CYBERSECURITY AND THE ECOLOGICAL DIMENSION OF DIGITIZATION

Irina MOROIANU ZLĂTESCU[*]

Abstract

Digitization is one of the most relevant topics of the world today. No matter where we are or what we do, it became impossible to escape the use of artificial intelligence, and, unfortunately, the threats this progress brings, including to the environment. One cannot deny the advantages technology offers, but, on the other hand, cybercrime found its way to our daily life. The article aims to give a clear and honest perspective on the field of cybercrime and cybersecurity.

Keywords: *cybercrime, cybersecurity, Ethical Charter, European General Data Protection Regulation*

***JEL Classification**: [K 24]*

1. Introduction

The procedure of the Council of the European Union stipulates that this institution is presided for a six months period (January-June, July-December) by rotation, based on a predetermined order, by each member state of the Union, which during this period has attributions regarding the organization and presiding of the meetings that take place, draws up compromises, issues conclusions and supervises the coherence and continuity of the decision-making process. Moreover, it aims for cooperation between all member states being reached in good conditions (Moroianu Zlătescu, 2008, pp. 53-55; Moroianu Zlătescu & Marinică, 2020, pp. 116-117).

The presidency of the Council, starting on January 1st, 2022 and up to June 30th, 2023, is provided by France, the Czech Republic and Sweden. The three states have long-term objectives to achieve, but each of them also has some priorities of its own. In the second semester of this year, the presidency is ensured by the Czech Republic, which however has a limited budget and which initially had set as priorities: the unified market, the post-Covid-19 recovery, digitization and, last but not least, the development of artificial intelligence. The Czech presidency of the Council of the EU has undertaken and continued what the French Presidency had achieved, namely creating a defensive system for Europe and a common strategy of the European Union, especially regarding the fight against hybrid threats such as misinformation, foreign interference and disruptions in cyberspace. Cyber security is and will be, under the given conditions, obviously, a goal that requires the deployment of an in-house communication system of the European Union. It offers a guarantee of the full

[*] Prof. Ph.D.,hab., Titular Member of the IACL-AIDC and of the ASJR.

sovereignty of the European Union over cyberspace[1]. During the last days of the Czech presidency, a Directive concerning the security of network and information systems (NIS2) was adopted[2] and it replaced the earlier Directive regarding measures for a high common level of security of network and information systems across the EU.[3] One of the purposes of NIS2 is to cover more broadly energy and healthcare entities and digital infrastructure service providers. The objective can also be extended to other sectors and entities, such as public administration, the food sector and waste management. The Directive came into force on 16th January 2023. The member states will have 21 months from the moment the Directive came into force, a period in which to adapt the provisions to their national law[4]. Nowadays things are happening in a place where the use of the Internet has expanded more and more, in all fields, even in those where digitization was not long ago present at a basic level, such as justice or administration, for example, more so during and after the Covid-19 pandemic (Epiney & Zlătescu, 2021, p. V), when, in order for life to continue its course, it was necessary to communicate and carry out the activity this way. Of course, under these circumstances, some problems have become evident, issues related to the knowledge and compliance with global, regional and national international standards regarding human rights during the health crisis, the use of digitization, in such a way that it can be done safely for the individuals. As life begins to return to normal, new challenges concerning human rights can be found, namely those caused by climate change and the danger it poses to our very existence. Specialists in the field draw attention to digital pollution and indicate that the global digital ecosystem is the cause of 2-4% of the global greenhouse gas emissions, i.e. it is twice as much as air transport.

2. The risks of the hyperconnected society

We live times where the society is becoming a hyper-connected society, where there is more and more talk about cybercrime and the cyber security measures needed to avoid digital vulnerability and acquire the necessary complex knowledge to react better, more promptly, in case of possible cyberattacks.

As we all known, cybercrime is a form of crime that actually reflects the extension of traditional crime, to which digitization expands its field, offering it new opportunities and new "performances" through the use of digital technologies. The Internet, recognized by the UN as a "driving force" in the development of the society, must follow the measures for the protection of human rights, so that the same rights that people have when they are not connected to the Internet are also protected when they are connected to the Internet (United

[1]www EU 2022.cz.

[2] Published in the Official Journal of the European Union on 27 December 2022.

[3] The member states must transpose the Directive into their national law on 2nd January 2023.

[4] Actual date: 18 October 2024.

Nations General Assembly Human Rights Council, 2012). Unfortunately, certain actors have taken over the Internet, using it as a means of performing certain actions for the purpose of enrichment, of influencing certain environments, of destabilizing society, of forcing certain persons, up to the point of their physical elimination. The computer, the network, the computer code, and the information thus become means of committing crimes. In fact, we are talking about the same crimes, which are committed with new means. Obviously, we are facing crimes in different fields, from economic crimes, crimes related to arms trafficking, drug dealing, trafficking in human beings, money laundering, blackmail, etc., but also criminal acts less known to the average person, committed through operations of fraud, blackmail, extortion, theft, misinformation, psychological manipulation, sabotage, scam, altering the purpose of using artificial intelligence by carrying out cyberattacks. New crimes have appeared, such as misappropriation of personal data, damage to computer resources, breaking into computer systems, use of computer viruses, etc. (Vasiu & Vasiu, 2011, p. 119).

The development of new technologies (L'Institut Suisse de Droit Compare Lausanne, 2005; Dugain & Labbé, 2016 p. 17) in the field of information and communication (Petroiu, 2014, p. 6) allows various crimes to be committed, going as far as murders, in an automated system, remotely, through the telecommunications system. Thus, a considerable number of targets can be reached. These are criminal acts that can be committed on a large scale, even going as far as using new technologies during armed and/or economic conflicts to reduce the enemy's capacity. In a context where data collection and processing is at the heart of the digital economy, where data acquires a market value and allows the development of digital services or artificial intelligence systems, everything is put into practice by numerous actors, who act according to the law or illicitly to obtain, by any means possible, the asset that the data represents. Retrieving of public, private or even personal data is today the basis of all strategies for the development of the digital economy, but also of crime, from mass surveillance to espionage.

3. Computer system malfunctions

One will always be tempted to assume that a criminal is behind a computer system malfunction. But there are also other situations, in which such a malfunction or even a data protection security incident is due to design errors, usage errors, incompetence or even factors related to force majeure or fortuitous events, such as earthquakes, floods, etc., or they may occur as a result of problems concerning energy or environmental resources (electricity, very high or very low temperatures, environments where an air conditioning is missing or defective, etc.). The Internet allows those who wish to cause cyberattacks and who have the professional training to be able to do so, to take action individually or in groups.

Most of the claims they make are related to work from home and in this context some people are asked to transfer sums of money to their bank account, paying significant charges. They are usually fraudulent, and belong to cybercrime, "a form of international organized crime possessing the features of this type of crime and subject to the conditions of existence adequate to this phenomenon, causing significant damage to society" (Bucur, 2016, pp. 79-84). They often pass through messages from financial agents, who serve as intermediaries and who can be easily identified, during a judicial (criminal) investigation, if the case may be. One should not overlook that many of the people involved in various frauds or money laundering cases, although they often started out of naivety, are considered by the justice system as accomplices and are to be sanctioned according the criminal law. The same goes for the Internet users who respond to requests regarding sending money to the accounts of third-party entities, whose involvement in illegal traffic they cannot verify.

Most often there is the possibility of "infecting" the computers through programs installed without the knowledge of the legitimate owner of the computer. This infected computer, which is also called a zombie, reacts when its remote control is activated. The zombie computer can then be used to carry out cyberattacks on other systems. These attacks can be sent through the Internet to different countries or they can reach a single target that they can affect. The affected system becomes unavailable and unable to perform the operations for which it was made.

Taking into account the fact that cybercriminals can act remotely, behind a screen and through technical intermediaries, even internationally, we find that they act remotely and even in cold blood. One more reason to create a certain state of security, especially since they have an extended field of action and a higher degree of protection. They may use anonymization tools, fake identities, or stolen identities to avoid being held accountable for their actions. Carrying out their activities in a familiar environment, without immediate physical risks, they do not have to endure the stress of the common criminal, who operates in a hostile environment and who risks being caught at any moment.

It is quite difficult to identify, locate and track a cybercriminal, especially if they operate in a cross-border manner. International criminal judicial cooperation is necessary in this case. Otherwise, both tracking down the suspect and bringing him to court is extremely difficult in cybercrime. Criminals in this field act either individually or in groups for a specific project and gathered around a common cause. Computer scientists specializing in cybercrimes, individuals specializing in traditional criminality and organized crime are always present, acting as criminals. Some are amateurs, others are professionals, and among them the most successful adapt very easily, but there are also people with various motivations (crooks, manipulators, but also drug and human being traffickers, terrorists, mercenaries).

In order for the fight against cybercrime to be successful, it is necessary, among other things, to increase the level of difficulty of accessing a system, so that a criminal has to bear significant costs and make special efforts to be able to carry out cybercrimes; increasing the degree of risk for the criminal to be identified and prosecuted; to proceed in such a way that the profit of the crime of cyberattack is less appealing; reducing the number of attractive targets for the criminal; minimizing opportunities for cybercriminals by mitigating technical, organizational and human vulnerabilities; developing and marketing reliable and solid digital solutions; transferring the responsibility regarding the vulnerability of IT solutions to the providers of these services; strengthening the effectiveness of cyber security measures; the application and use of security measures; knowing the threats and risks, creating an appropriate security posture; abandoning even the use of digitization if the risks cannot be properly managed.

4. Protection against cyber crime

Starting with the systems, services and applications used, data transmitted, saved or processed to the purpose of use, everything has value for cybercriminals. Their job is to get this asset.

The act of gaining unauthorized access to a computer system, known as hacking for the purpose of destroying or modifying resources, hijacking computer capabilities, changing their purpose, destroying security barriers, installing and determining the execution of malware (malicious) programs that may causing them to get from one system to another, i.e. causing a system to malfunction, stealing data that a computer hosts or locking it to make it unavailable are the most common cyber security incidents. That is why it is necessary to control the access that allows or not to authorize the use of resources in relation to the identity of the person who requested the access permission that was previously granted to him. Access control mechanisms help prevent criminals from accessing resources and preventing their unwanted use. In addition, it is necessary to know who accesses the information and for what purpose, the identities of those requesting access must be managed, after the presented identity could be verified beforehand. Identification allows the recognition of an entity already known. Access controls can be strengthened using double or triple authentication, by complementary means. This protection system makes hacking more difficult. If users need to authenticate, the same must be required for the service providers in question. Currently, it is considered that if a person is required to authenticate by the use of his body parts, and/or maybe even his DNA, we are already in a much safer realm, but we must not forget that biometric data recorded in digital form still remains vulnerable and still hackable. In case this data is altered, it is obvious that verification becomes downright impossible. As such, a person's biometric data, their behavioural data, as well as their identity must be stored under maximum security conditions. Since 2017, as stated by specialists, certain artificial intelligence applications use biometric features to produce fake content, especially video. Although they are built piece by piece on the computer, they give the impression that they are real (deep fake). Even their quality is sometimes extraordinary, which makes it difficult to distinguish a counterfeit video from an original one.

One should highlight that communication is very important in cyber security, as it actually includes all awareness actions to draw the public's attention to cyber risks and the behaviours that must be taken into account. Certainly, this is the only way to contribute to the development of cyber security.

Communication can take different forms depending on the environment. In the case of a person's employment, the organization communicates to him the rights and obligations regarding the use of IT resources as well as good practices in the field of cyber security and the consequences of non-compliance. As a rule, all this information can be found in an Ethical Charter that the parties undertake to respect by signing it.

Everyone's rights and obligations are clearly expressed in the Charter. The more numerous these rights and obligations are, the more the collaborators become active partners of cyber security, able to detect weak signals that allow a faster identification of possible fraud attempts on the respective IT system and, of course, IT malfunctions.

Conclusions

Anticipating crises, drawing a communication strategy that can work in cases of unwanted events due to cyber security breaches and communication in the event of a major crisis are essential. Let us not forget that, for example, multiple measures have been taken at the level of the European Union. The protection of personal data is, moreover, a fundamental right regulated by art. 8 of the Charter of Fundamental Rights of the European Union. The protection is ensured according to the European General Data Protection Regulation 2016/679 (Docksey, 2020, pp. 47-78) of the European Parliament and of the Council, issued on April 27th, 2016, which refers to the protection of natural persons with regard to the processing of personal data and the free movement of such data and which repeals Directive 95/46/EC (Chiriţă, 2021).

The international approach to the risks created by digitization and the perspective of a sustainable development of society, an approach regarding cyber security, implies security becomes everyone's responsibility otherwise there is a risk that the virtual environment remains vulnerable, and this determines us to deepen the ecological dimension of digitization. It is not enough to face cyber-attacks, if we are not able to analyse the political, economic, but also environmental challenges generated by digitization to create sustainable conditions of peace, at a time when criminality and the militarization of cyberspace raise issues regarding the effectiveness of international Internet governance tools and mechanisms. It is known that digitization contributes to the destruction of natural resources, the Internet is an energy consumer, a generator of greenhouse gases and a producer of e-waste, affecting the environment, and therefore the security of life. The question is how to control the indirect risks of the computerization of society. New technologies can contribute, we believe, to diminishing the impact on the environment. Depletion of natural resources, energy crises can cause cyber security breaches.

The first security criterion is that of availability, whether we refer to natural or energy resources, which can create conflicts. In order to deal with the threats to the environment by causing climate change, a faster evolution of new technologies is needed, so that when the advantages of using digitization are balanced against the ecological and security risks that this entails, the best choice be made.

Obviously, an analysis of the geopolitical, economic, social and technological situation regarding the digital ecosystem is required, in order to establish at the national and international level, with respect for fundamental human rights, the measures to fight cybercrime and cyberwars, in order to contribute to better cooperation and an international dialogue, through a cyber diplomacy. Only this way, taking into account the current evolution of technology, creating the conditions required for the exercise, promotion and protection of fundamental human rights, inter-conditioning the respect of fundamental rights with cyber progress, and with sustainable development, a democratic society can become stronger.

Bibliography

1. Bucur, A., 2016, “Tehnologia informației, universul comunicațiilor și drepturile omului”, *Punctul critic*, 3 (17), pp. 79-84.
2. Chiriță, A., 2021, “Limitări privind prelucrarea datelor biometrice cu utilizarea inteligenței artificiale în era GDPR”, Moroianu Zlătescu, I., Marinică, C.E., (ed. coord.) *Lost in translation, Inteligența artificială, Covid-19, Schimbări climatice*, Bucharest: Editura Universitară & Universul Academic, pp. 49-56.
3. Docksey, C., 2020, “The E.U approach to the protection of rights in the digital environment: today and tomorrow – State obligations and responsabilities of private parties – GDPR rules on data protection, and what to expect from the upcoming Privacy regulation”, *Human Rights Challenges in the Digital Age: Judicial Perspectives*, Strasbourg CEDEX: Council of Europe Publishing, pp. 47-78.
4. Dugain, M., Labbé, C., 2016, *L'Homme nu – La dictature invisible du numérique*, Paris: Editions Plon.
5. Epiney, A., Zlătescu, P.E., (Hrsg.), 2021, *SchweizerischesJahrbuch fur Europarecht 2020-2021*, Zürich: Stampfli Verlag AG, Schulthess Juristische Medien AG.
6. L'Institut Suisse de Droit Compare Lausanne, Université de Lausanne, 2005, *L'individu face aux nouvelles technologies. Surveillance, identification et suivi*. *Actes du Colloque international de 10 et 11 novembre 2004 à Lausanne*, 2005, Genève, Zurich, Bale: Schulthess Medias Juridiques S.A.

7. Moroianu Zlătescu, I., 2008, *Instituții europene și drepturile omului*, Bucharest: IRDO Publishing.
8. Moroianu Zlătescu, I., Marinică, E.C., *Instituțiile Uniunii Europene*, Bucharest: Editura universitară & Universul academic.
9. Petroiu, M., 2014, *Dreptul de acces la informațiile de interes public. De la litera legii la abuzul autorităților*, Bucharest: Hamangiu.
10. Vasiu, I., Vasiu, L., 2011, *Criminalitatea în cyberspațiu*, Bucharest: Universul Juridic.