JOURNAL OF LAW AND CORRUPTION REVIEW
16 PEACE, JUSTICE AND STRONG INSTITUTIONS
e-ISSN: 2965-3630
THE GLOBAL GOALS

THE IMPORTANCE OF COMPLIANCE AS A TOOL TO COMBAT CYBERCRIME

Luís Augusto Antunes Rodrigues[3]

ABSTRACT

Law 13.709/2018 - General Data Protection Law - is in force in Brazil, aiming to protect fundamental rights of freedom and personality. In this view, this proposal is closely linked to the analysis of the implementation of compliance rules in the business technology sectors in order to avoid cybercrime, identifying in practice what must be done aiming to eliminate the leakage of clients' data. This article will inform about the importance of compliance in cybercrime, how companies should provide conditions so that criminals do not have access to customer data. Business owners need to keep their technological security level very high, including several precautions explained throughout this paper. Companies must help in the fight against cyberattacks aiming to comply with specific laws. The need for the creation of specific rules will be demonstrated, thus avoiding Internet hacking. One cannot deny the advance of technology, but one must be aware that today we depend on it and that illegal acts will increasingly become a reality. What is sought is to identify specific means of combating cybercrime through the correct use of compliance in the technology sector of companies.

Keywords: Compliance; Cybercrime; Internet; Technology.

Data de aceite: 20/12/2022
DOI: https://doi.org/10.37497/CorruptionReview.5.2023.48
Organizado por Dr. Fabrizio Bon Vecchio – Presidente do Instituto Ibero-americano de Compliance -IIA, em parceria com o Instituto Superior de Administração e Línguas —ISAL. Funchal (Portugal).
Artigo aprovado no 2nd *Ibero-American Congress on Compliance, Governance and Anti-Corruption* (CIACGA 2021), Funchal (Portugal).

[3]Institutional Affiliation: UCA – Universidade Católica Argentina. Master's Degree Candidate in Tax Law. Email: luisaugustoantunes67@gmail.com

1 INTRODUCTION

According to the definition in Wikipedia, probably the most popular general reference on the Internet itself, the definition of "Internet" is as follows:

The Internet is a world-scale conglomeration of millions of computers interconnected by TCP/IP that allows access to information and all kinds of data transfer. It carries a wide variety of resources and services, including the documents interconnected through World Wide Web – (www) interconnections, and the infrastructure to support electronic mail and services such as instant communication and file sharing (MARQUES, 2012).

Given that the Internet is an information paradise and that these are true sources of wealth, it has attracted criminals because "where there is wealth, there is crime" (CORRÊA, 2000).

This can be seen when digital signals, which may represent huge amounts of money, can be intercepted and "stolen". Digital criminals no longer need to use their revolvers, pistols or rifles to rob a bank and exchange shots with police officers, often exposing their own lives. They now use the Internet and sophisticated software to commit the same crimes. They withdraw money from bank account holders without firing any shots and avoiding putting their lives at risk. But this is only one of the crimes that can be committed on the Internet. Throughout this article we will look at others, mainly in the business sphere, and how companies should beware of these scams. It is precisely in this prevention that the implementation of Compliance is very important.

2 DIGITAL CRIMES

According to Neil Barret, "digital crimes" would be: (...) the use of computers to help in illegal activities, subverting the security of systems, or using the Internet or banking networks in an illicit way" (BARRET, 2015).

We know that every society depends on information and therefore ends up being victim of simple threats to terrorism exercised in the largest world computer network.

As Neil Barret used to say: "(...) the information age affects not only our companies or electronic mail, but also the entire national infrastructure as the economy. If hackers can access existing computer systems in universities and companies, why not in banking, air traffic, railways, television and radio systems?" (BARRET, 2015).

We need to understand this new reality presented with the advent of the Internet, based on cutting-edge technology. How can this evolution be reconciled with the evolution of human relations? There is no alternative but to tirelessly seek to prevent the future implications resulting from this relationship between mankind and machines, where the structure and capacity offered by machines and new technologies will also be used by criminals and cyber-terrorists. These will use these new technologies to launder money, to hide files on illegal material, or even in an extreme situation, to organise a conspiracy against a certain order, of a Head of State for instance, which would even lead to a world war.

The Internet is certainly a place prone to fraud, mainly due to the impossibility of identifying its users and the imperfection of the computer programmes used to access and develop it. And in the wake of those who seek to curb these frauds and crimes, difficulties also arise, inherent to the new forms used for the current practice of crimes, the difficulty in punishing the perpetrators of these crimes and enforcing the right of the victim of such crimes, because such effectiveness collides with the right of secrecy of the data of those who are on the Internet.

Even the protection granted by the providers gives criminals a false sense of anonymity and, with this difficulty to identify them, even a sense of impunity because the legal system still lacks legal rules that cover the entire framework of crimes committed over the Internet.

And in the business field, how have companies been suffering with these new fraud options regarding their financial and/or accounting controls? What security can they offer to their employees and clients so that they do not have their data stolen by *crackers* or even the values taken from their current accounts?

3 CYBER SECURITY

Nowadays, information is an essential organisational asset and, consequently, it must be protected in the best possible way. Cyber security has as its primary objective to protect the integrity, availability and confidentiality of all and any information, being developed in companies to reduce the occurrence of cybercrimes. With the implementation of an effective compliance programme, companies will achieve these goals by following some basic procedures, such as: (a) Set up an adequate action plan; (b) Create a code of conduct; (c) Establish communication channels, internal and external; (d) Train all employees; (e) Monitor

the functioning of the entire programme and (f) Evaluate and correct problems during programme implementation.

The objectives of cybersecurity in companies will be achieved through the implementation of a set of rules and control, such as internal policies, effective management processes, internal procedures well adapted to the real needs of the company, lean organisational structures, software and hardware capable of identifying any anomalies in its operational, management, accounting and financial systems. These control mechanisms must be continuously monitored and updated to ensure perfect alignment with the objectives of the business in question.

We know that these cybercriminals have already hacked traditional organisations into the security area, such as Interpol, CIA, NASA, Pentagon, NATO, and many others, including also the main world banks and credit card operators. Cybercriminals operate worldwide and in an organised manner, defying all security measures, however strong and effective, and the main investigative bodies worldwide. Their primary purpose is to breach the confidentiality, integrity and availability of data and information. They indirectly tamper with the legality, ownership and traceability of content produced and stored on the Internet.

In certain situations, internal aspects in companies may stimulate the breaking of established rules. Frustration, indignation, forced work, internal pressure from managers, anger or a simple discontentment involving psychological, financial and/or social elements may motivate people to take the path of crime, both in the physical and digital environment. In the latter, they use skills and knowledge to the detriment of others. It is a reality in companies, especially large ones, that individuals who had trusted status have been involved in security breaches. Due to personal and professional factors, taking advantage of specific opportunities, flaws in the companies' control and the knowledge acquired internally, these people commit digital crime.

4 INTERNAL COMPLIANCE WITHIN ORGANISATIONS

And in practice, how can a Compliance Programme implemented in an organisation contribute to reduce the risks of occurrence of these crimes in its staff? As previously identified, some actions can and must be performed by the organisations with this purpose, such as:

a) Make a risk analysis - In this first stage it is necessary to evaluate all the conduct problems that the company may be subjected to according to the area in which it operates. It is important to highlight that the decree that regulates the Anticorruption Law provides for the

differentiation between companies regarding their relations with the international market and/or with the public administration.

b) Set up an adequate action plan - In this second stage it is necessary to plan an internal strategy with the purpose of implementing the compliance program. In this plan, in order to achieve the desired result, each step must be described, how these steps will be performed, in addition to key points, such as the disclosure, the training of employees and the monitoring of actions.

c) Create a code of conduct - In this third stage it is necessary that the document (planning developed in the previous stage) is clear, objective and pertinent to the company's reality. It is not important the aesthetics of the document, but its real meaning aligned with the values and needs of the organisation.

d) Establish internal and external communication channels - In the fourth stage, the code created has to be put into practice. To do so, reporting channels (ombudsman) and analysis of situations must be created and disclosed. These channels must be open both to the internal public (the company's employees) and to the external public (customers and suppliers), with the sole purpose of identifying fraudulent actions, erroneous and suspicious procedures, as well as to propose internal solutions in order to avoid future losses, consequent indemnification and/or lawsuits.

e) Train all employees - In this new stage it is necessary that all employees are aware of their responsibilities and their actions. However, even more important than this awareness is the fact that they adhere to the compliance program. In order to provide a greater engagement on their part, periodic trainings must be done together with awareness and internal communication campaigns.

f) Monitor the operation of the entire programme - In the sixth step it is essential to monitor the operation of each of the compliance program's actions. It is not enough to put them into practice, it is necessary to follow up the development and test each one of the programme components, incessantly, to be sure about its effectiveness.

g) Evaluate and correct the problems during the implementation of the programme - Last but not least, the solutions must not only consider isolated cases, but the entire environment that provided such occurrences. In other words, a compliance programme is not a simple postponement of solutions (when the management identifies the problems and keeps them in a "drawer" to be solved later). The main objective of the programme is to propose permanent changes in the conduct of the members of the company, thus avoiding countless problems in the future (maybe very soon!).

5 LAWS TO COMBAT CYBERCRIME

And what legal forms (laws) are some countries using to combat these cybercrimes?

In the United States of America, the laws related to this topic are divided into two categories, namely, state laws, which are responsible for curbing the relevant cases in each state, and federal laws that cover crimes with a higher impact, such as the movement of illicit funds and materials between states. Currently, almost all US states have laws regulating illicit access to computer systems (software) and data manipulation. The most interesting fact is that these regulations classify actions as the simple possession of information protected by computers, such as passwords.

The *Wire Fraud Act*, even before the advent of the Internet, a federal statute that regulates the matter, was concerned with registering illegal acts involving communication via telephone, telegraph, television, and other means, among states. Nowadays we can include the Internet in this modality, since the information exchanged in its virtual environment (data traffic) is directly related to communication between the States, shifting the competence to the Federal Justice.

Undoubtedly, the most important law related to cybercrime in the United States was enacted in 1986, called the Computer Fraud and Abuse Act. This law typified activities divided into several categories, with the purpose of clarifying to the violator of a certain system that his activity was illegal, and, therefore, would be susceptible to penalty, which are:

(a) accessing systems without authorisation, with the aim of obtaining restricted government information;

b) accessing systems without authorization, with the purpose of obtaining restricted financial information;

c) having the intention to access, without authorisation, any government computer, or any computer used by the government;

d) transmitting data through a computer for illicit purposes;

In this context, it is easy to understand the greater interest of the State over the private individual, as these categories mention, almost exclusively, government computers.

Unlike the United States, in the United Kingdom there is no difference between state and federal law. They are all equally applicable over the whole territory. The Computer Misuse Act was based on the model of the US laws. However, it went beyond the level of authorisation given to it. There are three types of crimes in the Act in general terms, the second and third being susceptible to deprivation of liberty, namely:

Section 1 - offence involving unauthorised gain of access to a computer not in authority. This is the most general of the specifications, ranging from "hacking" to attempts to locate specific information within a system.

Section 2 - offence involving unauthorised access to any computers for the purpose of violating the law, such as publishing information obtained, using information obtained, or for use of data for the purpose of breaching the security of other systems.

Section 3 - offence involving unauthorised access to computers, for the purpose of altering their data, thereby preventing authorised user operation or access.

In this context, in the United Kingdom, it is noted that the three sections of the Act manage to prohibit a wider range of cybercrimes, such as the publication of private, confidential and copyrighted material, as well as the creation and dissemination of viruses and other attacks, thus achieving its main goal, which is to typify the acts harmful to the technological development.

In Brazil the main laws dealing with this topic are: a) The Cybercrime Law (Law 12.737/2012); b) The law regulating E-commerce (Law 7.962/2013); c) the Civil Framework for the Internet (Law 12.965/2014); d) Citizen's Base Register (Law 10.046/2019) and the most important of them, the e) General Data Protection Law (Law 13.709/2018).

Until 2012, Brazil did not have any sanction for crimes of violation or invasion of systems or other digital devices (mobile phones, tablets and others), existing only some vague determinations in the Interception Law or hypotheses of some crimes committed by public officials against the public administration (specific laws).

However, due to facts involving the leak of intimate photos of a very well-known global actress, Brazil, through its legislators, realizing the existing gap on the subject, created Law no. 12.737/2012, adding articles 154-A and 154-B of the Brazilian Penal Code, not making changes until May 2021.

> Art. 154-A. Hacking into another's computing device, whether or not connected to the computer network, in order to obtain, alter or destroy data or information without the express or tacit authorisation of the user of the device or to install vulnerabilities in order to obtain an illicit advantage: (Amendment introduced by Law No. 14.155 of 2021)
>
> Penalty – confinement, from 1 (one) to 4 (four) years, and fine. (Drafted by Law No. 14.155, of 2021)

§ 1st The same penalty is incurred by anyone who produces, offers, distributes, sells or disseminates a device or computer programme with the intention of enabling the practice of the conduct defined in the preamble. (Included by Law No. 12.737, of 2012)

§ 2nd The penalty is increased by one-third (1/3) to two-thirds (2/3) if the hacking results in economic loss. (Drafted by Law No. 14.155, of 2021)

§ 3rd If the hacking results in obtaining the content of private electronic communications, commercial or industrial secrets, confidential information as defined by law, or unauthorised remote control of the invaded device: (Included by Law No. 12.737 of 2012)

Penalty – confinement, from 2 (two) to 5 (five) years, and fine. (Drafted by Law No. 14.155, of 2021)

§ 4th In the case under Paragraph 3, the penalty shall be increased by one to two-thirds if the data or information obtained is disclosed, commercialised or transmitted to third parties for any purpose. (Included by Law No. 12.737, of 2012)

§ 5th The penalty shall be increased by one-third to one-half if the crime is committed against: (Included by Law No. 12.737, of 2012)

I - President of the Republic, governors and mayors; (Included by Law No. 12.737, of 2012)

II - President of the Federal Supreme Court; (Included by Law No. 12.737, of 2012)

III - President of the House of Representatives, Federal Senate, State Legislative Assembly, Federal District Legislative Chamber or City Council; or (Included by Law No. 12.737, of 2012)

IV - Top manager of the direct and indirect federal, state, municipal or Federal District administration. (Included by Law No. 12.737, of 2012)

Criminal Action (Included by Law 12.737, of 2012)

Article 154-B. In the crimes defined in Article 154-A, proceedings shall only be initiated upon representation, except when the crime is committed against the direct or indirect public administration of any of the Powers of the Union, States, Federal District or Municipalities or against public utility concessionaires. (Included by Law 12.737, of 2012)

The recent creation of Law No. 14.155/21 increases the penalties provided in the Criminal Code for crimes known as cybercrime. According to the text of the law, the crimes of computer device violation, theft and swindling committed electronically or over the Internet are now even more serious. With the new legislation, the punishment that used to be detention for three months to one year and a fine is now one to four years of confinement and a fine, aiming to inhibit the actions of these cybercriminals.

The sanctioned law foresees that the penalty of confinement will be applied in more severe convictions and that the regime of compliance may be closed. Detention is applied to lighter convictions and does not allow the beginning of the sentence to be in a closed regime.

6 GENERAL DATA PROTECTION LAW (LAW 13.709/2018)

Law 13.109/18 came into force in August 2020, with the main objective to regulate the protection of personal data, as well as the privacy of data. It is a way to impose that companies and organisations deal more responsibly with people's information.

With this, the fundamental rights are ensured, which are freedom, privacy and also the development of the personality of the natural person.

With the General Data Protection Law in force, companies and organisations had to change their behaviour quickly. They have the obligation to develop a system that ensures full protection of the data of everyone who are born, live and/or are in the national territory, or of data that has been collected in the country.

Through this law both consumers and businesses themselves began to observe the importance of this protection, which applies to the digital world as well as to physical businesses. The law also deals with consent and permission to share data, since the data of a holder requires express authorisation to be shared, as well as the consumer has the right to request the cancellation or deletion of their information from any system where it is inserted.

The General Data Protection Law is a very important milestone in Brazil. With the advancement of the internet, the significant increase of e-commerce, as well as digital banking, the access and dissemination of important and private data has increased exponentially. As a result, data leakage has also increased.

Therefore, a law that regulates and supervises companies so that there are standards and software within them to protect their customers' data is undoubtedly an essential decision.

The strictness of law 13.709/18 guarantees a severe inspection to companies, to verify if in fact they are following the standards stipulated by the General Data Protection Law. The

body responsible for inspecting and presenting penalties for those who do not comply with the law is the National Authority for Personal Data Protection; the maximum authority to determine the fines to be applied for non-compliance with the law, as well as to guide these companies on the importance of protecting the data of their employees, consumers, suppliers and customers.

The Law comes to authorise punishment in case there is a cyberattack on some system, avoiding the use of this data for something illicit, especially sensitive data. After all, no personal data can be transferred without prior consent. The freedom to choose between giving or not giving must be exclusively of the individual.

In conclusion, we understand that companies in their work environment must provide conditions so that cybercriminals do not have access to their data. To succeed in this demand, the business person needs to keep his or her business security level very high, including some fundamental precautions, such as:

a) Continuous monitoring of the network to detect threats - it is necessary to constantly check, through specific and reliable software, the behaviour and possible changes of data on the network;

b) Always keeping the IT infrastructure up to date - this way the company avoids risks of invasion to their data;

c) Implant, whenever possible, a virtual private network - this way, the business person will provide a safer connection to his or her company's network and to the Internet;

d) Developing alternative plans in cases of data loss recovery - this way, the company will be able to create options in cases of emergency in the eventual loss of data.

7 CONCLUSION

Finally, one cannot deny the advancement of technology in our daily life. However, we must also be aware that nowadays there is an almost absolute dependence on the Internet and that illicit acts will increasingly become a reality. What we must seek all the time is to identify specific means to fight cybercrime through the correct use of compliance in the technology sector of companies.

REFERENCES

Azevedo e Souza, B. (2016). Direito, *Tecnologia e Práticas Punitivas*. Editora Canal Ciências Criminais.

Barret, N. (1997) *Digital crime*. London: Kogan Page.

Chandler, Y & Neal-Schuman, J. (1997). Guide *to finding legal and regulatory information on the Internet (serial).* Estados Unidos, dez.

Corrêa, T. G. (2010). *Aspectos Jurídicos da Internet*. Editora Saraiva.

Goodman, M. (2015). *Future crimes: tudo está conectado, todos somos vulneráveis e o que podemos fazer sobre isto*. São Paulo: HSM Editora.

Huber, P. (1997). *Law and disorder in cyberspace*. New York: Oxford University Press,

Inellas, G. C. Z. (2009). *Crimes na Internet. 2ª ed*. São Paulo: Juarez de Oliveira

Lucca, N., & Simão F., A. (2000). *Direito e Internet – Aspectos Jurídicos Relevantes* – Edipro.

Marques, J. & Faria, S., M. (2012). O *Direito na Era Digital*. Livraria do Advogado.

Olivo, L. C. C. (1998). *Direito e Internet: a regulamentação do ciberespaço*. Florianópolis: UFSC, CIASC.

Fisher, D. (1999) *Calúnias via Internet desafiam a Justiça. Gazeta Mercantil*, São Paulo, 11 março.

Lima, N. B. M. H. (1997). A *lei alcança o ciberespaço*. Diário Catarinense, Florianópolis, Caderno Informática.

Moron, A. P. F. (1996). A *Internet e o direito*. Travelnet jurídica, São Paulo.