World Bulletin of Management and Law (WBML)
Available Online at: https://www.scholarexpress.net
Volume-10 May-2022
ISSN: 2749-3601

DIGITAL FUTURE & CYBER SECURITY NECESSITY

1) Gulyamov Said Saidakhrarovich – Doctor of Sciences in Law (DSc), Professor, Head of the Private International Law Department, Tashkent State University of Law,
The web page: https://gulyamov.org/,
Gmail: said.gulyamov1976@gmail.com,
Phone number: +998900018779,
ORCID: 0000-0002-2299-2122
2) Khazratkulov Odilbek Tursunovich – PhD in Law, associate Professor of the Private International Law Department, Tashkent State University of Law.
Gmail: odilbekh@list.ru
Phone number: +998971327600
3) Eshbayev Gayrat Bolibek ugli – the student of the Tashkent State University of Law,
Gmail: esboevgajrat@gmail.com,
Phone number: +998903711585,
ORCID: 0000-0002-5273-1337

Article history:

Received: March 4th 2022
Accepted: April 4th 2022
Published: May 11th 2022

Abstract:

This article mainly considers the effect of cyber theft and data theft and its effect to the digital inheritance and analyses its consequences. However, this article considers the problems of electronic wills, which are the barriers to implement electronic wills instead of in a traditional, paper format.
The implementation of digital inheritance combined with increasing proportion of cyber-attacks. To protect digital inheritance, cyber security issues are essential on this article. Finally, article concerns the current situation in Uzbekistan and what measures must be done.

Keywords: Digital afterlife industry, Digital asset inheritance, Digital asset inheritance protocol, Data, Cyber security and theft, Transfer, Digital world, Digital transactions.

THE DIGITAL DEATH'S FUTURE. SUCCESSION OF DIGITAL ASSETS POSTHUMOUSLY

The many countries GDP takes financial benefit from social networks around the world and it is worth to highlight. The researchers as Carl J Öhman and David Watson supposed that a minimum of 1.4 billion users will pass away before 2100 if Facebook ceases to attract new users as of 2018.[1] The financial profit coming from the Digital Afterlife Industry estimated to $ 16-18 billion per annum in USA and £ 2 billion in UK in 2018.[2] We can assume that this money will be how much in 2050 globally and it may be even tripled in some countries, presumably. Actually, there are no national regulatory bodies, rules or standards for service providers to follow when managing the data of the deceased.[3]
Although these unresolved questions, researchers [4] suggested the digital asset inheritance system project to succeed digital inheritance. The model of transferring such an asset is name as the Digital Asset Inheritance. Also, they suggested some approaches but they still

[1] The authors are Carl J Öhman and David Watson. The title of the article is "Are the dead taking over Facebook? A Big Data approach to the future of death online" page 1 "Abstract, published on January-June 2019.
Online available at:
https://journals.sagepub.com/doi/10.1177/2053951719842540

[2] The authors of the book are Michael Arnold, Martin Gibbs, Tamara Kohn, James Meese and Bjorn Nansen. The title of the book is "Death and Digital Media", the first edition, published in 2017.
Online available at:
https://www.taylorfrancis.com/books/mono/10.4324/9781315688749/death-digital-media-michael-arnold-martin-gibbs-tamara-kohn-james-meese-bjorn-nansen

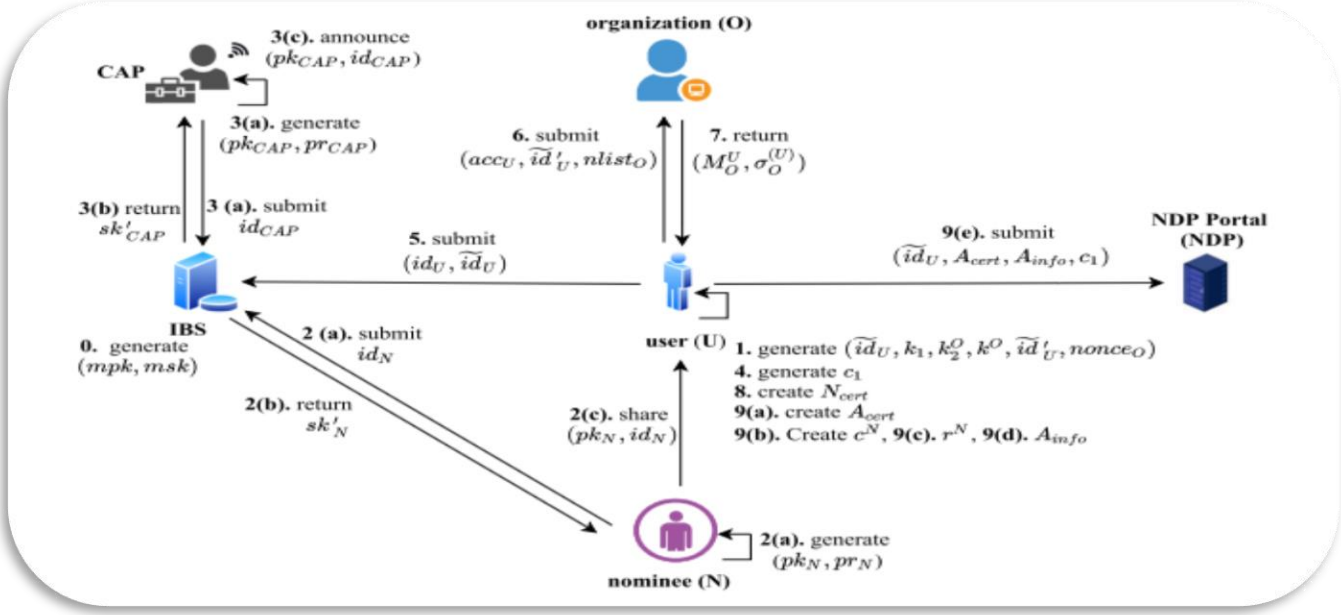
[3] Scolyer-Gray, P., Shaghaghi, A., Ashenden, D.: Digging your own digital grave: how should you manage the data you leave behind?
Online available at:
https://theconversation.com/digging-your-own-digital-grave-how-should-you-manage-the-data-you-leave-behind-143755, about Australia is given here:
https://hallandwilcox.com.au/thinking/what-happens-to-your-digital-wealth-on-death-and-incapacity/

[4] The authors are Ram Govind Singh, Ananya Shrivastava and Sushmita Ruj. The title of the article is "A Digital Asset Inheritance Model to Convey Online Persona Posthumously" published on 30 April, 2022.
Online available at: A Digital Asset Inheritance Model to Convey Online Persona Posthumously (springer.com)

World Bulletin of Management and Law (WBML)
Available Online at: https://www.scholarexpress.net
Volume-10 May-2022
ISSN: 2749-3601

could not define the method of uniting all digital data personal information or approving it with the big social network companies (for example Facebook, Instagram, Telegram, Twitter and etc.).

AI can be used to create a safer world, but at the same time, too much trust in automation and machines can pose a real threat. Uzbekistan, although later than other countries, nevertheless began to develop its strategy.[5]



[6]

This diagram demonstrates that how the predicted the digital asset inheritance system operates, represented by scholars.[7] Indeed, they concerned four stages as: stage 1 – registration, stage 2 – generation of nominee certificate, stage 3 – storing asset inheritance data, stage 4 – updation/deletion of nominee details at each organization. This procedure closely connected with algorithmic calculations. The authors state that their project digital asset inheritance protocol is secure to protect the assets from any threat.

The efficiency and types of the electronic wills

The development of electronic devices is definitely affecting to change the legal relationship among people by excessively using them in every corner of life. Simultaneously, it is affecting to establish the new types of currencies in an electronic and digital format, which cannot be touched by hand. Meanwhile, the USA practice highly influenced to digitalization by creating the different types of electronic wills as:

1. offline electronic wills;
2. online electronic wills;
3. qualified custodian electronic wills.[8]

Offline electronic wills are traditionally typed on a computer and stored on a hard drive. They have never printed or uploaded on a web survey. On the other hand, online electronic wills are stored in social accounts such as the Cloud, Google documents and etc. The last sort of electronic will is the custodian electronic will, which considers when a company becomes a custodian and it regulates, controls, creates, executes, stores the testator's will.

[5] The title of the article is "Strategies and future prospects of development of artificial intelligence: World experience", conclusion, the authors are Gulyamov Said Saidakhrarovich, Bozarov Sardor Sokhibjonovich, published on April 20th, 2022. Online available at: https://scholarexpress.net/index.php/wbml/article/view/841.

[6] Copied from the article. "Fig. 1 Pictorial description of Asset Management protocol Π1". The authors are Ram Govind Singh, Ananya Shrivastava and Sushmita Ruj. The title of the article is "A Digital Asset Inheritance Model to Convey Online Persona Posthumously" published on 30 April, 2022.
Online available at: A Digital Asset Inheritance Model to Convey Online Persona Posthumously (springer.com)

[7] *Ibid.*

[8] Harvard Law Review. Cyber law/Internet. What is an "Electronic will"? Development in the law.
Online available at: https://harvardlawreview.org/2018/04/what-is-an-electronic-will/

World Bulletin of Management and Law (WBML)
Available Online at: https://www.scholarexpress.net
Volume-10 May-2022
ISSN: 2749-3601

- **The USA court practice relating to regulate electronic wills and their application**

When a case appears before the court concerning the wills, the judges must find answers to the two following questions:

1. Whether an heir intends to succeed a will or not;
2. If an heir wants to succeed, then, based on which terms.

The succession of wills must be valid, written, signed and witnessed by more than one individual. [9] Traditionally, the inheritance process requires strict rules, which must be established in compliance with the law. But, the criticisms against these strict rules by scholars and professors forced them to change. In 1970, Professor John H. Langbein stated that formalities were needless to clarify a testator indeed wanted to succeed in his inheritance, it mostly represented the purpose of Wills Act formalities.[10] After a long period of time, the courts began analyzing the cases regulating to succeed the wills thoroughly than whether it complained with Wills Act of formalities or not.[11] Currently, almost all states require wills in a written format, a tangible document except for an electronic will.

The necessity for applying the electronic wills unlikely will be increased in the upcoming years. Professors Gerry Beyer and Claire Hargrove clarified the seven barriers which become the reason for decreasing the application of electronic wills:[12]

1. Technical barriers such as the lack of software that would provide adequate authentication;
2. Social barriers such as attorneys' reluctance to help create electronic wills;
3. Economic barriers such as the expense of implementing new technology;
4. Motivational barriers such as a lack of recognition of the potential benefits of electronic wills;
5. Obsolescence barriers stemming from changes in technology, and;
6. A general resistance to change.

The fast changes in digital world services, cloud services, electronic services, and social networks over the past decades definitely suggest that people become more addicted to using the internet because of its comfort. If we will take into consideration the statistics that 35% of American adults owned a smartphone in 2011, this percentage has nearly doubled up to 68% in 2015.[13]

A comparison of the social networking sites is also useful: In 2007, Twitter had just recently been established[14], Facebook users number counted nearly 58 million.[15] Currently, these two big social networks companies' users reached 2 billion users, respectively.[16] However, it seems that the barriers which are prescribed above by Professors Gerry Beyer and Claire Hargrove – motivational, social, technical, and other barriers are more silent. Despite these facts, people are

[9] The author is Gökalp Y. Gürer. The title of the article is "No Paper? No Problem: Ushering in Electronic Wills Through California's "Harmless Error" Provision". University of California, Davis, published in 2016.

[10] Langbein, supra note 16, at 489; see also Gürer, supra note 18, at 1965–66.

[11] ee, e.g., Martina v. Elrod, 748 S.E.2d 412, 414 (Ga. 2013) ("The doctrine of substantial compliance, though tolerant of 'variations in the mode of expression' utilized to satisfy statutory requisites, nonetheless requires 'actual compliance as to all matters of substance.'" (Quoting Gen. Elec. Credit Corp. v. Brooks, 249 S.E.2d 596, 602 (Ga. 1978))); Smith v. Smith, 348 S.W.3d 63, 63 (Ky. App. 2011) (holding that the doctrine of substantial compliance could not be used to deem a will compliant where it was signed by only one witness and two were usually required).

[12] Beyer & Hargrove, supra note 26, at 890–96. The title of the article is "Digital Wills: Has the Time Come for Wills to Join the Digital Revolution?". Published on February 2009. The author is Gerry W. Beyer from Texas Tech University.

[13] Monica Anderson, Technology Device Ownership: 2015, PEW RES. CTR. (Oct. 29, 2015), Online available at: http://www.pewinternet.org/2015/10/29/technology-device-ownership-2015/, https://perma.cc/AP3X-7ESX.

[14] Twitter was launched on March 21, 2006. Amanda MacArthur, The Real History of Twitter, in Brief, LIFEWIRE (Nov. 7, 2017), Online available at: https://www.lifewire.com/history-of-twitter-3288854, https://perma.cc/U3RU-M7AW

[15] Ami Sedghi, Facebook: 10 Years of Social Networking, in Numbers, THE GUARDIAN: DATABLOG (Feb. 4, 2014, 9:38 AM), Online available at: https://www.theguardian.com/news/datablog/2014/feb/04/facebook-in-numbers-statistics, https://perma.cc/5HYH-TE37

[16] Kathleen Chaykowski, Mark Zuckerberg: 2 billion Users Means Facebook's "Responsibility Is Expanding," FORBES (June 27, 2017, 1:37 PM), https://www.forbes.com/sites/kathleenchaykowski/2017/06/27/facebook-officially-hits-2-billion-users, https://perma.cc/GPJ4-EHC8

World Bulletin of Management and Law (WBML)
Available Online at: https://www.scholarexpress.net
Volume-10 May-2022
ISSN: 2749-3601

more reluctant to use them regularly than any other activity in various aspects of their lives.

The practice indicates that the usage of the internet is swiftly increasing despite any interruptions. Simultaneously, the proportion of users will be increasing.

As electronic devices and internet connections are increasing, testators become more inclined to save papers, even vital documents including personal data on such devices or services, and they are likely to expect those documents to have legal effects.

Innovations pushed for or promoted by commercial corporations, such as websites that allow testators to prepare wills inexpensively and simply, [17] statutes allowing private firms to serve as qualified custodians for electronic wills, services that assist in the creation of verified digital signatures, and electronic notaries imply that the private sector is working to make electronic wills viable.

The only thing that remains to be done to make electronic wills function is for courts and legislators to take a methodical approach to regulate and interpret them. For hundreds of years, there have been no substantial changes in the procedures related to the creation and execution of wills.[18] Courts and legislators must now comprehend the concerns that are likely to arise in the context of electronic wills. As a result, the broad term "electronic will" into the three types of fact patterns that are anticipated to emerge in this field. Offline, online, and qualified custodian electronic wills are susceptible to the generic electronic wills concerns of fraud and obsolescence, but each category has its own set of factors for courts and lawmakers to address. Finally, courts and legislators must decide how to best empower testators' freedom of disposition via their wills — regardless of how they choose to construct them.

Inheritance agreement in a digital age

Civil law is faced with the difficult challenges of a digital age. Some legal problems in Civil Law are not resolved till nowadays and it has to be legally regulated. Nevertheless, the government of Uzbekistan actively participates in the capital market through its SOEs and banks that issue, own, manage various securities, and render intermediary services in the financial market,[19] which really helps to develop civil law legislation in some extent.

Inheritance law is a part of Civil law and it also has some legal problems. For example, when inheriting a cryptocurrency or deciding what to do with a social account of the holder after his death. In particular, the new types of legal institutions, such as the inheritance contract impacts digitalization. In this regard, a dilemma concerns how the current regulation and the practice of applying the law must be effectively regulated.

An inheritance contract is assumed as an agreement, the terms of which determine the heir's circle and the procedure for the transfer of rights to the property of the testator after his death. [20] An analysis of the definition and legal norms makes it possible to understand that the main goal of introducing the structure of an inheritance contract is to provide the testator and potential heirs with the opportunity to formally succeed certain rights and obligations prescribed in the contract relating to each other. Obviously, the main problem here will be the potential heir's actions in favor of the testator in exchange for guarantees of receiving an inheritance in the near future.

It must be noted that this type of agreement is convenient for making the lifetime maintenance of testators. Because it becomes more effective from the moment when it is signed rather than a will. Also, the inheritance contract is more convenient for older testators, compared with the contract of life maintenance with a dependent, where the real estate ownership rights are not retained by the rent recipient. According to the inheritance contract, the right of ownership (an authority to dispose of) fully remains with the testator.

Nevertheless, there is the problem of establishing the relationship of the inheritance contract with relevant categories. Accordingly, a contract and a will. Unfortunately, the Civil Code of the Republic of Uzbekistan does not consider norms establishing the legal force ratio of a will and an inheritance contract. There are significant problems associated with the subject composition, the content, regulation of the inheritance contract, and the consequences of its violation.

---

[17] See, e.g., LEGALZOOM, https://www.legalzoom.com/sem/homepage/, https://perma.cc/ZB7H-932E

[18] See Caldwell, supra note 5, at 467.

[19] The authors are Said Gulyamov, Otabek Narziev, Sadoqat Safoeva, Jahongir Juraev. The title of the article is "State Role Securities Market Development in Uzbekistan", published on the American Journal of Political Science Law and Criminology, on June 18, 2021.

[20] Section V, inheritance law, chapter 66. General provisions on inheritance.
Online available at: https://lex.uz/docs/180550

World Bulletin of Management and Law (WBML)
Available Online at: https://www.scholarexpress.net
Volume-10 May-2022
ISSN: 2749-3601

Legal researchers of the inheritance law field have analyzed the structure of the inheritance agreement under different legal regimes, which made the unsatisfactory conclusion as "the degree of connection of the testator is so weak and the degree of risk of the heir is so huge which in fact, it makes a will with a clause on compensation for damages in case of cancellation".[21] It means that how much the inheritance contract is the most beneficial for the testator, the heirs carry the risks as much as possible.

On the other hand, it is criticized due to the lack of protection for the weaker participants in the turnover, especially those who due to their age or health status are at the risk zone of being misled. There is a position that this aspect is not sufficiently taken into account by our legislators in situations where fraudsters take advantage of the excessive gullibility of older people who were unable to adapt to the conditions of a market economy persuading them to make certain transactions. The hereditary contract establishes excellent conditions only for the elderly. The testator has the right to withdraw from the contract, and can freely dispose of the property but the other party to the contract (or other parties) is responsible for the maintenance of the testator simultaneously. The uniqueness of the inheritance contract under the Civil Code of the Republic of Uzbekistan is especially evident when compared with similar phenomena in other countries. For example, under German law, the parties are firmly bound by the agreement and the inheritance contract can be terminated only in exceptional cases.[22] Simultaneously, there is a problem of insufficient protection of the future heir. Having assessed all the risks, the heir might refuse to conclude an agreement with the testator. Consequently, there are doubts based on serious arguments that the inheritance contract will often be applied in practice. The potential positive effect of the inheritance agreement for the testator is leveled due to the reluctance to conclude it with potential heirs. It means that the practice of concluding the inheritance contracts and the complete absence of court decision on this matter means that it is too early to discuss about the core meaning of the inheritance contract.

The inheritance contract is effective just in some cases. For instance, it applies to the situation of inheriting the business assets and other property used in entrepreneurship.

An inheritance agreement can be concluded with the aim when the heir begins to develop the use of a digital account (social network account) registered for a commercial purpose. In this case, several economic and legal aspects instantly are resolved: the testator not only introduces the potential heir of the agreement but also transfers the necessary data like keys, passwords, user names, etcetera. Meanwhile, the testator will be able to change the needed data (password, key, etcetera) if he decides to find another heir, but then the heir can sue the testator for losses caused by terminating the contract or not complying with the requirements of the contract. Anyway, there will be economic and legal advantages for all parties of the contract.

The theory and law enforcement practice is now looking for mechanisms improving legislation. However, the practice of entrepreneurship and business activity should find the most effective answer to the application for specific relations of the inheritance contract. The results should be based on the recommendations of citizens and lawyers. Presumably, the legal regulations where the inheritance agreement can solve specific practical problems are entrepreneurship including the inherited rights relating to corporate regulations, as well as, digitalization.

Currently, the world is trying to establish the distinctive features of the inherited properties and access of heirs to them, discussing the digitalization process of society and the challenges that the inheritance law faced up with it. Consequently, cryptocurrency and digital rights are increasingly considered in practice as objects of property relations. Therefore, they are subject to inclusion in the estate. The problem of access to such objects will inevitably arise, the exact determination of what exactly the testator owned. These problems can be overcome with the help of a hereditary contract where the parties have the opportunity to determine the list of objects of hereditary succession (including those existing in a digital form), as well as, the procedure for their transfer. Such a mechanism is also beneficial for the testator, who will be sure that his digital objects will pass to the heir.

[21] The title of the article is "International inheritance law - avoiding conflicts of jurisdiction". The authors are Walter Häberling and Alexandra Schnyder. MLL Meyerlustenberger Lachenal Froriep Ltd. Switzerland, published on February 22, 2018.

Online available at:
https://www.lexology.com/library/detail.aspx?g=eff04523-1946-42d9-b026-cdd85288e5f1

[22] Kroiß, L. Vorsorge für den Erbfall durch Testament, Erbvertrag und Schenkung / L. Kroiß. – München. – Bech. – 2019. – 52 s.

World Bulletin of Management and Law (WBML)
Available Online at: https://www.scholarexpress.net
Volume-10 May-2022
ISSN: 2749-3601

Thus, the effectiveness of the inheritance contract digitalization can be expressed in two ways. *Firstly*, this is the definition of objects of hereditary succession, the origin, and existence of which may be known to a limited circle of people due to their digital nature: cryptocurrency, social network account or account in the game. In the inheritance contract, such objects will not only be listed but also clearly described. *Secondly*, it is a description of the order of transmission of objects that exist in a "digital" form (for example, the access obtaining order of a "key" to bitcoins). Therefore, the testator can place the key in a safe deposit box with the possibility of accessing it after his death.

The inheritance contract is a complex construction that has not been tested in practice. Its use is quite often not rational and it is often easier and more logical for the parties to choose constructions that are more familiar to practice – a will or life maintenance with a dependent. However, a hereditary contract can be effective and should be used by the parties, where the constructions recognized by practice do not allow the parties to achieve the goals they pursued. The above applies to situations of inheriting digital assets and for other objects, the legal regime of which is complicated due to their special nature and tied up with digitalization. However, the capital market is an indispensable tool of economic development and plays a key role in today's global financial economy, where transactions are carried out electronically and across international borders.[23]

The cyber law's influence on digitalization

The international cooperation against cybercrime must be carried out by all countries, which is predetermined both by the property of information as an object of encroachment and by the nature of committed crimes. An international expert on cybercrime law Stein Schjolberg stated that cyberspace is the fifth common need after land, sea, air, and space, which requires coordination, cooperation and special legal measures around the world".[24]

Indeed, all directions of law are directly dependent on the computer's cooperation and information networks in the IT technology world.

For the time being, information is recognized as one of the most important tools to influence. Therefore, its protection is so important task together with receipt and transmission in a digitalized world. For example, the revolutionary events of the so-called "Covid-19" in the world media and political discourse turned the role of information and communication technologies into the highest demand.

The swift changes in disseminating information through Internet, mainly through official networks played a crucial role against the people who wanted to hide their illegal actions from the international community and did not want to reveal their inadequate information concerning to committing crimes and wars.

At present, IT technologies are changing and combining with other technologies. In fact, participation of all countries will cut down the transnational cybercrime around the entire world and the negative consequences suddenly will be decreased. Even in trials AI began changing human beings even though it controls the minor issues.[25]

However, every second 12 people are cyber-attacked and nearly 56 million cybercrimes are committed annually based on Symantec Security analysis of an international cyber security service, the damage from which equals nearly 100 billion US dollars globally.[26]

Cybercrime violates the rights of both government and individuals. Undoubtedly, the peculiarities of information systems functioning, primarily the Internet requires cooperatively working with the various sectors as public and private, which is directly related to ensuring cyber security.[27] Nevertheless, the country is able to effectively implement a full-scale counteraction against cybercrime and create conditions to protect themselves so that people who are most susceptible to cyber-attack can build a more powerful system of protecting data information (for example, the financial

[23] The author is Gulyamov Said Saidakhrarovich – Doctor of Law, Professor, head of the Department of International Private Law of the Tashkent state university of Law. The title of the article is "The Institutional and Legal Framework of Emerging Capital Markets: The Experience of Cis Countries". Turkish Journal of Computer and Mathematics Education. Published on 05.04.2021

[24] Schjolberg Stein. A Cyberspace Treaty – United Nations Convention, Protocol on Cyber-Security and Cybercrime. Twelfth United Nations Congress on Crime Prevention and Criminal Justice. Salvador, Brazil, 12-19 April 2010.

[25] The title of the article is "Digitalization of international arbitration and dispute resolution by artificial intelligence". The authors are Said Gulyamov, Mokhinur Bakhramova, page 83, published on April 24th, 2022.

[26] Karpova D.N. Cybercrimes: a global issue and its solution. Vlas. The Power, 2014, no. 8, pp. 46-50. (Russian language).

[27] *Ibid.*

World Bulletin of Management and Law (WBML)
Available Online at: https://www.scholarexpress.net
Volume-10 May-2022
ISSN: 2749-3601

sector, banks, crypto assets of individuals, e-money and etc.).

Many researchers note that internet users want to use international social networks, educational institutions and others in order to accomplish their vicious goals even by violating the law. For example, the media played a major role in spreading fake news during the US presidential election.[28] It means that cybercrimes are committed even at a governmental level.

However, this is not the only one fact of committing international cyber-crime based on real facts on a governmental level.

The first internationally renowned hacker group is named "Anonymous" or as it is called for the convenience of coverage by the community "Humpty Dumpty" since all messages and "leaks" of information published on the network by members of this association were published on behalf of the fabulous and hidden character.[29] This group has existed since 2013, its list of targets included prominent politicians, officials, public figures and representatives of the media. In addition, this group of experts is credited with hacking the systems of the US Democratic National Committee and obtaining compromising evidence on the Democratic presidential candidate, which could influence the outcome of the US election campaign in 2016.[30] The specialists of this criminal group have been active for a long time and their targets are government networks, religious and corporate web pages, accounts of officials, and famous people. This group uses all methods of committing cybercrime to promote political ideas and spread freedom of speech, protection of human rights and freedom of data information. The ambiguity of this group's behavior has allowed the development of a lot of rumors and legends around their true goals, but the facts state that this organization sees freedom of speech and information, exposing corporate lies and inequality, and achieving political truth as its goal, which makes this group rather the idea of a movement around the world, especially considering the calls for participation that activists leave after a series of attacks.

However, this organization has many web pages on social networks, where their statements are published regarding any events or famous people at different times. For example, the page contains a video discussion on the topic of the US elections, containing information, probably obtained illegally, discrediting the honor and dignity of the US President, accusations of false statements, proposals about the future of the US during the presidential term and a video investigation into the death of Aaron Schwartz, an internet activist and free flow of information activist, which cited numerous violations of the Constitution by the authorities, with accusations of incitement to suicide, in addition, activists hacked into the website of the US Corrections Commission by posting a threatening message to employees.

International cooperation with cyber law protects digital transactions flow

Cybercrime is not a new phenomenon and specialized governmental bodies, international organizations on a regional and global scale and professors have begun studying cybercrime a long time ago. It should be noted that the applicability and effectiveness of these rules do not make results based on statistics in practice. However, the whole losses from cybercrime or cyber-attack would be nearly 90 trillion US dollars according to the Accenture Security report by 2030.[31]

It means that the different international acts actually have been adopted to combat cybercrime and cyber-attack. One of the first documents adopted in the 21st century, which outlined the main trends and highlighted the main aspirations of the signatory countries in the field of the information society, was the "Okinawa Charter of the Global Information Society"[32] adopted on July 22, 2000. This Charter noted the important

[28] The title of the article is "Influence of fake news in Twitter during the 2016 US presidential election". The authors are Alexandre Bovet & Hernán A. Makse, published on 02 January, 2019.
Online available at:
https://www.nature.com/articles/s41467-018-07761-2\

[29] Anonymous hacker group. Business Info and System Analytics GBA-327-CA03. The author is Dr. Bryan Reagan.
Online available at:
https://www.saintleo.edu/hubfs/Resource%20PDFs%20and%20DOCs/Academics/Center%20for%20Cybersecurity/Student%20Projects/2019/Anonymous%20Hacker%20Group.pdf

[30] The author is Slobodyan E. The title of the article is "What is the group of hackers Fancy Bears? // Arguments and Facts". Published on 14.09.2016
Online available at:
http://aif/ru/dontknows/file/chto_predstavlyaet_soboy_gruppirovka_hakerov_fancy_bears

[31] Bissel K., LaSalle R.M., Richards K., "The Accenture Security Index". Redefining security performance and how to achieve it in 2017, page 19.

[32] Online available at:
https://www.markle.org/sites/default/files/dotforce_2001_Okinawacharter.pdf

World Bulletin of Management and Law (WBML)
Available Online at: https://www.scholarexpress.net
Volume-10 May-2022
ISSN: 2749-3601

necessity of developing global information systems for interaction with countries and civil society.

In addition, the document concerns the importance of stimulating the development of information technologies, which help people and society by broadening their knowledge and getting new ideas. Moreover, this document concerns provisions for eliminating the digital division in the world, creating conditions for healthy and fair competition in information technology development. This document also contains provisions on maintaining constant, fast, reliable and secure access to information technology. Additionally, it implies the protection of intellectual property rights and it states that the efforts of the international community must be accompanied by concerted action to create crime-free cyberspace from any illegal actions in a cyber-world".[33]

The International Telecommunication Union through recommendations and guides formulate the key features of international information threat. So, a recommendation called "Global Cyber security Index"[34] was adopted under "Resolution 130 on strengthening the role of ITU in building confidence and security in the use of information and communication technologies".[35]

This Resolution was created to support the international cooperation initiative in the security field in order to facilitate the exchange of information and protection of information at the international level.

However, the global index performs the function of monitoring the legislation of the countries and based on these indicators, it creates the basis for the international legal regulation of international information cyber security. Additionally, the legal documents against cybercrime are adopted by the United Nations, for example, the United Nations Convention against Transnational Organized Crime[36] mentions the need for cooperation among UN member states in developing training programs, data collection and analysis, and other cooperation, creating cooperation to increase the effectiveness of the fight against organized crime using computers, various types of telecommunications and other methods using modern technologies as far as possible. The Republic of Uzbekistan assuming all the obligations outlined in this document, thereby the basic principles of the information society also signed this Protocol on July 8, 2008.[37]

One of the most important acts in the development of an international advancement against combating cybercrime is adopting the Convention on Cybercrime.[38] This Convention became the first international act regulating multilateral agreements to combat cyber-crime and other types of crimes in IT on a global and regional scale.

Additionally, this Convention created the foundation for procedural interaction between countries' specialized institutions, which signed Convention. Moreover, this Convention did not only play an important role in the European Union (hereinafter – EU) territory but also outside of the EU. Therefore, this Convention was signed by Japan, the USA, Australia, Canada, and several other countries. 50 countries are parties to this Convention and fully accept its terms and requirements and 5 states signed the document but did not ratify it.[39]

United Nations has been actively participating in the processes of interacting with countries and other regional organizations on ensuring cooperation in the cyber-security field in recent years. For example, a Resolution was adopted based on the results of the 12th UN Congress on Crime Prevention and Criminal Justice, which established an intergovernmental group of experts whose work was concerned with a comprehensive study of cybercrime problems around the world and analyzed the implemented measures by the UN Member States.[40]

The expert group prepared "a report on a comprehensive study of cybercrime" published in

[33] Okinawa Charter of the Global Information Society. Adopted on July 21, 2000.

[34] The Global Cybersecurity Index.
Online available at: https://www/itu.int/en/ITU-D/Cybersecurity/Pages/global-cybersecurity-index.aspx

[35] Online available at: https://www.itu.int/en/ITU-D/Cybersecurity/Documents/RES_130_rev_Dubai.pdf, https://www.itu.int/en/Pages/default.aspx

[36] United Nations Convention against Transnational Organized Crime and the Protocols Thereto. Adopted by the UN General Assembly on 15 November, 2000 by Resolution 55/25. Entered into force on 29 September 2003, in accordance with article 38. Signatories: 147
Online available at:
https://www.unodc.org/unodc/en/organized-crime/intro/UNTOC.html

[37] Online available at: https://lex.uz/docs/1304112

[38] Convention on Cybercrime, adopted on 23.11.2001 in Budapesht.

[39] Okinawa Charter of the Global Information Society. Adopted on July 21, 2000.

[40] Resolution adopted by the UN General Assembly // Twelfth United Nations Congress on Crime Prevention and Criminal Justice / A / RES / 65/230 1/01/2011.
Online available at:
http://www.unodc.org/documents/justice-and-prison-reform/AGMs/A_RES_65_230r.pdf

World Bulletin of Management and Law (WBML)
Available Online at: https://www.scholarexpress.net
Volume-10 May-2022
ISSN: 2749-3601

February 2013.[41] The experts of this group stated that most of the countries did not take into consideration the necessity of introducing additional measures according to cyberspace and cybercrime in their national legislation or Criminal Codes even though effective cooperation is already possible based on signed agreements, Conventions, and interactive mechanisms. Also, the "Doha Declaration" was prepared and approved under the auspices of the UN Office on Drugs and Crime in 2015,[42] which fully described the direction of fighting against crime and cybercrime.

The UN has a specialized agency the International Telecommunication Union (hereinafter – ITU), which was founded under the name of an International Telegraph Union in 1865 then, it became a specialized agency of the UN in 1947. Currently, the members of this organization are 193 countries and about 800 organizations, academic institutions, and business entities around the globe. The headquarter is located in Geneva, Switzerland. Meanwhile, there are more than 12 regional offices around the world. This Union is part of the UN as a specialized agency; its main directions include developing technical standards for broadcasting and joining the exchange of information and improving access to Information and communications technology (hereinafter – ICT) worldwide. Also, it includes analyzing and studying the violations of information exchange. In this regard, ITU launched the "ITU Global Cyber security Agenda", which was aimed at maintaining security and openness in the information society of the 21st century in 2007. This program concerned 5 main principles:

- Legislative measure;
- Implementation of technical initiatives;
- Organizational structuring;
- Capacity building in the information environment;
- International cooperation in this area.[43]

Meanwhile, this Union annually collects indexes of various research groups, organizations, business entities, and others by region, and country for analyzing in detail and presenting the dynamics of main trends, changes with new ideas concerning cyber security, and counts the cyber-attacks per year and etcetera.[44] As a result of a research conducted by ITU in 2017, the report "Global Cyber Security Index (GCI) 2017 demonstrated that the main measures and directions of countries combatting cybercrime are mainly based on planning strategic decisions by the five principles of the global cybercrime programs,[45] such as:

- implemented and done legal measures on the territory of the states based on functioning and existing institutions and structures for decreasing cyber-crime in matters of law;
- investigated the existing measures in the countries, organizations for the development of technical institutions and structures dealing with cybersecurity issues according to the technical and other applied rules;
- examined the present measures in the countries, organizations aimed at developing policies and strategies which directly coordinate cybersecurity at the national level according to the technical and organizational structuring rules;
- investigated the availability of activities of research and development, educational and qualification programs, certified organizations, and departments, which was involved in increasing the country's information potential country;
- explored the measures based on cooperation, partnership relations, and information exchange tools from different perspectives.

By reviewing the ITU report, it was found that countries were divided into 3 groups. The first group of countries where the development of cyber security is at the beginning level (it includes 96 countries whose index is the lowest and is only gaining up to 50 points compared with the best indicators). They are Central Asian, African, and Middle East countries, which have just begun implementing cybersecurity issues. The Republic of Uzbekistan is on this list.

The second group of countries is 77 in total, whose index variates from 50 to 89 points according to ITU experts, their level of cybersecurity is more advanced. These countries have developed comprehensive bilateral and multilateral agreements, frameworks, and integrated cybersecurity initiatives and programs globally. And the third group contains from the most developed countries.

[41] Comprehensive Cybercrime Study // United Nations Office on Drugs and Crime. Project, February 2013. UN-Vienna, 2013, page 360.

[42] Doha Declaration, adopted on April 19, 2015. The 13th United Nations Congress on Crime Prevention and Criminal Justice / UNODC. New York. Online available at: https://www.unodc.org/congress/en/previous/previous-13.html

[43] Index of cyber security. International Telecommunication Union, Geneva, 2017.

[44] *Ibid.*

[45] Online available at: https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2017-PDF-E.pdf

World Bulletin of Management and Law (WBML)
Available Online at: https://www.scholarexpress.net
Volume-10 May-2022
ISSN: 2749-3601

Meanwhile, a certain agreement was reached by the European Commission and the US regarding cross-border data transfer control. Also, the Directive 95/46/EC on the protection of individuals about the processing of personal data and the free movement of such data was adopted, where the guarantees for the protection of personal data were added.[46]

Nevertheless, countries should consider security measures directed to prevent illegal acts of spreading personal data, prevent unauthorized information, their modification, and illegal distribution by storing this information.

In most cases, countries are not obliged to monitor the network and block traffic. Then, it leads that the issue of the provider's responsibility and possible cooperation with law enforcement agencies and the cooperation limits.

When the entire world tried to fight against the COVID-19 pandemic, hackers used this situation for their benefit. Cyber threats skyrocketed even in the medicine sector. Hackers created the chaos and panic by the pandemic crisis. Phishing and hacking attacks have increased more than 5 or 6 times compared with their usual number of attacks over the past years. For example, they have begun using the virus to exploit users working online, remotely from a home.[47]

The UK and USA security officials have stated that a growing number of cybercriminals and other online violators are using the COVID-19 outbreak for their personal benefit. On April 8, 2020, the UK's National Cyber Security Center (NCSC) and the US Department of Homeland Security's Cyber Security and Infrastructure Agency revealed that advanced threat cybercrime groups are targeting individuals and organizations with a range of Malware and Ransomware.[48]

The countries' interaction combating cybercrime requires uniting the various countries' legal norms in fighting against cybercrime. In this case, the interaction of European Union member states, Europol, and Eurojust can positively influence on this process, where organizations' activity directly involves combatting cybercrime in the EU territory. Europol's work uses a system of analytical work files and data information generated and collected, which is mainly defined to support criminal investigations. Meanwhile, Eurojust activities are based on ensuring security in Europe.

Practice of Japan concerning digital inheritance

In Japan, a declining birthrate and mature population are intensifying at a speed phenomenal within the world. The country is already a super-aged society (a society in which the proportion of elderly persons who matured 65 a long time or more seasoned is more noteworthy than 21%) with its ratio of elderly people to the entire populace coming to 28.1% in 2018.[49] Against this foundation of a super-aged society, the expression "end-of-life planning" has come into well-known utilize to describe the making of progressed arrangements or the putting of one's issues in arranging for the most part by elderly individuals some time recently one's life concludes. Without any doubts, end-of-life arranging has gotten to be a social wonder in Japan centered approximately on the elderly.

In this way, it can be said that Japan, as a nation that has clearly gotten to be a super-aged society, is seeing the gradual formation of a culture that expects and plans for "death" in the shape of "end-of-life planning" (at the same time, whereas the need for end-of-life arranging is recognized, there are still many people who discover the subject of passing as well troublesome to handle and who cannot take the primary step in making preparations). Up to presently, end-of-life arranging has, by and large, centered on matters related to the burial service, gravesite, and inheritance. However, with the spread of digital gadgets such as personal computers and smartphones, the issue of "digital assets" is pulling in expanded consideration as they can pose issues when the client of an advanced gadget passes to Japan.

Nevertheless, Japanese legislation does not consider any special laws regulating the inheritance process of digital assets. Therefore, we will began discussing from

[46] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

[47] Online available at: https://www.cybersecurityintelligence.com/blog/cyber-attacks-up-500-in-a-month-4901.html

[48] The authors are Adhirath Kapoor, Ankur Gupta, Rajesh Gupta, Sudeep Tanwar, Gulshan Sharma and Innocent E. Davidson. The title of the article is Ransomware Detection, Avoidance, and Mitigation Scheme: A Review and Future Directions. Published on 21 December, 2021.
Online available at: file:///C:/Users/user/Downloads/sustainability-14-00008.pdf, https://www.ncsc.gov.uk/news/warning-issued-uk-usa-healthcare-organisations

[49] Online available at: https://www.stat.go.jp/english/data/handbook/c0117.html#:~:text=Japan's%20total%20population%20in%202020,of%2010%20million%20or%20more.

World Bulletin of Management and Law (WBML)
Available Online at: https://www.scholarexpress.net
Volume-10 May-2022
ISSN: 2749-3601

Japanese legislation regulating property law. We well know that two types of property exist as tangible and intangible property and the same types exist in Japan. It cannot be said that offline data is a thing that occupies a part of space, so it is not a tangible entity (but rather an intangible). As a result, property rights including the right of ownership to offline data cannot be considered and any heirs (family of the deceased) cannot inherit ownership of the deceased's offline data.[50]

The archival practice of digital inheritance

Getting digital inheritance through a notary office is one of the secure ways of succeeding digital inheritance. Because a testator transfers its property or a digital property to the notary, and then, they will keep this secret till the requirements of a testator written on a will are fulfilled even though the notary can use it for their own benefit. But we have not analyzed that how data information will be stored in the archive, or how it will be regulated. Now we will move on discussing this topic. To regulate this procedure has been established "Digital Archiving and Networked Services (hereinafter – DANS)" in the Netherlands.[51] This service includes and regulates different types of services such as "NARCIS - the Dutch Research Information System, EASY - the Electronic Self Archiving System for datasets".[52] It could control, manage and preserve the data sources more accessible and easier. DANS have begun exchanging data information with these systems. EASY data collection is based on gathering information concerning archeology in a legal deposit archive,[53] which means that information of the EASY relates to the social sciences. Storing data information is not globally regulated till nowadays. The organizational part, exchanging and saving data information between countries, how disputes concerning digital data inheritance are not regulated. Some social networks rejected sharing data information of people even for government authorities because their companies adopted privacy policy rules. Because of these factors, crimes concerning to illegal spread of data information is increasing in a high speed.

CONCLUSION

Regulating digital assets could not find its solution, countries view is varied from one another. On the one hand, the problem relating to the cyber security is so significant and the number of cyber-attacks is increasing around the world. The President of Uzbekistan Shavkat Mirziyoyev has announced turning the country into an IT regional center recently, the government is planning to invest 100 million US dollars by the end of 2022.[54] On the other hand, the question of regulating the digital inheritance is open around the world.

Meanwhile, many countries infrastructure concerning to regulate digital inheritance is not ready for implementing one unified legal system. Therefore, they are not trying to regulate this process. Even they regulate the digital inheritance process, then, they have to suddenly invest to investigate cyber law security, which requires not only finance but also highly qualified programmers, IT specialists and etc. However, AI encompasses a wide range of concepts and systems, but it may be defined as a collection of algorithms that can alter and generate new algorithms in response to learning inputs and data, rather than depending exclusively on the inputs they were built to recognize.[55] The realities of today absolutely determine that cryptocurrencies and the technologies underlying them have a huge potential from economical side, implementing a balanced legislative policy, which is combined with private and public legal relations. Additionally, the works of the famous American economist, Nobel Prize winner in economics field in 1991, the author of the "transaction costs" theorem Ronald Coase, who clearly noted that the market requires the approval of legal norms that would

[50] The author is Atsuda Matsushi, Japan Digital Shuukatsu (End-of-life-planning) Association Representative. The title of the article is "Manual for Handling Digital assets Left by the Deceased", page 2, "legal considerations of inheriting offline data", page 2, published in 2020.

[51] DANS, founded in 2005 as an institute of the Royal Netherlands Academy of Arts and Sciences (KNAW) and of the Netherlands Organisation for Scientific Research (NWO), has cumulative responsibility for 50 years of digital research data in the social sciences and humanities from its predecessor organizations. Online available at: AM15ProceedingsBorgmanDANS-FINAL20150819 (acm.org), page 2.

[52] *Ibid.* Page 2.

[53] *Ibid.* Page 2.

[54] Online available at: https://www.gazeta.uz/ru/2022/04/14/ict/

[55] The title of the article is "Issues of Legal Regulation of Robotics in the Form of Artificial Intelligence". The author of the article is Said Gulyamov and Sardor Yusupov, published 23 May, 2022. Online available at: https://scholar.google.com/citations?view_op=view_citation&hl=ru&user=kqUdLCsAAAAJ&sortby=pubdate&citation_for_view=kqUdLCsAAAAJ:WA5NYHcadZ8C.

World Bulletin of Management and Law (WBML)
Available Online at: https://www.scholarexpress.net
Volume-10 May-2022
ISSN: 2749-3601

determine the rights and obligations of people, who is doing transactions. He also stated that making a balance of private and public interests in market economy relations and is so difficult concerning to trade and retail. Therefore, activities should depend on the legal system of the country in the market.

The application of Ronald Coase statement is appropriate to apply into the market economy rules, primarily, for the cryptocurrency market. Moreover, cryptocurrency allows market participants to make settlements cheaper and faster. In this regard, the legal regulation of digital financial assets should be thoughtful.

It is significant to determine the objects of legal regulation for making simple and understandable rules simple within the dispositive priority regulation. Otherwise, it will be difficult to control the jurisdictions of developed economies which have entered towards technological and innovative processes a long time ago and will reduce transaction costs by taking advantage in digital financial assets market in Uzbekistan. The further measures must be implemented by thoroughly discussing and analyzing this topic and this process must not be postponed in any case.

World Bulletin of Management and Law (WBML)
Available Online at: https://www.scholarexpress.net
Volume-10 May-2022
ISSN: 2749-3601

BIBLIOGRAPHY

1. The authors are Carl J Öhman and David Watson. The title of the article is "Are the dead taking over Facebook? A Big Data approach to the future of death online" page 1 "Abstract, published on January-June 2019.
2. Online available at: https://journals.sagepub.com/doi/10.1177/2053951719842540
3. The authors of the book are Michael Arnold, Martin Gibbs, Tamara Kohn, James Meese and Bjorn Nansen. The title of the book is "Death and Digital Media", the first edition, published in 2017.
4. Online available at: https://www.taylorfrancis.com/books/mono/10.4324/9781315688749/death-digital-media-michael-arnold-martin-gibbs-tamara-kohn-james-meese-bjorn-nansen
5. Scolyer-Gray, P., Shaghaghi, A., Ashenden, D.: Digging your own digital grave: how should you manage the data you leave behind?
6. Online available at: https://theconversation.com/digging-your-own-digital-grave-how-should-you-manage-the-data-you-leave-behind-143755,
7. about Australia is given here: https://hallandwilcox.com.au/thinking/what-happens-to-your-digital-wealth-on-death-and-incapacity/
8. The authors are Ram Govind Singh, Ananya Shrivastava and Sushmita Ruj. The title of the article is "A Digital Asset Inheritance Model to Convey Online Persona Posthumously" published on 30 April, 2022.
9. Online available at: A Digital Asset Inheritance Model to Convey Online Persona Posthumously (springer.com)
10. The title of the article is "Issues of Legal Regulation of Robotics in the Form of Artificial Intelligence". The author of the article is Said Gulyamov and Sardor Yusupov, published 23 May, 2022. Online available at:
11. https://scholar.google.com/citations?view_op=view_citation&hl=ru&user=kqUdLCsAAAAJ&sortby=pubdate&citation_for_view=kqUdLCsAAAAJ:WA5NYHcadZ8C
12. Harvard Law Review. Cyber law/Internet. What is an "Electronic will"? Development in the law. Online available at: https://harvardlawreview.org/2018/04/what-is-an-electronic-will/
13. The author is Gökalp Y. Gürer. The title of the article is "No Paper? No Problem: Ushering in Electronic Wills Through California's "Harmless Error" Provision". University of California, Davis, published in 2016.
14. Langbein, supra note 16, at 489; see also Gürer, supra note 18, at 1965–66.
15. ee, e.g., Martina v. Elrod, 748 S.E.2d 412, 414 (Ga. 2013) ("The doctrine of substantial compliance, though tolerant of 'variations in the mode of expression' utilized to satisfy statutory requisites, nonetheless requires 'actual compliance as to all matters of substance.'" (Quoting Gen. Elec. Credit Corp. v. Brooks, 249 S.E.2d 596, 602 (Ga. 1978))); Smith v. Smith, 348 S.W.3d 63, 63 (Ky. App. 2011) (holding that the doctrine of substantial compliance could not be used to deem a will compliant where it was signed by only one witness and two were usually required).
16. Beyer & Hargrove, supra note 26, at 890–96. The title of the article is "Digital Wills: Has the Time Come for Wills to Join the Digital Revolution?". Published on February 2009. The author is Gerry W. Beyer from Texas Tech University.
17. Monica Anderson, Technology Device Ownership: 2015, PEW RES. CTR. (Oct. 29, 2015), Online available at: http://www.pewinternet.org/2015/10/29/technology-device-ownership-2015/, https://perma.cc/AP3X-7ESX.
18. Twitter was launched on March 21, 2006. Amanda MacArthur, The Real History of Twitter, in Brief, LIFEWIRE (Nov. 7, 2017), Online available at: https://www.lifewire.com/history-of-twitter-3288854, https://perma.cc/U3RU-M7AW
19. Ami Sedghi, Facebook: 10 Years of Social Networking, in Numbers, THE GUARDIAN: DATABLOG (Feb. 4, 2014, 9:38 AM), Online available at: https://www.theguardian.com/news/datablog/2014/feb/04/facebook-in-numbers-statistics, https://perma.cc/5HYH-TE37
20. Kathleen Chaykowski, Mark Zuckerberg: 2 billion Users Means Facebook's "Responsibility Is Expanding," FORBES (June 27, 2017, 1:37 PM), https://www.forbes.com/sites/kathleenchaykowski/2017/06/27/facebook-officially-hits-2-billion-users, https://perma.cc/GPJ4-EHC8

World Bulletin of Management and Law (WBML)
Available Online at: https://www.scholarexpress.net
Volume-10 May-2022
ISSN: 2749-3601

21. See, e.g., LEGALZOOM, https://www.legalzoom.com/sem/homepage/, https://perma.cc/ZB7H-932E
22. See Caldwell, supra note 5, at 467.
23. The authors are Said Gulyamov, Otabek Narziev, Sadoqat Safoeva, Jahongir Juraev. The title of the article is "State Role Securities Market Development in Uzbekistan", published on the American Journal of Political Science Law and Criminology, on June 18, 2021.
24. Section V, inheritance law, chapter 66. General provisions on inheritance. Online available at: https://lex.uz/docs/180550
25. The title of the article is "International inheritance law - avoiding conflicts of jurisdiction". The authors are Walter Häberling and Alexandra Schnyder. MLL Meyerlustenberger Lachenal Froriep Ltd. Switzerland, published on February 22, 2018. Online available at: https://www.lexology.com/library/detail.aspx?g=eff04523-1946-42d9-b026-cdd85288e5f1
26. Kroiß, L. Vorsorge für den Erbfall durch Testament, Erbvertrag und Schenkung / L. Kroiß. – München. – Bech. – 2019. – 52 s.
27. The author is Gulyamov Said Saidakhrarovich – Doctor of Law, Professor, head of the Department of International Private Law of the Tashkent state university of Law. The title of the article is "The Institutional and Legal Framework of Emerging Capital Markets: The Experience of Cis Countries". Turkish Journal of Computer and Mathematics Education. Published on 05.04.2021
28. Schjolberg Stein. A Cyberspace Treaty – United Nations Convention, Protocol on Cyber-Security and Cybercrime. Twelfth United Nations Congress on Crime Prevention and Criminal Justice. Salvador, Brazil, 12-19 April 2010.
29. The title of the article is "Digitalization of international arbitration and dispute resolution by artificial intelligence". The authors are Said Gulyamov, Mokhinur Bakhramova, page 83, published on April 24th, 2022.
30. Karpova D.N. Cybercrimes: a global issue and its solution. Vlas= The Power, 2014, no. 8, pp. 46-50. (Russian language).
31. The title of the article is "Influence of fake news in Twitter during the 2016 US presidential election". The authors are Alexandre Bovet & Hernán A. Makse, published on 02 January, 2019. Online available at: https://www.nature.com/articles/s41467-018-07761-2\
32. Anonymous hacker group. Business Info and System Analytics GBA-327-CA03. The author is Dr. Bryan Reagan. Online available at: https://www.saintleo.edu/hubfs/Resource%20PDFs%20and%20DOCs/Academics/Center%20for%20Cybersecurity/Student%20Projects/2019/Anonymous%20Hacker%20Group.pdf
33. The author is Slobodyan E. The title of the article is "What is the group of hackers Fancy Bears? // Arguments and Facts". Published on 14.09.2016 Online available at: http://aif/ru/dontknows/file/chto_predstavlyaet_soboy_gruppirovka_hakerov_fancy_bears
34. Bissel K., LaSalle R.M., Richards K., "The Accenture Security Index". Redefining security performance and how to achieve it in 2017, page 19.
35. Online available at: https://www.markle.org/sites/default/files/dotforce_2001_Okinawacharter.pdf
36. Okinawa Charter of the Global Information Society. Adopted on July 21, 2000.
37. The Global Cybersecurity Index. Online available at: https://www/itu.int/en/ITU-D/Cybersecurity/Pages/global-cybersecurity-index.aspx
38. Online available at: https://www.itu.int/en/ITU-D/Cybersecurity/Documents/RES_130_rev_Dubai.pdf, https://www.itu.int/en/Pages/default.aspx
39. United Nations Convention against Transnational Organized Crime and the Protocols Thereto. Adopted by the UN General Assembly on 15 November, 2000 by Resolution 55/25. Entered into force on 29 September 2003, in accordance with article 38. Signatories: 147. Online available at: https://www.unodc.org/unodc/en/organized-crime/intro/UNTOC.html
40. Online available at: https://lex.uz/docs/1304112
41. Convention on Cybercrime, adopted on 23.11.2001 in Budapesht.
42. Okinawa Charter of the Global Information Society. Adopted on July 21, 2000.
43. Resolution adopted by the UN General Assembly // Twelfth United Nations Congress on Crime Prevention and Criminal Justice / A / RES / 65/230 1/01/2011. Online available at:

World Bulletin of Management and Law (WBML)
Available Online at: https://www.scholarexpress.net
Volume-10 May-2022
ISSN: 2749-3601

http://www.unodc.org/documents/justice-and-prison-reform/AGMs/A_RES_65_230r.pdf
44. Comprehensive Cybercrime Study // United Nations Office on Drugs and Crime. Project, February 2013. UN-Vienna, 2013, page 360.
45. Doha Declaration, adopted on April 19, 2015. The 13th United Nations Congress on Crime Prevention and Criminal Justice / UNODC. New York. Online available at: https://www.unodc.org/congress/en/previous/previous-13.html
46. Index of cyber security. International Telecommunication Union, Geneva, 2017.
47. Online available at: https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2017-PDF-E.pdf
48. Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.
49. Online available at: https://www.cybersecurityintelligence.com/blog/cyber-attacks-up-500-in-a-month-4901.html
50. The authors are Adhirath Kapoor, Ankur Gupta, Rajesh Gupta, Sudeep Tanwar, Gulshan Sharma and Innocent E. Davidson. The title of the article is Ransomware Detection, Avoidance, and Mitigation Scheme: A Review and Future Directions. Published on 21 December, 2021. Online available at: file:///C:/Users/user/Downloads/sustainability-14-00008.pdf, https://www.ncsc.gov.uk/news/warning-issued-uk-usa-healthcare-organisations
51. Online available at: https://www.stat.go.jp/english/data/handbook/c0117.html#:~:text=Japan's%20total%20population%20in%202020,of%2010%20million%20or%20more.
52. The author is Atsuda Matsushi, Japan Digital Shuukatsu (End-of-life-planning) Association Representative. The title of the article is "Manual for Handling Digital assets Left by the Deceased", page 2, "legal considerations of inheriting offline data", page 2, published in 2020.
53. DANS, founded in 2005 as an institute of the Royal Netherlands Academy of Arts and Sciences (KNAW) and of the Netherlands Organisation for Scientific Research (NWO), has cumulative responsibility for 50 years of digital research data in the social sciences and humanities from its predecessor organizations. Online available at: AM15ProceedingsBorgmanDANS-FINAL20150819 (acm.org), page 2.
54. Online available at: https://www.gazeta.uz/ru/2022/04/14/ict/
55. The title of the article is "Strategies and future prospects of development of artificial intelligence: World experience", conclusion, the authors are Gulyamov Said Saidakhrarovich, Bozarov Sardor Sokhibjonovich, published on April 20th, 2022. Online available at:
56. https://scholarexpress.net/index.php/wbml/article/view/841.