The Criminal Manipulation in Government Medical Statistics During COVID-19 Crisis: A Comparative Study

Dhia Moslem Abd Alameer Ghaibi[1], Asseel Abd Ali Shehad[2]

[1]Lecturer, [2]Postgraduate student, Department of Criminal Law, Faculty of Law, University of Kufa, Najaf, Iraq

Abstract

Manipulating government medical data is one of the intentional crimes that occur on medical informational data, whether by intentionally introducing misleading and wrong information or deleting and amending the data to change the truth. Despite the existence of laws to criminalize these acts, whether in Iraqi law or comparative law in general, in addition to the international conventions that oblige countries to develop legal texts to combat cybercrimes. Therefore, there are problems related to the activation of texts associated with manipulating government medical data, especially data on infection with Coronavirus. Providing some countries with misleading or incorrect information that does not reflect the current reality must be put to an end, especially since this disease is a fatal and dangerous disease that transmits very quickly and must be accurately determined without any tampering with the governmental medical data.

Keywords: *Criminal Manipulation, COVID-19, Government Medical Statistics*

Introduction

We are about to study the crime that affects government data and information inside the system without the information system itself. It differs from the corruption of disrupting the information system [1]. Criminal behavior is defined by criminal behavior. It is the act of assault that occurs on the data and information inside the processing systems, i.e., the data, without continuing to attack the information system itself [2, 3].

This article focuses on manipulating medical data on coronavirus disease. Manipulation is usually committed at any point of the computer's or other electronic device's operation, whether in the background when entering or removing data from the information system or even before the data is entered [4]. Additionally, fraud is carried out by an individual who has the authority to view and use information or by someone who developed these systems and assisted in the data entry [5].

There is no specific definition in the laws in force for this crime. Several pieces of legislation provide for the crime of data manipulation. In France, the legislator in the French penal code provides for the crime of fraud in the 1988 French Penal Code and the new law [6]. It includes or how they are processed and transmitted shall be punishable by incarceration for a period of three months to three years and a fine of 2000 French francs [7]. Up to five hundred thousand, or one of two penalties. Some of the preceding text see that the legislator used multiple phrases and was the subject of criticism by the jurists, as in a direct or indirect representation, making it challenging to interpret what is meant. As for the new penal code came categorically without strange expressions or the object of criticism, which is what the mechanism of Article 323/3 indicated. It specified the acts that tamper with the data by mentioning the entry, deletion, modification, extraction, reproduction, transmission, and retention that came to be understood and did not mention the previous expressions in the old law. It also came and described the act of fraudulent entry, imposing a five-year jail sentence and a 75,000-euro fine.

In Egypt, the Egyptian legislator criminalizes the crime of tampering with the Law on Combating

Information Technology Crimes when discussing the corruption of assault against the state's information system in Article of [8]. It was stipulated that any previous acts shall destroy that data, information, website, private account, information system, e-mail, destroying, distorting, changing, changing their designs, copying them. Additionally, it involves altering the direction, republishing it, or altogether canceling it in whatever way. The punishment is incarceration and a fine of not less than one million pounds and not more than five million pounds [9]. We remember that Egyptian law defines tampering with illegal behavior as modifying, exploiting, or erasing it entirely or in part, regardless of how these acts are carried out [10]. This is clear that the legislator has protected the state's data and information, and even the website, e-mail, and information systems. However, he did not define the precise length of imprisonment and only specified the maximum permissible, and it was more fitting for the legislator to decide the duration of imprisonment.

In Iraq, the Information Crimes Bill of 2011 stipulates in Article Three, Paragraph B, the crimes of erasing or modifying saved data, electronic devices, systems, communication networks, and harming subscribers and beneficiaries [11]. It also clarified that these acts must result in harm to the subscribers [12]. Regarding the 2019 Computer Crimes Bill, it was referred to in Article 5's third paragraph, which states that the sentence is increased if the offense involves national security information and data, or national economy information which data, and ends in their cancellation, or delete, kill, or alter them [13]. We note from the above that he mentioned the cancellation and deletion of the term, which are of the same meaning. The legislator had to say one synonym and mentioned its change, which is intended to be modified. The legislator was required to display terms indicating the act of manipulation, as the French legislator had done.

The Arab Model Law of 2003 also stipulates the manipulation of data in Article 2 [14]. It referred to the act of modification and considered it an aggravating circumstance resulting from the crime of breaching the processing systems [15, 16]. The UAE Information Technology Crimes Law also referred to this crime and stipulated in Article 2 of it to change as well [16].

Background

Pillars of Criminal Data Manipulation

The illegal action of this crime is defined by three distinct acts: the act of insertion, the act of erasure, and the act of alteration, which together constitute the crime's material aspect [17]. The moral component is defined by criminal intent, and we will discuss the concepts of the two components separately:

The Physical Pillar of Data Manipulation

In this pillar, we show the criminal act, what is the subject of this act, and the criminal consequence of this act:

A - Criminal behavior: The French legislator specified in Article 323/3 of the Penal Code the acts involved in manipulation, which are entry, extraction, retention, erasure, modification, sending, and reproduction. This broad definition of these acts is the difference in the forms in which information is available, such as government information, military, commercial, or other information, which prompted the French legislator to put protection on all of them. This is what he went to in the Iraqi Information Crimes Bill of 2012, which was also specified in Article 3 for the crime of illegal entry and defined in Paragraph B the acts involved in manipulation [18]. As defined by the Budapest Agreement in Article 4, other legislation was limited to granting this protection to a part of it. As is the case in the Syrian legislature, it specified some types without the different types as in the Electronic Signature Law of 2009. Nevertheless, we can define legally criminal acts according to what the French legislator has defined because it has taken all the acts as follows:

1 - Acts related to fraudulent entry, exit, or retention of data: these are the first acts stipulated in Article 323/3 CE of French law. Therefore, we must clarify the meaning of the entry and the purpose of the output is. The

entry provides the system with information that needs to be processed or providing it with information necessary to go through the processing of this information [19]. It may also be defined as (adding new information or different information inside the system, that is, wrong, and therefore it is processed, leading to different results than it was). However, the entry is the introduction of information into the information system. Still, this entry can be harmful programs, such as programs, for example, whose purpose is to distort, destroy and destroy this information or data [20]. This method is considered one of the most dangerous and most widespread methods because its speed and ease of use characterize it. It is also the most common method that causes significant economic losses in all government sectors, whether public or private.

2- Acts related to reproduction or retransmission of data by fraudulent means: As for these actions, data are manipulated from a distance. Manipulation, in this case, is one of the easiest and most common types of means to be used.

3- Acts involving the unauthorized erasure or alteration of records. There are many designations for this act, including replacing, erasing, and deletion. The term erasing refers to the act of removing a portion of information fixed on magnetized support to obliterate, delete, or move it to a saved region of the brain, or is removing a part of the information stored within the device [19]. The Council of Europe made a distinction in its recommendation between two types of data deletion, the first being data erasure. The second is concealing these data to prevent access to them.

B - **The location of the crime**: After we have identified the acts that express the criminal behavior that constitutes the material corner, we must make it clear that these acts are only responding to a specific place, which is the data that has been processed, i.e., transformed into symbols and signals that represent those data.

C - **Criminal consequence**: The crime of tampering with data is considered one of the crimes of damage that leads to inevitable damage to this data, which is represented by the change of information from its actual state to a wrong state with any of the acts constituting the criminal behavior, which is the entry, modification, and erasure. Therefore, this crime is not sufficient to be a threat to the information and its integrity. Instead, actual harm must result from it, which is (change).

The Moral Pillar of Data Manipulation

This crime is considered an intentional crime that requires the availability of the criminal intent represented by the two elements of knowledge and will; that is, the perpetrator knows that his behavior is unlawful, an assault on data. Thus, a choice is directed to commit the criminal behavior acts (insertion, deletion, or modification). Consequently, this crime is realized as soon as the general intent is present; that is, the goal is not required to be specific or conclusive.

Manipulating Government Medical Data For Covid-19 Patients

Before discussing this crime, we must identify the obstacles related to determining government data:

1- Obstacles related to identifying government medical and private data for Coronavirus patients.

Tests are not accurate and disproportionate:

It reveals by mistake and in a remarkable way a more significant number of negative tests than what they incorrectly show from the positive tests, which means that there is a tendency to consider people healthy when they are already infected with the virus [21]. Some research indicates that the rate of false-negative screening may exceed 30%. This means that estimates of the actual number of infections must be inflated again.

- The number of tests does not equal the number of people who have already been tested:

Due to the inaccuracy of the tests or the tests, some people are examined twice to confirm their results. This suggests that comparing the ratio of the population discussed to the number of individuals discovered to be sick paints a false image of fact, providing another

justification to assume that the actual number of infected people is more significant. There is also a change in the number of statistics because people are not admitted to the hospital and the decrease in hospital admissions. After all, the emergency rooms are overcrowded with patients.

The Statistics Are Inexact Because They Do Not Correspond To Reality

Some patients sometimes die weeks after hospital admission, and they are usually hospitalized for a week or more after infection with the virus is confirmed [22].

Fatalities That Occur Outside Of Hospitals Are Not Reported

When a person dies at home or anywhere else, those often don't count, and that's a big problem. When France began reporting deaths in nursing homes, the number of deaths increased by 40%, and when Belgium was keen to count deaths outside hospitals, it discovered that 40% of them were in nursing homes.

2- Criminal responsibility for tampering with government medical and private data for Corona patients

The privacy of individuals is a significant challenge, especially in a crisis like Covid19. It is no small challenge, especially in countries with legislation protecting data privacy, such as the European Union GDPR for data protection and the US HIPAA privacy rules that protect citizens' medical records, to prevent the dangerous consequences of a data breach. Despite these challenges, there are additional crimes related to tampering with government medical data, as follows:

- Hiding The Real Numbers By Hospitals

Some hospitals may hide some data about the death of people infected with the Coronavirus by deleting or modifying the data. This does not affect the evaluation of the hospital and its medical staff. Here we are facing a crime in manipulating the data. Thus, all legal procedures for the crime of data manipulation must be applied against the hospital through the deliberate entry of incorrect information or deletion and modification.

- Hide Real Numbers By Some Countries

Officials in some countries may conceal the amount of genuine Corona cases within their borders, as some countries, including China, Indonesia, Iran, and possibly the United States, have been accused of doing. Here we are facing a crime that must be taken into consideration. But here is the problem when we face a state that conceals its information or deletes information from its government programs. Despite international conventions on combating information crimes, they do not place responsibility before the state itself if it conceals information or provides misleading or incorrect information.

Conclusions and Discussion

The crime of manipulating government medical data is one of the intentional crimes that occur on medical informational data, whether by intentionally introducing misleading and wrong information or deleting and amending the data to change the truth. Despite the existence of laws to criminalize these acts, both in Iraqi and comparative law as well. In addition to international conventions that oblige states to develop legal texts to combat cybercrime. There is an urgent need to activate texts related to manipulating government medical data and related to data and statistics on the Coronavirus. Furthermore, the need to oblige countries to provide correct, not misleading or false information that does not reflect the current reality, especially that this disease is fatal in society and is transmitted rapidly among individuals and has become a global epidemic that must be eliminated by determining the correct numbers of infection with this disease accurately and without concealing the facts About the existence of mutated viruses in these countries.

Source of Funding: Self-funding

Conflict of Interest: The authors declare no conflict of interest, financial or otherwise.

Ethical Clearance: Taken from institutional ethical committee of University of Kufa, Iraq.

References

1. Maguire, M. and S. McVie, Crime data and criminal statistics: A critical reflection. Vol. 1. 2017: Oxford University Press Oxford.
2. Cooper, J.A. and J. Cooper, Computer-security technology. 1984.
3. Al-Fatlawi, Q.A., D.S. Al Farttoosi, and A.H. Almagtome, Accounting Information Security and IT Governance Under COBIT 5 Framework: A Case Study. 2021.
4. Heymann, S.P., Legislating Computer Crime. Harv. J. on Legis., 1997. 34: p. 373.
5. ALJAWAHERI, B.A.W., et al., COVID-19 Lockdown, Earnings Manipulation and Stock Market Sensitivity: An Empirical Study in Iraq. The Journal of Asian Finance, Economics and Business, 2021. 8(5): p. 707-715.
6. Baron, G.-L. and E. Bruillard, Technologies de l'information et de la communication et indigènes numériques: quelle situation? STICEF (Sciences et Technologies de l'Information et de la Communication pour l'Éducation et la Formation), 2008. 15: p. 12 pages.
7. Deffayet, S., Nouvelles Technologies de l'Information et de la Communication (NTIC) et contrôle dans la relation managériale. Recherches sociologiques, 2002. 33(1): p. 27-48.
8. Kadum, H.A., N. hassan Ibrahim, and A.H.J. Attiya, LEGISLATIVE PUBLIC INTERNATIONAL LAW MECHANISMS TO COMBAT MODERN TECHNOLOGY CRIMES. PalArch's Journal of Archaeology of Egypt/Egyptology, 2020. 17(7): p. 6455-6474.
9. Saad, R., Egypts Draft Cybercrime Law Undermines Freedom of Expression. Atlantic Council, April, 2015. 24.
10. Hemdani, M., Data Protection in Egypt.
11. Kritia, H.H.A., Learning about the Characteristics of the Initiation of Information Crime. Learning, 2019. 7(8).
12. Ghareb, M.I. and F.M. Sedeeq, Electronic Crimes And The International Community Legislation: Comparative Analytical Study.
13. Abd ALNomani, M.M. and A.H.T. Birmani, INFORMATIONAL DESTRUCTION CRIME; A COMPARATIVE STUDY. PalArch's Journal of Archaeology of Egypt/Egyptology, 2020. 17(3): p. 2266-2281.
14. Aldhaheri, S. and H. Almagwashi, A Comparative Research between the KSA and UAE Cybercrimes Legislations. International Journal of Computer Science and Information Security (IJCSIS), 2019. 17(11).
15. Younies, H. and T. Na, Effect of cybercrime laws on protecting citizens and businesses in the United Arab Emirates (UAE). Journal of Financial Crime, 2020.
16. Rajan, A.V., R. Ravikumar, and M. Al Shaer. UAE cybercrime law and cybercrimes—An analysis. in 2017 International Conference on Cyber Security And Protection Of Digital Services (Cyber Security). 2017. IEEE.
17. Francillon, J., Infractions relevant du droit de l'information et de la communication. Revue de science criminelle et de droit penal compare, 2010(1): p. 170-181.
18. AL_khafagy, B.M.S., INTERNATIONAL EFFORTS TO COMBAT CYBERCRIME. PalArch's Journal of Archaeology of Egypt/ Egyptology, 2020. 17(6): p. 3034-3054.
19. Maurel, L., R. Martinez, and J. Gasnault, Droit de l'information. Documentaliste-Sciences De L'information, 2008. 45(4): p. 24-27.
20. Visset, P., Les pratiques documentaires des chercheurs en sciences exactes, naturelles et médicales dans les régions périphériques: le cas des Antilles et de la Guyane. 2002.

21. Kawchuk, G., et al., Misinformation about spinal manipulation and boosting immunity: an analysis of Twitter activity during the COVID-19 crisis. Chiropractic & manual therapies, 2020. 28(1): p. 1-13.
22. Naudé, W. and R. Vinuesa, Data, global development, and COVID-19: Lessons and consequences. 2020: WIDER Working Paper.