DOI: https://doi.org/10.14505/jarle.v11.3(49).38

Integration of e-Government Bases as a Means for Ensuring Economic (Tax) and Information Security

Bagdat T. SEITOV
Department of Special Legal Disciplines,
Law Enforcement Academy under the Prosecutor General's Office of Kazakhstan,
Kosshy, Kazakhstan
astana0020@mail.ru

Medet S. ZARKENOV
Department of Special Legal Disciplines,
Law Enforcement Academy under the Prosecutor General's Office of Kazakhstan,
Kosshy, Kazakhstan
zarkenov@gmail.com

Nazarbek Sh. ZHEMPIISSOV
Department of Special Legal Disciplines,
Law Enforcement Academy under the Prosecutor General's Office of Kazakhstan,
Kosshy, Kazakhstan
oxbridge23@gmail.com

Oleg B. KHUSSAINOV
Department of International Law,
Institute of Sorbonne-Kazakhstan,
Abai Kazakh National Pedagogical University,
Almaty, Kazakhstan
husainov60@bk.ru

Dauren P. UTEPOV
Department of Special Legal Disciplines,
Law Enforcement Academy under the Prosecutor General's Office of Kazakhstan,
Kosshy, Kazakhstan
dauka_1986@mail.ru

Suggested Citation:

Seitov, B.T. *et al.* 2020. Integration of e-Government Bases as a Means for Ensuring Economic (Tax) and Information Security. *Journal of Advanced Research in Law and Economics*, Volume XI, Summer, 3(49): 1039 – 1044. DOI: 10.14505/jarle.v11.3(49).38. Available from: http://journals.aserspublishing.eu/jarle/index

Article's History:

Received 14th of March, 2020; Received in revised form 6th of April, 2020; Accepted 15th of May, 2020;
Published 30th of June, 2020.

Abstract:

In this article, on the basis of an integrated approach, a comparative legal method of cognition, it is proposed to integrate the bases of electronic governments to improve measures to effectively counter economic crime and ensure economic security. Given the global progress in dynamically developing market and civil property relations, in the context of the digitalisation of the economy, the methods of committing many crimes are evolving, their qualitative characteristics and methods of commission are changing. According to the authors, the information model of the integration of electronic systems of tax and other state bodies into a single electronic system will successfully prevent and combat crimes in the field of IT-technologies at the initial

stage of using information systems. In the future, the integration of electronic 'Governments for citizens' of different countries available for use by citizens and organisations in the field of taxes, public procurement, etc. into a single system will significantly increase information and economic security at the global level.

Keywords: government procurement; digital information; informatization and communications; cybersecurity; tax crime.

JEL Classification: H20; L81; L86.

Introduction

In everyday life, any of the citizens of countries with highly developed economies uses information and communication technologies. For example, paying taxes or participating in a public procurement tender involves the use of certain computer programs or electronic government (filing a tax return, issuing an invoice by a taxpayer, drawing up an electronic application for participation in a tender, etc.). At the same time, the state's primary task is to protect against fraud already at the stage of providing false information to state bodies. It is important at the initial stage to recognise the criminal intent of an unscrupulous user and stop his illegal actions. Today, states are constantly working to counter crimes committed using cyber technology, are actively taking all the necessary cyber protection measures, but the efforts made do not allow eradicating cyber threats. In this regard, the next barrier to ensuring security with insufficient protection of state electronic information resources is the legislative barrier in the form of the prospect of criminal prosecution (Konyavsky and Ross, 2020).

For these purposes, a whole chapter is provided in the field of informatisation and communication of the Criminal Code of Kazakhstan (2014). To achieve unlawful intentions and commit a crime, offenders often commit through 'unlawful access to information protected by law'. These acts formally fall under the disposition of Art. 205 of the Criminal Code, but only with the proof of intent. In practice, investigators cannot always prove the intent of a guilty (or do not pay attention to the accompanying article of the Criminal Code of Kazakhstan). In general, evidence is of the utmost importance in any legal process: on its basis, the court decides on the fault of a criminal suspect or on the liability of a party to civil law relations. Traditionally, evidence is divided into material (documents, photographs, etc.) and oral (evidence of witnesses). In the current Code of Criminal Procedure of Kazakhstan (2014) documents also include materials containing computer information (Brodskiy *et al.* 2019).

Sources of materials containing computer information are electronic devices: computers and peripherals, computer networks, mobile phones, digital cameras and other portable devices, including devices for storing information, as well as the Internet (Electronic Evidence Guide…2014). Information from these sources does not have a separate physical form. At the same time, electronic evidence is very similar to traditional evidence: the party that relies on them in the trial must demonstrate that they reflect the same circumstances and factual information that existed at the time an offence was committed. In other words, it is necessary to show that the data has not been modified, added or deleted, and no changes have been made (cannot be made) to them.

1. Security Features when Using Information and Communication Technologies in Kazakhstan

Electronic data have no material embodiment, so it is much easier to change or fake than traditional forms of evidence. This creates additional difficulties for the judicial system: it is necessary to develop such rules for the handling of electronic data that will ensure the reliability of evidence. Nevertheless, the norms of the criminal, criminal procedure law in this area require improvement, and possibly even an adequate tightening. At the same time, cybercrimes pose a particular danger, which undermine economic and social security in general and cause significant material damage. Offences committed using information technology in Germany (2006), France (2008), the UK (2008) and many other countries forced them to be identified as national (Guitton 2013). It must be understood that cyberthreats can come either from states, groups of people, or individuals. The former are classified as various kinds of interference in the internal affairs of another state, military operations, espionage (O'Connell, 2012). Crimes committed by groups of people are characterised by the presence of some obsessed idea, the actions of which are aimed at achieving a specific criminal goal. For example, organised criminal groups committing acts of terrorism, extremism. Among the common crimes committed by individuals using information technology, one can single out such as theft of funds from accounts, cyber fraud.

In Kazakhstan, public relations in the field of informatisation are regulated by the Law of Kazakhstan 'On Informatisation' of November 24, 2015. The objectives of this Law are the formation and ensuring the development of information and communication infrastructure, the creation of conditions for the development of local content in the production of goods, works and services in the field of information and communication technologies for information support of social and economic development and competitiveness of Kazakhstan. One of the basic principles of the Law is to ensure safety when using information and communication technologies (Law of Kazakhstan No. 418-V…2015). However, there are some drawbacks to this Law, which, in our opinion, hinder the

development of cybersecurity. An example is the definition of the term 'Information Security Incident Response Service'. The term includes the following: the organisation, based on the analysis of information security events, provides advice and technical assistance in eliminating the consequences of information security incidents (paragraphs 30-4 of Article 1 of the Law of Kazakhstan 'On Informatisation' (2015)). In the current wording, the term restricts actions and does not provide for the possibility of an organisation taking measures to prevent, protect against information security incidents, and if necessary, respond according to the degree of danger to a threat. Thus, for an authorised organisation, this definition, in addition to eliminating the consequences, should be supplemented with new powers for the prevention, protection, and most importantly the timely response to information security incidents.

In general, in order to prevent cyber threats, it is important for the legislative, executive, special and law enforcement bodies to study the entire system of interconnections of information and communication structures, paying attention to filling in the gaps in the regulatory legal acts regulating legal relations in this area, to improve methods for counteracting various offences, etc. Comprehensive strengthening of cybersecurity can favourably affect the work of functionaries in convenient and simple calculation, paying taxes and other obligatory payments from organisations and citizens, when submitting applications for public procurement, etc. On the other hand, in order to conveniently interact with citizens by states in the digital age, various innovations are being tested to ensure functionality and free access to electronic information resources. At the same time, it is important to minimise various kinds of cyberthreats. The functional structure of many e-governments still requires the improvement of information systems that are not yet integrable with other objects of the information and communication infrastructure of e-government. Cybercrimes challenge the whole world and national borders of Kazakhstan. All of the alleged threats encourage looking for appropriate solutions to protect against unwanted cybercrime.

In pursuance of the Message of the Head of Kazakhstan N. Nazarbayev, the authorised bodies developed the concept of 'Cyber shield of Kazakhstan', the purpose of which is to ensure the information security of society and the state in the field of informatisation and communication, as well as protecting the privacy of citizens when they use digital technologies (Message from the President of Kazakhstan…2017). In addition, the State Program 'Digital Kazakhstan' focused on enhancing cybersecurity, including increasing the resiliency of information systems of Kazakhstan, protecting the circuit in the field of information and communication technologies and increasing overall information security, starting from technical means and ending with creating a culture of safe behavior for citizens and companies in public networks (Decree of the Government of Kazakhstan…2017).

The commission of traditional mercenary crimes using information technology is still considered something remote for the simple reason that these crimes remain latent, they are inherently cross-border. In addition, digitalisation, including cybersecurity, has not yet found its distribution in various parts of the world, and authorised structures for the most part are still preparing to repel cyber-attacks. Given these shortcomings and the lack of proper attention to this issue, government bodies still do not show due interest in identifying crime patterns using digital technologies. Most economic crimes are already committed using information banking technologies, because digital technologies open up new possibilities for committing various types of tax evasion schemes, legalisation of criminal proceeds, 'cash-out' operations, etc. Given the great susceptibility to various types of abuse, special attention should be paid to the issues of combating tax violations and public procurement. One such example of information vulnerability is the identified corruption scheme committed on the public procurement portal by specialists of the Centre for Analysis and Investigation of Cyber Attacks.

Private data from auctions and tenders were assessed using the 'Yandex. Metrika'. This tool is often used by marketers to track and record user activity on a specific Internet resource. So, in the 'Yandex. Metrika' 'Webvisor' panel, it is possible to follow the history of all user actions (mouse movements, keystrokes, etc.), in particular, the set prices (The Ministry of Finance…2019). This example clearly demonstrates the possibility of using information technology for criminal purposes, and the ability of national information systems to prevent and record such criminal acts is important.

Progressive informational programs – spies can also significantly affect economic damage through the use of corruption schemes, and for many states this is an ongoing problem, and these issues require constant due attention. Earlier, the media published facts of hacking of the Public Procurement Portal. In particular, in 2013, an incident was detected on the public procurement website with the presence of an unlawful change in the text in ongoing public procurement (Obscene verses posted…2019). In addition, in 2014, according to the official resource of public procurement of Kazakhstan, the modules of the portal 'Competition and Auction', 'Price offers' were subjected to a DDoS attack, as a result of which the resource was unavailable (Kazakhstan's public procurement site…2019).

2. Analysis of the Implementation of Integrated Measures for the Implementation of Digital Technologies in State Structures of Kazakhstan

Today, in Kazakhstan, digitalisation is rapidly developing in all government agencies. The 'Government for Citizens' functioned successfully, which was created to increase the efficiency of the functioning of state structures and to provide quality public services. With the help of the introduced technologies, the state was able to provide citizens with convenience, accessibility, and information interaction with state bodies. Services have become electronic, efficiency has been increased, conditions for corruption have been reduced (Decree of the Government of Kazakhstan…2017). However, it should be noted that to date, there is no information interaction and integration of electronic systems in economic sectors.

Practice shows that offenders, in participating in public procurements, resort to various fraudulent activities by submitting false information to the Public Procurement Portal in order to become a winner in a competition. For example, by the verdict of the District Court No. 1 of the Medeu district of Almaty dated July 18, 2018, B. was found guilty of an offence under article 189 of paragraph 4 of paragraph 2 of the Criminal Code of Kazakhstan (2014). According to the materials of the case, the authorised bodies established that B.'s shell organisation presented deliberately fake documents, namely: bank guarantees on behalf of BankCenterCredit JSC, fake subcontracting agreements with other organisations and a number of other fictitious documents (Bank of judicial acts…2019).

In order to exclude facts on the provision by taxpayers participating in public procurement of fake banking documents, it is advisable to integrate the database of banking and tax systems in the public procurement information system. In this case, this mechanism will exclude contact with a participant in a public procurement contest, thereby excluding the possibility of providing fictitious documents, participation in the competition of taxpayers involved in illegal cash transactions and money laundering. At the same time, integrable data, namely bank guarantees and other documents received from the database of respective banks will testify to their authenticity.

Thus, on the basis of the above methodology, it is possible to modernise information systems of state revenues and public procurement by introducing the ability to integrate the necessary documents from various databases of relevant authorised bodies to fulfil the necessary obligations. This measure will accelerate the collection of documents and reduce administrative barriers to the collection of documents by legal entities and individuals, and will impede the participation of firms that were deliberately set up for cash transactions or that were previously noticed in non-fulfilment of tax obligations to the state (having arrears). In addition, integrable documents received from authorised bodies will be reliable and will exclude the possibility of falsification of these documents. Moreover, these innovations will eradicate corruption in integrable areas.

The only problem in this direction is providing the necessary protection for the database of authorised bodies from unauthorised access to information. For example, using the Telegram bot of the 'Fines and Taxes' channel, it is possible to check taxes, fines, deadlines for inspection, state transport number and other personal data on an individual or legal entity of Kazakhstan (Fines and taxes 2018). Free access to these data involves the introduction of effective information security. Consequently, cybersecurity remains relevant in the development of e-government. According to the Internet source Zakon.kz, to increase budget revenues, the State Revenue Committee of the Ministry of Finance is actively implementing projects to optimise and automate tax and customs administration procedures. One of the main goals of the Committee in this direction is to create a national system of traceability of goods from import/production to final sale. As part of the automation of customs procedures, last year, more than 850 thousand customs declarations were processed through the ASTANA-1 IS, of which 85% were issued automatically.

The basis for documented goods traceability is the 'Virtual Warehouse' module, which currently applies only to vehicles. The module employs 943 taxpayers, which received 75 thousand cars, of which 54 thousand were sold through electronic invoices. In the future, phased inclusion of other goods is planned. Since December 2018, the information system 'Electronic invoices' implemented jointly with the World Bank, has implemented electronic contracts and acts of completed work. To date, more than 173 million electronic invoices have been issued in the system. Also, in December last year, the Risk Management System was put into commercial operation. The system allows to analyse a large amount of data, automate business processes, reduce working time costs and identify new areas of risk of violations of tax and customs laws. As a result of developing risk models, about 50 billion tenge was recovered in the budget (7.9 trillion tenge of taxes…2019). In addition, the active introduction of advanced information technologies during remote monitoring allowed an authorised body to optimise the number of control measures (Bondarenko *et al.* 2019). As a result of optimisation for 2016-2018, the number of tax audits was reduced by 52% (7.9 trillion tenge of taxes…2019). According to the source of Zakon.kz, the Ministry of Finance, within the

framework of the 'Reform of Tax Administration' project, is improving the web application 'Taxpayer Cabinet', through which taxes are calculated and paid by legal entities, and also modernises the equipment of this system.

Currently, a transition to a new architecture is underway, thanks to which a separate application server will be allocated for each tax form, and there are 38 of them. This will allow more flexible management of application and equipment performance depending on the type of declaration and terms of submission, while eliminating any restrictions on the availability of the 'Taxpayer Cabinet,' Ruslan Ensebaev, Vice Minister of Finance said (Kazakhstan has simplified the process…2019). Systematic work to improve information systems includes the creation of new subsystems and integration with data from other government bodies. So, in September 2019, the subsystem 'Local taxes' of the 'Integrated Database' information system was put into operation. Today, the advantages of integrating information systems are obvious. For example, in order to carry out exact calculations on land tax and real-estate tax in a centralised order, the systems of the State Revenue Committee of the Ministry of Finance with the IS 'State Land Cadastre' of the Committee for Land Management of the Ministry of Agriculture and the database of the 'Real Estate Register' of the Ministry of Justice were integrated.

Currently, in Kazakhstan, citizens can pay taxes on transport, real estate and land tax through the mobile applications of second-tier banks. For example, making tax payments through the 'Kaspi Bank' application does not require additional data from taxpayers. At the same time, information in the system automatically comes from the corresponding databases. Such work facilitates the payment of taxes, reduces the number of offences and reduces problems associated with debt, fines and blocking taxpayers' accounts. According to the results of 2018, the annual plan for tax revenues of the state budget within the competence of the State Revenue Committee was executed by 101.9% (with the plan of 7 741.2 billion tenge, actually received 7 890.0 billion tenge overfulfilling by 148.9 billion tenge), including:

- on tax revenues of the republican budget by 101.8% (against the plan of 5 592.4 billion tenge, 5 694.9 billion tenge was received, overfulfilling by 102.5 billion tenge);
- on tax revenues of the local budget by 102.2% (against the plan of 2 148.8 billion tenge, 2 195.1 billion tenge was received, overfulfilling by 46.4 billion tenge) (7.9 trillion tenge of taxes…2019).

As a result of comprehensive work on the integration of data from various government agencies, notifications of upcoming tax payments through SMS messages are available. Short text messages about tax amounts are sent to mobile phones of citizens registered in the Base of Mobile Citizens and who are owners of land or real estate.

Conclusions

Thus, timely law-making in conjunction with the use of advanced information technologies in the field of informatisation and communications has significantly increased the effectiveness of combating crimes. In connection with the advent of digital technology, it may be argued that some functional actions of programs are carried out automatically using information systems. As a result, all responsibility may be erroneously transferred to inanimate equipment. Nevertheless, one cannot ignore the fact that a person can directly influence any technical device and information system.

The blind faith of an incompetent person in automated technology requires confidence in the exclusion of the influence of the human factor on certain algorithms of information technology, ignorance of the mechanism of the information system itself. In this regard, it is advisable to comprehensively develop cybersecurity, in particular, to analyse all the information systems of the Internet space in all spheres of public relations with the help of civilian control and public opinion. The active participation of consumers of electronic services and interaction with state authorised bodies will improve the quality of electronic services provided to the population and organisations, including payment services, reduce the risks of committing economic crimes, as well as crimes committed using information technology, and increase revenues to the state budget.

References

[1] Bondarenko, S. *et al.* 2019. Modelling instruments in risk management. *International Journal of Civil Engineering and Technology,* 10(1): 1561-1568.

[2] Brodskiy, A.V. *et al.* 2019. Identification in digital economy computer systems. *Journal of Communications Technology and Electronics,* 64(12): 1493-1499.

[3] Guitton, C. 2013. Cyber insecurity as a national threat: overreaction from Germany, France and the UK? *Journal European Security,* 1: 21-35.

[4] Konyavsky, V. and Ross, G. 2020. New method for digital economy user's protection. *Lecture Notes in Networks and Systems,* 78: 221-230.

[5] O'Connell, M.E. 2012. Cyber security without cyber war. *Journal of Conflict & Security Law,* 17(2): 187-209.

*** 7.9 trillion tenge of taxes were received in 2018 in the state budget of Kazakhstan. 2019. https://www.zakon.kz/4958538-7-9-trln-tenge-nalogov-postupilo-v-2018.html

*** Bank of judicial acts: Supreme Court of Kazakhstan. 2019. https://sud.gov.kz/rus/content/bank-sudebnyh-aktov.

*** Code of Criminal Procedure of Kazakhstan. 2014. http://adilet.zan.kz/rus/docs/K1400000231.

*** Decree of the Government of Kazakhstan No. 827 'On the state program 'Digital Kazakhstan'', 2017. http://adilet.zan.kz/rus/docs/P1700000827.

*** Electronic Evidence Guide: A basic guide for police officers, prosecutors and judges. 2014. Council of Europe Handbook. https://au.int/sites/default/files/newsevents/workingdocuments/34122-wd-annex_4_-_electronic_evidence_guide_2.0_final-complete.pdf.

*** Fines and taxes. 2018. http://www.shtrafkzbot.info.

*** Kazakhstan has simplified the process of paying taxes. 2019. https://www.zakon.kz/4989714-v-kazahstane-uprostili-protsess-oplaty.html

*** Kazakhstan's public procurement site was subjected to a DDoS attack. 2019. https://tengrinews.kz/internet/sayt-goszakupok-kazahstana-podvergsya-ddos-atake-251881/.

*** Law of Kazakhstan No. 418-V ZRK 'On Informatization'. 2015. http://adilet.zan.kz/rus/docs/Z1500000418.

*** Message from the President of Kazakhstan 'Third Modernization of Kazakhstan: Global Competitiveness'. 2017. http://adilet.zan.kz/rus/docs/K1700002017.

*** Obscene verses posted on the public procurement website. 2019. https://tengrinews.kz/story/nepristoynyie-stihi-razmestili-na-sayte-goszakupok-243754/.

*** The Criminal Code of Kazakhstan. 2014. http://adilet.zan.kz/rus/docs/K1400000226.

*** The Ministry of Finance responded to the CARK accusations. 2019. https://tengrinews.kz/kazakhstan_news/minfin-otvetil-na-obvineniya-tsarka-384856/.