are essential for the forensic accounting profession (Afriyie et al., 2022; Law & Yuen, 2016). Auditors investigate financial and non-financial records as evidence of fraud, utilizing their legal abilities they are able to evaluate the legal risks of a case (Fadilah et al., 2019).

Other skill sets for forensic accounting include: good written and oral communication, statistics, information technology, psychology, interviewing, problem solving, analytic thinking, and criminology (Carnes & Gierlasinski, 2001; Gottschalk, 2016; Tiwari & Debnath, 2017; Popoola et al., 2015). Aside from these skills, the forensic accountant should have an inner instinct and be able to identify key indicators to uncover the possibility of fraud (Tiwari & Debnath, 2017).

According to Yogi Prabowo (2013), a forensic accountant must have three basic characteristics:

- Mentality: Aspects such as right and wrong, the capacity to endure pressure, and a puzzle-solving mindset
- Method: The skills and knowledge required to accomplish the forensic accountant's responsibilities, which include fraud detection, a systematic process of fraud investigation, evidence principles, and investigation report and presentation

Table 13.2 Studies about the skills and abilities of forensic accountants

Author(s)	Year of pub.	Source title	Methodology	Main findings
Afriyie, S. O.; Akomeah, M. O.; Amoakohene, G.; Ampimah, B. C.; Ocloo, C. E.; Kyei, M. O.	2022	*International Journal of Public Administration*	Questionnaires and statistical analysis	The study discovered that the ability to analyse a situation, effective written communication, specific legal knowledge, investigative intuitiveness, auditing skills, and competency skills all play an important role in fraud control.
Carnes, K.C.; Gierlasinski, N.J.	2001	*Managerial Auditing Journal*	Literature review	As colleges and universities revise their accounting programmes to meet new certification and accreditation standards, the supply of forensic accounting skills, which are critical in fraud detection, may finally be catching up to the rising demand.
DiGabriele, J. A.	2009	*Journal of Applied Accounting Research*	Nationwide survey and statistics (ANOVA)	Forensic accounting knowledge is essential for properly assessing the risk of fraud.
Fadilah, S.; Maemunah, M.; Nurrahmawati; Lim, T. N.; Sundary, R.I.	2019	*Polish Journal of Management Studies*	Survey with a quantitative approach	Some forensic accounting skills are useful in fraud detection, while others are only useful after fraud has been detected.
Gottschalk, P.	2016	*Journal of Information & Knowledge Management*	Case study—evaluation of 13 investigation reports	According to the findings of the research, examiners with forensic accounting knowledge are required when collecting evidence from financial transactions. Furthermore, if the task is to determine whether or not a criminal incident occurred, relevant

(continued)

Table 13.2 (continued)

Author(s)	Year of pub.	Source title	Methodology	Main findings
				legal knowledge should be applied.
Kleinman, G.; Anandarajan, A.	2011	*Journal of Accounting Education*	Literature review and case study	In order to avoid inattentional blindness, in addition to the accounting and tracing aspects of forensic accounting, forensic accountants should be aware of the context in which fraud occurs as well as how it is facilitated.
Law, P.; Yuen, D.	2016	Applied Economics	Survey questionnaires and multinomial logistic regressions	The findings of this study indicate that fraud auditors have higher levels of professional scepticism than general auditors. Fraud auditors with a sceptical mindset may be more likely to detect fraud risks in the workplace.
Popoola, O.M.J., Che-Ahmad, A.B., Samsudin, R.S.	2015	*Accounting Research Journal*	Survey questionnaires and Partial Least Square—Structural Equation Modelling	The results of the research show a positive relationship between forensic accountants' attribute and proficiency competences and their ability to assess the risk of fraud and represent fraud-related problems.
Tiwari, R. K.; Debnath, J.	2017	*Journal of Financial Regulation and Compliance*	Literature review	In addition to auditing, accounting, statistics, information technology, legal, and human behaviour skills, which are all essential for the success of a forensic accounting investigation, forensic accountants should have an inner instinct and be able to identify

(continued)

Table 13.2 (continued)

Author(s)	Year of pub.	Source title	Methodology	Main findings
				key indicators to uncover the possibility of fraud.
Yogi Prabowo, H.	2013	*Journal of Money Laundering Control*	Literature review, in-depth interview, and a focus group discussion	A forensic accountant must have three fundamental components: mentality, method, and experience.

Source: own processings

- Experience: An important means for a forensic accountant to improve his or her skills, knowledge, and mentality through direct involvement in fraud investigation activities

A study that has a different approach is the one conducted by Kleinman and Anandarajan (2011), which analyses the role of inattentional blindness during the investigation process. The study defines perceptual blindness as the inability to see things that are right in front of one's eyes. It can be caused by a general lack of focus caused by mental distractions, as well as a strong focus on a specific item of interest or expectation, caused by a number of heuristics, such as the anchoring, framing, selective perception, confirmation bias, and illusory correlation. In order to effectively detect and prevent fraud, forensic accounting should avoid inattentional blindness and remain objective. Forensic accountants must be able to see the big picture and understand not only the accounting aspects of fraud, but also the environment in which it occurs and how it is enabled by events in one's environment.

Another study that focuses on a single characteristic is that of Law and Yuen (2016), who investigated the impact of professional scepticism on the likelihood of fraud detection. According to this study, individuals who are sceptical about evidence or its sources will be more critical in evaluating information or messages and will require more convincing evidence before concluding that an assertion is correct, compared to individuals who are less sceptical. As a result, we can conclude that scepticism is another characteristic of a good forensic accountant and professionals with a sceptical mindset are more likely to detect fraud.

Not all forensic accounting skills are equally useful in the fraud detection process, with some being more useful during the fraud detection process and others afterward. More specifically, some forensic accounting skills, such as auditing, communication, psychological, criminological, victimological, and technology abilities, are useful in fraud detection, whereas other skills, such as investigative and legal skills, are more useful after the fraud has been discovered (Fadilah et al., 2019). According to Gottschalk (2016), examiners with forensic accounting knowledge are required when collecting evidence from financial transactions. Meanwhile, relevant legal

knowledge should be applied if the task is to determine whether or not a criminal incident occurred.

To summarize, previous research discovered that forensic accounting knowledge is essential for correctly evaluating the risk of fraud and that there is a positive relationship between forensic accountants' characteristics and competences and their capacity to assess the likelihood of fraud and represent fraud-related problems (Digabriele, 2009; Popoola et al., 2015).

5.2 *Regarding Techniques Used in Financial Forensics and their Efficiency in Detecting Fraud*

Each forensic accounting assignment is a unique process. As a result, mission approaches will differ, but we can identify some generic steps that forensic accountants take, which are depicted in Fig. 13.5.

Forensic accountants do not use just one technique in their investigations; indeed, they employ a diverse range of techniques that integrate both numerical analysis and the observation and examination of the behaviour of those involved in the case (Honigsberg, 2020). Table 13.3 summarizes previous studies considered in analysing forensic techniques and their effectiveness in detecting fraud, organized by author(s), year of publication, source title, methodology, and main findings.

In order to detect the presence of inappropriate financial behaviour, forensic accountants use not only strictly accounting approaches, but also statistical methods that are not exclusively accounting and can be utilized in other contexts. Several methods have been described in the literature, including target beating, anomalies in post-decimal and in first digits, artificial neural networks, and abnormal accruals. Table 13.4 describes some of the techniques used in forensic accounting based on previous research (Honigsberg, 2020; Qu et al., 2020; Arboleda et al., 2018; Kiliç, 2020).

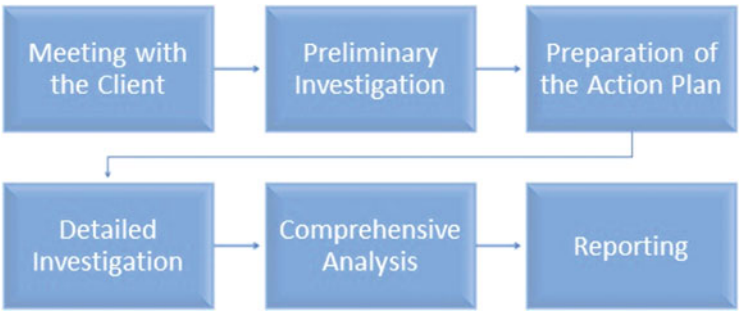


Fig. 13.5 Steps in the forensic accounting mission. Source: created by the author, based on Akinbowale et al. (2020) and the FBI website

Table 13.3 Studies considered in analysing forensic techniques and their effectiveness in detecting fraud

Author(s)	Year of pub.	Source title	Methodology	Main findings
Akinbowale O. E., Klingelhöfer H.E., Zerihun M. F.	2020	*Journal of Financial Crime*	Literature review	In comparison to other branches of the accounting profession, forensic accounting looks further than numbers and it can be used in the organizational control system to successfully mitigate fraud.
Akinbowale, OE; Mashigo, P; Zerihun, MF	2021	*Academy of Accounting and Financial Studies Journal*	Statistical analysis	The research demonstrates the viability of integrating forensic accounting and management control as anti-cyberfraud tools in banks.
Arboleda F. J. M., Guzman-Luna J. A., Torres I. D.	2018	*Computer Fraud and Security*	Literature review and statistical analysis	The findings of the study indicate that there is fraud in the data examined. However, operators only provide indications of potential frauds; Benford's Law is inconclusive in determining whether or not there are frauds in the analysed data, and it must be supplemented with other techniques.
Halilbegovic S., Celebic N., Cero E., Buljubasic E., Mekic A.	2020	*Eastern Journal of European Studies*	Statistical analysis (Beneish M-Score, t-test, correlation and regression)	The Beneish model is applicable on the market of the Federation of Bosnia and Herzegovina and accurately detects financial statements manipulation.
Honigsberg, C.	2020	*Annual Review of Law and Social Science*	Literature review and statistical analysis	There are numerous predictive models available to detect financial manipulation as fast as possible. Traditional models were based on

(continued)

Table 13.3 (continued)

Author(s)	Year of pub.	Source title	Methodology	Main findings
				financial data and concentrated on statistical or accounting anomalies. Recent interdisciplinary models that incorporate new data analysis techniques such as artificial intelligence and machine learning, as well as psychological and quantitative analysis, are more efficient.
Isaković-Kaplan Š., Demirović L., Proho M.	2021	*Croatian Economic Survey*	Statistical analysis (Benford's Law)	The use of Benford's law technique in the examination of financial statement fraud allows forensic accountants to identify data distributions that do not follow the phenomenon of the first digit more rapidly and easily, but it has some limitations in providing a precise assessment about the presence of the fraud.
Khatun, A., Ghosh, R., Kabir, S.	2022	*Arab Gulf Journal of Scientific Research*	Statistical analysis (Beneish M-Score and t-test)	The research shows that the Beneish Model can be used to identify banks in Bangladesh that manipulated their financial data. Moreover, the most relevant practices of financial manipulation are overstating revenues, increasing intangible assets, lowering costs, and accruals.
Kilic, B. I.	2020	*Contemporary Issues in Audit Management and Forensic Accounting*	Literature review	As technology-based approaches to uncovering fraud, the forensic accountant should be able to use

(continued)

Table 13.3 (continued)

Author(s)	Year of pub.	Source title	Methodology	Main findings
				analytical examination procedures, computer-aided audit techniques, artificial intelligence, fuzzy logic models, artificial neural networks, expert systems, data mining, and digital analysis methods.
Kruger P.S., Yadavalli V.S.S.	2017	*South African Journal of Industrial Engineering*	Benford's Law	Benford's law, like most other statistical tests, is not perfect, but it does provide a valuable way of performing certain types of statistical analysis when applicable. Statistical inference is an important tool, but it must be used with caution. Considering the explosion in data availability, effective monitoring mechanisms to detect the presence of irregularities and anomalies in large data sets are required and Benford's law may be applicable in such cases.
Máté D., Sadaf R., Tarnóczi T., Fenyves V.	2017	*Polish Journal of Management Studies*	Statistical analysis (Benford's Law, advanced goodness-of-fit statistical techniques)	The findings demonstrate the unreliability of Benford's law in the case of wholesale companies, along with the uncertainty of financial statement manipulation. According to the authors, a greater understanding of fraud prevention and detection is important in the success of governance policies to resolve the

(continued)

Table 13.3 (continued)

Author(s)	Year of pub.	Source title	Methodology	Main findings
				negative consequences of upcoming financial crises.
Ozturk, M. S.; Usul, H.	2020	*Contemporary Issues in Audit Management and Forensic Accounting*	Statistical analysis (rule-based expert systems and Benford's Law)	In the field of forensic accounting, rule-based expert systems and Benford's Law can be used to detect fraud.
Qu, H., Steinberg, R., Burger, R.	2020	*Nonprofit and Voluntary Sector Quarterly*	Statistical analysis (Benford's Law)	The study supports the use of Benford analysis in non-profit financial data. The authors did identify a potential false-positive problem, indicating that Benford analysis requires further refinement in order to accurately detect fraud. In order to correctly identify fraud, Benford's Law should be used in conjunction with other forensic accounting tools.
Rehman A., Hashim F.	2021	*Corporate Governance*	Descriptive cross-sectional survey design; Partial least squares structural equation modelling and StatisticalPackage for Social Sciences.	The results of the study indicate that forensic accounting has a significant positive impact on sustainable corporate governance; additionally, forensic accounting can be used as part of the corporate governance system to eliminate fraud and achieve sustainable corporate governance.
Shbeilat, M. K.; Alqatamin, R. M.	2022	*Journal of Governance & Regulation*	Mixed method approach (questionnaire and interviews)	The study's findings show that forensic accounting techniques assist in combating money laundering activities.

Source: own processings

Table 13.4 Techniques used in forensic accounting

Technique	Description
Target beating	This method examines whether a firm manipulates losses and gains based on a specific threshold that does not reflect reality.
Data visualization	Forensic accountants can use data visualization methods to identify specific trends and patterns that may indicate a suspicion of fraud.
Benford's Law	It suggests that the distribution of natural data's leading digits is non-uniform. This law has been frequently implemented in order to recognize suspicious data during fraud investigations. Benford's Law stipulates that the leading digit 1 tends to appear more often than the leading digit 9 in natural data. Other fraud detection techniques, such as same-same-same and same-same-different, were developed starting from the Benford's Law.
Anomalies in post-decimal digits	By examining trends in the final digit of observations in a distribution, investigators can predict financial reporting misconduct. Firms, for instance, are incentivized to report earnings per share numbers that have the post-decimal digit five or higher because these digits will be rounded to the higher cent.
The relative size factor	Applying this technique that highlights unusual fluctuations, forensic accountants can identify outliers or unusual data that may occur due to error or fraud.
Artificial neural networks	This method is employed to determine the connection among processes in a set of data and to classify, evaluate, predict, and control these operations.
Abnormal accruals, such as the Jones Model (1991) and the M-Beneish Score (1999)	There are many studies that develop models to identify poor financial reporting quality based on abnormal accruals levels such as the model developed by Healy (1985), the model proposed by Dechow and Sloan (1991), the M-Beneish Score (1999), the Jones Model (1991), and the Model of Kothari et al. (2005). Firms with high abnormal accruals are the most likely to have overstated their performance by accruing for items that would improve their accounting performance.
Audit-based predictors	An increasing number of researchers propose using audit design data to forecast misreporting. This method is derived from the premise that auditors differ and that clients of certain auditors are more likely to engage in financial reporting misconduct than clients of other auditors.

Source: Own processings

With regard to the effectiveness of these methods, the Benford Law was applied by Qu et al. (2020), Arboleda et al. (2018), Máté et al. (2017), Isaković-Kaplan et al. (2021), and Kruger and Yadavalli (2017). Qu et al. (2020) applied Benford's Law to non-profit financial data and discovered that, while this technique can be used to detect fraud in this type of data, it has the potential for false-positives. The authors propose some solutions to this problem that can be with further refinement and the application of other statistical methods. Arboleda et al. (2018) reached a similar conclusion using warehouse data, discovering that the results can be used as a guide, but they are not conclusive in determining the presence of fraudulent activity and must be supplemented with other techniques. Máté et al. (2017) examine wholesale trade companies from 2009 to 2015 and demonstrate the unsustainable nature of Benford's Law in the case of these enterprises, highlighting the uncertainty of financial statement manipulation. On the other hand, Isaković-Kaplan et al. (2021) discovered that accounting data of entities in Bosnia and Herzegovina follow the phenomenon of the first digit, thereby supporting the applicability of Benford's Law to accounting datasets. The study by Kruger and Yadavalli (2017) discovered that while Benford's Law is not perfect, it does provide a useful method for conducting certain types of statistical analysis and is applicable to various types of data.

As for the applicability of the Beneish Model in the context of forensic accounting, Khatun et al. (2022) examined its validity using a sample of listed banks from Bangladesh for the period from 2009 to 2018, concluding that this model can be used to distinguish between manipulators and non-manipulators. Furthermore, among the eight ratios of the model, the most influential are days' sales in a receivable index (DSRI), sales growth index (SGI), asset quality index (AQI), gross margin index (GMI), and total accruals to total assets (TATA). Another study, conducted by Halilbegovic et al. (2020), discovered that out of 68 companies that were manipulating financial information, the Beneish model correctly identified 54 of them, representing 79.41\% in total. Therefore, it can be concluded that the Beneish model is applicable on financial statements and effectively aids in the detection of fraud.

Nowadays, forensic accountants are required to deal with frauds caused by the malevolent use of information technologies, such as cyber-violations, data manipulation within the enterprises, illegitimate transactions, illegal bank transactions, and theft of intellectual property, personal data, and digital assets. These cases highlight the importance of using information technology to detect and prevent fraud and corruption (Kiliç, 2020). The studies carried out by Kiliç (2020) and Oztürk and Usul (2020) identified rule-based expert systems, examination procedures, computer-aided techniques, artificial intelligence, fuzzy logic models, artificial neural networks, data mining, and digital analysis methods as some of the technology-based approaches to uncovering fraud.

Recent models that incorporate psychological, quantitative, and innovative data analysis techniques like artificial intelligence and machine learning perform better than models built solely on financial data (Honigsberg, 2020). In other words, this interdisciplinary approach appears likely to improve forensic accountants' ability to predict fraud.

Concerning the use of forensic accounting to combat fraud, Akinbowale et al. (2021) demonstrated the feasibility of using forensic accounting and the management control system as tools for combating cyberfraud in the banking sector and Shbeilat and Alqatamin (2022) found that forensic accounting techniques aid in the reduction of money laundering operations. Furthermore, according to Rehman and Hashim (2021), who studied the relationship between forensic accounting and sustainable corporate governance in companies, financial forensics has a significant direct impact on sustainable corporate governance and can be used as part of the corporate governance system to eliminate fraud.

5.3 Regarding Difficulties and Benefits in the Development of the Forensic Accounting Profession

Table summarizes previous studies considered in analysing the challenges and opportunities in the development of the forensic accounting profession, organized by author(s), year of publication, source title, methodology, and main findings.

According to the analysed literature, the benefits of financial forensics services are (Gangwani, 2021; Sahdan et al., 2020; Alshurafat, 2022):

- They can help local government meet the growing challenge of fraud.
- Forensic accountants in companies may assist in facing fraud, which is likely to increase in size and complexity.
- They can promote responsible corporate governance, ensuring business's profitability.
- They improve the trustworthiness of financial reporting.
- Forensic accountants assist individuals and companies in the resolution of commercial disputes by providing solid advice and accurate analysis.
- Through mediation and arbitration efforts, forensic accountant's work leads to the prevention of bankruptcy, the reduction of family separations, stress, and, in some cases, the prevention of suicide.

According to the results included in Table 13.5, we found that the literature identified the following difficulties in the development of the forensic accountant profession (Alshurafat, 2022; DiGabriele & Huber, 2015; Rezaee & Burton, 1997; Sahdan et al., 2020; Dubinina et al., 2018):

- Forensic accounting requires a different and broader set of knowledge, training, and expertise than traditional accounting and auditing and the current accounting curriculum is insufficiently responsive to the demand for forensic accounting education and practice in the society.
- To develop and expand forensic accounting, foreign experience in the training of specialists in this field must be considered.
- Audit, consulting, and legal firms must expand their forensic accounting functionalities.

Table 13.5 Studies considered in analysing the difficulties and benefits in the development of the forensic accounting profession

Author(s)	Year of pub.	Source title	Methodology	Main findings
Alshurafat, H.	2022	*Meditari Accountancy Research*	Qualitative data from semi structured interviews with Australian forensic accountants and academics	The findings of the research indicate that forensic accounting in Australia meets only a part of the sociological criteria for a profession. To be recognized as a profession in Australia, forensic accounting must fulfil essential criteria such as autonomy and commitment.
DiGabriele, J. A., & Huber, W. D.	2015	*Accounting Research Journal*	Descriptive research study—Literature review	Forensic accounting researchers should employ more research methods than those that are currently employed so that forensic accounting research can be subjected to the full range of research methods.
Dubinina, M.; Ksonzhyk, I., Syrtseva, S.	2018	*Baltic Journal of Economic Studies*	Literature review	To develop and expand forensic accounting, it is necessary to consider foreign experience in the training of specialists in this field. Moreover, audit, consulting, and legal firms must broaden their forensic accounting services. Domestic companies that use forensic accounting will be more effective in managing their business risks by making optimal management decisions and ensuring their company's profitability.
Gangwani, M.	2021	*Journal of Financial Crime*	Likert scale questionnaire to obtain perception of Academicians and Practitioners; statistical analysis	It was discovered that insiders working in banks collaborated with outsiders to commit fraudulent activities, resulting in bank failures. Moreover, forensic accountants and traditional accountants

(continued)

Table 13.5 (continued)

Author(s)	Year of pub.	Source title	Methodology	Main findings
				are different, and the adoption of forensic accounting in India would help regulatory bodies do their jobs more efficiently.
Rezaee, Z., & Burton, E. J.	1997	*Managerial Auditing Journal*	Mail survey of both accounting academicians and forensic accounting practitioners	The study indicates that the demand for forensic accounting education and practice will keep going up and that forensic accounting education should be integrated into accounting curricula.
Sahdan, M. H., Cowton, C. J., & Drake, J. E.	2020	*Public Money & Management*	Survey	The study discovered that forensic accounting services are currently underutilized by English local governments and that there are mixed levels of satisfaction among those who had used financial forensics services. Nonetheless, greater understanding of what forensic accounting services have to offer, perhaps through case studies of successful implementation, would assist local governments in making better decisions about how and when to use these services.

Source: Own processings

- Standards and guidelines for this profession are missing.
- There is a demand for a better understanding of what forensic accounting services can provide, possibly through case studies of successful implementation.
- There is need for the development of a more detailed understanding of how specific financial forensic services can be profitably used.

6 Discussions

Regarding the efficacy of forensic accounting in fraud prevention, the study concludes that it can be considered a highly effective tool in preventing fraud if practiced by well-qualified professionals who have participated in rigorous training programmes and who master techniques from various fields.

Concerning the first research question, previous literature discovered that forensic accounting skills and knowledge are considered necessary for correctly assessing the possibility of fraud and that there is a positive relationship between investigative accountants' features and competences and their ability to assess the likelihood of fraud and represent fraud-related problems. Because fraud is an interdisciplinary issue that necessitates an understanding of a variety of different areas of knowledge for prevention and investigation, forensic accountants should have a diverse set of skills and expertise. These characteristics are all part of the forensic accountant's profile, but they require more attention from universities and professional bodies that train accounting specialists in order to be used and applied during investigations. In terms of skills and knowledge, the services provided by a well-trained forensic accountant can be a useful tool for businesses in the prevention of fraudulent activities.

With respect to the second research question, which concerns the effectiveness of forensic accounting techniques in detecting fraud, the findings of this study suggest that they must be combined in order to detect fraud correctly. Models developed recently that combine psychological, quantitative, and innovative data analysis methods outperform models based only on financial data. Furthermore, it is discovered that the Beneish model is more accurate and conclusive than Benford's Law, which can only be used as a guide and calls for further investigation. With other words, in order to be effective in fraud detection and prevention, professionals should combine behavioural, quantitative, and digital analysis techniques. Furthermore, they must select and apply multiple statistical methods in order to obtain accurate results about the presence of fraud. Overall, forensic accounting can be considered an effective tool in fraud prevention from a technical standpoint; however, specific training is also required in this case.

The benefits related to the development of the forensic accountancy profession are related to assisting in the general fight against fraud, increasing the credibility of companies' financial statements, but also increasing transparency and promoting sustainable corporate governance. The difficulties associated with the implementation of the forensic accounting profession, on the other hand, have a negative impact on its effectiveness in preventing and combating fraud. In this regard, this profession requires standards and regulations, as well as promotion by emphasizing the benefits of forensic accounting services at the corporate level. As a result, it can be concluded that, in order to be a useful tool in fraud prevention, the function of forensic accountant requires further development and greater public attention.

7 Conclusions

This chapter has presented an assessment, analysis, and evaluation of the research around the effectiveness of forensic accounting as a tool in fraud prevention by considering a sample of 30 articles that address the following topics:

- Skills and abilities of forensic accountants
- Techniques used in forensic accounting
- Difficulties and benefits in the development of the forensic accounting profession

The main results of the study suggest that the abilities and skills, as well as the techniques used in forensic accounting, make this function an effective tool in detecting and preventing fraud; however, they require more attention from universities and specialized bodies that prepare accounting professionals in order to be employed and applied throughout investigations. Furthermore, in order to be a valuable tool in fraud prevention, forensic accounting must be recognized as a distinct profession, which involves the development of guidelines and regulations.

The study's findings will benefit both the academic literature and practice. This research can help businesses and decision makers improve fraud prevention and detection methods. This research can also be used in schools to update and improve the accounting and audit curriculum. It also serves as a guide in the development of the forensic accountant profession by highlighting its techniques, skills, and knowledge. The findings of this study have a social impact because they aid in the prevention and detection of fraud and outline the social implications of the forensic accounting profession.

The limitations of this study are related to the presence of a small and insufficiently diverse sample of studies, with most studies focusing on the United States context and literature in this field being in the process of development.

In area of forensic accounting, there is significant potential for further study. The following have been identified as future research directions:

- To conduct sociological research on the application of the forensic accounting profession in countries other than Australia
- To investigate the role of forensic accountants in companies and in the context of corporate governance
- To carry out research on the improvement of the forensic accountancy profession

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

References

Achim, M. V., & Borlea, N. S. (2020). *Economic and financial crime. Corruption, shadow economy, and money laundering*. Springer.

Afriyie, S. O., Akomeah, M. O., Amoakohene, G., Ampimah, B. C., Ocloo, C. E., & Kyei, M. O. (2022). Forensic accounting: A novel paradigm and relevant knowledge in fraud detection and prevention. *International Journal of Public Administration., 46*, 615–624. https://doi.org/10.1080/01900692.2021.2009855

Akinbowale, O. E., Klingelhöfer, H. E., & Zerihun, M. F. (2020). An innovative approach in combating economic crime using forensic accounting techniques. *Journal of Financial Crime, 27*(4), 1253–1271. https://doi.org/10.1108/JFC-04-2020-0053

Akinbowale, O. E., Klingelhöfer, H. E., & Zerihun, M. F. (2021). The integration of forensic accounting and the management control system as tools for combating cyberfraud. *Academy of Accounting and Financial Studies Journal, 25*(2), 1–14.

Albrecht, W. S. (1991). Fraud in government entities: The perpetrators and the types of fraud. *Government Finance Review, 7*(6), 27–30.

Alshurafat, H. (2022). Forensic accounting as a profession in Australia? A sociological perspective. *Meditari Accountancy Research, 30*(2), 395–423. https://doi.org/10.1108/MEDAR-04-2020-0865

Arboleda, F. J., Guzman-Luna, J. A., & Torres, I.-D. (2018). Fraud detection-oriented operators in a data warehouse based on forensic accounting techniques. *Computer Fraud and Security, 2018*(10), 13–19. https://doi.org/10.1016/S1361-3723(18)30098-8

Beneish, M. D. (1999). The detection of earnings manipulation. *Financial Analysts Journal, 55*(5), 24–36. https://doi.org/10.2469/faj.v55.n5.2296

Bologna, G. J., & Lindquist, R. J. (1995). *Fraud auditing and forensic accounting: New tools and techniques*. Wiley.

Carnes, K. C., & Gierlasinski, N. J. (2001). Forensic accounting skills: Will supply finally catch up to demand? *Managerial Auditing Journal, 16*(6), 378–382. https://doi.org/10.1108/02686900110395514

Cressey, D. R. (1953). *Other people's money: A study of the social psychology of embezzlement*.

Dechow, P. M., & Sloan, R. G. (1991). Executive incentives and the horizon problem. *Journal of Accounting and Economics, 14*(1), 51–89. https://doi.org/10.1016/0167-7187(91)90058-S

Digabriele, J. A. (2009). Implications of regulatory prescriptions and audit standards on the evolution of forensic accounting in the audit process. *Journal of Applied Accounting Research, 10*(2), 109–121. https://doi.org/10.1108/09675420910984673

DiGabriele, J. A., & Huber, W. D. (2015). Topics and methods in forensic accounting research. *Accounting Research Journal, 28*(1), 98–114. https://doi.org/10.1108/ARJ-08-2014-0071

Dubinina, M., Ksonzhyk, I., & Syrtseva, S. (2018). Forensic accounting: The essence and prospects of development in Ukraine. *Baltic Journal of Economic Studies, 4*(1), 131–138. https://doi.org/10.30525/2256-0742/2018-4-1-131-138

Ehioghiren, E. E., & Atu, O. (2016). Forensic accounting and fraud management: Evidence from Nigeria. *Igbinedion University Journal of Accounting, 2*(8), 245–308.

Fadilah, S., Maemunah, M., Nurrahmawati, L. T. N., & Sundary, R. I. (2019). Forensic accounting: Fraud detection skills for external auditors [Rachunkowość forensyczna: Umiejętności wykrywania nadużyć finansowych dla zewnętrzni audytorzy]. *Polish Journal of Management Studies, 20*(1), 168–180. https://doi.org/10.17512/pjms.2019.20.1.15

Free, C., & Murphy, P. R. (2015). The ties that bind: The decision to co-offend in fraud. *Contemporary Accounting Research, 32*(1), 18–54. https://doi.org/10.1111/1911-3846.12063

Gangwani, M. (2021). Suitability of forensic accounting in uncovering bank frauds in India: An opinion survey. *Journal of Financial Crime, 28*(1), 284–299. https://doi.org/10.1108/JFC-07-2020-0126

Giannetti, M., & Wang, T. Y. (2016). Corporate scandals and household stock market participation. *Journal of Finance, 71*(6), 2591–2636. https://doi.org/10.1111/jofi.12399

Gottschalk, P. (2016). Knowledge management in criminal investigations: The case of fraud examiners. *Journal of Information and Knowledge Management, 15*(4), 1650043. https://doi.org/10.1142/S021964921650043X

Gurun, U. G., Stoffman, N., & Yonker, S. E. (2018). Trust busting: The effect of fraud on investor behavior. *Review of Financial Studies, 31*(4), 1341–1376. https://doi.org/10.1093/rfs/hhx058

Halilbegovic, S., Celebic, N., Cero, E., Buljubasic, E., & Mekic, A. (2020). Application of Beneish M-score model on small and medium enterprises in Federation of Bosnia and Herzegovina. *Eastern Journal of European Studies, 11*(1), 146–163.

Healy, P. M. (1985). The effect of bonus schemes on accounting decisions. *Journal of Accounting and Economics, 7*(1–3), 85–107. https://doi.org/10.1016/0165-4101(85)90029-1

Honigsberg, C. (2020). Forensic accounting. *Annual Review of Law and Social Science, 16*, 147–164. https://doi.org/10.1146/annurev-lawsocsci-020320-022159

Institute of Internal Auditors. (2022). *Factsheet: Fraud and corruption.* Retrieved from https://www.iia.org.au/sf_docs/default-source/technical-resources/2018-fact-sheets/factsheet-fraud-and-corruption.pdf

International Federation of Accountants. (2022, September). Action *Plan for fighting corruption and economic crime*. Retrieved from https://www.ifac.org/knowledge-gateway/contributing-global-economy/discussion/ifacs-action-plan-fighting-corruption-and-economic-crime

Isaković-Kaplan, Š., Demirović, L., & Proho, M. (2021). Benford's law in forensic analysis of income statements of economic entities in Bosnia and Herzegovina. *Croatian Economic Survey, 23*(1), 31–61. https://doi.org/10.15179/ces.23.1.2

Jones, J. J. (1991). Earnings management during import relief investigations. *Journal of accounting research, 29*(2), 193–228. https://doi.org/10.2307/2491047

Karpoff, J. M., Lee, D. S., & Martin, G. S. (2008). The cost to firms of cooking the books. *Journal of Financial and Quantitative Analysis, 43*(3), 581–611. https://doi.org/10.1017/S0022109000004221

Kedia, S., & Philippon, T. (2009). The economics of fraudulent accounting. *Review of Financial Studies, 22*(6), 2169–2199. https://doi.org/10.1093/rfs/hhm016

Khatun, A., Ghosh, R., & Kabir, S. (2022). Earnings manipulation behavior in the banking industry of Bangladesh: The strategical implication of Beneish M-score model. *Arab Gulf Journal of Scientific Research, 40*(3), 302–328. https://doi.org/10.1108/AGJSR-03-2022-0001

Kiliç, B. I. (2020). The effects of big data on forensic accounting practices and education. *Contemporary Studies in Economic and Financial Analysis, 102*, 11–26. https://doi.org/10.1108/S1569-375920200000102005

Kleinman, G., & Anandarajan, A. (2011). Inattentional blindness and its relevance to teaching forensic accounting and auditing. *Journal of Accounting Education, 29*(1), 37–49. https://doi.org/10.1016/j.jaccedu.2011.08.002

Kothari, S. P., Leone, A., & Wasley, C. (2005). Performance-matched discretionary accruals. *Journal of Accounting & Economics, 39*, 163–197. https://doi.org/10.1016/j.jacceco.2004.11.002

Kruger, P. S., & Yadavalli, V. S. (2017). The power of one: Benford's law. *South African Journal of Industrial Engineering, 28*(2), 1–13. https://doi.org/10.7166/28-2-1753

Law, P., & Yuen, D. (2016). Professional scepticism in two economies with cultural differences and the public interest: Evidence from China and the United States. *Applied Economics, 48*(2), 89–106. https://doi.org/10.1080/00036846.2015.1073845

Lilienthal, G. I., & Ayub, Z. A. (2021). The fit and proper person test: Development and dissolution of human capital. In *Human capital and development* (pp. 299–345). Nova Science Publishers.

Máté, D., Sadaf, R., Tarnóczi, T., & Fenyves, V. (2017). Fraud detection by testing the conformity to Benford's law in the case of wholesale enterprises [Wykrywanie nadużyć finansowych przez badanie zgodności z prawem Benforda w przypadku przedsiębiorstw handlu hurtowego]. *Polish Journal of Management Studies, 16*(1), 115–126. https://doi.org/10.17512/pjms.2017.16.1.10

Okpako, A. E., & Atube, E. N. (2013). The impact of forensic accounting on fraud detection. *European Journal of Business and Management, 5*(26), 61–70.

Oztürk, M. S., & Usul, H. (2020). Detection of accounting frauds using the rule-based expert systems within the scope of forensic accounting. In *Contemporary issues in audit management and forensic accounting* (Vol. 102, pp. 155–171). Emerald Publishing.

Petra, S., & Spieler, A. C. (2020). *Accounting scandals: Enron, Worldcom, and global crossing*. Emerald Publishing Limited.

Popoola, O. M., Che-Ahmad, A. B., & Samsudin, R. S. (2015). An empirical investigation of fraud risk assessment and knowledge requirement on fraud related problem representation in Nigeria. *Accounting Research Journal, 28*(1), 78–97. https://doi.org/10.1108/ARJ-08-2014-0067

PricewaterhouseCoopers. (2019). *Forensic accounting, PwC*. Retrieved from https://www.pwc.co.nz/services/forensic-services/forensic-accounting.htm

Puntillo, P., Gulluscio, C., Huisingh, D., & Veltri, S. (2021). Reevaluating waste as a resource under a circular economy approach from a system perspective: Findings from a case study. *Business Strategy and the Environment, 30*(2), 968–984.

Qu, H., Steinberg, R., & Burger, R. (2020). Abiding by the law? Using Benford's Law to examine the accuracy of nonprofit financial reports. *Nonprofit and Voluntary Sector Quarterly, 49*(3), 548–570. https://doi.org/10.1177/0899764019881510

Rehman, A., & Hashim, F. (2021). Can forensic accounting impact sustainable corporate governance? *Corporate Governance (Bingley), 21*(1), 212–227. https://doi.org/10.1108/CG-06-2020-0269

Rezaee, Z., & Burton, E. J. (1997). Forensic accounting education: Insights from academicians and certified fraud examiner practitioners. *Managerial Auditing Journal, 12*(9), 479–489. https://doi.org/10.1108/02686909710185206

Sahdan, M. H., Cowton, C. J., & Drake, J. E. (2020). Forensic accounting services in English local government and the counter-fraud agenda. *Public Money and Management, 40*(5), 380–389. https://doi.org/10.1080/09540962.2020.1714208

Selimoğlu, S. K., & Altunel, M. (2020). Forensic accounting and fraud audit in Turkey (2008–2018). *Contemporary Studies in Economic and Financial Analysis, 102*, 219–244. https://doi.org/10.1108/S1569-375920200000102017

Shbeilat, M. K., & Alqatamin, R. M. (2022). Challenges and forward-looking roles of forensic accounting in combating money laundering: Evidence from the developing market. *Journal of Governance and Regulation, 11*(3), 103–120. https://doi.org/10.22495/jgrv11i3art10

Smith, G. S., & Crumbley, D. L. (2009). How divergent are pedagogical views toward the fraud/forensic accounting curriculum? *Global Perspectives on Accounting Education, 6*, 1.

Tiwari, K. R., & Debnath, J. (2017). Forensic accounting: A blend of knowledge. *Journal of Financial Regulation and Compliance, 25*(1), 73–85. https://doi.org/10.1108/JFRC-05-2016-0043

Utama, A. A., & Basuki, B. (2022). Exploration of themes based twitter data in fraud-forensic accounting studies. *Cogent Business and Management, 9*(1). https://doi.org/10.1080/23311975.2022.2135207

Van Akkeren, J., & Buckby, S. (2017). Perceptions on the causes of individual and fraudulent co-offending: Views of forensic accountants. *Journal of Business Ethics, 146*(2), 383–404. https://doi.org/10.1007/s10551-015-2881-0

Vidas, T., Kaplan, B., & Geiger, M. (2014). OpenLV: Empowering investigators and first-responders in the digital forensics process. *Digital Investigation, 11*, S45–S53.

Yogi Prabowo, H. (2013). Better, faster, smarter: Developing a blueprint for creating forensic accountants. *Journal of Money Laundering Control, 16*(4), 353–378. https://doi.org/10.1108/JMLC-05-2013-0017

Zahra, S. A., Priem, R. L., & Rasheed, A. A. (2007). Understanding the causes and effects of top management fraud. *Organizational Dynamics, 36*(2), 122–139. https://doi.org/10.1016/j.orgdyn.2007.03.002

Isabella Lucuț-Capraș is a PhD student at Babeș-Bolyai University, Faculty of Economics and Business Administration, Finance specialization. She has a master's degree in Accounting and Audit expertise, from the same faculty. Her research focuses on issues such as forensic accounting, corporate governance and issues related to economic and financial crime such as the manipulation of financial statements, with the role of the forensic accountant being a major topic in fraud prevention. She is contributor of the project titled "Intelligent analysis and prediction of the economic and financial crime in a cyber-dominated and interconnected business world", conducted over the period 2021–2023, financed from the Romanian Ministry of Education and Research, CNCS—UEFISCDI, project number PN-III-P4-ID-PCE-2020-2174 (www.fincrime.net).

Monica Violeta Achim is full professor and doctoral supervisor in the field of Finance at the Faculty of Economics and Business Administration, Babeş-Bolyai University, Cluj-Napoca, Romania. With over 24 years of experience in academia, she has published as author and co-author, over 150 scientific articles and 25 books. Her most recent reference work is the book Economic and Financial Crime. Corruption, Shadow Economy and Money Laundering, published by Springer. In 2020, she earned an Award for Excellence in Scientific Research at Babeş-Bolyai University, Faculty of Economics and Business Administration, Cluj-Napoca, Romania, in recognition of the results obtained in her research activity. She heads a big grant titled "Intelligent analysis and prediction of economic and financial crime in a cyber-dominated and interconnected business world," conducted over the period 2021–2023, financed from the Romanian Ministry of Education and Research, CNCS—UEFISCDI, project number PN-III-P4-ID-PCE-2020-2174 (www.fincrime.net).

Chapter 14
Cyber-Attacks, Cryptocurrencies and Cyber Security

Guglielmo Maria Caporale, Woo-Young Kang, Fabio Spagnolo, and Nicola Spagnolo

Abstract This chapter provides comprehensive evidence on the effects of cyber-attacks (cyber-crime, cyber espionage, cyber warfare and hacktivism) and cyber security on three types of cryptocurrencies (Bitcoin, Ethereum and Litecoin). Our methodology is based on time series regressions using cyber-attack data; for the analysis, we consider realised returns, realised volatilities, trading volumes and risk-adjusted returns. Stronger cyber security is found to increase realised and risk-adjusted returns, to reduce risk and to increase trading volumes as investors build up their confidence to trade in a safer digital environment. Ethereum, which is a smart contract, benefits the most from cyber security. Bitcoin and Litecoin investors can be characterised as risk-loving and overreact in their attempt to exploit arbitrage opportunities in the event of cyber-attacks targeting cryptocurrency exchanges and industry sector; this type of behaviour is attenuated (intensified) by stronger cyber security in the case of the former (latter) type of attacks. On the other hand, Bitcoin investors in particular become risk-averse when cyber-attacks hit the US government sector. Ethereum is relatively more immune to cyber-attacks regardless of their targets and types in comparison to Bitcoin and Litecoin. However, hacktivism increases risk for all three cryptocurrencies considered. Our results suggest that policy makers and regulators need to be better informed about the impact of cyber-attacks on cryptocurrencies and that more appropriate strategies should be designed and put in place to enhance cyber security.

G. M. Caporale (✉) · W.-Y. Kang
Department of Economics and Finance, Brunel University London, Uxbridge, UK
e-mail: guglielmo-maria.caporale@brunel.ac.uk

F. Spagnolo
Department of Economics and Finance, Brunel University London, Uxbridge, UK

Department of Economics, University of Messina, Messina, Italy

N. Spagnolo
Department of Economics and Finance, Brunel University London, Uxbridge, UK

Università degli Studi della Campania, "Luigi Vanvitelli", Naples, Italy

M. V. Achim (ed.), *Economic and Financial Crime, Sustainability and Good Governance*, Contributions to Finance and Accounting,
https://doi.org/10.1007/978-3-031-34082-6_14

Keywords Cyber-attacks · Cryptocurrencies · Cyber security

JEL Classification C22 · E4 · G1

1 Introduction

Despite their rather recent introduction, cryptocurrencies are now very widely used and their exchanges have rapidly become a favourite target for cyber-attackers including cyber criminals, hackers and fraudsters (Stankiewicz, 2021). According to Kevin Mandia, a CEO of the FireEye cyber security corporation, there is a direct correlation between the increase in ransomware attacks and the advent of cryptocurrencies (Singh, 2021). Tesla have also experienced cyber-attacks by hackers attempting to install software on their computers to mine coins without their knowledge or consent, a process which is known as crypto-jacking (BBC News 2021).

In general terms, a cyber-attack can be defined as an attack from one or more computers against other computers or networks aiming at disabling and/or managing the latter and obtaining access to information, thereby compromising its confidentiality, integrity and availability. This breach of security represents a form of cyber risk, which has been found to be significant in the case of the financial sector (see Kopp et al., 2017). Such cyber threat can be detrimental to cryptocurrencies that are not regarded as similar to other standard assets and for which empirical evidence is limited (Liu & Tsyvinski, 2018).

The present study provides comprehensive evidence on the effects of cyber-attacks (using data collected from Hackmageddon, http://www.hackmageddon.com) and cyber security on the realised returns, risk-adjusted returns, realised volatilities and trading volumes of the three cryptocurrencies (Bitcoin, Ethereum and Litecoin). More specifically, it investigates the effects of four different types of cyber-attacks (cyber-crime, cyber-espionage, hacktivism and cyber-warfare) on cryptocurrencies, four target sectors (cryptocurrency exchange, government, industry and finance) and 113 countries. Furthermore, it aims to investigate whether cyber-security attenuates those effects. Risk-adjusted returns (the return-to-risk ratio) are constructed using realised returns and weighted realised covariances as the return and risk components, respectively; this measure considers the systemic risk (correlation) and change in market capitalisations among cryptocurrencies in addition to each currency's own risk, which could all be affected by cyber-attacks. We estimate time series regressions at the daily frequency over the period from 12 August 2015 to 28 February 2019; the model also includes appropriate control variables, namely, stock market liquidity and financial market uncertainty.

We find that enhanced cyber security increases both the (realised and risk-adjusted) returns and the trading volumes of cryptocurrencies by reducing risk and boosting investor confidence in the safety of the digital environment. Ethereum, which is a smart contract, benefits more from cyber security than Bitcoin and Litecoin. Investors in the two latter cryptocurrencies can be characterised as risk-

loving arbitrageurs overreacting to cyber-attacks targeting cryptocurrency exchanges and the industry sector; this type of behaviour is attenuated (intensified) by stronger cyber security in the case of the former (latter) type of attacks. By contrast, in the case of cyber-attacks on the US government sector, Bitcoin investors exhibit risk-aversion. Ethereum is the most immune to cyber-attacks of the three cryptocurrencies considered. However, all of them are vulnerable to hacktivism-type cyber-attacks increasing risk. Thus, it appears that cyber security should be enhanced by designing appropriate strategies for each sector, cryptocurrency and attack type to provide a safer digital trading environment for (cryptocurrency) investors (van Hardeveld et al., 2017).

Our study contributes to the finance literature focusing on Fintech, which is widespread interest across the globe (Chen et al., 2019; Goldstein et al., 2019). Fintech includes seven categories: cybersecurity, mobile transactions, data analytics, blockchain, peer-to-peer (P2P), robo-advising and Internet of things (IoT) (Chen et al., 2019).[1] Our analysis adds to the understanding of Fintech in its blockchain and cybersecurity aspects and extends the empirical asset pricing literature on cryptocurrencies.

The remainder of the chapter is organised as follows. Section 2 reviews the relevant literature. Section 3 describes the data and the methodology. Section 4 presents the empirical results. Section 5 offers some concluding remarks.

2 Literature Review

In recent years, cryptocurrencies have established themselves both as an alternative to fiat money (see Yermack, 2018) and as a tradable asset used for risk-hedging purposes (see Bouri et al., 2017a, b).

The impact of cyber-attacks on cryptocurrency markets and the economy as a whole has been analysed in various recent papers. For instance, Benjamin et al. (2019) estimated that cyber-attacks from criminals operating in underground web communities such as Darknet have resulted in estimated annual losses of $445 billion for the global markets (see Graham, 2017). In another interesting study, Bouveret (2018) used a Value-at-Risk (VaR) framework to measure cyber risk and the resulting losses in a number of countries. More recently, Despotović et al. (2023) conducted a thorough study of cyber security issues which resulted in a list of recommendations for banks, fintech companies and end users.

In the case of cryptocurrencies, given their distinctive features (see Corbet et al., 2019a), different methods are required to estimate and manage risk (see Platanakis &

[1] Chen et al. (2019) define the peer-to-peer (P2P), robo-advising and Internet of things (IoT) as follows. Peer-to-peer (P2P): Software, systems, or platforms that facilitate consumer-to-consumer financial transactions. Robo-advising: Computer systems or programs that provide automated investment advice to customers or portfolio managers. Internet of things (IoT): Technologies relating to smart devices that gather data in real time and communicate via the internet.

Urquhart, 2019). Cyber-attacks are considered a very important risk factor by both small and large "miners," whose task is to group unconfirmed transactions into new blocks and add them to the global ledger known as the "blockchain" (see Hileman & Rauchs, 2017). Benjamin et al. (2019) provided some evidence on the disruptions caused by cyber security breaches in the case of the cryptocurrency markets; these have also been targeted for the purpose of illicit online drug trading (see Martin, 2014), which has given rise to a number of ethical issues (see Martin & Christin, 2016). Shanaev et al. (2020) warned that if any individual or group of coin miners controls over 50% of the network mining, they can take over the chain, especially in the case of cryptocurrencies with small proof-of-work and low hash rates. An et al. (2021) find that cyber security risk is a major impediment to raising capital through initial coin offerings (ICOs), which better investor protection (e.g., protection of investor right protection and the legal system functionality) provided by institutions can mitigate this negative impact.

Caporale et al. (2019) used a Markov-switching non-linear specification to analyse the effects of cyber-attacks on returns in the case of four cryptocurrencies (Bitcoin, Ethereum, Litecoin and Stellar) over the period between 8 August 2015 and 28 February 2019. They found significant negative effects on the probability of cryptocurrencies staying in the low volatility regime. Caporale et al. (2021) investigated how cyber-attacks affect mean and volatility spillovers between three cryptocurrencies (Bitcoin, Litecoin and Ethereum) using a trivariate GARCH-BEKK model. They found evidence that cyber-attacks strengthen cross-market linkages, which leads to reduced portfolio diversification opportunities. Corbet et al. (2019b) estimated a DCC-GARCH model and documented that cryptocurrency hacks increase both the volatility of the currencies hacked and their correlations with other cryptocurrencies; further, they decrease price discovery for the hacked currencies in comparison to others. As for the effects on returns, abnormal ones are observed preceding the hack, which revert to zero when this is publicly announced. However, this research is limited to 17 hacking events on the cryptocurrency exchanges within less than a year.

Developing strategies to deal with and possibly prevent cyber-crime has therefore become very important (see van Hardeveld et al., 2017). In the case of the USA, a specific concern has been the use of cryptocurrencies to avoid sanctions. It has been suggested that a task force including agencies from the Departments of the Treasury, State, Justice and Defence should be created to focus in particular on the cracking of blockchain cryptography to trace transactions (see Konowicz, 2018). More recently, Ramos et al. (2022) have highlighted the existence of a gap between legal and technical research in the field of crypto-assets and cyber risks in Europe and proposed an interdisciplinary approach aimed at providing policy makers with practical support regarding their regulatory decisions.

As can be gathered from the above review, none of the existing studies considers a wide range of cyber-attacks in different categories and their effects on the risk-adjusted returns and trading volumes of cryptocurrencies and various sectors in the presence of cyber security. In this study, we aim to contribute to the literature by addressing all these issues by means of a suitable empirical framework. Our

empirical analysis yields informative new findings about the effectiveness of cyber security and differences in the trading behaviour of Bitcoin, Ethereum and Litecoin investors when cyber-attacks occur.

3 Data and Methodology

3.1 Cryptocurrency Data

We collect daily data on the closing prices and trading volumes for the three cryptocurrencies (Bitcoin, Ethereum and Litecoin) over the period between 12 August 2015 and 28 February 2019 from the website www.CryptoDataDownload.com; this provides historical data for traded prices using the Application Programming Interface (API) service and is a reliable cryptocurrency data source as pointed out by Alexander and Dakos (2020). Bitcoin, Ethereum and Litecoin are selected as the main blockchain, smart contract and altcoin (alternative coin) platforms for cryptocurrencies. We also choose five main exchanges (Bitfinex, Coinbase, Gemini, Kraken and Poloniex) that are common to the three cryptocurrencies under examination.[2] We then compute market capital-weighted indices, which are based on the five exchanges. The natural log returns are used for the estimation of the models. We show these in Fig. 14.1.

We use realised returns, realised volatility, trading volume and risk-adjusted returns as the dependent variables whose dynamics are analysed in the presence of cyber-attacks as well as cyber security. The return and volume data enable us to compute the return-to-risk ratio—it is essential to use risk-adjusted returns in the case of cryptocurrencies since they are more volatile than standard assets such as stocks and derivatives. As a risk measure, we consider the correlation (i.e., the systemic risk for cryptocurrencies) and change in the trading volumes of cryptocurrencies in addition to each cryptocurrency's own risk (i.e., volatility), which could all be affected by cyber-attacks. Therefore, we compute the risk-adjusted returns of cryptocurrencies as follows:

$$r_{i,t} = \frac{\mu_{i,t}}{\sqrt{w_t \times \sigma_t^{Rcov} \times w_t'}}, \tag{14.1}$$

where the components are estimated as below:

[2]The www.CryptoDataDownload.com website does not provide all the cryptocurrency exchanges for each country. Thus, we select from this source data for five major exchanges (the same as in Alexander and Dakos (2020)) in the US and the UK that are common to the three cryptocurrencies being examined (Bitcoin, Ethereum and Litecoin) and were available at the time when they were collected.

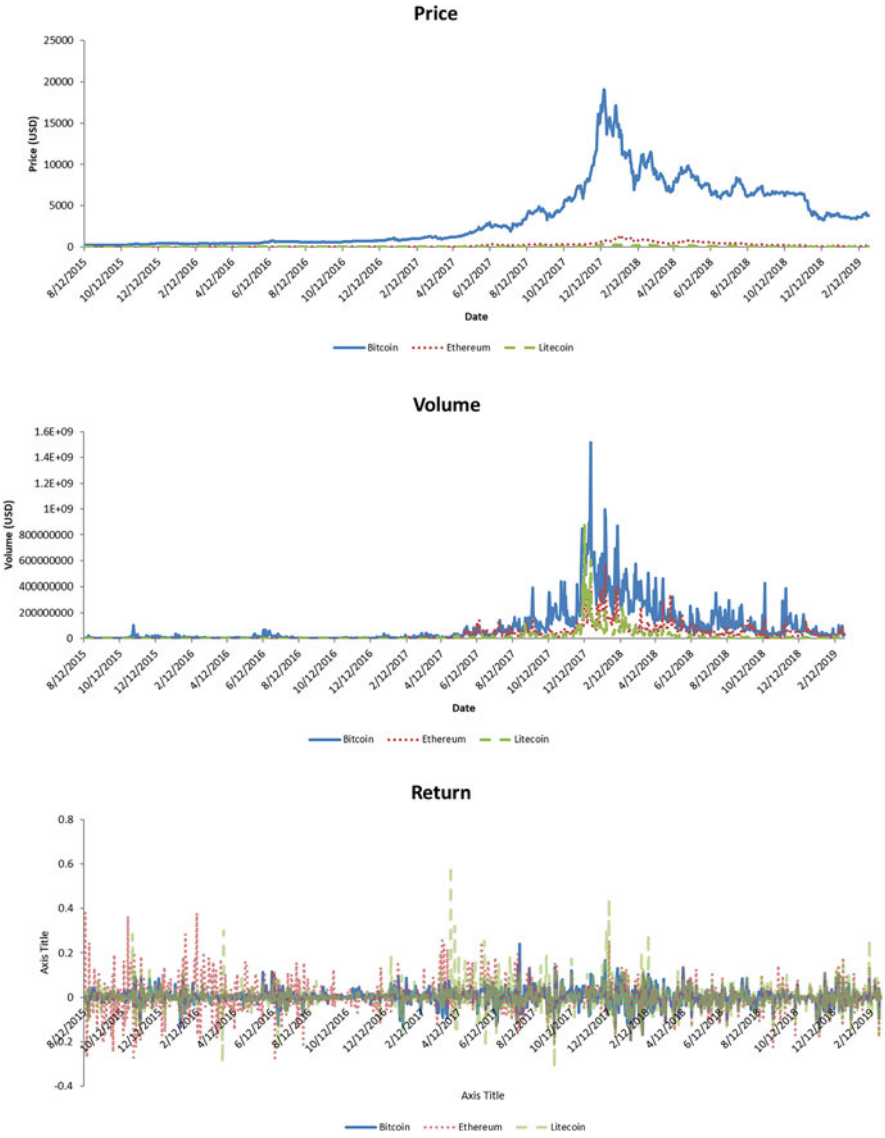


Fig. 14.1 Cryptocurrencies. Source: own processings

$$\mu_{i,t} = \frac{1}{t}\left(\ln\frac{P_{i,2}}{P_{i,1}} + \ln\frac{P_{i,3}}{P_{i,2}} + \cdots + \ln\frac{P_{i,t}}{P_{i,t-1}}\right) \tag{14.2}$$

$$\begin{aligned} w_t \times \sigma_t^{Rcov} \times w_t' &= (w_{1,t} \;\; w_{2,t} \;\; w_{3,t}) \begin{pmatrix} \sigma_t^{1,1} & \sigma_t^{1,2} & \sigma_t^{1,3} \\ \sigma_t^{2,1} & \sigma_t^{2,2} & \sigma_t^{2,3} \\ \sigma_t^{3,1} & \sigma_t^{3,2} & \sigma_t^{3,3} \end{pmatrix} \begin{pmatrix} w_{1,t}' \\ w_{2,t}' \\ w_{3,t}' \end{pmatrix} \\ &= \left(\frac{P_{1,t} \times V_{1,t}}{\sum_{i=1}^{3}(P_{i,t} \times V_{i,t})} \;\; \frac{P_{2,t} \times V_{2,t}}{\sum_{i=1}^{3}(P_{i,t} \times V_{i,t})} \;\; \frac{P_{3,t} \times V_{3,t}}{\sum_{i=1}^{3}(P_{i,t} \times V_{i,t})}\right) \\ &\quad \begin{pmatrix} \sigma_t^{1,1} & \sigma_t^{1,2} & \sigma_t^{1,3} \\ \sigma_t^{2,1} & \sigma_t^{2,2} & \sigma_t^{2,3} \\ \sigma_t^{3,1} & \sigma_t^{3,2} & \sigma_t^{3,3} \end{pmatrix} \begin{pmatrix} \frac{P_{1,t} \times V_{1,t}}{\sum_{i=1}^{3}(P_{i,t} \times V_{i,t})} \\ \frac{P_{2,t} \times V_{2,t}}{\sum_{i=1}^{3}(P_{i,t} \times V_{i,t})} \\ \frac{P_{3,t} \times V_{3,t}}{\sum_{i=1}^{3}(P_{i,t} \times V_{i,t})} \end{pmatrix} \end{aligned} \tag{14.3}$$

$$\sigma_t^{i,j} = \frac{\sum_{t=1}^{t}\left(\ln\left(\frac{P_{i,t}}{P_{i,t-1}}\right) \times \ln\left(\frac{P_{j,t}}{P_{j,t-1}}\right)\right)}{t}. \tag{14.4}$$

$\mu_{i,\,t}$ is the realised return, namely, the time-varying drift coefficient of the stochastic differential equation we assume cryptocurrency i to follow at time t—this is the return component. $P_{i,\,t}$ is the price of cryptocurrency i at time t, $V_{1,\,t}$ is its trading volume of cryptocurrency i at time t, and $w_{i,\,t}$ $\left(= \frac{P_{i,t} \times V_{i,t}}{\sum_{i=1}^{N}(P_{i,t} \times V_{i,t})}\right)$ its market capitalisation ($P_{i,\,t} \times V_{i,\,t}$) weight across N different types of cryptocurrencies (where $i = 1, \cdots, N$) at time t. N is equal to three in our case since our sample includes three cryptocurrencies, namely, Bitcoin ($i = 1$), Ethereum ($i = 2$) and Litecoin ($i = 3$). w_t is a ($1 \times N$) vector whose elements are the volume weights $w_{i,\,t}$ of all three cryptocurrencies at time t. w_t' is a transpose of the vector w_t. $\sigma_t^{i,j}$ is the realised covariance between cryptocurrencies i and j at time t. σ_t^{Rcov} is the realised covariance at time t using all three cryptocurrencies' realised covariance $\sigma_t^{i,j}$ in a ($N \times N$) matrix form. The resulting $\sqrt{w_t \times \sigma_t^{Rcov} \times w_t'}$ is used as the risk component. $r_{i,\,t}$ is the risk-adjusted return of cryptocurrency i at time t. We denote $\sqrt{w_t \times \sigma_t^{Rcov} \times w_t'}$ as $\sqrt{R\text{cov}^w}$, and r_{Bitcoin}, r_{Ethereum} and r_{Litecoin} as *Bit_RAR*, *Eth_RAR* and *Lit_RAR*, respectively, throughout the chapter.

3.2 Cyber-Attack Data

The recent developments in technology of networking and cyberspace, including cryptocurrencies using blockchain technology, have been highly beneficial. However, the rapid growth in these fields has also promoted unethical practices using these technologies to exploit others, which include cyber-attacks (Uma & Padmavathi, 2013). These are an attempt to damage, destroy or gain illegal access to a computer network or system (Bodford & Kwan, 2018).

The cyber-attack data are taken from the website http://www.hackmageddon.com/, which shows the cyber-attack timeline by target industry, country and cyber-attack type at a daily frequency. The Hackmageddon's cyber-attacks are collected from public sources such as blogs and news sites. Therefore, the sample collection cannot be complete, but it aims to provide a wide overview of the cyber-attack threat landscape across the globe (Passeri, 2020). We have collected data on 4006 daily cyber-attacks (including daily overlaps) from 12 August 2015 to 28 February 2019 for four target sectors, namely, the government (*Gov*), industry (*Ind*), finance (*Fin*) and cryptocurrency exchange (*Crypto*) sectors, and created in each case binary variables equal to 1 for the sector affected and 0 for the others. Thus, there are four cyber-attack binary variables, namely, cyber-crime (*CC*), cyber espionage (*CE*), hacktivism (*H*) and cyber warfare (*CW*), each being equal to 1 if the corresponding type of attack occurs and 0 otherwise. However, *CW* is dropped from the model to avoid the dummy variable trap. Since multiple cyber-attacks may occur within a day, we use the added-up binary figures of these per day, which shows the daily intensity in terms of cyber-attack target and type merging into 1157 daily cyber-attacks without daily overlaps in total.

According to Uma and Padmavathi (2013), cyber-crime can be defined as a criminal offence, which involves a computer either as an object or a tool to commit a material component of the offence; cyber espionage is the cracking technique and malicious software (e.g., Trojan horses and spy ware) used to obtain information without the permission of the holder from individuals, groups and governments for gaining benefits through illegal abuse methods; cyber warfare is the use of computer technology to penetrate a nation's computer network in order to cause damage or disruption. Hacktivism is instead "the act of gaining access to (and control over) third-party computer systems" (Bodford & Kwan, 2018).

Figures 14.2 and 14.3 show, respectively, the cyber-attack targets and types considered in the analysis. It is apparent from Fig. 14.2 that the industry sector (54.5%) is the most frequent target of cyber-attacks, which suggests that it is more vulnerable, compared to other sectors (e.g., government, financial and cryptocurrency exchange) that have stronger cyber security protections. In particular, the cryptocurrency exchanges appear to be the least targeted, presumably because their blockchain technology works effectively against cyber-attacks and this being a new sector hackers need time to learn how to attack it successfully.

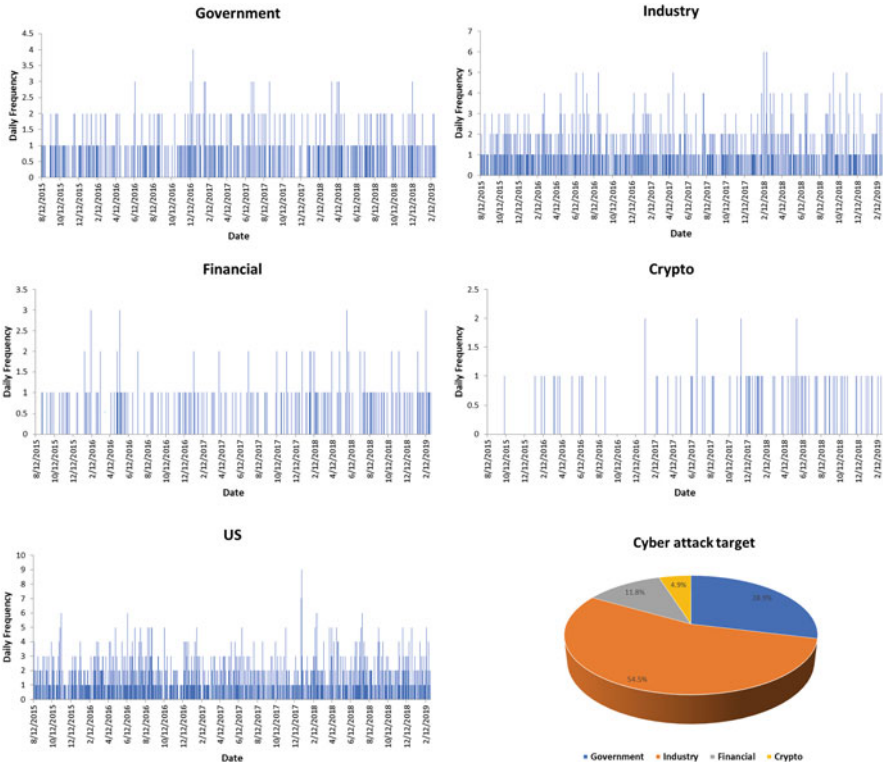


Fig. 14.2 Cyber-attacks by target

Figure 14.3 shows that cyber-crime (77.6%) is the most frequent type of cyber-attack, and cyber warfare (3.2%) the least frequent; this is not surprising, since the latter is an attack on a nation's computer network and thus on a larger scale relative to other types of cyber-attacks. North America (United States and Canada), the UK and India have been the most frequently targeted by cyber-attacks of the 113 countries considered (Appendices 2 and 3).[3] There were also 930 cyber-attacks targeting more than one country, which is the second most frequent case (see Appendix 2); this is plausible since by their nature cyber-attacks are world-wide events without geographical restrictions.

[3] In Appendix 2 'More than one country' and 'Unknown' country sources are dropped since they cannot be displayed as countries in Appendix III, where the darker shades indicate more frequent cyber-attacks per day in a given country.

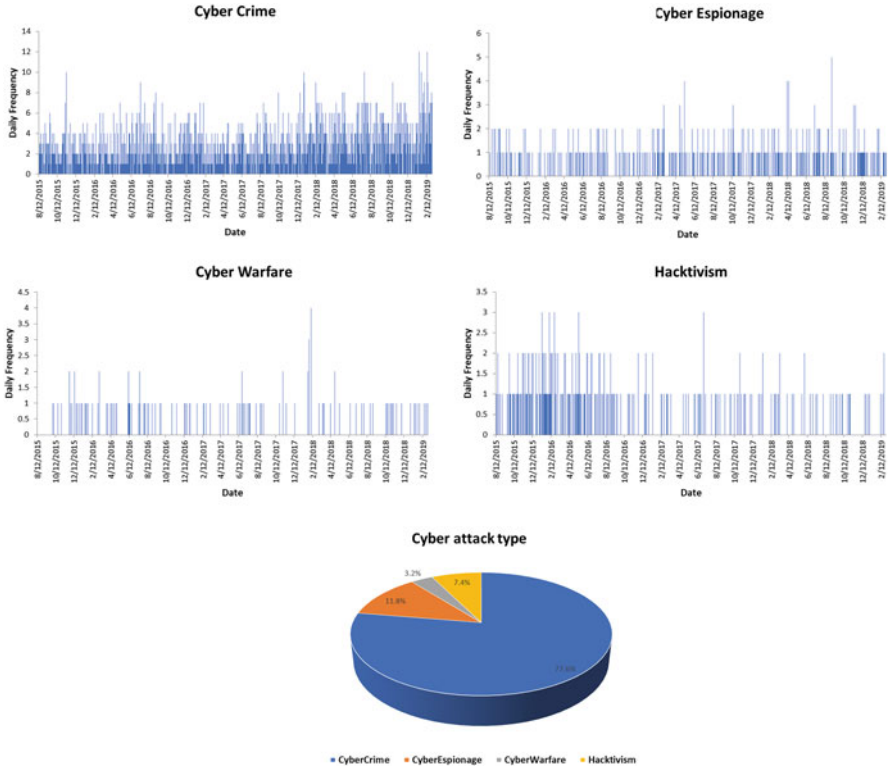


Fig. 14.3 Cyber-attacks by type. Source: own processings

3.3 Cyber Security

As our cyber security measure, we use the daily ISE (International Securities Exchange) Cyber Security Index from the Nasdaq Global Indexes available on the Bloomberg platform. The index started on 31 December 2010 with a base value of 100.00 and includes companies actively involved in providing cyber security technology and services. These must be a direct hardware/software developer or a service provider of cyber security with a minimum free float market capitalisation of $100 million and three-month average daily dollar trading volume of $1 million and also to be listed on an eligible exchange as of the reference dates (i.e., at the end of January, April, July and October each year) with securities seasoned at least three calendar months. The chosen index uses weights for the market capitalisations of the individual companies as well as their corresponding sector. Therefore, the index provides a benchmark for companies developing hardware and/or software, which protects access to files, websites and networks, both locally and from external origins, or companies that use these tools to provide consulting and/or cyber security services to their clients (Nasdaq Global Indexes, 2020). Throughout the analysis, we

assume that higher stock prices (i.e., ISE cyber security index) for cyber security firms indicate more customer satisfaction (Fornell et al., 2006) with their cyber security services providing stronger and/or wider cyber protection across sectors.

3.4 Control Variables

We use the daily liquidity (*Liq*) and change in global financial market uncertainty index (ΔVIX) as our financial market control variables. *Liq* is a percent-cost liquidity proxy, which is based on daily data measured using the following FHT (Fong, Holden and Trzcinka) method developed by Fong et al. (2017):

$$\text{FHT} \equiv S \equiv 2\sigma N^{-1}\left(\frac{1+z}{2}\right), \tag{14.5}$$

where

$$z \equiv \text{Zeros} \equiv \frac{\text{ZRD}}{\text{TD} + \text{NTD}}. \tag{14.6}$$

$$N\left(\frac{S}{2\sigma}\right) - N\left(\frac{-S}{2\sigma}\right) = z. \tag{14.7}$$

ZRD is the number of zero return days, TD is the number of trading days, and NTD is the number of no-trade days in a given month. Further, S is the percentage transaction cost, $N^{-1}()$ is the inverse of the cumulative normal distribution function, and σ is the standard deviation of the daily stock return over a month. Thus, Liq is the percent transaction cost S, which is an increasing function of zero returns and the volatility of the return distribution (Eq. 14.5) based on the theoretical probability of a zero return being in the middle region of returns assumed to be normally distributed with zero mean and variance σ^2 (Eq. 14.7) (Fong et al., 2017). The stock prices for our sample countries are collected from Bloomberg in daily frequency. *VIX* is the Chicago Board Options Exchange (CBOE) volatility index also collected from Bloomberg. We use the daily percentage change (Δ) of this index as our global financial market uncertainty control variable.

3.5 Summary Statistics

Table 14.1 shows summary statistics for the series being analysed, namely, cyber-attack target and types (Panel A), the financial market control variables (liquidity (*Liq*) and the change in global financial market uncertainty (ΔVIX) in Panel B), the cyber security index (*Cyber_Sec* in Panel B), and the logs of returns (R), realised return (*Mu*), realised volatility (RV), weighted realised covariance ($Rcov^{w}$), natural

Table 14.1 Data description

Variable	Description
Gov	Cyber-attacks targeting the government sector. It is set equal to 1 if this sector is targeted (which may happen multiple times per day) and 0 otherwise. We use the daily total as a measure of daily intensity.
Ind	Cyber-attacks targeting the industry sector. It is set equal to 1 if this sector is targeted (which may happen multiple times per day) and 0 otherwise. We use the daily total as a measure of daily intensity.
Fin	Cyber-attacks targeting the financial sector. It is set equal to 1 if this sector is targeted (which may happen multiple times per day) and 0 otherwise. We use the daily total as a measure of daily intensity.
Crypto	Cyber-attacks targeting the cryptocurrency exchange sector. It is set equal to 1 if this sector is targeted (which may happen multiple times per day) and 0 otherwise. We use the daily total as a measure of daily intensity.
CC	Cyber-attack type of cyber-crime. It is set equal to 1 if this sector is targeted (which may happen multiple times per day) and 0 otherwise. We use the daily total as a measure of daily intensity.
CE	Cyber-attack type of cyber espionage. It is set equal to 1 if this sector is targeted (which may happen multiple times per day) and 0 otherwise. We use the daily total as a measure of daily intensity.
CW	Cyber-attack type of cyber warfare. It is set equal to 1 if this sector is targeted (which may happen multiple times per day) and 0 otherwise. We use the daily total as a measure of daily intensity.
H	Cyber-attack type of hacktivism. It is set equal to 1 if this sector is targeted (which may happen multiple times per day) and 0 otherwise. We use the daily total as a measure of daily intensity.
US	Cyber-attack targeting the United States. It is set equal to 1 if this sector is targeted (which may happen multiple times per day) and 0 otherwise. We use the daily total as a measure of daily intensity.
Bit_R	Bitcoin log returns
Eth_R	Ethereum log returns
Lit_R	Litecoin log returns
Bit_Mu	Bitcoin realised returns
Eth_Mu	Ethereum realised returns
Lit_Mu	Litecoin realised returns
Bit_RV	Bitcoin realised volatility
Eth_RV	Ethereum realised volatility
Lit_RV	Litecoin realised volatility
Bit_V	Natural logarithm of Bitcoin volume
Eth_V	Natural logarithm of Ethereum volume
Lit_V	Natural logarithm of Litecoin volume
$Rcov^w$	Weighted realised covariance computed using Bitcoin, Ethereum and Litecoin.
Bit_RAR	Bitcoin risk-adjusted return ($= \frac{Bit\_Mu}{\sqrt{Rcov^w}}$)
Eth_RAR	Ethereum risk-adjusted return ($= \frac{Eth\_Mu}{\sqrt{Rcov^w}}$)
Lit_RAR	Litecoin risk-adjusted return ($= \frac{Lit\_Mu}{\sqrt{Rcov^w}}$)

(continued)

Table 14.1 (continued)

Variable	Description
Cyber_Sec	The ISE (International Securities Exchange) Cyber Security Index is our cyber security measure collected from Nasdaq Global Indexes through Bloomberg. We use the daily figure of this index, which comprises companies actively involved in providing cyber security technology and services. We assume that higher stock prices for the cyber security firms indicate more customer satisfaction (Fornell et al., 2006) with their cyber security services and stronger and/or wider cyber protections across sectors.
Liq	The liquidity measure computed using the stock index of the country hit by a cyber-attack. We use the average liquidity across the countries hit within the same day.
VIX	Chicago Board Options Exchange (CBOE) volatility index

Notes: The data cover the period from 12 August 2015 to 28 February 2019

logarithm of trading volume (V) and risk-adjusted return (RAR) of the three cryptocurrencies under investigation (Bitcoin (Panel C), Ethereum (Panel D) and Litecoin (Panel E)) in daily frequencies. In panel F, we show the 96 stock indices used to obtain our country-specific liquidity variables for which we calculate the daily average if they belong to the same cyber-attack incident hitting multiple countries at once. The control variables (Liq and ΔVIX) are lagged by one year to avoid hindsight bias. We winsorise all variables at the 1st and 99th percentiles.

In most cases, the distributions of cyber-attacks target and type data are positively skewed; the exception is cyber-crime (CC), which is negatively skewed. In other words, cyber-crime tends to occur very frequently on average relative to other types of cyber-attacks (CE, CW and H) or those targeting certain sectors (Gov, Ind, Fin and $Crypto$) or countries (US). We also find that in our sample liquidity, global financial market uncertainty (ΔVIX) and cyber security are positively skewed. Liq is a unit-less, non-negative measure (Fong et al., 2017), most of its summary statistics having an absolute value much smaller than 1%, unlike the dependent variables which instead exceed 1% in most cases. Therefore, we use the scaled Liq measure multiplied by 100. On the other hand, the $Cyber\_Sec$ measure is a relatively large, non-negative three-digit global index which we scale by dividing by 100. Finally, ΔVIX is the daily percentage change in the VIX index, which can be either positive or negative, with many absolute values larger than 1%, and it is not scaled.

We drop from the sample two cyber-attacks that targeted Belarus and Nepal since these two countries do not have an appropriate stock market index to calculate liquidity as above. Thus, we consider 96 countries market indices (Panel F) out of a total of 113 (Appendix 2) with overlapping or non-existing stock indices to calculate country-specific liquidity. We find that Bitcoin exhibits the largest trading volume (Bit_V) and risk-adjusted returns (Bit_RAR) and Litecoin the lowest (Lit_V and Lit_RAR). The composite risks for the three cryptocurrencies under investigation, measured by the square root of weighted realised covariance ($\sqrt{Rcov^w}$), are generally high, which results in a negatively skewed distribution.

Table 14.2 shows summary statistics for cyber-attack target and types (Panel A), the underlying liquidity, block chain's hash rate, global financial market uncertainty

Table 14.2 Summary statistics

Panel A: Cyber-attacks targets and types									
	Gov	*Ind*	*Fin*	*Crypto*	*CC*	*CE*	*CW*	*H*	*US*
Mean	0.47	0.88	0.19	0.08	2.67	0.40	0.10	0.25	1.31
Median	0	1	0	0	2	0	0	0	1
Std.	0.68	0.99	0.44	0.27	1.84	0.62	0.30	0.52	1.20
25th	0	0	0	0	1	0	0	0	0
75th	1	1	0	0	4	1	0	0	2
N	1156	1156	1156	1156	1156	1156	1156	1156	1156

Panel B: Liquidity, hash rate, global financial market uncertainty and investor protection			
	Liq	*ΔVIX*	*Cyber_Sec*
Mean	0.57%	0.0%	2.92
Median	0.51%	0.0%	2.81
Std.	0.25%	6.4%	0.55
25th	0.39%	−2.9%	2.50
75th	0.70%	2.0%	3.43
N	1148	1156	1156

Panel C: Bitcoin and $\sqrt{Rcov^w}$						
	Bit_R	*Bit_Mu*	$\sqrt{Bit\_RV}$	*Bit_V*	*Bit_RAR*	$\sqrt{Rcov^w}$
Mean	0.17%	0.19%	4.55%	17.02	6.14%	3.15%
Median	0.23%	0.18%	4.50%	17.13	6.00%	3.12%
Std.	3.67%	0.05%	0.23%	1.74	1.33%	0.44%
25th	−1.09%	0.15%	4.37%	15.45	5.10%	2.80%
75th	1.67%	0.24%	4.62%	18.42	7.02%	3.66%
N	1156	1156	1156	1156	1156	1156

Panel D: Ethereum					
	Eth_R	*Eth_Mu*	$\sqrt{Eth\_RV}$	*Eth_V*	*Eth_RAR*
Mean	0.33%	0.11%	9.12%	14.70	1.45%
Median	−0.05%	0.41%	8.21%	16.30	12.76%
Std.	6.71%	1.02%	2.30%	3.79	40.20%
25th	−2.87%	0.28%	7.74%	12.63	8.45%
75th	3.36%	0.56%	9.96%	17.73	17.38%
N	1156	1156	1156	1156	1156

Panel E: Litecoin					
	Lit_R	*Lit_Mu*	$\sqrt{Lit\_RV}$	*Lit_V*	*Lit_RAR*
Mean	0.14%	0.12%	9.57%	13.43	3.63%
Median	−0.08%	0.13%	9.12%	14.91	3.66%
Std.	5.38%	0.11%	1.17%	3.67	3.14%
25th	−2.13%	0.02%	8.91%	10.52	0.71%
75th	2.14%	0.22%	10.22%	16.32	6.85%
N	1156	1156	1156	1156	1156

Panel F: Countries and market indices	
Country	Market indices
Australia	S & P/ASX 200 INDEX

(continued)

Table 14.2 (continued)

Panel F: Countries and market indices	
Country	Market indices
Greece	Athex Composite Share Price Index
Barbados	Barbados Exchange Comp
Belgium	BEL 20 INDEX
Romania	BUCHAREST BET INDEX
Bahrain	BB ALL SHARE INDEX
Bosnia and Herzegovina	Bosnia BIRS Index
Lebanon	BLOM STOCK INDEX
Iran	TEHRAN STOCK EXCHANGE
Hungary	BUDAPEST STOCK EXCH INDX
Panama	Bolsa de Panama General
Colombia	COLOMBIA COLCAP INDEX
Costa Rica	BCT Corp Costa Rica Index
Sri Lanka	SRI LANKA COLOMBO ALL SH
Cambodia	Cambodia SE Comp Index
Cyprus	GENERAL MARKET INDEX CSE
Tanzania	Tanzania Share Index
United Arab Emirates	DFM GENERAL INDEX
Bangladesh	DSE Broad Index
Syrian Arab Republic	DSE Weighted Index
Ecuador	ECUINDEX
Egypt	EGX 30 INDEX
Malaysia	FTSE BURSA MAL TOP 100
Kenya	FTSE NSE Kenya 25
Namibia	NAMIBIA OVERALL INDEX
Italy	FTSE MIB INDEX
Spain	IBEX 35 INDEX
Iceland	OMX Iceland All-Share PR
Russian Federation	MOEX Russia Index
Chile	S & P/CLX IPSA (CLP) TR
Iraq	ISX GENERAL INDEX
South Africa	FTSE/JSE AFRICA ALL SHR
Indonesia	JAKARTA COMPOSITE INDEX
Jordan	AMMAN SE GENERAL INDEX
Pakistan	KARACHI 100 INDEX
Kuwait	KWSE All Share
Malta	MALTA STOCK EXCHANGE IND
Maldives	Maldives Stock Exch Indx
Argentina	S & P MERVAL TR ARS
Mongolia	MSE Top 20 Index
Oman	MSM30 Index
Nigeria	NIGERIA STCK EXC ALL SHR

(continued)

Table 14.2 (continued)

Panel F: Countries and market indices	
Country	Market indices
New Zealand	S & P NZX All Index
Philippines	PSEi—PHILIPPINE SE IDX
Palestine	PEX Genral Index
Puerto Rico	GDB PUERTO RICO STOCK IX
Portugal	PSI 20 INDEX
Rwanda	Rwanda St Ex Share Index
Slovakia	SLOVAK SHARE INDEX
Switzerland	SWISS MARKET INDEX
Fiji	SPSE Market Cap Wgt TR
European Union	Euro Stoxx 50 Pr
Estonia	OMX TALLINN OMXT
Trinidad and Tobago	TRINIDAD & TOBAGO CMPOSITE
Tunisia	Tunis SE TUNINDEX
Uganda	USE LSI Index
Virgin Islands	FTSE 100 INDEX
Lithuania	OMX VILNIUS OMXV
Vietnam	HO CHI MINH STOCK INDEX
Zimbabwe	Zimbabwe All Share Index
Austria	AUSTRIAN TRADED ATX INDX
Australia	S & P/ASX 200 INDEX
Brazil	BRAZIL IBOVESPA INDEX
Canada	S & P/TSX COMPOSITE INDEX
China	CSI 300 INDEX
Czech Republic	PRAGUE STOCK EXCH INDEX
Germany	DAX INDEX
Denmark	OMX COPENHAGEN 20 INDEX
Finland	OMX HELSINKI 25 INDEX
France	CAC 40 INDEX
Hong Kong	HANG SENG INDEX
Ireland	IRISH OVERALL INDEX
Israel	TA-125 Index
India	S & P BSE SENSEX INDEX
Italy	FTSE MIB INDEX
Japan	NIKKEI 225
Korea (South)	KOSPI INDEX
Kazakhstan	Kazakhstan KASE Stock Ex
Luxembourg	LUXEMBOURG LuxX INDEX
Montenegro	MONEX INDEX
Mexico	S & P/BMV IPC
Netherlands	AEX-Index
Norway	OBX STOCK INDEX

(continued)

Table 14.2 (continued)

Panel F: Countries and market indices	
Country	Market indices
Poland	WSE WIG INDEX
Qatar	QE Index
Russian Federation	MICEX INDEX
Saudi Arabia	TADAWUL ALL SHARE INDEX
Sweden	OMX STOCKHOLM 30 INDEX
Singapore	Straits Times Index STI
Thailand	STOCK EXCH OF THAI INDEX
Turkey	BIST 100 INDEX
Taiwan	TAIWAN TAIEX INDEX
Ukraine	PFTS Index
United Kingdom	FTSE 100 INDEX
United States of America	DOW JONES INDUS. AVG
Venezuela	VENEZUELA STOCK MKT INDX

and investor protection (Panel B), and three cryptocurrencies including Bitcoin, Ethereum and Litecoin where *Bit*, *Eth* and *Lit* denote Bitcoin (Panel C), Ethereum (Panel D) and Litecoin (Panel E), respectively. *_R*, *_Mu*, *_RV*, *_V* and *_RAR* stand for log return, realised return, realised volatility, natural logarithm of trading volume and risk-adjusted return for the daily cryptocurrency data in turn (e.g., *Bit_R* indicates log returns in the case of Bitcoin). $\sqrt{R\text{cov}^w}$ is the square root of weighted realised covariance computed using Bitcoin, Ethereum and Litecoin. The data for cyber-attacks, liquidity, hash rate and the five cryptocurrencies are daily and span the period from 12 August 2015 to 28 February 2019; they have been collected from http://www.hackmageddon.com, Bloomberg and www.CryptoDataDownload.com. The *Gov* (government sector), *Ind* (industry sector), *Fin* (financial sector), *Crypto* (cryptocurrency exchange) and *US* (United States) series are binary variables equal to one if the cyber-attack targets these sectors or country, and zero otherwise. The *CC* (cyber-crime), *CE* (cyber-espionage), *CW* (cyber-warfare) and *H* (hacktivism) and binary variables are equal to one if they match the cyber-attack type and zero otherwise. For all binary variables, we use the added-up figures per day as cyber-attacks may happen multiple times within a day. *Liq* is a liquidity measure computed using the stock index of the country hit by a cyber-attack. In the case of cyber-attacks targeting multiple countries, the average liquidity measure across those countries is used. ΔVIX is the Chicago Board Options Exchange (CBOE) volatility index in daily percentage change to proxy the uncertainty in the global financial market. *Cyber_Sec* is the cyber security index collected from Bloomberg. We winsorise all variables at the 1st and 99th percentiles. We report the mean, median, std. (standard deviation), 25th (25th percentile), 75th (75th percentile) and *N* (number of observations) of each variable, as well as the list of countries with the corresponding market indices included in our sample (Panel F).

3.6 Cyber-Attack Effects Associated with Cryptocurrencies and Cyber Security

We analyse the effect of cyber-attacks on the realised return (Mu_t), realised volatility (RV_t), trading volume (V_t) and risk-adjusted return (RAR_t) of cryptocurrencies and their relationship with cyber security ($Cyber\_Sec_t$). In particular, we analyse how cryptocurrencies are affected by cyber-attack targets (i.e., cryptocurrency exchange ($Cyber_{i,t}$), government ($Gov_{i,t}$), industry ($Ind_{i,t}$) and finance ($Fin_{i,t}$) sectors and US versus non-US countries (US_t)), types (i.e., cyber-crime ($CC_{i,t}$), cyber-espionage ($CE_{i,t}$), cyber-warfare ($CW_{i,t}$) and hacktivism ($H_{i,t}$)) and cyber security ($Cyber\_Sec_t$) whilst controlling for the change in global financial market uncertainty (ΔVIX_t) and stock market liquidity ($Liq_{i,t}$) in country i at day t allowing multiple cyber-attacks to occur on a single day. ΔVIX_t represent the global financial uncertainty control variables, and $Liq_{i,t}$ is the country-specific financial market control variable which we use the average value if there are multiple countries involved at day t. The cyber-attack target and types are binary variables equal to one if the cyber-attack matches a given type or target and zero otherwise. Our dataset includes multiple cyber-attack incidents within a single day. Therefore, we add up each of these binary variables within each day to obtain daily values which represent cyber-attack intensity measures without date overlaps. We estimate the following time series regression, where the $u_{i,t}$ is the error term and X denotes the realised return (Mu_t), realised volatility (RV_t), trading volume (V_t) and risk-adjusted return (RAR_t) of the three cryptocurrencies, Bitcoin (Bit), Ethereum (Eth) and Litecoin (Lit):

$$\begin{gathered} X_t = \beta_0 + \beta_1(Cyber\_Sec_t) + \beta_2\left(Crypto_{i,t}\right) + \beta_3(Gov_{i,t}) + \beta_4(Ind_{i,t}) + \beta_5(Fin_{i,t}) \\ + \beta_6(CC_{i,t}) + \beta_7(CE_{i,t}) + \beta_8(CW_{i,t}) + \beta_9(H_{i,t}) \\ + \beta_{10}\left(Crypto_{i,t} \times Cyber\_Sec_t\right) + \beta_{11}(Gov_{i,t} \times Cyber\_Sec_t) + \beta_{12}(Ind_{i,t} \times Cyber\_Sec_t) \\ + \beta_{13}(Fin_{i,t} \times Cyber\_Sec_t) + \beta_{14}(CC_{i,t} \times Cyber\_Sec_t) + \beta_{15}(CE_{i,t} \times Cyber\_Sec_t) \\ + \beta_{16}(CW_{i,t} \times Cyber\_Sec_t) + \beta_{17}(H_{i,t} \times Cyber\_Sec_t) + \beta_{18}(US_t) + \beta_{19}\left(Liq_{i,t}\right) + \beta_{20}(\Delta VIX_t) \\ + u_{i,t} \end{gathered} \tag{14.8}$$

4 Results and Discussions

Our aim is to analyse the effects of cyber-attacks on the risk-adjusted returns, realised volatility and trading volumes of three cryptocurrencies (Bitcoin, Ethereum and Litecoin) accounting for the cyber security level whilst controlling for the underlying country-specific stock market liquidity and global uncertainty measure. There is no multicollinearity among the regressors according to our Pearson correlation matrix (see Appendix 1).

4.1 Cyber-Attack Effects on the Realised Returns and Realised Volatilities of Cryptocurrencies and Cyber Security

The results in Tables 14.3 and 14.4 indicate that stronger cyber security leads in all cases to higher realised returns (*Bit_Mu*, *Eth_Mu*, *Lit_Mu*) and lower realised volatilities (or risk) (*Bit_RV*, *Eth_RV*, *Lit_RV*), though the size of these effects varies across the cryptocurrencies considered: Ethereum, which uses a smart contract platform, benefits the most (*Cyber_Sec* = 0.389, 0.39 (Table 14.3) and *Cyber_Sec* = −2.334, −2.34 (Table 14.4)), followed by Litecoin (*Cyber_Sec* = 0.134, 0.136 (Table 14.3) and *Cyber_Sec* = −1.358, −1.367 (Table 14.4)) and Bitcoin (*Cyber_Sec* = 0.055, 0.056 (Table 14.3) and *Cyber_Sec* = −0.118, −0.121 (Table 14.4)), the latter two both relying mainly on the blockchain itself. Table 14.3 also shows that Bitcoin and Litecoin overreact to cyber-attacks targeting cryptocurrency exchanges (*Crypto*) and industry sectors with cyber security protection (*Ind* × *Cyber_Sec*), which could be attributed to investors becoming more risk-loving and willing to take arbitrage opportunities to invest in cryptocurrencies in such cases. On the other hand, cyber-crime with cyber security (*CC*× *Cyber_Sec*) discourages Bitcoin and Litecoin investments by resulting in a higher degree of risk aversion and lower realised returns. In the case of the cyber-attacks targeting the USA, Bitcoin realised returns are most negatively affected, which suggests that Bitcoin investors become more risk-averse. By contrast, there is no effect on Ethereum realised returns. When cyber-attacks hit the government sector (*Gov*), risk decreases in the case of Bitcoin, which possibly reflects heightened national security. Hacktivism (*H*) is the most significant variable increasing risks for all three cryptocurrencies considered. This is plausible as Android Trojans (which run on the Android operating system as games, system updates or utilities)[4] can make attacks from hackers more effective by identifying crypto wallet owners and giving access to their wallets. Therefore, cryptocurrencies are likely to be the main target for hackers specialising in web-based attacks (Group-IB, 2017). We also find that an increase in stock market liquidity (*Liq*) reduces realised returns: As the stock market becomes attractive to investors because of its higher liquidity, they become less interested in investing in cryptocurrencies, whose realised returns then decrease—in other words, investors regard stock and cryptocurrency markets and substitutes.

Table 14.3 presents the time series regression results using the cryptocurrencies' realised returns (*Bit_Mu*, *Eth_Mu*, *Lit_Mu*) as dependent variables affected by cyber security (*Cyber_Sec*) considering cyber-attack target sectors (*Gov, Ind, Fin, Crypto*), types (*CC, CE, CW, H*) and US target (*US*) and controlling for global financial market uncertainty change (ΔVIX) and country specific stock market liquidity (*Liq*). We report the *F*-statistics, adjusted R^2 and number of observations (*N*). The standard

[4] https://www.f-secure.com/en (Accessed 6 January 2021).

Table 14.3 Effects of cyber-attacks on cryptocurrency realised returns

	Bit_Mu (1)		*Eth_Mu* (2)		*Lit_Mu* (3)	
Intercept	0.068*** (0.008)	0.233*** (0.004)	−0.296* (0.179)	0.912*** (0.085)	−0.225*** (0.014)	0.172*** (0.007)
Cyber_Sec	0.055*** (0.002)	0.056*** (0.002)	0.389*** (0.056)	0.39*** (0.057)	0.134*** (0.005)	0.136*** (0.004)
Crypto	0.014*** (0.005)	0.016*** (0.005)	0.173 (0.108)	0.214* (0.119)	0.024*** (0.009)	0.031*** (0.009)
Gov	−0.001 (0.002)	−0.001 (0.002)	−0.03 (0.047)	−0.022 (0.047)	−0.003 (0.004)	−0.003 (0.004)
Ind	0.001 (0.002)	0 (0.002)	−0.032 (0.035)	−0.025 (0.035)	0 (0.003)	−0.001 (0.003)
Fin	0.001 (0.003)	0.001 (0.003)	0.055 (0.067)	0.055 (0.068)	0.003 (0.005)	0.003 (0.005)
CC	0.001 (0.001)	0.002** (0.001)	0.026 (0.023)	0.028 (0.024)	0 (0.002)	0.003 (0.002)
CE	0.002 (0.002)	0.003 (0.002)	0.023 (0.049)	0.019 (0.049)	0.004 (0.004)	0.006 (0.004)
CW	−0.002 (0.004)	−0.001 (0.004)	0.121 (0.094)	0.104 (0.095)	−0.002 (0.008)	−0.002 (0.007)
H	−0.002 (0.003)	−0.002 (0.003)	−0.047 (0.059)	−0.128* (0.067)	−0.004 (0.005)	−0.003 (0.005)
Crypto × *Cyber_Sec*		−0.012 (0.008)		−0.237 (0.192)		−0.03** (0.015)
Gov × *Cyber_Sec*		0.001 (0.004)		0.074 (0.088)		0.004 (0.007)
Ind × *Cyber_Sec*		0.007*** (0.003)		0.017 (0.059)		0.012*** (0.005)
Fin × *Cyber_Sec*		0.002 (0.005)		−0.098 (0.115)		0 (0.009)
CC× *Cyber_Sec*		−0.008*** (0.001)		−0.024 (0.034)		−0.013*** (0.003)
CE× *Cyber_Sec*		−0.003 (0.004)		−0.031 (0.091)		−0.007 (0.007)
CW× *Cyber_Sec*		−0.007 (0.007)		−0.14 (0.169)		−0.01 (0.013)
H× *Cyber_Sec*		0 (0.005)		−0.278** (0.119)		−0.001 (0.009)
US	−0.003** (0.001)	−0.004*** (0.001)	−0.013 (0.031)	−0.02 (0.031)	−0.004 (0.002)	−0.005* (0.002)
Liq	−0.057*** (0.005)	−0.054*** (0.005)	−1.353*** (0.112)	−1.368*** (0.113)	−0.072*** (0.009)	−0.067*** (0.009)

(continued)

Table 14.3 (continued)

	Bit_Mu (1)		*Eth_Mu* (2)		*Lit_Mu* (3)	
ΔVIX	0 (0)	0 (0)	−0.004 (0.004)	−0.004 (0.004)	0 (0)	0 (0)
Adjusted R^2	0.43	0.44	0.17	0.17	0.52	0.53
F-stats	72.67***	46.79***	20.93***	13.06***	105.4***	66.58***
N	1148	1148	1148	1148	1148	1148

errors are in the brackets. ***, ** and * denote significance at the 1%, 5% and 10% levels, respectively.

Table 14.4 presents the time series regression results using the cryptocurrencies' realised volatilities (*Bit_RV*, *Eth_RV*, *Lit_RV*) as dependent variables affected by cyber security (*Cyber_Sec*) considering cyber-attack target sectors (*Gov, Ind, Fin, Crypto*), types (*CC, CE, CW, H*) and US target (*US*) and controlling for global financial market uncertainty change (*ΔVIX*) and country specific stock market liquidity (*Liq*). We report the *F*-statistics, adjusted R^2 and number of observations (*N*). The standard errors are in the brackets. ***, ** and * denote significance at the 1%, 5% and 10% levels, respectively.

4.2 Cyber-Attack Effects on the Trading Volumes of Cryptocurrencies and Cyber Security

The evidence in Table 14.5 implies that stronger cyber security (*Cyber_Sec*) increases trading volumes (*Bit_V*, *Eth_V*, *Lit_V*), presumably by creating a safer financial environment and making investors more confident. Again it is Ethereum which benefits the most from enhanced cyber security (*Cyber_Sec* = 0.757, 1.005), followed by Litecoin (*Cyber_Sec* = 0.591, 0.842) and Bitcoin (*Cyber_Sec* = 0.419, 0.498)—it is therefore the cryptocurrency for which stronger cyber security has the most beneficial effects in every respect, namely, in terms of realised returns, risks and trading volumes. Investor confidence resulting from cyber security is undermined in all cases by cyber-attacks hitting the cryptocurrency exchanges (*Crypto* × *Cyber_Sec*), especially by cyber-crime (*Crypto* × *CC*) and cyber warfare (*Crypto* × *CW*), whilst Hacking (*H*) only affects Ethereum negatively. By contrast, cyber-attacks hitting the industry sector in the presence of strong cyber security (*Ind* × *Cyber_Sec*) lead to overreactions and more arbitrage trading. Finally, higher stock market liquidity (*Liq*) reduces trading volumes, which confirms that investors regard stock and cryptocurrency investments as substitutes as previously found.

Table 14.5 presents the time series regression results using the cryptocurrencies' trading volumes (*Bit_V*, *Eth_V*, *Lit_V*) as dependent variables affected by cyber security (*Cyber_Sec*) considering cyber-attack target sectors (*Gov, Ind, Fin, Crypto*), types (*CC, CE, CW, H*) and US target (*US*) and controlling for global financial

Table 14.4 Effects of cyber-attacks on cryptocurrency realised volatilities

	Bit_RV (1)		*Eth_RV* (2)		*Lit_RV* (3)	
Intercept	4.624*** (0.035)	4.277*** (0.017)	14.512*** (0.338)	7.623*** (0.161)	12.8*** (0.155)	8.84*** (0.074)
Cyber_Sec	– 0.118*** (0.011)	– 0.121*** (0.011)	– 2.334*** (0.106)	– 2.34*** (0.107)	– 1.358*** (0.049)	– 1.367*** (0.049)
Crypto	0.004 (0.021)	−0.009 (0.023)	−0.183 (0.203)	−0.289 (0.224)	−0.017 (0.093)	−0.07 (0.103)
Gov	−0.02** (0.009)	−0.022** (0.009)	−0.092 (0.089)	−0.11 (0.089)	−0.05 (0.041)	−0.056 (0.041)
Ind	0.007 (0.007)	0.01 (0.007)	0.048 (0.065)	0.047 (0.066)	0.022 (0.03)	0.029 (0.03)
Fin	0 (0.013)	−0.005 (0.013)	−0.109 (0.126)	−0.132 (0.128)	−0.013 (0.058)	−0.026 (0.059)
CC	−0.002 (0.005)	−0.006 (0.005)	−0.017 (0.044)	−0.025 (0.046)	−0.003 (0.02)	−0.014 (0.021)
CE	−0.004 (0.01)	−0.007 (0.01)	0.012 (0.092)	0.011 (0.093)	−0.005 (0.042)	−0.015 (0.043)
CW	0.002 (0.018)	−0.002 (0.018)	−0.15 (0.177)	−0.127 (0.178)	−0.069 (0.081)	−0.069 (0.082)
H	0.055*** (0.012)	0.045*** (0.013)	0.196* (0.111)	0.299** (0.127)	0.202*** (0.051)	0.203*** (0.058)
Crypto × *Cyber_Sec*		0.049 (0.037)		0.496 (0.362)		0.232 (0.166)
Gov × *Cyber_Sec*		0.032 (0.017)		0.108 (0.166)		0.079 (0.076)
Ind × *Cyber_Sec*		−0.012 (0.012)		−0.063 (0.112)		−0.022 (0.051)
Fin × *Cyber_Sec*		0.031 (0.022)		0.271 (0.216)		0.115 (0.099)
CC× *Cyber_Sec*		0.012* (0.007)		0.054 (0.064)		0.041 (0.029)
CE× *Cyber_Sec*		0.021 (0.018)		0.026 (0.172)		0.08 (0.079)
CW× *Cyber_Sec*		−0.05 (0.033)		0.062 (0.318)		0.029 (0.146)
H× *Cyber_Sec*		−0.04* (0.023)		0.278 (0.224)		−0.024 (0.103)
US	0.011* (0.006)	0.011* (0.006)	0.071 (0.058)	0.076 (0.059)	0.023 (0.027)	0.026 (0.027)
Liq	0.444*** (0.022)	0.437*** (0.022)	2.427*** (0.211)	2.429*** (0.214)	1.2*** (0.097)	1.182*** (0.098)
ΔVIX	0.001 (0.001)	0.001 (0.001)	0.004 (0.008)	0.004 (0.008)	0 (0.004)	0 (0.004)
Adjusted R^2	0.37	0.38	0.41	0.41	0.53	0.53
F-stats	57.17***	36.02***	68.66***	41.64***	107.2***	65.13***
N	1148	1148	1148	1148	1148	1148

Table 14.5 Effects of cyber-attacks on cryptocurrency trading volumes

	Bit_V (1)		*Eth_V* (2)		*Lit_V* (3)	
Intercept	11.259*** (0.242)	17.562*** (0.113)	4.09*** (0.499)	17.01*** (0.235)	1.04** (0.496)	14.459*** (0.234)
Cyber_Sec	2.084*** (0.076)	2.122*** (0.075)	4.358*** (0.157)	4.415*** (0.156)	4.526*** (0.156)	4.605*** (0.155)
Crypto	0.419*** (0.145)	0.498*** (0.158)	0.757** (0.299)	1.005*** (0.328)	0.591** (0.298)	0.842*** (0.326)
Gov	−0.086 (0.063)	−0.091 (0.063)	−0.061 (0.131)	−0.046 (0.13)	−0.14 (0.13)	−0.139 (0.13)
Ind	0.022 (0.047)	0.005 (0.047)	−0.103 (0.096)	−0.14 (0.097)	−0.027 (0.096)	−0.078 (0.096)
Fin	0.056 (0.09)	0.029 (0.09)	0.063 (0.185)	0.043 (0.188)	0.028 (0.185)	0.015 (0.186)
CC	0.039 (0.031)	0.081** (0.032)	0.062 (0.064)	0.134** (0.067)	0.049 (0.064)	0.129* (0.066)
CE	0.111* (0.066)	0.126* (0.066)	0.207 (0.136)	0.243* (0.136)	0.149 (0.135)	0.187 (0.135)
CW	−0.025 (0.126)	−0.032 (0.126)	−0.118 (0.261)	−0.108 (0.261)	−0.216 (0.26)	−0.197 (0.259)
H	0.017 (0.079)	−0.035 (0.09)	− 0.436*** (0.163)	− 0.551*** (0.186)	−0.135 (0.162)	−0.142 (0.185)
Crypto × *Cyber_Sec*		−0.476* (0.255)		− 1.168** (0.53)		−1.151** (0.526)
Gov × *Cyber_Sec*		0.22* (0.117)		0.251 (0.243)		0.306 (0.242)
Ind × *Cyber_Sec*		0.178** (0.079)		0.405** (0.163)		0.441*** (0.162)
Fin × *Cyber_Sec*		0.131 (0.152)		−0.058 (0.316)		0.02 (0.314)
CC× *Cyber_Sec*		− 0.237*** (0.045)		− 0.381*** (0.094)		− 0.428*** (0.094)
CE× *Cyber_Sec*		0.023 (0.121)		−0.389 (0.251)		−0.204 (0.249)
CW× *Cyber_Sec*		−0.513** (0.224)		−0.173 (0.465)		−0.413 (0.462)
H× *Cyber_Sec*		−0.273* (0.158)		−0.507 (0.328)		−0.152 (0.326)
US	−0.054 (0.042)	−0.077* (0.042)	−0.038 (0.086)	−0.073 (0.086)	−0.077 (0.086)	−0.11 (0.086)
Liq	− 0.745*** (0.151)	− 0.675*** (0.151)	− 3.789*** (0.311)	− 3.689*** (0.312)	− 1.453*** (0.31)	− 1.286*** (0.31)

(continued)

Table 14.5 (continued)

	Bit_V (1)		*Eth_V* (2)		*Lit_V* (3)	
ΔVIX	0.006 (0.006)	0.006 (0.006)	−0.003 (0.012)	−0.003 (0.012)	0.014 (0.012)	0.014 (0.012)
Adjusted R^2	0.48	0.49	0.53	0.54	0.50	0.51
F-stats	89.19***	57.04***	108.8***	67.94***	97.56***	61.39***
N	1148	1148	1148	1148	1148	1148

market uncertainty change (ΔVIX) and country-specific stock market liquidity (*Liq*). We report the *F*-statistics, adjusted R^2 and number of observations (*N*). The standard errors are in the brackets. ***, ** and * denote significance at the 1%, 5% and 10% levels, respectively.

4.3 Cyber-Attack Effects on the Risk-Adjusted Returns of Cryptocurrencies and Cyber Security

Table 14.6 suggests that stronger cyber security (*Cyber_Sec*) also increases risk-adjusted returns (*Bit_RAR*, *Eth_RAR*, *Lit_RAR*); in this case, the beneficial impact on Ethereum is even stronger (*Cyber_Sec* = 11.83, 11.879) relative to Litecoin (*Cyber_Sec* = 3.489, 3.565) and Bitcoin (*Cyber_Sec* = 0.581, 0.624). Again investors in the latter two cryptocurrencies overreact to cyber-attacks hitting cryptocurrency exchanges (*Crypto*) whilst Ethereum investors do not. Instead, hacktivism (*H*) significantly reduces the risk-adjusted returns in the case of Ethereum even in the presence of enhanced cyber security (*H* × *Cyber_Sec*). On the other hand, in the case of Bitcoin and Litecoin, cyber-crime has a bigger negative impact on risk-adjusted returns, especially when cyber security is present (*CC* × *Cyber_Sec*). Cyber-attacks hitting the USA are again most damaging for Bitcoin, which confirms that Bitcoin investors become risk-averse in such an event as already found for realised returns.

Stock market liquidity (*Liq*) also tends to reduce the risk-adjusted returns of the cryptocurrencies under investigation. In a previous study, Wei (2018) showed that in the case of cryptocurrencies, more liquidity decreases volatility as market efficiency improves. As already mentioned, our findings suggest that stock investors regard stock and cryptocurrency markets as substitutes: As active cryptocurrency traders become less likely to arbitrage any signs of return predictabilities in less liquid cryptocurrency markets relative to stock markets (Wei, 2018), the liquidity risk increases in cryptocurrency markets and so does volatility (Table 14.4), whilst trading volumes decrease (Table 14.5), which leads to lower risk-adjusted returns, consistently with our previous findings.

Table 14.6 Effects of cyber-attacks on cryptocurrency risk-adjusted returns

	Bit_RAR (1)		*Eth_RAR* (2)		*Lit_RAR* (3)	
Intercept	5.902*** (0.216)	7.688*** (0.101)	−6.149 (7.169)	31.626*** (3.41)	−4.876*** (0.446)	5.454*** (0.21)
Cyber_Sec	0.581*** (0.068)	0.624*** (0.067)	11.83*** (2.251)	11.879*** (2.266)	3.489*** (0.14)	3.565*** (0.139)
Crypto	0.317** (0.13)	0.39*** (0.141)	5.587 (4.304)	6.769 (4.756)	0.699*** (0.268)	0.919*** (0.293)
Gov	0.063 (0.057)	0.06 (0.056)	−1.858 (1.882)	−1.583 (1.89)	−0.069 (0.117)	−0.067 (0.116)
Ind	0.026 (0.042)	−0.013** (0.042)	−1.576 (1.387)	−1.316 (1.406)	0.007 (0.086)	−0.049 (0.087)
Fin	−0.006 (0.08)	−0.001 (0.081)	1.887 (2.666)	1.761 (2.721)	0.053 (0.166)	0.052 (0.167)
CC	−0.003 (0.028)	0.045 (0.029)	1.37 (0.924)	1.502 (0.966)	−0.005 (0.057)	0.077 (0.059)
CE	0.046 (0.059)	0.079 (0.058)	1.389 (1.958)	1.271 (1.97)	0.132 (0.122)	0.18 (0.121)
CW	−0.098 (0.113)	−0.069 (0.112)	5.214 (3.753)	4.655 (3.782)	−0.042 (0.234)	−0.008 (0.233)
H	−0.159** (0.071)	−0.074 (0.08)	−2.132 (2.347)	−5.316** (2.694)	−0.162 (0.146)	−0.11 (0.166)
Crypto × *Cyber_Sec*		−0.314 (0.228)		−7.795 (7.682)		−0.984** (0.473)
Gov × *Cyber_Sec*		−0.096 (0.105)		3.845 (3.53)		0.088 (0.217)
Ind × *Cyber_Sec*		0.18 (0.07)		0.937 (2.367)		0.361** (0.146)
Fin × *Cyber_Sec*		0.021 (0.136)		−3.355 (4.586)		−0.02 (0.282)
CC× *Cyber_Sec*		−0.213*** (0.04)		−1.204 (1.365)		−0.396*** (0.084)
CE× *Cyber_Sec*		−0.103 (0.108)		−1.796 (3.637)		−0.252 (0.224)
CW× *Cyber_Sec*		−0.03 (0.2)		−5.641 (6.743)		−0.196 (0.415)
H× *Cyber_Sec*		0.263* (0.141)		−11.433** (4.756)		0.089 (0.293)
US	−0.104*** (0.037)	−0.115*** (0.037)	−0.615 (1.24)	−0.934 (1.253)	−0.115 (0.077)	−0.143* (0.077)

(continued)

Table 14.6 (continued)

	Bit_RAR (1)		*Eth_RAR* (2)		*Lit_RAR* (3)	
Liq	– 2.387*** (0.135)	– 2.285*** (0.134)	– 50.854*** (4.475)	– 51.446*** (4.528)	– 2.763*** (0.279)	– 2.598*** (0.279)
ΔVIX	−0.003 (0.005)	−0.003 (0.005)	−0.073 (0.173)	−0.07 (0.173)	0.002 (0.011)	0.002 (0.011)
Adjusted R^2	0.29	0.32	0.14	0.15	0.45	0.47
F-stats	40.18***	27.5***	17.06***	10.73***	80.38***	51.24***
N	1148	1148	1148	1148	1148	1148

Table 14.6 presents the time series regression results using the cryptocurrencies risk-adjusted returns (*Bit_RAR*, *Eth_RAR*, *Lit_RAR*) and realised covariance ($\sqrt{R\text{cov}^w}$) as dependent variables affected by cyber security (*Cyber_Sec*) considering cyber-attack target sectors (*Gov, Ind, Fin, Crypto*), types (*CC, CE, CW, H*) and US target (*US*) and controlling for global financial market uncertainty change (ΔVIX) and country-specific stock market liquidity (*Liq*). We report the *F*-statistics, adjusted R^2 and number of observations (*N*). The standard errors are in the brackets. ***, ** and * denote significance at the 1%, 5% and 10% levels, respectively.

On the whole, our results corroborate those of van Hardeveld et al. (2017) and thus confirm the key importance of designing appropriate strategies to enhance cyber security.

5 Conclusions

This chapter sheds new light on the effects of cyber-attacks and cyber security on three cryptocurrencies (Bitcoin, Ethereum and Litecoin). It considers four different types of cyber-attacks (cyber-crime, cyber-espionage, hacktivism and cyber-warfare) as well as four target sectors (cryptocurrency exchange, government, industry and finance). The cyber-attacks data are collected from Hackmageddon (http://www.hackmageddon.com), and realised returns, realised volatilities, trading volumes and risk-adjusted returns of the cryptocurrencies under investigation are used for the analysis. The risk-adjusted returns are calculated using the realised return and weighted realised covariance as measures of return and risk, respectively.

Our findings suggest that stronger cyber security is effective in increasing (decreasing) realised and risk-adjusted returns (risk) of the cryptocurrencies under examination, even in the presence of cyber-attacks. Cyber security also creates a safer digital environment, which encourages investors to increase their cryptocurrency trading volumes. Ethereum benefits the most (in terms of realised returns, risk-adjusted returns, risks and trading volumes) from cyber security. When cyber-attacks hit the cryptocurrency exchanges and industry sector, cryptocurrency

(Bitcoin and Litecoin) investors become risk-loving arbitragers and overreact; stronger cyber security attenuates (intensifies) the effects of such attacks on the former (latter) sector. On the other hand, Bitcoin investors in particular become risk-averse when cyber-attacks hit the US government sector. Hacktivism appears to be the most significant threat to all three cryptocurrencies in terms of the associated risks. On the whole, the evidence provided in this study represents useful information for the cryptocurrency investing community, cyber law enforcement agents, cyber-crime investigation units, policy makers, regulators and other practitioners in addition to the academic community. In particular, it confirms the key role of policy makers in creating an effective cyber security framework to ensure a smooth functioning of the cryptocurrency markets even in the presence of cyber-attacks and thus facilitate trading regardless of the risk profile of investors. It should be acknowledged, though, that our analysis has some limitations; specifically, future work should also consider alternative model specifications, such as vector autoregressions and multivariate GARCH models, with the aim of checking the robustness of our findings to the use of different methodologies.

Appendices

Appendix 1: Variable Correlations

The following table presents the Pearson's correlation matrix for the variables in our sample. *** stands for significance at the 1% level, ** at the 5% significance level and * at the 10% level

	(a)	(b)	(c)	(d)	(e)	(f)	(g)	(h)	(i)	(j)	(k)	(l)
Gov (a)	1.00***											
Ind (b)	−0.01	1.00***										
Fin (c)	−0.05*	0.03	1.00***									
Crypto (d)	−0.03	−0.10***	−0.03	1.00***								
CC (e)	0.16***	0.48***	0.29***	0.10***	1.00***							
CE (f)	0.33***	0.12***	−0.01	0.04	0.10***	1.00***						
CW (g)	0.15***	0.08**	0.03	0.01	0.02	−0.01	1.00***					
H (h)	0.19***	0.02	0.00	−0.04	−0.12***	−0.10***	0.01	1.00***				
US (i)	0.23***	0.43***	0.11***	−0.05	0.60***	0.15***	0.05*	0.01	1.00***			
Liq (j)	0.04	−0.04	0.01	−0.02	0.01	0.01	−0.02	0.15***	−0.09***	1.00***		
VIX (k)	0.01	−0.07**	−0.05	0.04	−0.06**	0.03	0.01	−0.03	−0.12***	−0.03	1.00***	
Cyber_sec (l)	0.03	0.00	0.09***	0.14***	0.29***	0.12***	−0.04	−0.27***	0.02	−0.04	−0.01	1.00***

Appendix 2: Cyber-Attack Target Country and Count

Cyber-attack target country	Cyber-attack count
United States of America	1519
More than one country	930
United Kingdom	231
Unknown	102
India	92
Canada	84
Russian Federation	76
Australia	65
Italy	65
Korea (South)	58
Japan	54
France	44
China	41
Germany	37
Ukraine	36
Brazil	35
Israel	29
Netherlands	28
Thailand	22
Turkey	22
Ireland	21
South Africa	21
Hong Kong	20
Pakistan	20
Sweden	18
Iran	17
Saudi Arabia	17
Switzerland	16
New Zealand	16
United Arab Emirates	15
Singapore	14
Spain	13
Mexico	13
Philippines	12
Taiwan	12
Austria	9
Belgium	9
Norway	9
Azerbaijan	8
Czech Republic	8
Denmark	8

(continued)

Appendix 2: (continued)

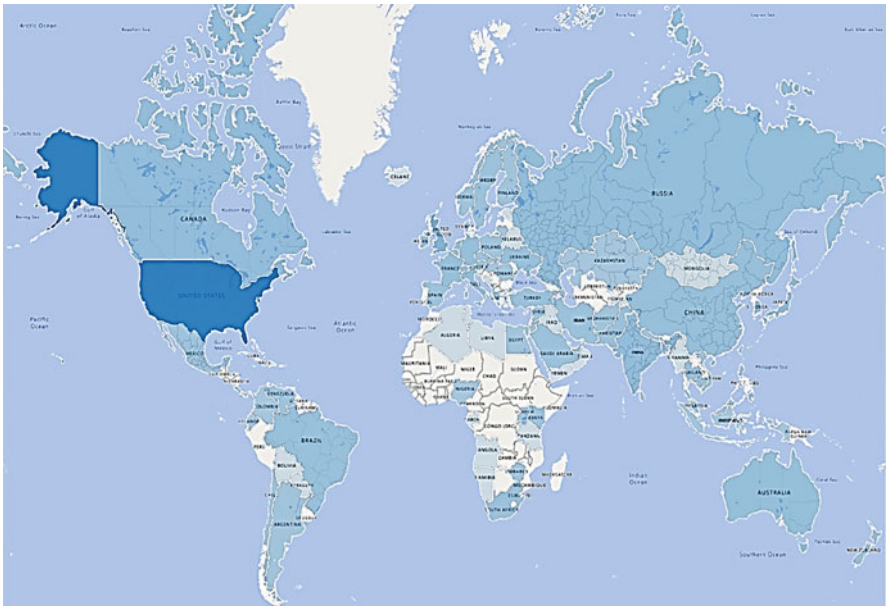
Cyber-attack target country	Cyber-attack count
Kenya	8
Poland	8
Venezuela	8
Greece	7
Malaysia	7
Vietnam	7
Armenia	6
Bangladesh	6
European Union	6
Chile	5
Finland	5
Panama	5
Syrian Arab Republic	5
Afghanistan	4
Argentina	4
Cyprus	4
Cambodia	4
Korea (North)	4
Malta	4
Qatar	4
Zimbabwe	4
Egypt	3
Lebanon	3
Sri Lanka	3
Luxembourg	3
Montenegro	3
Nepal	3
Romania	3
Slovakia	3
Albania	2
Barbados	2
Cocos (Keeling) Islands	2
Colombia	2
Costa Rica	2
Ecuador	2
Hungary	2
Indonesia	2
Jordan	2
Kuwait	2
Cayman Islands	2
Kazakhstan	2
Lithuania	2
Nigeria	2

(continued)

Appendix 2: (continued)

Cyber-attack target country	Cyber-attack count
Palestine	2
Uganda	2
Angola	1
Bosnia and Herzegovina	1
Bahrain	1
Bolivia	1
Bahamas	1
Belarus	1
Dominican Republic	1
Algeria	1
Estonia	1
Fiji	1
Gabon	1
Guernsey	1
Guam	1
Iraq	1
Iceland	1
Libya	1
Myanmar	1
Mongolia	1
Maldives	1
Namibia	1
Oman	1
Puerto Rico	1
Paraguay	1
Rwanda	1
Tajikistan	1
Tunisia	1
Trinidad and Tobago	1
Tanzania	1
Virgin Islands	1
Yemen	1

Appendix 3: Visualisation of Cyber-Attacks Across the Globe



References

Alexander, C., & Dakos, M. (2020). A critical investigation of cryptocurrency data and analysis. *Quantitative Finance, 20*(2), 173–188.

An, J., Duan, T., Hou, W., & Liu, X. (2021). Cyber risks and initial coin offerings: Evidence from the world. *Finance Research Letters, 41*, 1–8.

BBC News. (2021). *Tesla investigates claims of crypto-currency hack*. Retrieved September 14, from https://www.bbc.com/news/technology-43140005

Benjamin, V., Valacich, J. S., & Chen, H. (2019). DICE-E: A framework for conducting Darknet identification, collection, evaluation with ethics. *MIS Quarterly, 43*(1), 1–22.

Bodford, J. E., & Kwan, V. S. Y. (2018). A game theoretical approach to hacktivism: Is attack likelihood a product of risks and payoffs? *Cyberpsychology, Behavior and Social Networking, 21*(2), 73–77.

Bouri, E., Gupta, R., Tiwari, A., & Roubaud, D. (2017a). Does bitcoin hedge global uncertainty? Evidence from wavelet-based quantile-in-quantile regressions. *Finance Research Letters, 23*, 87–95.

Bouri, E., Molnár, P., Azzi, G., Roubaud, D., & Hagfors, L. I. (2017b). On the hedge and safe haven properties of bitcoin: Is it really more than a diversifier? *Finance Research Letters, 20*, 192–198.

Bouveret, A. (2018). *Cyber risk for the financial sector: A framework for quantitative assessment, IMF Working Paper no. 18/143*.

Caporale, G. M., Kang, W.-Y., Spagnolo, F., & Spagnolo, N. (2019). Non-linearities, cyber attacks and cryptocurrencies. *Finance Research Letters, 7692*, 1–10.

Caporale, G. M., Kang, W.-Y., Spagnolo, F., & Spagnolo, N. (2021). Cyber-attacks, spillovers and contagion in the cryptocurrency markets'. *Journal of International Financial Markets, Institutions and Money, 2021*, 1–19.

Chen, M. A., Wu, Q., & Yang, B. (2019). How valuable is FinTech innovation? *The Review of Financial Studies, 32*(5), 2062–2106.

Corbet, S., Lucey, B., Urquhart, A., & Yarovaya, L. (2019a). Cryptocurrencies as a financial asset: A systematic analysis. *International Review of Financial Analysis, 62*(C), 182–199.

Corbet, S., Cumming, D. J., Lucey, B. M., Peat, M., & Vigne, S. A. (2019b). *Investigating the dynamics between price volatility, price discovery, and criminality in cryptocurrency markets*. Retrieved from SSRN https://ssrn.com/abstract=3384707

Despotović, A., Parmaković, A., & Miljković, M. (2023). Cybercrime and cyber security in Fintech. In S. Benković, A. Labus, & M. Milosavljević (Eds.), *Digital transformation of the financial industry. Contributions to finance and accounting*. Springer. https://doi.org/10.1007/978-3-031-23,269-5_15

Fong, K. Y. L., Holden, C. W., & Trzcinka, C. A. (2017). What are the best liquidity proxies for global research? *Review of Finance, 21*(4), 1355–1401.

Fornell, C., Mithas, S., Morgeson, F. V., & Krishnan, M. S. (2006). Customer satisfaction and stock prices: High returns, low risk. *Journal of Marketing., 70*(1), 3–14.

Goldstein, I., Jiang, W., & Karolyi, G. A. (2019). To FinTech and beyond. *The Review of Financial Studies, 32*(5), 1647–1661.

Graham, L. (2017). *Cybercrime costs the global economy $450 billion: CEO, CNBC*. Retrieved from http://www.cnbc.com/2017/02/07/cybercrime-costs-the-global economy-450-billion-ceo.html

Group-IB. (2017). *Hi-Tech crime trends 2017*. Retrieved January 6, 2021, from https://www.group-ib.com/resources/threat-research/2017-report.html

Hileman, G., & Rauchs, M. (2017). *Global cryptocurrency benchmarking study*. Cambridge Centre for Alternative Finance, Judge Business School, University of Cambridge.

Konowicz, D.R. (2018). *The new game: Cryptocurrency challenges US Economic Sanctions.* Faculty of the United States Naval War College.

Kopp, E., Kaffenberger, L., & Wilson, C. (2017). *Cyber risk, market failures, and financial stability, IMF Working Paper no. 17/185*.

Liu, Y., & Tsyvinski, A. (2018). *Risks and returns of cryptocurrency, NBER Working Paper No. 24877*, pp. 1–25.

Martin, J. (2014). Lost on the Silk Road: online drug distribution and the cryptomarket. *Criminology and Criminal Justice, 14*(3), 351–367.

Martin, J., & Christin, N. (2016). Ethics in cryptocurrency research. *International Journal of Drug Policy, 35*, 84–91.

Nasdaq Global Indexes. (2020), *ISE cyber security index (HXR) methodology*. Retrieved January 5, 2021, from https://indexes.nasdaqomx.com/docs/Methodology_HXR.pdf

Passeri, P. (2020). Cyber Attacks Statistics. https://www.hackmageddon.com/2020/08/13/june-2020-cyber-attacks-statistics

Platanakis, P., & Urquhart, A. (2019). Portfolio management with cryptocurrencies: The role of estimation risk. *Economics Letters, 177*, 76–80.

Ramos, S., Mélon, L., & Ellul, J. (2022). Exploring blockchains cyber security techno-regulatory gap. An application to crypto-asset regulation in the EU. In *10th Graduate Conference in Law and Technology, Sciences Po (2022)*. Retrieved from SSRN https://ssrn.com/abstract=4148678 or https://doi.org/10.2139/ssrn.4148678

Shanaev, S., Shuraeva, A., Vasenin, M., & Kuznetsov, M. (2020). Cryptocurrency value and 51% attacks: evidence from event studies. *Journal of Alternative Investments, 22*(3), 65–77.

Singh, P. (2021). *Increase in ransomware attacks 'absolutely aligns' with rise of crypto, FireEye CEO says, CNBC*. Retrieved September 14, 2021, from https://www.cnbc.com/2021/06/28/fireeye-ceo-spike-in-ransomware-attacks-absolutely-aligns-with-crypto-rise-.html

Stankiewicz, K. (2021). *Cloudflare CEO says crypto exchanges are a popular target for cyber attackers, CNBC*. Retrieved September 14, 2021, from https://www.cnbc.com/2021/09/13/cloudflare-ceo-says-crypto-exchanges-are-a-popular-target-for-cyber-attackers.html?&qsearchterm=crypto%20hack

Uma, M., & Padmavathi, G. (2013). A survey on various cyber attacks and their classification. *International Journal of Network Security, 15*(5), 390–396.

Van Hardeveld, G. J., Webber, C., & O'Hara, K. (2017). Deviating from the cybercriminal script: Exploring tools of anonymity (mis)used by carders on cryptomarkets. *American Behavioral Scientist, 61*(11), 1244–1266.

Wei, W. C. (2018). Liquidity and market efficiency in cryptocurrencies. *Economics Letters, 168*, 21–24.

Yermack, D. (2018). The potential of digital currency and blockchains. *NBER Reporter, 1*, 14–17.

Guglielmo Maria Caporale is Professor of Economics and Finance, Divisional Lead for Economics and Econometrics and Director of the Centre for Empirical Finance at Brunel University London. He is also a CESifo Research Network Fellow. Prior to taking up his current position, he was a Research Officer at the National Institute of Economic and Social Research in London; a Research Fellow and then a Senior Research Fellow at the Centre for Economic Forecasting at London Business School; Professor of Economics at the University of East London; Professor of Economics and Finance and Director of the Centre for Monetary and Financial Economics at London South Bank University (LSBU). He has also been Visiting Professor at both London Metropolitan University and LSBU, Research Professor at DIW Berlin and an NCID (Navarra Center for International Development) Non-Resident Fellow. He carries out editorial duties for various academic journals (including *Journal of International Money and Finance*, *International Review of Economics and Finance*, *International Economics*, *Machine Learning with Applications*, *Journal of Economics and Finance*) and has published extensively in leading academic journals such as *Journal of International Money and Finance*, *Journal of Banking and Finance*, *Journal of Empirical Finance*, *Journal of Financial Markets, Institutions & Money*, *International Journal of Finance and Economics*, *European Journal of Finance*, *International Review of Financial Analysis*, *Economics Letters*, *Finance Research Letters*, *Journal of Time Series Analysis*, *Journal of Financial Econometrics*, *Oxford Bulletin of Economics and Statistics*, *Econometric Reviews*, *Journal of Forecasting*, *Journal of Economic Psychology*, *Review of International Economics*, *Canadian Journal of Economics*, *Journal of Macroeconomics*, *Quarterly Review of Economics and Finance*, *International Review of Economics and Finance*, *Empirical Economics*, *Journal of Economics and Finance* and several others.

Woo-Young Kang is a Lecturer in Finance at Brunel University London since 2017 when he completed his PhD in Finance at Cranfield School of Management in the UK. He is also a graduate of Boston University (BA Economics, 2006; MSc Mathematical Finance, 2009) in US and Sogang University (MBA Finance, 2008) in South Korea with finance industry experience. He teaches Financial Markets and Global Financial Markets for the undergraduate and graduate levels, respectively. His research areas are in Asset Pricing, Banking, Financial Markets, Financial Engineering and Corporate Finance. He has published his research in leading international peer-reviewed journals, including the *Journal of Banking and Finance*, the *Review of Quantitative Finance and Accounting*, the *Journal of International Financial Markets, Institutions and Money* and the *Finance Research Letters*. His research are being presented at leading academic conferences, such as the meetings of the Southern Finance Association, the Eastern Finance Association and the Southwestern Finance Association.

Fabio Spagnolo holds a Ph.D. in Economics from the University of London and is currently affiliated with Brunel University London, UK and the University of Messina, Italy. His research are in the fields of econometrics, economics and finance and has published in Economics Letters, Journal of Applied Econometrics, Journal of Econometrics, Journal of International Money and Finance, Journal of Peace Research, Journal of Time Series Analysis and Oxford Bulletin of Economics and Statistics.

Nicola Spagnolo holds a Ph. D. in Economics from the University of London. His research interests are in finance, statistical methods and applied econometrics. He has published extensively on the following topics: (i) the analysis of financial risk, (ii) Markov switching models, (iii) modelling energy prices, (iv) financial crises determinants, (v) risk management and vi) modelling structural breaks in financial variables.

Chapter 15
Cyber Risk Insurance Framework Considerations

Călin Mihail Rangu, Nicolae Pană, and Mircea Constantin Șcheau

Abstract Cyber insurance is a necessity in the context of the digital transformation of society. We live in a world where the chains of usual operation, in general, and those of development and research in informatics must face the associated risks. Prevention and recovery processes are complemented by mitigation processes, which suppose, among others, complex cyber insurances, which involve a priori analyses and evaluations, before concluding the insurance policy and post-factum, after the occurrence of the insured risk.

The study seeks to substantiate the need to develop clear procedures, with levels and stages defined as much detailed as possible, formulating and assuming policies, supporting regulations, sectoral strategies to increase the level of maturity of consumers, individuals, institutions, and private legal entities, regarding protection against cyber threats. The study has identified the need for cooperation between insurers (and re-insurers alike) to provide appropriate types of coverage and exclusions, while splitting the risk among them.

We also intend to introduce in the article the schematic presentation of a reporting system to the state authority of attacks and losses generated by cyber risks, including those directed against critical infrastructures. This type of reporting can ensure transparency for the insurers about the entities they intend to ensure. Nevertheless, given the sensitive information it entails, the implementation details should be carefully thought out.

Keywords Risk management · Underwriting · Cyber security · Privacy · Data integrity · Availability

C. M. Rangu
Business Administration and Economical Sciences School, Danubius University of Galati, Galati, Romania

N. Pană
Academy of Business Studies, Bucharest, Romania

M. C. Șcheau (✉)
European Research Studies, Babeș-Bolyai University, Cluj-Napoca, Romania
e-mail: mircea.scheau@ubbcluj.ro

M. V. Achim (ed.), *Economic and Financial Crime, Sustainability and Good Governance*, Contributions to Finance and Accounting,
https://doi.org/10.1007/978-3-031-34082-6_15

JEL Classification D81 · G22 · M15 · O33

1 Introduction

Information and communication technology is present in daily activity, both on a personal and professional level, in services and products trained to support critical infrastructures. The financial sector of insurance, as always, follows the line of the economic evolution, keeping the rhythm of development. The insurance sector can't ignore the new virtual concept of living based on the homogenization and the connection between the Internet of Things distributed network and the Internet of People, participating in the construction of a global network, named the Internet of Everything. Although this new resulting network, which represents a link between the real and the virtual world, is exposed to great security risks generated by concrete threats, which increasingly fructify personal vulnerabilities, the biunivocal link related to the insurance system has more steps to be followed until it is validated. At the same time, we cannot imagine a new world that excludes the insurance culture. The virtual world is exposed to a higher rate of risk, so the experts in the insurance domain are called to analyze and provide solutions to build a new safer digital environment for business and people. This chapter aims to explore possibilities of legal regulation and development of new insurance products that can sustain the consolidation of the new digital world, the Internet of Everything, in a safer and predictable process. The practicians in the insurance sector have already identified the necessity of tailored insurance products that are able to cover the risk in the digital economy.

The present economy of private life is a field of research where at least three disciplines are bound: economics, law, and computer science. All analysis in this area is based on the assessment of the cost-benefit economic trade-offs that natural persons make when providing personal data in the economic transactions (the so-called "privacy calculus"), as well as the competitive implications of personal data protection for service providers. Any research in this area must begin with a study of demand and supply, where the demand is generated by the consumers for services offered by the information society.

When assessing the risks generated by cyber-attacks on these abstract intangible assets, it is particularly important to distinguish between personal information and private information, depending on how they are used in the economy. From the perspective of Bobek (2021), personal information (e.g., personal data) has the power of differentiation, because it highlights a person from an amorphous group of individuals, while private information, on the other hand, represents a tool for gaining influence in the market due to the unequal distribution of information among actors (e.g., consumers, firms), where one player owns the information and the other does not. In our opinion, when analyzing the object of the insurance contract, this distinction is particularly important because the assessment of risk and damages can be substantially different depending on the category where we place the information/data subject to the insured risk (risk of disclosure). The monetization of the right to

privacy and the protection of personal data is an important step for the analysis of the insured risk.

Given this disciplinary interconnection necessary to manage the risks generated by cyber-attacks, it is particularly important to identify and evaluate the protected legal value connected to the economic value. When we are looking at a risk situation that may affect personal information, we refer to the individual's right to privacy, but when private information is in danger, we can mainly refer to the right to property (e.g., intellectual property). In both cases, we are dealing with human rights guaranteed by international legal instruments. Focusing on the essence of the protected human right requires maturity when approaching the regulating in the cyber risk insurance market, as damages cannot be quantified without referring to this abstract asset of the rights holder.

According to the obligations established bin international law by UN Secretary—General & UN Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (2015), the states are responsible for adopting preventive conduct and countering the effects of cyber-attacks in that they "*cooperate to prevent harmful ICT practices and should not knowingly allow their territory to be used for internationally wrongful acts using ICT. It called for the increased exchange of information and assistance to prosecute terrorist and criminal use of ICTs.*" The report of the UN expert group in the field of information technology and international security talks about the concept of cyber-diligence, a conduct aimed to build procedural and legislative guarantees to effectively protect individual rights that may be affected by cyber-attacks. As we are analyzing the coordinates of the new digital world, we cannot ignore these obligations of the states to watch over the security of cyber space or of the Internet of Everything. At the same time, regarding the obligation of diligence, states must be evaluated according to their effective capacity (technological endowment, GDP, qualified human resource, etc.) to counteract the effects of a cyber-attack. As Provost (2002) also says, the same degree of cyber-diligence cannot be requested from a highly industrialized state (e.g., USA, Japan, Germany) compared to a less economically developed state (e.g., Ghana, Trinidad Tobago). Like these regulations, the duty of care incumbent on the insured user against the risks generated by cyber-attacks must be carried out in direct correlation with his financial, technological, human capacity. For example, it is obvious that the risk of network infection is much higher in the case of a small- or medium-sized enterprise whose employees do not have knowledge of information technology and data transmission, than in the case of a company active in the field of developing complex computer programs. The level of cyber culture of the collective that implements the hardware equipment or databases in a company is decisive in establishing the degree of probability of the risk of exposure of the company to a cyber-attack. Why is very important this evaluation between actors in the digital world and their obligation of risk control? Because legal solutions and insurance products must be tailored according to their real capacity of administration and watching of the digital economy. At the same time, the obligation of cyber-diligence imposed by the international treaties is forcing the state to adopt minimal protectives rules for their citizens and companies.

These obligations involve the adoption of a minimal set of legal rules that should create an equilibrium on the insurance market, based on demand and supply.

At the international level, as we present in the "Evolution and Current Situation related to cyber risk insurance" section, some of specialized studies reveal the evolution of the cyber-attacks, their effect on fundamental human rights, considering the individual as a consumer of the services offered by the information society. The aim of these studies is to reveal the necessity of conceptual transformations, the repositioning of decision-making factors in relation to the final consumer and a comprehensive picture of the immediate reality that requires solutions. In the section "Active Problems," we will focus on the factors inhibiting the controlled development of the cyber insurance market and risk management, trying to find solutions to the identified problems in the "Discussions and proposals" section. This chapter aims to offer some answers to the challenges that the cyber insurance ecosystem is facing very steeply. In the "Conclusions" chapter, the main ideas presented in the study and their possible effect will be synthesized.

2 Evolution and Current Situation Related to Cyber Risk Insurance

To propose a dedicated insurance product for a new social or economic context, we need to identify the protected value and the insurable risk that may affect the identified value. When approaching the cyber risks that affect the security of insurable information systems, we propose as a benchmark the definition stated by ENISA (2022) according to which a threat is "*any circumstance or event with the potential to have a negative impact on an asset through unauthorized access, destruction, disclosure, modification of data, and/or denial of service.*" According to the ENISA (2015) on threats and assets, an asset is defined as "*. . . anything of value. Assets can be abstract assets (such as processes or reputation of the natural/legal entity), virtual assets (e.g., data), physical assets (cables, hardware equipment), human resources, money.*" Until now, most studies and insurance products have focused on assets that are mainly related to information and communication technology (ICT) in the sphere of Internet infrastructure, being less interested in the sphere of human rights (abstract assets) that can be affected by cyber-attacks. For example, personal data is currently traded between service providers like any other commodities, so this evidence must be analyzed as individual market transactions. According to the studies carried out by Jentzsch et al. (2012) also under the auspices of ENISA, 47% of the interviewed service providers treated personal data as a commercial good and 48% disclosed that they share data with third parties. Therefore, it is important to understand and secure the economic dimension of private life as a central component of the notion of cyber risk. We may say that cyber risk is composed of, or rather includes, a multitude of other risks that may affect the personal security or the digital assets of individuals, private companies, or

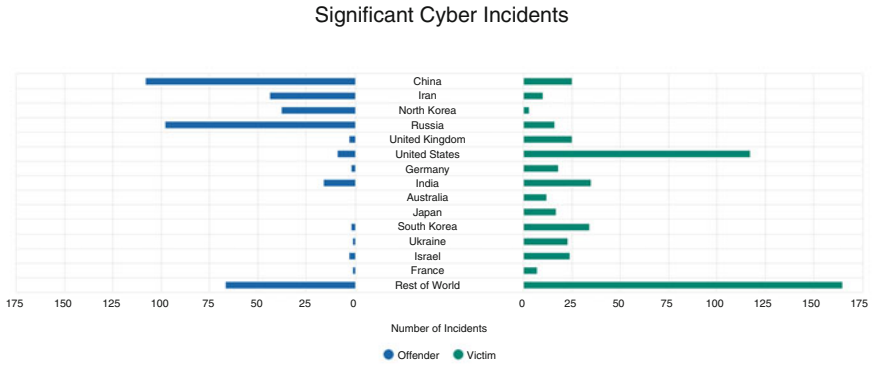


Fig. 15.1 Image of August 2022 cyber-attacks and victims, CSIS & Hackmageddon (2022)

institutional organizations. These subjects may lose financial and/or non-financial assets. Cyber risks may arise either as a result of intentional attacks (e.g., *terrorist attacks, state-sponsored attacks or attacks by activist groups, criminal activities, blackmail or for purely personal reasons)* or accidental events *(collateral victims, data deletions, accidental interruptions of services).*

According to Fauntleroy et al. (2015), "*cyberinsurance is a risk transfer product that corporations can buy to mitigate losses due to information technology (IT) problems.*" Based on the results of a study conducted by the Geneva Association (2018), the authors Badea and Rangu (2019) conclude that cyber risk is certainly the biggest challenge facing modern economies. The risk can be generated both by improper IT management, poor standards implementations, lack of control, the misuse of information technology, and deliberate attacks launched by criminals with the aim of taking control, destroying, blocking, or modifying computer programs and computer structures. By compromising the confidentiality, availability, or integrity of data and services, activities can be interrupted, critical capabilities can become unavailable, assets can be affected, and society and human lives can be endangered.

If we analyze the recent reports, it demonstrates that major attacks are on the rise worldwide according to CSIS & Hackmageddon (2022). Comparing the number of cyber-attacks reported in June 2019 with the ones reported in June 2020 and 2021, we observe an accelerated growth from 144 (in 2019) to 194 (in 2020) and 212 (in 2021). In 2022, we have an exponential evolution of cyber-attacks growing to 233, 62% more than 2019. Figure 15.1 shows the distribution of victims by country of origin in a study delivered in August 2022. It is noted that an impressive number of countries are very exposed to cyber-attacks. These figures demonstrate that cyber insurance finds its applicability on a large scale, in quite a varied field.

The figures we presented highlight the large number of cyber-attacks that cause various damages to legal entities and individuals. This situation calls for a new insurance product of more comprehensive cyber insurance policies capable of covering more negative effects. However, given the degree of unknown negative

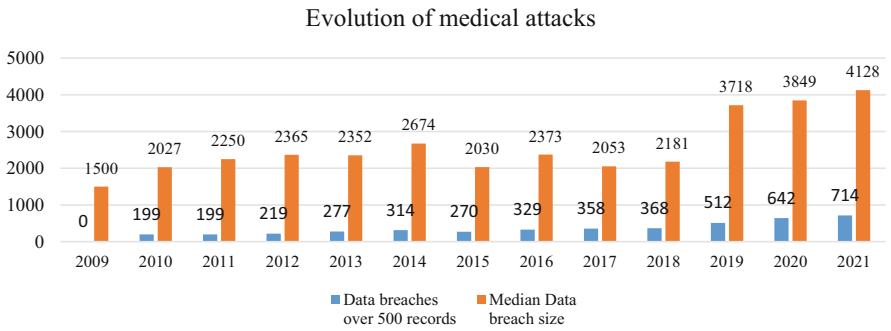


Fig. 15.2 Evolution of medical attacks in August 2022. Source: Authors adaptation based on CSIS & Hackmageddon (2022) published data

consequences, insurers must establish specific criteria to define such potentially negative outcomes, which automatically entails an increase in the cost of the policy for the insured entity, natural person, legal entity, or institution and in consequently, to a diminishing appetite for such cyber insurances. To prevent cost escalation, one approach would be to spread the risk between several insurers. Also, insurers and large consulting firms offer insurance products of this kind bundled with other IT management products and intervention in the event of a cyber-attack. The health sector also brings new challenges. Cyber-attacks in the medical area are more and more present, and this domain is becoming more affected by technological evolution. We may notice that the attacks and data leaks presented in Fig. 15.2 are directly proportional to the median attack size.

Cyber risk insurance market has reached $9 billion in 2021, more than half coming from the North American market, with a portfolio growth ranging from 35% to 113%. According to Faulkner (2022), there are approximately 180 groups of underwriters on a direct basis in cyber insurance and the market is expected to grow over $20 billion in premiums paid by 2025. The increase will be due to the improvement of education, the popularization of the types of risks, the role of insurance, the activity carried out remotely, the increased attention of the regulators, and finally, the increase in the number of cyber-attacks. Other analysts predict a growth of up to $40 billion by 2025. The area of accelerated development is likely to be in countries with relatively less developed markets and individual user markets. One of the strategies can combine real estate insurance with that related to software products, thus leading to the emergence of specialized distribution agents, such as managing general agents (MGAs). However, the increase in frequency and severity of attacks will affect the profitability of these products and we can expect an increase in premiums, exposures, changes in terms, and conditions, etc.

The report elaborated by Marsh (2021) reveals an increase in damages from the occurrence of cyber risks due to the increase in the vulnerability of remote activities, an explosion of ransomware attacks, which extends to D&O liability insurance of directors, executives, and/and shareholders and other forms of cybercrime, with an obvious discrepancy between the amounts requested and those actually paid. The

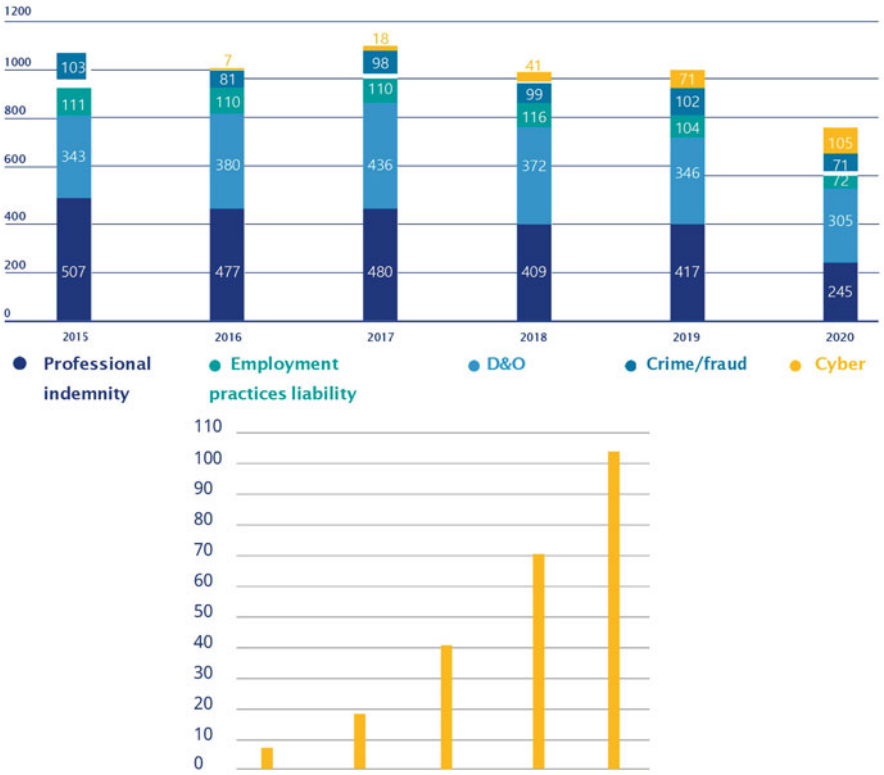


Fig. 15.3 Evolution of cybercrime and claim rate in 2021. Source: Authors presentation based on Marsh (2021) data

increase in maliciousness is closely related to the increase in cybercrime attacks, and Fig. 15.3 clearly shows the accelerated increase in cyber maliciousness (marked in orange), but this still represents only 4% of the total maliciousness. The industries with the most cyber damage are manufacturing (8%), CMT (6%), while financial institutions are at around 3%.

This data clearly shows that damage has increased exponentially in recent years. The driving factors for such an effect can range from the increase in the number of cybercriminals, the accessibility of cybercrime tools for script kiddies, to the lack of adequate cyber security measures implemented by organizations, etc. In terms of prevention, the insurer can influence one of the most important aspects related to preventive security measures, requesting for the issuance and coverage of the insurance to reflect the provisions of the good practice guidelines. This entails, among other things, that the types and amount of direct and indirect damages covered can be determined by the insurer according to its risk appetite. One way to increase both the number of types of claims covered and their amount is to build a

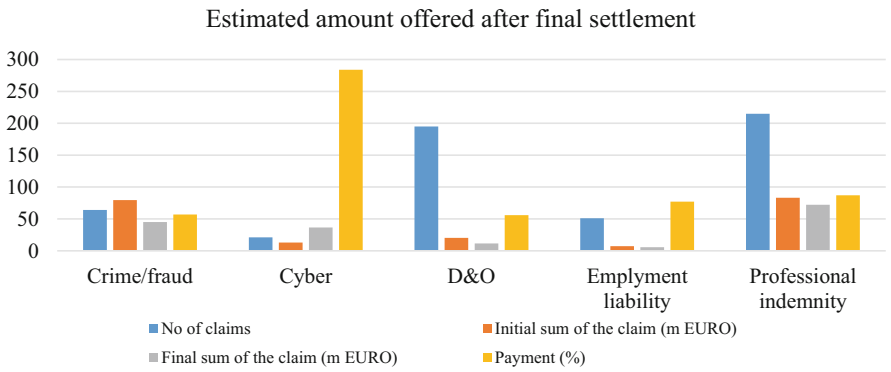


Fig. 15.4 Final settlement of damages against the original estimated amount claimed. Source: Authors presentation based on Marsh (2021) data

group of insurers to cover the insured entity, a task quite difficult for a single insurer to handle. This involves a distributed insurance mechanism, with distributed risk and increased transparency about the insured entities and their cybersecurity track record.

The same report presents the situation in the field of cyber insurance for which much more was paid than in the case of claims, the difference between the amount requested for payment and the amount finally settled being 284%. This colossal difference, as can be seen in Fig. 15.4, is generated by the additional costs behind direct damages, such as business interruption, additional labor costs, third party claims, D&O impact of these incidents.

In the IBM (2022) report, 550 organizations from 17 countries and 17 different industries affected by data breaches between March 2021 and March 2022 were analyzed. The conclusions are quite alarming, as 83% of organizations have been affected more than once, 79% of critical infrastructures are not modeled on a zero-trust architecture, 19% have been affected by contamination or other means due to some business partners, and finally, 45% of the total data leakage occurred from cloud computing environments. The average loss for a data breach was approximately $4.35 million, with an average of $4.85 million for critical infrastructure. The average cost per registration differs in 2022 also by country. As an example, the losses for the USA are about 9.44 million USD, for Turkey they are about 1.11 million USD, while for France we have an average cost of 4.34 million USD for a data loss. Of course, the total loss is influenced by several key factors related to the impact of technologies; an overview is presented in Fig. 15.5. Paradoxically (or not), it marks the 12th year in a row that the medical industry has posted significant losses of approximately $10.10 million, a 41% percentage increase, placing it far ahead of the top financial companies in second place with an average recorded loss of $5.97 million. In this context, the average loss due to a ransomware attack, excluding ransom demands, is approximately USD 4.54 million.

Year	Average/record cost of a data breach	Average total cost of a data breach
2016	158,00 USD	4,00 USD
2017	141,00 USD	3,62 USD
2018	148,00 USD	3,86 USD
2019	150,00 USD	3,92 USD
2020	146,00 USD	3,86 USD
2021	161,00 USD	4,24 USD
2022	164,00 USD	4,35 USD

Authors adaptation based on IBM Security (2022) data

Fig. 15.5 The evolution of costs related to data loss. Authors adaptation based on IBM Security (2022) data

The use of security solutions based on Artificial Intelligence and automation led in certain cases to a decrease in losses of approximately 5.05 million USD and a shortening of the detection period by approximately 74 days, from 323 days to 249 days. Also, losses for companies that have specialized emergency response teams that conduct stress tests, regularly review and update response plans, were 58% lower.

3 Active Problems

European Systemic Risk Board (ESRB) (2022) published an analysis on the vulnerabilities of the European Union's financial system, according to which the main major risks refer to the deterioration of macroeconomic indicators in tandem with the tightening of monetary policies, the possible steep decline in asset prices, and the deterioration of asset quality and profitability of institutions of credit. If the first and second risks are caused/influenced, among others, by the fluctuation of prices and other economic indicators, the third risk is affected by structural factors, competition between old and new financial services providers (etc.), correlated with the exposure of the financial—banking system to cyber risks, which can also affect other interrelated critical infrastructures.

Threats represent "*Any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations…*" according to Dempsey et al. (2011). In our presented context, this definition, accepted by specialists as a benchmark, must be completed with reference to elements related to motivation, intention, internal or external character, behavioral elements that generate risk, etc.

According to the evolution of the risks that affect individuals, legal entities, and institutions, cyber risk insurance must be adapted to respond to the challenges imposed by the new digital society states (Orlando et al., 2017). We must look more carefully at the inhibitors of the development of these insurances related to the technical environment on which cyber-attacks take place, some of them being:

- The lack of appropriate expertise and own standards that consider the dynamics and very rapid technological evolution in this field, the information asymmetry, and the problem of establishing control points that will remain valid for a long time—in the context where it is not enough to have checkpoints if they are not effective.
- Lack of coordination in determining the frequency of occurrence of incidents and damages. The rapid evolution of attacks is said to be an obstacle to developing statistics on which to build subscription models. The absence of statistical data is determined, among other things, by the complete non-provision of data on attacks, which become partially available only after the attack became public, as we will also mention in the "Limitations of the study and future directions" section.
- Non-full compliance with European Union directives and non-uniformity of the connection type, coupled with a lack of experience in cyber risk management, creates difficulties in assessing attacks and potential damage. Attacks are carried out on intangible assets, which are not always properly defined or revealed, and therefore, the amount of damage is difficult to assess. More concretely, a tangible attack takes place on intangible assets, not evaluated correctly initially, the effect being unpredictable, and thus, the price of an insurance is difficult to establish. We can talk about a still unorganized, immature, unregulated, and insufficiently regulated cyber risk insurance market, with various inclusions and exclusions, with limitations generated by the lack of experience of insurers and a limited framework of guarantee and reinsurance.
- Unpredictability and at the same time large-scale interdependence of risks, with rapid expansion due to technological heterogeneity. A vulnerability identified but not addressed according to best practice guidelines can spread globally almost instantly, with effects difficult to estimate, and secondary liabilities can add up to be greater than the initial liability. An increase in the value of the losses is also influenced by the time to identify the attack, the losses being in many cases directly proportional.
- Forensic techniques are not yet evolutionarily aligned to provide solid and rapid support for cybercrime units.
- The differences in approach to the phenomenon by the big suppliers and the different dynamism of the systems create difficulties in identifying effective countermeasures on several levels and lead to an oversizing and an overloading of the security structures—not effectively correlated with the level of security.

In a Delloite (2017) study, it is stated that "*insurers don't know what they don't know when they have to assess IT risks*" and we believe that the vicious circle of cyber insurance presented in Fig. 15.6 speaks for itself. We understand these issues

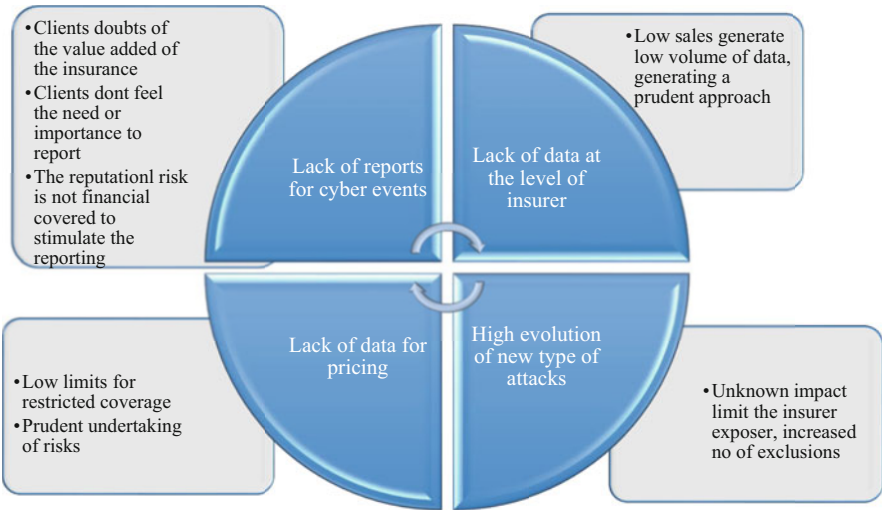


Fig. 15.6 Vicious circle of cyber insurance. Sources: Authors figure based on Delloite (2017) information

especially when new technologies are released without performing sufficient relevant functional tests or without considering the vulnerabilities that could be created by the integration of such technologies. The novelty demanded by the public and the desire to always be ahead of the competition turn into major risk factors that cannot be covered by insurance.

Without solid training in the field, it is difficult even for underwriters to understand that cyber risks can also affect other insurance markets, which at a superficial glance have nothing to do with IT. An example is represented by the real estate markets, which are closely related to the financial markets, as a large part of the financial capital is invested in them. A study conducted by LaSalle (2022) regarding operational technology threats and the level of cyber coverage of property insurance reveals that many international investors and owners of major properties worldwide are not aware of the coverages offered by insurance policies that they have for running commercial activities. They mistakenly believe that property insurance, economic-financial loss insurance, or similar products are somehow equivalent to cyber insurance. Moreover, some of the policyholders consider that cyber risks are included in general risks or that damage to IT systems can be borne/paid for by the insurer because the initial risk occurred. It is wrongly considered that flood or fire risk cover also includes, in the alternative, losses caused to IT systems, networks, or databases, etc.

The above argues that covered in the event of a total lack of assessment, inadequate risk assessment or insufficient data to analyze regarding the insured entity and the cyber insurance environment, all of these can lead to a decrease in the number of types of damages, which can also lead to an increase in insurance policy costs and, consequently, to a decrease in the number of insured entities.

4 Discussions and Proposals

In the cyber risk insurance ecosystem mentioned by Labunets et al. (2019), we identify the main actors:

- The insurer, which is "*a party that assumes risks of another party in exchange for payment*" according to Marotta et al. (2017), its purpose being to expand the market and develop a profitable business—with the obligation of strict risk assessment and management.
- The insurance broker, which can be a small, medium, or large company, the consultant for the company that wants to outsource its risk.
- The consumer/insured/customer of the insurance company, as the beneficiary of the products and to the services offered.
- The insurer's internal or external experts (risk assessors, forensic investigators, legal consultants, etc.).
- The authorities that establish public policies are added to the requirements, with the aim of improving security, protecting consumers, ensuring the resilience of the ecosystem, etc.
- The reinsurer, which takes over part of the insured risk.
- The regulatory body defined as "*public organization that is involved in rulemaking and can also be responsible for investigation or audit, monitoring, dispute decision, and enforcement*" as also mentioned (David Levi-Faur, 2011).
- The security provider, as an extremely important factor in reducing risks, implements measures, to monitor and to assure detection and prevention. Technical services for good IT security can be provided by an insurer task force specialized, by a trusted partner of the insurer, by an external certified security firm, or by the client if they have sufficient resources.
- The vendors of security products or services, as the know-how technical implementation to manage the cyber risks.
- The threat, the external environment or insiders which are the attack vector, and benefit of the client vulnerabilities.

Researchers are also an important part of the ecosystem because their studies are a great source of information for public policies, cyber security providers, and distributors of necessary products or services directly connected to the activities of the companies and institutions involved. We believe that the paths of interdependence explained in detail by Labunets et al. (2019) and presented in Fig. 15.7 are eloquent.

North (1999) argues that "*without being able to measure accurately whatever it is you are trying to enforce, there cannot be effective enforcement, even as a possibility*" and regarding the subject under discussion, it is absolutely necessary to quote the opinion of several established experts, one of them is Kshetri (2018) considering that in order to overcome the aforementioned impediments "*proper assessment of cyber-threat, cyber-vulnerability, and consequences of cyber-attacks are needed to gain a better understanding of cyber risks facing the firm. Insurance companies have realized that there is a fundamental need for better risk assessment tools.*" Beside

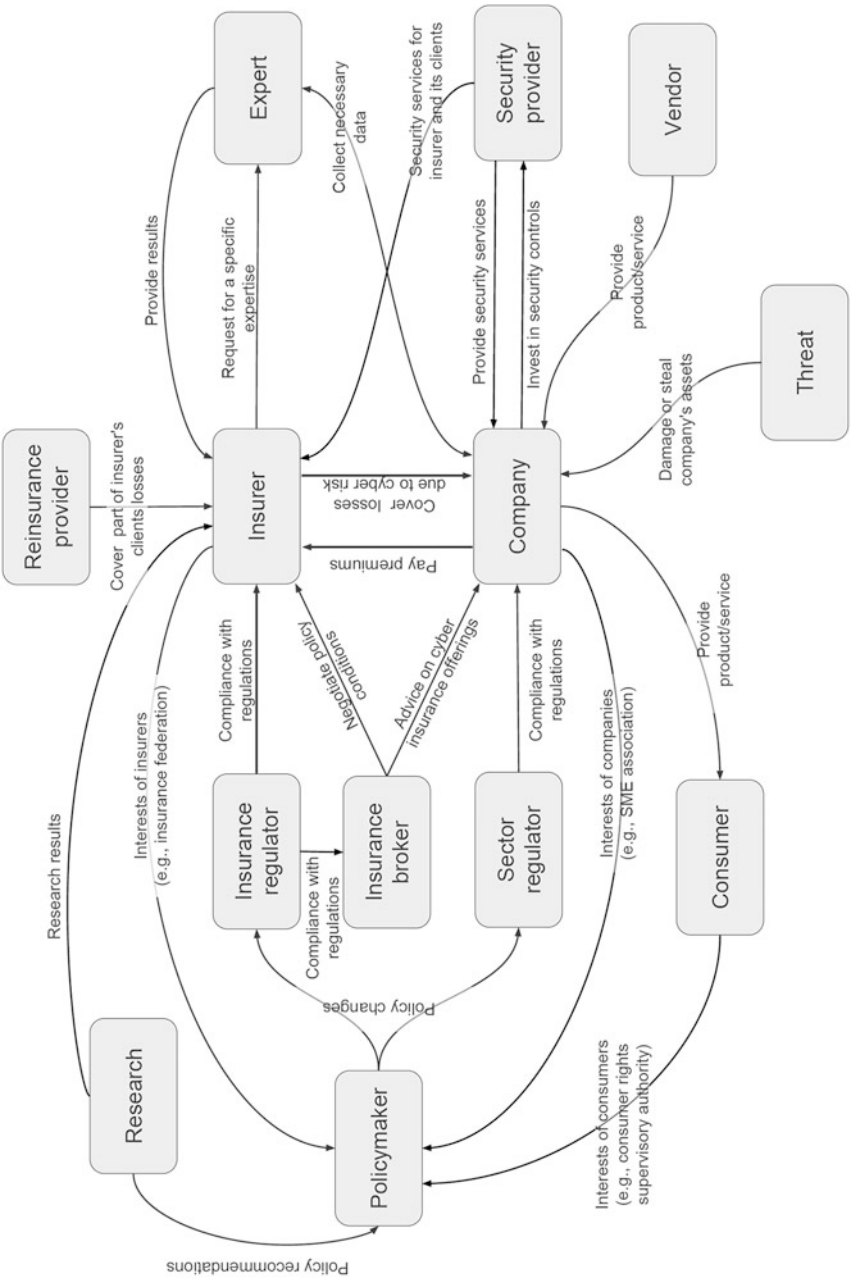


Fig. 15.7 Cyber insurance ecosystem. Sources: Katsiaryna Labunets et al. (2019)

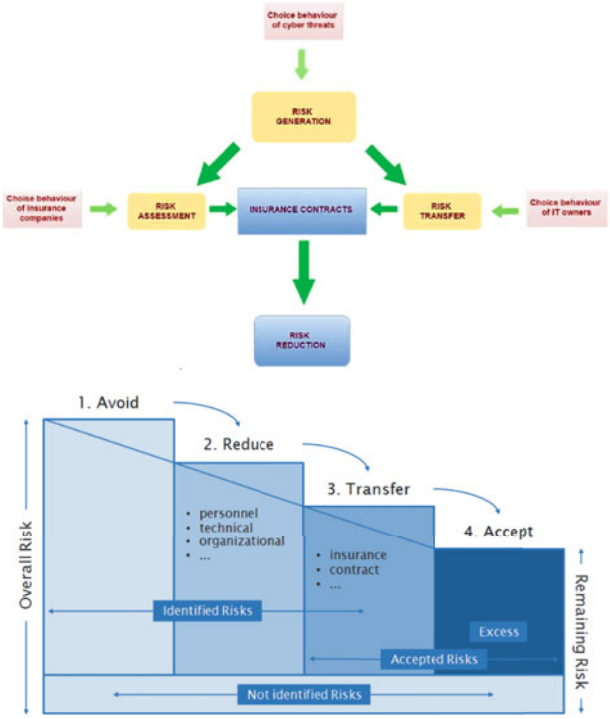
this, Boer and Monroe (2019) *"highlights the strong emphasis by insurance providers on prevention, preparation and incident response, as well as protection.*"

For this reason, the risk management approach is very important, and insurance is the key for covering the risk, especially in a world marked by an inconsistent dynamism of cyber-attacks. In this context, management risk assessment can be carried out based on a security self-assessment questionnaire, as recommended by Romanosky et al. (2019), based on standards (ISO 27,000, NIST 800-30, COBIT 2019, etc.) or using predictive models. A suggestive graphic form based on material developed by Ruef (2017) and Vasileiadis et al. (2019), which captures, among others, the specific regulatory issues and key directions, policies, and interventions needed to support risk insurance cybernetic, etc., is presented in Fig. 15.8. In order to prevent both the reluctance of the consumer/insured and/or the merchant/insurer/insurance company, as well as to support the development of the cyber insurance market, several insurance associations have developed their own insurance risk management model, which can be seen as a preamble for an extensive analysis at the level of each member country of the European Union with a view to the uniform implementation of a common strategy, after the elaboration of a European directive accompanied by the normative acts of implementation.

A cyber insurance European regulation should consider several aspects related to the subject matter of the insurance as the purpose, the main insurance and any related insurance, loss coverage, the time of occurrence, the covered period, general exclusions, specific exclusions, compensation schemes, definition deductibility, definition of excess, retroactivity of coverage, maturity considered as necessary measures to facilitate the adoption of cyber insurance, the alignment of all policies regarding cyber risk, etc. Labunets et al. (2019) considered that establishing standards or best practices regarding cyber security and requirements regarding cyber risk policies represents a great step for the unification of the system of sanctions, etc.

To avoid possible inconveniences, which may cause major losses for the business and even for the society, investors, owners, consumers, and traders must ensure that the cyber risk is expressly provided for in the insurance policy. Finally, it is important to explain as concretely as possible what this risk means, what it covers, and what are the levels of protection that such property, classified as an asset or liability, must have to be insured from a cyber point of view. Any analysis prior to the conclusion of an insurance contract should provide for a series of questions to be answered to be certain of an adequate level of security. A minimum of key cyber investigative controls is also required to verify the risk exposure of assets and/or liabilities. These controls, followed by periodic or real-time monitoring, should address both the software and hardware components.

Thus, our proposal is to have an interconnected ecosystem of insurers and reinsurers, which assumes a distributed risk for cyber insurance issued by one of the participants in this ecosystem. This situation can be improved by centralizing the cyber incident history of insured entities and a standardized approach to gathering information about preventive security measures applied at the level of the insured entity. The proposed measures lead to better consistency in approach and better



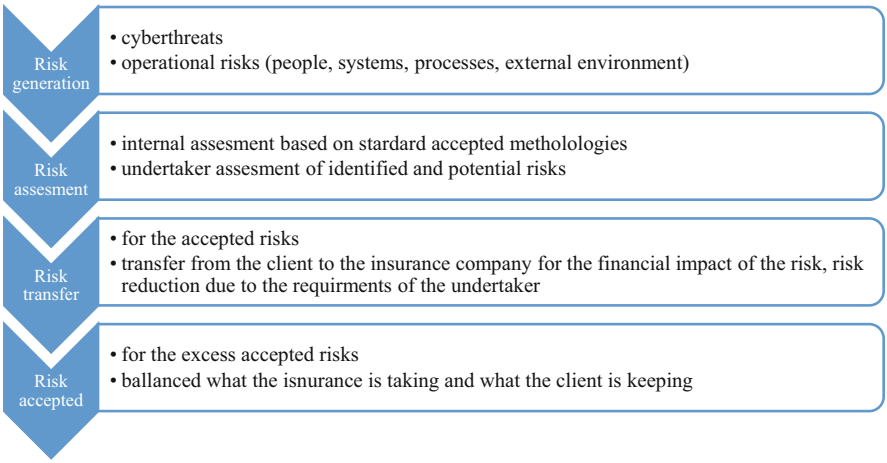


Fig. 15.8 Insurance and strategy in risk management. Sources: Ruef (2017) and Vasileiadis et al. (2019)) and Authors figure based on Ruef (2017) and Vasileiadis et al. (2019)

visibility of the real risks associated with a certain insured entity, with a direct beneficial effect on the costs paid by the insured entity and the insurer.

There is global concern for this topic, and the International Association of Insurance Supervisors (IAIS) supports insurance companies with a series of useful analyses in the process of creating products and services needed by the IT&C insurance market. From the document prepared by IAIS (2022), and publicly submitted for consultation, the idea emerges that one of the considerations for the establishment of a Pool, which would facilitate overcoming some of the problems reported by insurance companies, would be motivated by the high costs in the event of a cyber-attack, which could not be borne by a single insurance company, especially if we consider critical infrastructures, big data centers, etc. The insurance Pool could concentrate in a single space or in several spaces, some with a back-up role or to ensure the continuity of the activity, specialized staff, and thus the relatively high costs, even for outsourced services, could be distributed and supported by several companies. We also believe that problems related to professional liability insurance, financial loss insurance, exclusion of risks from classic products, etc., could also be solved.

Given the transnational character of the cyber-attacks and their massive impact on critical infrastructure at regional level, we propose the establishment of such a Pool at a European level. Usually, cyber-attacks have a negative impact that extends to several states, maybe affecting assets of a company established in various regions, the costs of the disaster being impossible to bear by a single insurer, as in the case of an earthquake. For example, a cyberattack on a nuclear plant or against an energetic system may produce a bigger disaster than an earthquake of 7 degrees on the Richter scale and the insurers may find themselves in a situation without sustainable financial solution. In such a situation, the existence of an insurance Pool established at a European level, involving all insurers present on the common European market, may be an effective solution to support the costs of the insurance policies. Establishing a regional or even international insurance Pool is in accordance with the cyber-diligence imposed to the states by the international law and may represent a materialization of the obligation of states to cooperate to counteract the disastrous effects of a cyber-attack with transnational implications.

5 Conclusions

We believe that cyber risks should be analyzed according to the risk areas and the short-, medium-, and long-term impact on civil society, in general, and on the cyber insurance ecosystem applying the same risk matrix that applies to other structures. In this direction of analysis and action, international bodies together with specialized providers, and consulting companies, with representative associations of insurance companies, and with consumer representatives should admit the importance of initiating, building, and sustaining a joint, focused and concerted effort, in order to find the best solutions as an urgent response to the effects that can be recorded due to

incidents that could affect horizontally and vertically the parties involved, both national or regional companies, whose operation is particularly important, multinational companies, which through their activity can to majorly influence the social impact, but above all, the critical infrastructures.

Related to the subject of this study, for a cyber risk insurance to be adequate to the needs of the applicant, an integrated approach is required so that the cyber security strategy of the infrastructure aims primarily at preventing attacks and rapid recovery in the event of an incident. It should be noted that the cyber insurance policy has the role of reducing the impact on the systems, and implicitly the business, which cannot fully cover the expectations of those interested, although the large, specialized companies in the field offer additional consulting, monitoring, and intervention services when producing risks. In this context, the creation of a cyber insurance POOL could address several needs and diminish the potential shock in the new ecosystem of insurance markets.

6 Limitations of the Study and Future Directions

We must admit that the publications that provide access to specialized information related to the subject of study are not necessarily presented in an academic context, but rather by different companies that build reports necessary to highlight certain aspects considered to be necessary. Another limitation is due to the avoidance of reporting to the competent authorities, insufficient reporting, sometimes truncated reporting, or even false reporting in certain cases. However, these limitations determine an increase in the value of this chapter through which the authors try to present the global situation from a completely different perspective, as a preamble to establishing a strategy to approach the phenomenon as unitary as possible. Therefore, the authors propose to continue the study and formulate other proposals to submit to regulatory bodies in the field at international level to be debated, approved, and implemented.

Acknowledgments This paperwork was carried out under the auspices of the Center for Research on Socio-Economic Dynamics in Sustainable Development (CC-DiSEDD), Danubius University of Galati, Romania.

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

References

Badea, L., & Rangu, C. M. (2019). Asigurarea riscului cibernetic - o mare provocare cu care se confruntă economiile moderne. *Revista de Studii Financiare, 6*.

Bobek, M. (2021). *Reports of cases – Case C-245/20*. Court of Justice of the European Union - Opinion of Advocate General Bobek delivered on 6 October 2021 (ECLI:EU:C:2021:822).

Boer, M., & Monroe, M. F. (2019). *Cyber risk insurance update: Advances in risk management*. Prioritizing Prevention and Protection, Institute of International Finance.

CSIS & Hackmageddon. (2022). *Statistics*. Retrieved from https://www.hackmageddon.com/category/security/cyber-attacks-statistics/

Deloitte. (2017). *Demystifying Cyber insurance coverage: Clearing obstacles in a problematic but promising growth market, A report by the Deloitte Center for Financial Services*. Deloitte University Press.

Dempsey, K., Chawla, N. S., Johnson, A., Johnston, R., Jones, A. C., Orebaugh, A., Scholl, M., & Stine, K. (2011). *Information Security Continuous Monitoring (ISCM) for federal information systems and organizations*. Special Publication 800-137, National Institute of Standards and Technology (NIST), U.S. Department of Commerce.

European Systemic Risk Board. (2022). *Warning of the European systemic risk Board of 22 September 2022 on vulnerabilities in the union financial system (ESRB/2022/7)*. European System of Financial Supervision.

Faulkner, M. (2022). *Beazley and Chubb top cyber market share*. Lloyd's List Intelligence, Informa UK Limited.

Fauntleroy, J. C., Wagner, R. R., & Laura, O. A. (2015). *Cyber insurance-managing cyber risk. Technical report*. Institute for Defense Analyses.

Geneva Association. (2018). *Understanding and addressing global insurance protection gaps*.

IBM Security. (2022). *Cost of a data breach report 2022*. IBM Corporation.

International Association of Insurance Supervisors (IAIS). (2022). *Issues paper on insurance secto operational resilience*. Draft for Public Consultation.

Nicola Jentzsch, Sören Preibusch, Andreas Harasser, Demosthenes Ikonomou, ENISA, Rodica Tirtea, Study on monetising privacy. An economic model for pricing personal information The European Union Agency for Network and Information Security (ENISA), 2012.

Kshetri, N. (2018). The economics of cyber-insurance. *IEEE Computer Society, 20*(6), 9–14. https://doi.org/10.1109/MITP.2018.2874210

Labunets, K., Pieters, W., van Gelder, P., van Eeten, M., Branley-Bell, D., Briggs, P., Coventry, L., Vila, J., & Gómez, Y. (2019). *Supporting cyberinsurance from a behavioural choice perspective*. CYBECO-WP7-D7.1-v1.0-TUD.

LaSalle, J. L. (2022). *You may not have the cyber insurance coverage you think you do, report*.

Levi-Faur, D. (2011). *Handbook on the politics of regulation*. Edward Elgar.

Marotta, A., Martinelli, F., Nanni, S., Orlando, A., & Yautsiukhin, A. (2017). Cyber-insurance survey. *Computer Science Review., 24*, 35–61. https://doi.org/10.1016/j.cosrev.2017.01.001

Marsh. (2021). *Financial lines: Time to build resilience - 2021 claims analysis and trends, report*.

North, D. C. (1999). Dealing with a nonergodic world: institutional economics: Property rights and global environment. *10 Duke Environmental Law & Policy Forum 1-12, 10*(1), 1–12.

Orlando, A., Marrota, A., Nanni, S., & Martinelli, F. (2017). Cyber - Insurance survey. *Computer Science Review, 24*(24), 35–61. https://doi.org/10.1016/j.cosrev.2017.01.001

Provost, R. (2002). *State responsibility in international law*. Editorial Routledge. https://doi.org/10.4324/9781315242439

Romanosky, S., Ablon, L., Kuehn, A., & Jones, T. (2019). Content analysis of cyber insurance policies: How do carriers' price cyber risk? *Journal of Cybersecurity, 5*(1), tyz002. https://doi.org/10.1093/cybsec/tyz002

Ruef, M. (2017). *Cyber insurance – Benefits and uses*. Risk Rating and Methodologies.

The European Union Agency for Network and Information Security (ENISA). (2015). *Guideline on threats and assets, technical guidance on threats and assets in Article 13a*. Retrieved from https://resilience.enisa.europa.eu/article-13/guideline_on_threats_and_assets/Guideline_on_Threats_and_Assets_v_1_1.pdf

The European Union Agency for Network and Information Security (ENISA). (2022). *Glossary - Threat and risk management*. Retrieved from https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/current-risk/risk-management-inventory/glossary

UN Secretary-General & UN Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security. (2015). *Report (A/70/174) of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security: Note/by the Secretary-General*. General Assembly, United Nations.

Vasileiadis, N., Couce, A., Benito, P., Tsekeridou, S., Vila, J., Baylon, C., Cousin, M., Baylon, C., Pieters, W., Labunets, K., Briggs, P., Branley-Bell, D., & Ríos, D. (2019). *Supporting cyberinsurance from a behavioural choice perspective*. CYBECO WP2-D2.3(d)-v2.0-TREK.

Călin Mihail Rangu is associate professor at the Business Administration and Economical Sciences School of Danubius University of Galati and Director in Policyholder Guarantee Fund of Romania. He was director in Financial Supervision Authority (FSA), and National Bank of Romania, President of the Institute of Financial Studies, Vice-president of EIOPA InsurTech Task Force, President of FSA Shareholder Group in Consumer Protection, Board Member of EFICERT, and Coordinator of Fintech HUB of FSA. He has a broad experience in management, banking and insurance, operational risks, IT security, consumer experience, IT and financial services, products, and technologies. Călin is double-licensed in economics and engineering, PhD in neural networks applied in financial series processing, MBA graduate in banking and finance, University Lector, MBA Lector. He acted also as director in Raiffeisen Bank and general director of Romanian subsidiary of Raiffeisen Informatik Austria Group. He published scientific articles, over 100 general articles and four books, being organizer or speaker in major Romanian conferences related to financial and banking sectors, consumer protection, ADR, IT, cyber-fares, operational risk management, or management and processes.

Nicolae Pană is the founding President of the International Association for Law, Culture, and Information Society—LEGALITC. He has attended post-graduate master's and international doctorate studies in law at the Carlos III University of Madrid, Spain and "Acad. Andrei Radulescu" Legal Institute of Romanian Academy. He is postdoc researcher at The Bucharest University of Economic Studies and has experience in teaching Law, Community Manager and Social Media Management courses at Spanish and Romanian universities. He is the author and co-author of several articles and paper works in the field of law and he has expertise in information society law, electronic commerce, civil law, labor law, European funds and computer crime.

Mircea Constantin Șcheau is PhD in Public Order and National Security with a theme of interest for the economic and security domains "*Cybercrime regarding Financial Transfers,*" who received "Victor Slăvescu Prize" awarded by Romanian Academy. Author/co-author of three volumes. More than fifty scientific articles on management, law enforcement, critical infrastructure, information technology, artificial intelligence, defense, cybersecurity, lecturer in numerous international conferences, Honorary associate researcher at University of Craiova, Constanta Maritime University, Danubius University of Galati, and member, inter alia, of European Research Institute at Babes-Bolyai University. He is a member of the project titled "Intelligent analysis and prediction of the economic and financial crime in a cyber-dominated and interconnected business world," conducted over the period 2021–2023, financed from the Romanian Ministry of Education and Research, CNCS—UEFISCDI, project number PN-III-P4-ID-PCE-2020-2174 (www.fincrime.net).