European Proceedings of
Social and Behavioural Sciences
EpSBS

www.europeanproceedings.com

e-ISSN: 2357-1330

DOI: 10.15405/epsbs.2021.04.02.202

GCPMED 2020
Global Challenges and Prospects of the Modern Economic Development

NEW TRENDS IN CORPORATE CRIME

E. A. Tolchina (a)*
*Corresponding author

(a) Business Rights Commissioner in Ulyanovsk region, Ulyanovsk, Lev Tolstoy Str., 58, ipka73@icloud.com

Abstract

Corporate crime worldwide is one of the key and most dangerous areas of economic crime. An increase in corporate crime leads to an increase in the corruption of public servants; an increase in the unemployment rate; tax evasion; monopolization of a number of segments of the economy and a decrease in competitiveness, which leads to a deterioration of the investment climate, and the activation of money laundering processes. In Russia, the problem of countering corporate crime is no less acute than in the rest of the world. The concept of corporate crime is currently quite vague, and covers a wide range of criminal acts from fraud to corruption. Today, there is an active increase in corporate crime. Damage from economic crimes is associated with financial losses and loss of assets, and companies also bear the cost of conducting investigations. The increase in the number of new types of criminal activity that could be classified as corporate is largely due not only to the activities and motivation of managers, but also to larger factors, such as shortcomings in the legal regulation of management processes, the use of material and other resources by managers, insufficient control by law enforcement agencies and imperfect criminal legislation regulating responsibility for corporate crimes. The author has studied the key approaches to defining the concept and essence of corporate crime in Russia and in the world. As a result of the study the author has identified the key trends prevailing in the structure of corporate crime.

Keywords: Corporate crime, criminal law, counteraction, falsification of accounting reports, trends

https://doi.org/10.15405/epsbs.2021.04.02.202
Corresponding Author: E. A. Tolchina
Selection and peer-review under responsibility of the Organizing Committee of the conference
eISSN: 2357-1330

1. Introduction

The institution of responsibility for corporate crimes emerged in the middle of the XVIII century, gradually growing, it acquired the forms of an independent direction within the framework of the system of countering economic crime. Corporate crime, as a particular manifestation of economic crime, does not currently have a well-established doctrinal definition, and the criminal acts covered by it also vary. This situation is justified because of the collective nature of their analyzed category (it may cover both criminal acts in business and other economic activities, and criminal acts in cyberspace, ecology, etc.). As interpreted by the IMF (International Monetary Fund), this concept covers criminal activities related to money laundering, fraud, bribery, tax evasion and corruption (International Monetary Fund, 2001).

A group of domestic criminologists led by Dolgova (1999) suggests considering corporate crime as a set of illegal actions committed on behalf of the heads of the corporation, both by themselves and their representatives. While noting some of the advantages of the proposed definition, we note that it does not take into account the selfish motivation of managing persons and their illegal activities on behalf of the corporation. At the same time, other authors understand corporate crimes as the set of all socially dangerous acts, whether criminal, civil or administrative, that are committed by the managers of corporations or by the corporate entity itself (Marshall &Yeager, 1980) or in other words are defined as crimes committed for the firm by the firm or its agents when conducting business (Gottschalk, 2020).

Some authors suggest that this concept should be understood as illegal, prohibited by law, punishable behavior of a corporation or an employee (employee) acting on behalf of the corporation (Simpson, 2002). Taking into account the existing differences in the interpretation of this concept, two schools have been formed in science in understanding of the corporate crime subjects. Representatives of the first scientific school adhere to the interpretation of corporate crime as "white-collar" in the interpretation of Sutherland et al. (1983), in which only a separate stratum of society is involved. In turn, "revisionists" hold the position that such crime does not have a "class" or "social" affiliation, and anyone can be involved in it (Alalehto & Larsson, 2012).

Separate studies have focused on the relationship between corporate management and corporate crimes. Most of the studies is devoted to the relationship between corporate crimes and revenue generation in corporate management, compliance with corporate reporting procedures, and management activities (Hasnan et al. 2014). In our opinion, corporate finance is a set of economic relations that arise in the process of formation, distribution and use of funds in connection with the production and implementation of products, works and services. For the purposes of criminal law, corporate finance should be considered as the property of legal entities, and corporate financial crime - as an independent layer of economic crime associated with the economic activities of corporations.

When defining the concept of corporate crime, it is very important to distinguish this term from "white-collar" crime, economic crime and organized crime (Šikman, 2013). Undoubtedly, certain types of corporate crimes are covered by the concept of white-collar crime, at the same time, corporate crime is part of economic crime, and in some cases may have signs of organized crime.

In our opinion, corporate crimes should be understood as a set of financial crimes, such as misrepresentation of information in the financial statements of corporations, stock market manipulation and insider trading, commercial bribery, direct or indirect bribery of public officials, fraud and other types

https://doi.org/10.15405/epsbs.2021.04.02.202
Corresponding Author: E. A. Tolchina
Selection and peer-review under responsibility of the Organizing Committee of the conference
eISSN: 2357-1330

of theft, as well as misuse of funds in bankruptcy proceedings and bankruptcy, and laundering of criminal proceeds committed for selfish purposes on behalf of the corporation and in its interests.

According to the General Prosecutor's Office of the Russian Federation, 16% of economic crimes registered in Russia are committed by entrepreneurs or on every sixth. Of the 104,927 economic crimes registered in Russia in 2019, 16,756 were committed by business entities (1.3% more than in 2018). Half of them (8,004) were frauds (Article 159 of the Criminal Code of the Russian Federation) or 3.7% of all crimes identified over the year under this article (Criminal Code of the Russian Federation from 13.06.1996 No. 63-FZ). Only 427 frauds involved deliberate non-performance of contractual obligations in the field of business activity.

According to statistics, most frequently the entrepreneurs were prosecuted under articles on tax crimes (Article 198-199.2 of the Criminal Code of the Russian Federation) - for entrepreneurs, 79.5% of all revealed offences of misappropriation or embezzlement (Article 160 of the Criminal Code of the Russian Federation) - 691 crime, illegal use of a trademark (Article 180 of the Criminal Code of the Russian Federation) - 277 crimes, currency offenses (Article 193, 193.1 of the Criminal Code of the Russian Federation) - 259, abuse of authority (Article 201 of the Criminal Code of the Russian Federation) - 156 crimes, illegal creation of a legal entity (Article 173.1 of the Criminal Code of the Russian Federation) - 153, production, purchase or sale of goods without marking (Article 171.1 of the Criminal Code of the Russian Federation) - 152 and legalization of funds or other property acquired through crime (Article 174.1 of the Criminal Code of the Russian Federation) - 151 or almost every fifth of the crimes in this article (Criminal Code of the Russian Federation from 13.06.1996 № 63-FZ; Tass, 2020).

A 2017 study found that only in the United States, companies suffered losses of $ 50 billion due to the illegal occupation of their property by employees (Meerts, 2019). The FBI recognized employee thefts as the fastest-growing crimes in the United States (Greer, 2017). The American employers' association cites the following statistics: companies lose 20% of profits from theft committed by employees; 55% of employees-robbers are managers; 20% of employees are aware of the theft committed in their company.

Statistics for the last 2 years show that approximately half of all corporate fraud cases in India occurred in the infrastructure sector and the real estate market, the other 34% occurred in the financial sector. The authors believe that the increase in the number of cases of corporate fraud is associated both with the low efficiency of the authorities' actions and with the desire of companies to hide their problems from external attention (Gupta, 2020).

According to a survey conducted by PWC, the number of reports of fraud in Russia has significantly increased, 66 % of respondents said that their companies have experienced economic crimes. Misappropriation of assets remains the most common form of economic crime in Russia, followed by bribery and corruption, fraud in the procurement of goods and services, and cybercrime. According to the survey, the share of senior managers among scammers is growing. According to surveys of consulting companies, no company, regardless of size or industry, is literally protected from corporate financial crimes (PWC, 2018).

The analysis of Russian and foreign criminal legislation, and the practice of its application, as well as theoretical provisions allow to conclude that corporate crime, like any other type of crime, has its own characteristics and characteristic forms of criminal activity. Corporate crime, like all economic crime, is a

https://doi.org/10.15405/epsbs.2021.04.02.202
Corresponding Author: E. A. Tolchina
Selection and peer-review under responsibility of the Organizing Committee of the conference
eISSN: 2357-1330

volatile and fickle phenomenon. In this regard, the study of the main trends observed both in corporate crime itself and in the issues of bringing to justice for such crimes is very timely and necessary.

2. Problem Statement

Corporate crime, being a dynamic area of criminal activity, is undergoing constant changes and transformations. Today, there is an active growth of corporate crime. Thus, about a third of companies have experienced economic crimes in the past two years, and the loss incurred exceeded 1 million US dollars, which is slightly higher than the global average (PWC, 2018). Damage from economic crimes is associated with financial losses and loss of assets, companies also bear the costs of conducting investigations. At the same time, the increase in the number of new types of criminal activities that could be attributed to corporate activities is largely due not only to the activities and motivation of managers, but also to larger factors, such as shortcomings in the legal regulation of management processes, the use of material and other resources by managers, insufficient control by law enforcement agencies and imperfection of criminal legislation regulating responsibility for corporate crimes. The study attempts to identify the key trends observed in corporate crime, as well as to identify the most effective forms of countering it.

3. Research Questions

The problem of countering corporate crime remains relevant over the past few decades. Despite this, it is impossible to say that science and practice have developed effective ways to counter it. Being a dynamic phenomenon, corporate crime is undergoing significant changes that require transformation and the methods used to counter it. In the course of the study, the author is supposed to find an answer to the question: what is the state of corporate crime today? What types of abuse prevail in it? What provisions of the law provide counteraction to the specified criminal phenomena? And what effective measures have been taken by law enforcement agencies?

4. Purpose of the Study

In the context of the systemic transformation of the economy, the problem of countering corporate crime has acquired a special criminological acuteness and political significance. The purpose of this study is to analyze the key trends observed in the processes that directly or indirectly affect corporate crime, and directly related to it. To achieve this goal, the author analyzed the "cases" of major corporate scandals, the available scientific literature on corporate financial crime, as well as the explanations of regulators on these criminal manifestations, which allowed to identify the main trends.

5. Research Methods

The main methods of this study are the descriptive method, methods of observation, interpretation, comparison and generalization. In addition, theoretical methods of analysis, synthesis, induction, deduction and classification, the method of content analysis were used. The author also analyzed the existing literature on various aspects of corporate crime. This provided the proper theoretical part of the study. The analysis of

https://doi.org/10.15405/epsbs.2021.04.02.202
Corresponding Author: E. A. Tolchina
Selection and peer-review under responsibility of the Organizing Committee of the conference
eISSN: 2357-1330

the literature revealed the main directions of theoretical studies in the field of corporate crime. During the work on the study, the "cases" of corporate crimes were studied in detail, including the enforcement actions of the SEC related to accounting and audit violations. This made it possible to highlight the range of criminal acts committed by and on behalf of corporations as corporate crimes.

6. Findings

In the course of the study, we identified the following trends in corporate crime:

1. An increase in the number of internal violators.

Studies show an increase in the number of internal incidents among representatives of the corporate community. The number of respondents of the global survey, who noted that among those who committed economic crimes, the main share is accounted on employees of the company, increased from 46 % in 2016 to 52 % in 2018, while the number of senior managers among malefactors is also growing. Thus, the share of senior managers among domestic offenders increased from 15 % to 39 % (PWC, 2018).

Company managers, together with the financial manager (accountant), are directly responsible for non-compliance with accounting regulations. In this sense, the existence of an audit committee or audit management in the company is intended to contribute to more effective management of the company to achieve its goals. Thus, it is assumed that the risks faced by the company have already been identified by management and the latter is able to take sufficient and well-founded measures to ensure that the risks are minimized. In other words, corporate management, as the system by which business entities are managed and controlled, is directly responsible for the true and fair value of the financial condition reflected in the accounting records (Achim & Borlea, 2020). However, in fact, a paradox arises.

Abdullah and Said (2018) cite interesting results of their study based on data from Commission for securities of Malaysia: almost all cases of corporate crimes were committed by persons holding the posts of directors, as well as top managers of companies. While the corporate management paradigm defines directors and top management as the main controllers acting in the interests of companies and shareholders, the managers are the ones who are responsible for corporate financial irregularities in these companies. The study also shows that the personal qualities of directors and top managers, as well as their human values, influence the frequency of corporate financial crimes (Abdullah & Said, 2018). In this aspect, the example of the Libor scandal is relevant, when the British Bank Barclays admitted the fact of manipulating a key indicator that focuses on the interest rates of financial products in the amount of 360 trillion dollars. Tom Hayes became the first banker to be brought to trial in connection with an international conspiracy to manipulate rates. He was sentenced to 11 years in prison in August 2015 (Milligan, 2020).

2. An increase in the number of attacks related to the violation of financial statements.

Financial reporting has always been the most interesting target for corporate criminals. Major financial scandals that have erupted around the world have been based on creative accounting practices combined with fraud and complicity in audit firms to cover up the problems these organizations face. In some cases, large audit companies were either accomplices in fraudulent schemes, or were in good faith mistaken and could not detect the criminal intent of the company's managers, which is why they were found guilty in financial losses caused to the companies that were subjected to fraud, and were punished with compensation (Achim & Borlea, 2020).

https://doi.org/10.15405/epsbs.2021.04.02.202
Corresponding Author: E. A. Tolchina
Selection and peer-review under responsibility of the Organizing Committee of the conference
eISSN: 2357-1330

Let's remember the case of the Volkswagen auto group, manipulated reporting by conducting tests for the measurement of the exhaust level of their diesel engines in the US and Europe that led to loss of 78 billion euros. Or the case of energy giant Enron (damage is 74 billion dollars), or WorldCom the company where the forgery of financial statements at a cost of 107 billion dollars and imprisonment of the head of WorldCom to 25 years. Liability for violation of financial accounting is a combination of administrative and criminal penalties imposed on responsible corporate officials.

In Russian legislation, for violations in accounting and tax accounting, administrative responsibility of the organization is possible under Article 120 of the Tax Code of the Russian Federation, the penalty will be applied to an organization that repeatedly violated the established accounting rules in one tax period: untimely or incorrectly reflected transactions on accounting accounts or did not create and store primary and accounting documents. An official may be brought to administrative responsibility under Article 15.11 of the Code of administrative offences of the Russian Federation (Code of administrative offences of the Russian Federation from 30.12.2001 No. 195-FZ).

For misrepresentation of financial documentation, not only administrative responsibility can occur, but also criminal responsibility. In accordance with article 172.1 of the Criminal Code of the Russian Federation, criminal prosecution is provided for falsification of accounting reports. Falsification refers to the introduction of deliberately false, unconfirmed information about transactions, obligations, property and assets of the company. Such distortions are made in order to conceal signs of bankruptcy of an economic entity, repeal of a license or appointment of a temporary administration. The maximum possible sanction is 4 years in prison.

In the United States, corporate crimes have been criminalized under the Sarbanes-Oxley Act or the Act of public company accounting reform and investor protection since 2002. The law significantly tightened the responsibility for corporate crimes, in particular, for falsifying financial statements. Thus, under the law, corporate managers who sign a financial report that does not meet the established requirements are subject to a fine of no more than 1,000,000 dollars or a prison sentence of no more than 10 years, or both. If the specified actions were committed intentionally, the head of the corporation must be fined no more than 5,000,000 US dollars, or imprisoned for no more than 20 years, or both.

3. Increasing the share of cybercrime in the structure of corporate crime and increasing the use of technology to combat corporate crime.

Digitalization is one of the dominant trends in the development of modern business. We are seeing an increase in the spread of a number of "smart" devices that can control various processes. Organizations on the Russian market have been working for several years to develop artificial intelligence technologies for their business tasks. First of all, solutions using such technologies are used to optimize internal business processes. The total effect of implementing AI solutions for respondent companies amounted to about 60 billion rubles in 2019 (additional income amounted to more than 27 billion rubles and savings amounted to more than 32 billion rubles) (Rostelecom & Tadviser, 2020).

Technologies are also used to monitor economic crime. In Russia, more and more companies are using technology as the main tool for detecting economic crimes than in the world as a whole, in particular in such areas as fraud detection, anti-bribery and corruption, and comprehensive verification of the reliability of business partners.

https://doi.org/10.15405/epsbs.2021.04.02.202
Corresponding Author: E. A. Tolchina
Selection and peer-review under responsibility of the Organizing Committee of the conference
eISSN: 2357-1330

Undoubtedly, technologies are also being adopted by cybercriminals. In the context of the pandemic, when business has moved to online, and all communication is carried out through corporate networks, there is a steady multiple increase in the number of cyber attacks on business infrastructure. According to Group IB (2020), in 2019, many Ransomware operators moved away from attacks on ordinary users and switched their attention to companies from various industries and government authorities. The attacks on these victims are of great benefit for the attackers. There are usually the following initial attack vectors:

- deleterious emailing;
- gaining access to the internal network through compromising authentication data;
- operation of publicly available applications, including VPN-related ones. After the initial compromise; many cryptographic operators first try to get higher access rights, and then attempt to access other accounts using various software. The number of sold accesses to corporate networks increases from year to year, but the main peak of sales occurred in 2020, an increase of 2.6 times. It is expected that specialized trading platforms for placing lots with access to corporate networks will appear, which may lead to an even greater increase in incidents.

Official data also confirm these trends. In the first half of 2020, the number of crimes in the field of information technologies in Russia increased by 91.7% compared to the same period last year, and the share of these illegal acts in the overall crime structure reached 22.3% (Russian Interior Ministry, 2020).

The US SEC statement (2018) notes that companies face an ever-changing cybersecurity threat landscape in which hackers use a complex set of tools to carry out cyber attacks, including the use of stolen access data, malicious programs, ransomwares, fishing, structured query input language attacks, and distributed denial of service attacks, among other things (Securities and Exchange Comission (SEC), 2018). The objectives of cyber attacks vary widely and may include the theft or destruction of financial assets, intellectual property, or other confidential information belonging to companies, their customers, or their business partners. Cyber attacks can also be aimed at disrupting the activities of public companies or their business partners. In order to protect the interests of investors, the SEC has required public companies to inform investors about significant risks and incidents in the field of cybersecurity. The requirement is mandatory not only for companies that have been subjected to cyber attacks, but also for those who are exposed to significant cybersecurity risks, but may not yet have been the target of cyber attacks.

7. Conclusion

The results of our study have shown that more and more Russian and international companies are facing corporate crimes. Today we can distinguish the following main trends in the structure of corporate crime: a growing number of insiders, the increase in the number of abuse related to violation of financial reporting, the growth of cybercrimes in the structure of corporate crime and increased use of technologies to combat corporate crimes. In these circumstances, many companies are increasing their spendings on countering criminal encroachments, increasing their participation in the audit sphere, but the problem still remains. The identified trends indicate systemic shortcomings that inevitably lead to corporate crimes. In these circumstances, risk assessment is more relevant and necessary than ever for all companies and corporations. This will provide an understanding of the vector of measures to prevent criminal attacks.

Undoubtedly, the main damage from corporate encroachments is estimated in monetary terms, but we should not forget about the costs caused by the business reputation of the company. Transparency in identifying the facts of criminal manipulation and informing stakeholders about the measures taken to investigate and prevent economic crimes can minimize the damage to the company's reputation both from outside and within it (PWC, 2018). Cybercrime is projected to become one of the most devastating threats to corporations in the near future. While most companies have a plan of actions in the case of a cybersecurity breach, only a few have conducted a cyber risk assessment.

References

Abdullah, W. N., & Said, R. (2018). The influence of corporate governance and human governance towards corporate financial crime: A conceptual paper. *Developments in Corporate Governance and Responsibility*, *13*, 193-215. https://doi.org/10.1108/S2043-052320180000013014

Achim, M. V., & Borlea, S. N. (2020). Economic and financial crime. *Studies of Organized Crime, 20*. Springer. https://doi.org/10.1007/978-3-030-51780-9_1

Alalehto, T., & Larsson, D. (2012). Vem är den ekonomiske brottslingen?: En jämförelse mellan länder och brottstyper. *Sociologisk Forskning*, *49*(1), 25-44.

Code of administrative offences of the Russian Federation from 30.12.2001 № 195-FZ. http://www.consultant.ru/document/cons_doc_LAW_34661/

Criminal Code of the Russian Federation from 13.06.1996 № 63-FZ. http://www.consultant.ru/document/cons_doc_LAW_10699/

Dolgova, A. I. (1999). *Criminology.* NORMA-INFRA-M.

Gottschalk, P. (2020). *Corporate responses to financial crime. SpringerBriefs in Criminology.* Springer. https://doi.org/10.1007/978-3-030-51452-5_11

Greer, B.J. (2017). The growth of cybercrime in the United States. https://www.researchgate.net/publication/320781855_The_Growth_of_Cybercrime_in_the_United_States

Group IB (2020) Hi-Tech crime trends 2020/2021. https://securityaffairs.co/wordpress/111434/cyber-crime/hi-tech-crime-trends.html

Gupta, D. K. (2020). Growing needs of forensic audit in corporate and banking frauds in India. https://ssrn.com/abstract=3624001

Hasnan, S., Rahman, R. A., & Mahenthiran, S. (2014). Determinants of fraudulent financial reporting: Evidence from Malaysia. *Jurnal Pengurusan*, *42*, 103-117. https://doi.org/10.17576/pengurusan-2014-42-09

International Monetary Fund (2001). *Financial system abuse, financial crime and money laundering-background paper*. https://www.imf.org/external/np/ml/2001/eng/021201.htm

Marshall, B. C., & Yeager, P. C. (1980). *Corporate crime*. Free Press.

Meerts, C. (2019). Investigations: Employee theft of employer property. In L. Shapiro, & M. H. Maras (Eds.), *Encyclopedia of Security and Emergency Management*. Cham: Springer. https://doi.org/10.1007/978-3-319-69891-5_87-3

Milligan, E. (2020). Libor trader Tom Hayes to be released from jail in January. https://www.bloomberg.com/news/articles/2020-11-02/convicted-libor-trader-hayes-to-be-released-from-jail-in-january

PWC (2018). Anti-fraud: What measures do companies take? Russian review of economic crimes for 2018? https://www.pwc.ru/ru/forensic-services/assets/PwC-recs-2018-rus.pdf

Rostelecom, & Tadviser (2020). How much artificial intelligence earns in Russia: Research by Tadviser and Rostelecom. https://www.company.rt.ru/press/news/d457435/

Russian Interior Ministry (2020). On the state of crime in the Russian Federation in the 1st half of 2020. https://мвд.рф/reports/item/21551069/

Securities and Exchange Commission (SEC) (2018). Commission statement and guidance on public company cybersecurity disclosures. A rule by the on 02/26/2018.

https://www.federalregister.gov/documents/2018/02/26/2018-03858/commission-statement-and-guidance-on-public-company-cy

Šikman, M. (2013). Corporate crime - New approaches and future challenges. In D. Čaleta & M. Vršec (Eds.), *Management of Corporate Security – New Approaches and Future Challenges* (pp. 103-114). Institut of Corporate Security.

Simpson, S. S. (2002). *Corporate crime, law, and social control (Cambridge studies in criminology).* Cambridge University Press.

Sutherland, E., Geis, G., & Goff, C. (1983). *White collar crime: The uncut version.* Yale University Press.

Tass (2020). In Russia, 16% of economic crimes are committed by entrepreneurs. https://tass.ru/ekonomika/8554543