Social Sciences
2024, Vol. 13, No. 5, pp. 192-196
https://doi.org/10.11648/j.ss.20241305.17

Review Article

A Comprehensive Survey on the Role of Law in Different Applications in Computer Science

Basma Mohamed[1, *], **Khaled Eid Abdel Moneim Abdel Fattah**[2]

[1]Department of Information Systems, Giza Higher Institute for Managerial Sciences, Tamouh, Egypt
[2]Department of Private Law, Giza Higher Institute for Managerial Sciences, Tamouh, Egypt

Abstract

One significant tool for addressing the concerns associated with the use of one of the applications in computer science is the law. Numerous laws and rules governing the use of computer science are designed to safeguard users, customers, and society at large. Law uses norms created by governmental and social institutions to control behavior. Programming is used to explore digital information in computer science. Computers got more potent and smaller as they evolved through generations, utilizing various technologies such as integrated circuits. Cyber law regulates online behavior and deals with matters pertaining to intellectual property, privacy, domain names, and other legal concerns. A few of the many concerns that the law must address in order to mitigate the electronic crimes are protecting privacy and security, upholding justice, limiting civil and criminal liability, ensuring safety, and controlling the application of AI in the workplace. Guidelines that people and organizations have to follow when utilizing computer science applications, making sure that these requirements are met in full. Additionally, as companies must commit to recording AI usage procedures and making clear the use of data and algorithms, the regulation fosters accountability and openness. By doing this, the possibility of prejudice and mistakes when utilizing AI is decreased. This survey provides a self-contained introduction to cybercrimes and types of cybercrimes. We also present ways to combat cybercrime and limit its spread.

Keywords

Cybercrimes, Threatening Individuals, Blackmail

1. Introduction

It makes sense that the first and most evident uses of deontic logic in computer science would be in the creation of what are sometimes referred to as "legal expert systems," given its roots in the analytical study of ethics and law. Systems designed to aid in the examination of legal texts, the inferences made from them, and the application of those conclusions to real and hypothetical circumstances. In fact, the literature on legal knowledge representation makes frequent allusions to deontic logic [1].

Nevertheless, there are very few examples of systems that have used a deontic logic, either explicitly or implicitly. Additionally, deontic logic has received very little attention in comparison to the vast amount of published material that is devoted to the representation of law in computer.

The overall aim that develop and present here is that many other types of organizational structures, including computer

*Corresponding author: bosbos25jan@yahoo.com (Basma Mohamed)

Received: 28 August 2024; **Accepted:** 18 September 2024; **Published:** 10 October 2024

systems and legislation, can be considered examples of normative systems at the proper degree of abstraction.

Agents can be individual people or groups of people, or they can be computer systems or groups of computer systems. Normative systems encompass legal frameworks, abstract representations of computer systems, and hybrid systems that involve the interaction of human and computer actors.

Our focus is on highlighting the importance of taking a normative systems perspective and demonstrating the functions of deontic logic and the logic of action in the formulation of computer system models, the representation of law, and the specification of rules intended to control human-computer interaction (such as access-control regulations).

Another benefit of the example is that it's simple to picture how a computer system to automate a portion of the library's operations. This enables us to bring up a variety of issues: issues that develop with computer specification systems. Consider the following situation. The Chief Librarian requests that created a computerized version of the library's policies in order to increase the library's efficiency.

One step to do would be to select suitable formal language, utilize this to create an accurate representation of what believe the rules to be, and then use an automated reasoning system to bring the representation to life: provided a synopsis. This computer software would determine what legal, or quasi-legal, consequences would seem to follow in the event of an actual or hypothetical state of affairs. It could be used, for instance, to provide guidance on the particular duties and rights that librarians and borrowers have under certain conditions. When one thinks of artificial intelligence in relation to law, this is the software that most readily comes to mind.

Slobodan et al. [2] gave a survey of applications of the theory of graph spectra to computer science.

The necessity to safeguard customers from the exploitation of their personal data has impacted the global landscape of data privacy regulations, particularly in light of occurrences involving the illicit sale and acquisition of consumer data by FinTech applications [3]. Due to this, strict data protection laws have been passed in a number of jurisdictions, with the goal of defending consumers' rights to safety, security, and privacy in the digital economy [4].

The recognition of the critical role that data plays in the FinTech industry—both as a source of innovation and growth and as a conduit for cybersecurity threats and privacy violations—has fueled the development of these regulations. As a result, laws pertaining to data privacy have been developed to protect individuals' right to privacy while also promoting technological advancement [5].

The dynamic and ever-changing landscape at the convergence of data privacy regulations and financial technology (FinTech) is a reflection of both the growing significance of data in the digital economy and the speed at which technology is developing. FinTech companies are at the vanguard of this convergence, managing a complicated web of international data privacy requirements as they use technological improvements to deliver innovative financial services [6].

In recent years, artificial intelligence techniques have emerged as one of the most valuable and advanced methods. As a result, these methods are important in a variety of domains, such as information security and cyberspace [7, 8]. The term "artificial intelligence" describes the capacity of robots, electronics, software, and gaming consoles to be conscious of, retain, and utilize information similarly to how the human brain functions when making decisions [9]. These methods gather experimental data and then make use of it. Put another way, artificial intelligence-capable devices have electronic brains that can process information and carry out necessary tasks. The widespread usage of Internet networks and their accessibility, particularly with the introduction of 5G technology, have led to the recent birth of the phrase "cybersecurity" [10]. On computers or other electronic devices, data, information, and programs are vulnerable to theft and access by unauthorized individuals who then use that information to commit a variety of electronic crimes. In this way, businesses want to create artificial intelligence-based methods for anticipating computer intrusions, attacks, and cybercrime activities. These procedures are more effective than professionals at verifying whether users accessing the network are permitted to do so and what information is housed there. Because these methods are so effective at learning, remembering, and completing tasks fast, they also save professionals a great deal of time and effort. Repetitive patterns can also be preserved by artificial intelligence algorithms [11, 12].

2. Cybercrime Implementation and Approaches for Addressing It

In the era of the spread of information technology, we have become more vulnerable to falling victim to electronic crimes. The spread of technology and modern means of communication is a double-edged sword. They can be used to facilitate communications around the world. They are one of the most important means of transmission of different cultures around the world in order to bridge the distances between different countries and civilizations. But they can also be used to cause serious harm to specific people or entire institutions in order to serve personal political or material goals [13].

3. The Concept of Electronic Crimes (Information Crimes)

Cybercrime is an act that causes serious harm to individuals, groups, or institutions, with the aim of blackmailing the victim and distorting their reputation in order to achieve material gains or serve political goals using computers and modern means of communication such as the Internet [14].

Cybercrimes are aimed at stealing information and using it in order to cause serious psychological and material harm to the victim, or to reveal important security secrets related to

important institutions in the state or data and accounts of banks and individuals. Cybercrime is similar to regular crime in its elements of Where the perpetrator, the victim, and the perpetrator of the crime are present, but it differs from a regular crime depending on the environment and means used. Electronic crime can take place without the presence of the person committing the crime at the scene of the event, and the means used are modern technology, modern means of communication, and information networks [15].

4. Types of Cybercrimes

4.1. First: Crimes That Cause Harm to Individuals

Through it, a group of individuals or a specific individual is targeted in order to obtain important information related to his accounts, whether bank or online, and these crimes are represented in:

Impersonation: In which the criminal lures the victim and extracts information from him in indirect ways, and targets private information in order to benefit from it and exploit it to achieve material gains or defame the reputation of specific people, turn the environment upside down, and spoil relationships, whether social or work relationships [16].

Threatening individuals: Through hacking and theft of information, the criminal accesses the victim's personal and very private information, then blackmails him in order to earn money and incite him to carry out illegal acts in which he may be harmed [17].

Discrediting: The criminal uses the stolen information and adds some false information, then sends it via social media or via email to many individuals for the purpose of distorting the victim's reputation and destroying them psychologically [18].

Incitement to illegal acts: The criminal uses stolen information about specific individuals and exploits it to blackmail victims by carrying out illegal acts related to prostitution, drug trafficking, money laundering, and many other electronic crimes.

4.2. Second: Crimes That Cause Harm to Institutions

Systems hacking [19]:

1. Cybercrimes cause great losses to institutions and companies, represented by material losses and system losses, as the criminal penetrates the network systems of institutions and companies and obtains valuable information, especially about the companies' systems, and then uses the information in order to serve his personal interests, which is to steal money and destroy the company's systems. Supporting the management process, which causes serious losses to the company or institution.
2. It is also possible to steal information about employees of institutions and companies, incite and blackmail them in order to destroy the internal systems of institutions, install spy devices on accounts and systems, and seek to penetrate and control them to achieve material and political gains.
3. Cybercrimes related to penetrating networks, accounts, and systems negatively affect the state of the economy in the country, and also cause many problems related to the threat to the country's national security if they are not controlled and combated competently. The percentage of cybercrimes and information crimes around the world represents 170%, and the percentage is increasing. Day after day, which puts us all in grave danger due to violations and hacking of systems and accounts.
4. Hacking and controlling websites, and then using them to serve the interests of dangerous entities that aim to destabilize the country's security, control the minds of young people, and incite them to carry out illegal acts.
5. Destruction of systems: This type of destruction is done using common methods, namely electronic viruses, which spread in the system and cause chaos and destruction. This causes many losses associated with destroyed files and their importance in the management and organization of companies and institutions.

Or destroying the main server that everyone in the organization uses in order to facilitate business. This is done by hacking into the organization's employee accounts on the organization's information network and accessing all accounts at the same time. This causes a complete failure of the server, leading to its destruction and thus disrupting the business of companies and institutions.

4.3. Third: Money Crimes

Seizing bank accounts [20]:

It involves hacking into bank accounts and accounts related to state institutions and other private institutions. Credit cards are also stolen, then seized and the money in them stolen.

Violation of intellectual and literary property rights:

It is the manufacture of non-original copies of programs and multimedia files and their dissemination through the Internet, and this causes huge losses in software and audio manufacturing institutions.

4.4. Fourth: Crimes Targeting State Security

Spyware:

Many spyware programs are widespread and used for political reasons, which threaten the security and safety of the state. The criminal plants the spyware within the electronic systems of institutions, so the enemies of the nation demolish the regime's systems and view military plans related to the country's security. Therefore, it is considered one of the most dangerous information crimes.

Terrorist organizations use deception:

Terrorists rely on the use of modern means of communication and the Internet in order to broadcast and disseminate false information, which may lead to destabilization in the country and cause chaos in order to implement political interests and terrorist plans, and to mislead the minds of young people in order to benefit from personal interests.

Ways to combat cybercrime and limit its spread [21]:

1. Educating people everywhere about the causes of cybercrimes and how they are carried out. The media has an important role in educating citizens about the seriousness of cybercrimes, and it must also be pointed out how to deal with them and protect against them.
2. Avoid publishing any personal photos or personal information on social networking sites or any other sites, so as not to be stolen and then blackmailed by cybercrime perpetrators.
3. Do not reveal passwords for any account, whether it is a bank account, credit card, or account on a specific website. They must also be changed constantly to ensure that they do not fall into the wrong hands.
4. Avoid using any programs of unknown origin, and you should also avoid entering any unknown codes or passwords to avoid exposure to hacking and theft of the accounts used.
5. Avoid opening any unknown emails, so that your computer system is not hacked and all your personal information, accounts, and passwords are stolen.
6. Installing anti-virus and hacking protection programs in order to maintain the safety of the user's device and the confidentiality of its information.
7. Establishing deterrent penal laws for cybercrime perpetrators, in order to limit their spread.
8. Developing ways and means to accurately track and catch cybercrime perpetrators.

5. Conclusion

A lot of cybercrimes and cybercrime vulnerabilities are committed with the use of data. While data offers countless opportunities to its users (individuals, businesses, organizations, and governments), some have taken use of these advantages for illegal activities. In particular, the gathering, storing, analyzing, and sharing of data facilitates a great deal of cybercrime as well as the extensive gathering, storing, using, and dispersing of data without the informed consent and choice of users and without the required legal and security safeguards.

In this paper, we have introduced an introduction to the electronic crimes and types of cybercrimes. We also presented ways to combat cybercrime and limit its spread.

Abbreviations

LES	Legal Expert Systems
EC	Electronic Crimes

Conflicts of Interest

The authors declare no conflicts of interest.

References

[1] Jones, A. J., & Sergot, M. (1993). On the characterisation of law and computer systems: The normative systems perspective. *Deontic logic in computer science: normative system specification*, 275-307.

[2] Cvetković, D., & Simić, S. (2011). Graph spectra in computer science. *Linear Algebra and its Applications*, *434*(6), 1545-1562, https://doi.org/10.1016/j.laa.2010.11.035

[3] Sinaga, N. P. (2021). Perlindungan hukum bagi konsumen yang data pribadinya diperjualbelikan di aplikasi fintech peer-to-peer lending, Nusantara Law and Opinion Journal, 2(2). https://doi.org/10.51622/njlo.v2i02.366

[4] Stevani, W., & Sudirman, L. (2021). Urgensi Perlindungan Data Pengguna Financial Technology terhadap Aksi Kejahatan Online di Indonesia. Journal of Judicial Review, 23(2), 197-216, https://doi.org/10.37253/jjr.v23i2.5028

[5] Dorfleitner, G., Hornuf, L., & Kreppmeier, J. (2023). Promise not fulfilled: FinTech, data privacy, and the GDPR. *Electronic Markets*, *33*(1), 33, https://doi.org/10.1007/s12525-023-00622-x

[6] Oyewole, A. T., Oguejiofor, B. B., Eneh, N. E., Akpuokwe, C. U., & Bakare, S. S. (2024). Data privacy laws and their impact on financial technology companies: a review. *Computer Science & IT Research Journal*, *5*(3), 628-650, https://doi.org/10.51594/csitrj.v5i3.911

[7] Li, J. H. (2018). Cyber security meets artificial intelligence: a survey. *Frontiers of Information Technology & Electronic Engineering*, *19*(12), 1462-1474, https://doi.org/10.1631/FITEE.1800573

[8] Zhang, Z., Ning, H., Shi, F., Farha, F., Xu, Y., Xu, J.,. & Choo, K. K. R. (2022). Artificial intelligence in cyber security: research advances, challenges, and opportunities. *Artificial Intelligence Review*, 1-25, https://doi.org/10.1007/s10462-021-09976-0

[9] Mijwil M. M., "Implementation of Machine Learning Techniques for the Classification of Lung X-Ray Images Used to Detect COVID-19 in Humans," Iraqi Journal of Science, vol.62, no. 6., pp: 2099-2109, July 2021. https://doi.org/10.24996/ijs.2021.62.6.35

[10] Cáceres-Hidalgo, J., & Avila-Pesantez, D. (2021, October). Cybersecurity study in 5g network slicing technology: A systematic mapping review. In *2021 IEEE Fifth Ecuador Technical Chapters Meeting (ETCM)* (pp. 1-6). IEEE, https://doi.org/10.1109/ETCM53643.2021.9590742

[11] Ghosh, T., Al Banna, M. H., Rahman, M. S., Kaiser, M. S., Mahmud, M., Hosen, A. S., & Cho, G. H. (2021). Artificial intelligence and internet of things in screening and management of autism spectrum disorder. *Sustainable Cities and Society*, *74*, 103189, https://doi.org/10.1016/j.scs.2021.103189

[12] Adadi, A., Lahmer, M., & Nasiri, S. (2022). Artificial Intelligence and COVID-19: A Systematic umbrella review and roads ahead. *Journal of King Saud University-Computer and Information Sciences*, *34*(8), 5898-5920, https://doi.org/10.1016/j.jksuci.2021.07.010

[13] Malby, S., Jesrani, T., Bañuelos, T., Holterhof, A., & Hahn, M. (2015). Study on the effects of new information technologies on the abuse and exploitation of children. *United Nations Office on Drugs and Crime: Vienna, Austria*.

[14] Mekkawi, M. (2022). Cyber Blackmail between Threats and Protection: A study in Egyptian and American legislations. *Journal of Law and Emerging Technologies*, *2*(2), 53-116, https://doi.org/10.54873/jolets.v2i2.71

[15] Sarkar, G., & Shukla, S. K. (2023). Behavioral analysis of cybercrime: Paving the way for effective policing strategies. *Journal of Economic Criminology*, 100034, https://doi.org/10.1016/j.jeconc.2023.100034

[16] Umejiaku, N. O., & Uzoka, N. C. (2021). An Overview of Social Media Related Cybercrimes and Its Legal Remedy. *LASJURE*, *2*, 50.

[17] Joshi, S., Singh, S. K., & Sharma, M. (2023). Cybercrime by Minors. In *Cybercrime in Social Media* (pp. 143-166). Chapman and Hall/CRC.

[18] Lakshmanan, A. (2019). Literature review on Cyber Crimes and its Prevention Mechanisms. *no. February. pp*, 1-5, https://doi.org/10.13140/RG.2.2.16573.51684

[19] Biju, J. M., Gopal, N., & Prakash, A. J. (2019). Cyber attacks and its different types. *International Research Journal of Engineering and Technology*, *6*(3), 4849-4852.

[20] Zhang, Z., Salerno, J. J., & Yu, P. S. (2003, August). Applying data mining in investigating money laundering crimes. In *Proceedings of the ninth ACM SIGKDD international conference on Knowledge discovery and data mining* (pp. 747-752), https://doi.org/10.1145/956750.956851

[21] Sviatun, O. V., Goncharuk, O. V., Roman, C., Kuzmenko, O., & Kozych, I. V. (2021). Combating cybercrime: economic and legal aspects. *WSEAS Transactions on Business and Economics*, *18*, 751-762, https://doi.org/10.37394/23207.2021.18.72