Classification of Cybercrimes in GCC Countries

Submitted: 2 June 2023
Reviewed: 24 June 2023
Revised: 25 June 2023
Accepted: 2 November 2023

Viktor Anatolyevich Shestak*
https://orcid.org/0000-0003-0903-8577
Alyona Dmitrievna Tsyplakova**
https://orcid.org/0000-0001-8564-0696

Article submitted to peer blind review

DOI: https://doi.org/10.26512/lstr.v16i1.48885

Abstract

[Purpose] For the time being, one of the most cyber resilient countries not only in the Middle East, but worldwide is Kingdom of Saudi Arabia alongside with the United Arab Emirates that pioneered the criminalization of computer-related offences. The question is what country has evolved enough thought years and may set an example in order to reform other Arab legislation.

[Methodology/Approach/Design] This study is a description investigation of cybercrimes in the Kingdom of Saudi Arabia, the United Arab Emirates, the Kingdom of Bahrain, the Sultanate of Oman, the State of Qatar and the State of Kuwait mainly based on genetic, systematic-functional and systematization methods. Data on features of translation, as well as legal framework of GCC members and comparison of provisions of the Budapest convention on cybercrime and the Arab convention on combatting information technology offences summarized in Tables.

[Findings] Not only does the terminology in Arab states vary from conventional approach, but the structure and categories are atypical in contrast to international documents such as the Budapest convention on cybercrime. Since there is no unity within even 6 members of Gulf Cooperation Council, it calls for harmonization and either update of the Arab Convention on combating information technology offences or implementing the GCC Model Law (Riyad Document).

Keywords: Cybercrimes. GCC. Arab Countries. Computer Crimes.

* Doctor of Juridical Science, Professor of the Department Criminal Procedure, Moscow Academy of the Investigative Committee of the Russian Federation (Moscow, Russian Federation). Address: 12, Vrubel Street, Moscow, Russia, 125080. E-mail: viktor_shestak@mail.ru.

** Lecturer of the Department of Criminal Law, Criminal Procedure and Criminology, MGIMO University (Moscow, Russian Federation). Address: 76, Prospect Vernadskogo Moscow, Russia, 119454. E-mail: tsyplakova.a.d@my.mgimo.ru.

INTRODUCTION

Although the Kingdom of Saudi Arabia and the United Arab Emirates lagged behind in the 2010s according to various cyber security indices, as of 2020 they are the leaders in this area not only among Arab countries, but also worldwide. They are ranked 2nd and 5th in the 2020 Global Cybersecurity Index of the International Telecommunication Union (ITU, 2020). The UAE is the most digitized economy among Arab countries (Elmasry T., Benni E., Patel J., aus dem Moore J.P., 2016). In 2016, the UAE accounted for 5% of all cyberattacks in the world (Altaher N., 2016). Between 2018 and 2020, there were about 166,667 victims of cybercrime in the UAE, which according to experts, indicated a 70% increase in encroachments (Al Amir S., 2022). For 2021, the Dubai Police Department received 25,841 reports on cybercrimes. About $4.9 million was recovered, while losses amount to about $746 million a year (Al Amir S., 2022). The Arab Convention on combating information technology offences (Cairo, 21.12.2010) adopted within the Arab League is based precisely on the Saudi and Emirati regulation (The Gulf Centre for Human Rights, 2018). For these reasons, the authors consider the legislation and approaches of the UAE and the KSA as a model and compares them with the provisions of other GCC member states.

TERMINOLOGY AND DIFFICULTIES WITH TRANSLATION

The Arab states' legislation has its official English translations and often contain such a notion as cybercrimes. However, the authentic texts have a variety of terminology (see Table 1). The group of crimes in question is referred to as electronic (Arabic "الجرائمُ الإلكترونيةُ"), informational (Arabic "الجرائمُ المعلوماتيةُ "), in the sphere of Computer Science or Informatics (Arabic "جرائمُ المعلوماتيةِ") or information technology (Arabic "جرائمُ المعلوماتِ"). The legal framework of Arab states differs from international practice in both structure and content.

№	Notion in Arabic (Authentic Texts)	Notion in English (Official Translation)	Notion in English (Author's Translation from Arabic)
1	الجرائمُ الإلكترونيةُ	Cybercrimes	Electronic Crimes
2	الجرائمُ المعلوماتيةُ	Cybercrimes	Informational Crimes
3	جرائمُ المعلوماتيةِ	Cybercrimes	Crimes in Sphere of Computer Science (Informatics)
4	جرائمُ تقنيةِ المعلوماتِ	Cybercrimes; Information Technology Crimes	Information Technology Crimes

Table 1 – Comparison of Authentic Naming of Cybercrimes in Arabic and English with the Author's Translation in English

CLASSIFYING CYBERCRIMES

Because of the religious nature of Islamic law, there are traditionally three categories of crimes based on the applicable penalties: hadd, qisas and ta'zir. The acts in question belong to the sphere of non-Koranic criminal law, but retain certain features of the Islamic tradition (Mathias Rohe, 2009). Hence, insulting Islamic holy places or religious rites or the sacred places, religious rites of other religions, insulting one of the recognized monotheistic religions, aiding and abetting the commission of sins, or promoting sins, are commonly recognized as offences in the religious legal family. For instance, one may take article 37 of the Emirati Federal Decree-Law No. 34 of 2021 on Combating Rumors and Electronic Crimes (the UAE FDL No. 34/2021). Islamic legal doctrine states that the criminal law can only regulate ta'zir offenses (Al-Assoumi N.A., 2000). Nevertheless, a number of corpora delicti (including those mentioned above) are similar to hudud. Such a classification is classic, but it does not allow to understand the specifics of the crimes under consideration.

International Level

First, we are going to compare the Arab Convention on Combating Information Technology Offences (Cairo, 21.12.2010) (Arabic "الاتفاقية العربية لمكافحة جرائم تقنية المعلومات") (the Arab Convention) and the Convention on Cybercrime (Budapest, 23.11.2001) (the Budapest Convention). The Arab Convention distinguishes offenses against the CIA triad1 as the target of the offense and the offenses related to the use of IT as a means of committing the offense. The former includes illegal access (art. 6), illegal interception (art. 7), violation of data integrity, data forgery (art. 8), improper use of IT tools (art. 9), and the latter implies IT tools forgery (art. 10), fraud (art. 11), offences against public order, morality and safety (art. 12, 13, 14 and 15), offences relating to trafficking in and laundering of money (art. 15 and 16), offences relating to copyright and other intellectual rights (art. 17) and misuse of electronic means of payment (art. 18). Since the foreign scholars often depict Budapest Convention as an ideal example to update the Arab Convention provisions, a more detailed comparison of the offences covered by both Conventions is contained in Table 2.

1 The CIA triad involves confidentiality, integrity and availability.

Offence	**The Budapest Convention**	**The Arab Convention**
Illegal Access to a Computer System/Information Technology (IT)	Article 2: Computer System	Article 6: IT
Illegal Access, Interception or Acquisition Of Data	Articles 2, 3: Computer Data	Articles 6, 7, 18: IT Data
Illegal Interference with Data	Article 4: Computer Data	Article 8: IT Data
Illegal Interference with the Functioning of a System/IT	Article 5: Computer System	Article 6: IT
Computer Misuse Tools	Article 6: Devices	Article 9: IT Means
Forgery	Article 7: via Computer	Articles 8, 10: With Data or by IT Means
Fraud	Article 8: via Computer	Article 11: Data, Information; Via Operating Systems and Communication Systems; With Electronic Instruments, Programmes and Sites
Illicit Use of Electronic Payment Tools	—	Article 18
Offenses Related to Copyright and Adjacent Rights	Article 10	Article 17

Computer-Related Offences Involving Racism or Xenophobia	Articles 3, 4, 5 of the Additional Protocol	—
Computer-Related Denial or Justification of Genocide or Crimes Against Humanity	Article 6 of the Additional Protocol	—
Offences Related to Child Pornography	Article 9: via Computer System	Article 12: By Means of IT
Offecnes Related to Terroristic Activity	—	Article 15: By Means of IT
Money Laundering	—	Article 16: Related to Organized Crime Committed by Means of IT
Illicting Trafficking	—	Article 16: Related to Organized Crime Committed by Means of IT
Offences Against Against Public Order, Morality or Security	—	Articles 12, 13, 14, 15
Law Enforcement Investigation-Related Offences	Article 16 (3), Article 20 (3), Article 21 (3)	Article 23 (3), Article 28 (3), Article 29 (3)

Table 2 – Comparison of the Budapest Convention and the Arab Convention

The second group of crimes mentioned above is also subdivided into content-related offenses and assaults committed out of mercenary or other personal interest or with the intent to cause harm. Arab scholars have noted that Omani and Bahraini legislation follow the Budapest Convention' model (Salem F., Fiscbach T., 2017; Billah M. M., 2018), but this is not entirely true. Originally,

Law of the State of Qatar No. 14 dated 02.10.2014 on Combating Electronic Crimes (Qatar Law No. 14-2014) was also supposed to be based on this model, but it was abandoned. Moreover, the structure laid down by the lawmakers cannot serve as a basis for classification because of the disjointed approaches.

National Level

General Approach

By comparing the legal framework of Arab countries, it is possible to classify crimes based on the legal act criminalizing different offences, because experts traditionally refer to cyberlaws other than those that directly regulate electronic crimes. The list given in Table is not exhaustive, without taking into account Criminal codes, legislation on combating terrorism and money laundering.

№	State	Author's Translation from Arabic	Official Translation on English
1.1	The Kingdom of Saudi Arabia	Regulation[2] dated 27.03.2007 on Combatting Crimes in Informatics	Anti-Cyber Crime Law 1428 H
1.2		Regulation[3] dated 27.03.2007 on Electronic Transactions	Electronic Transactions Law 1428 H
1.3		Regulation[4] dated 29.11.2000 on Press and Publications	Printing and Publication Law
2.1	The United Arab Emirates	Federal Decree Law No. 34/2021 on Combatting Rumours and Electronic Crimes	Federal Decree Law No. 34 of 2021 on Combatting Rumours and Cybercrimes
2.2		Federal Decree Law No. 46/2021 on Electronic Transactions and Trust Services	Federal Decree Law No. 46 of 2021 on Electronic Transactions and Trust Services

[2] Regulation or nizam in Arabic equals to Law, but this notion is not applicable in general as to Saudi Arabia
[3] Idem.
[4] Idem.

2.3		Federal Decree Law No 45/2021 on Protecting Personal Data	Federal Decree Law No 45 of 2021 regarding the Protection of Personal Data
2.4		Federal Decree Law No. 2/2015 on Combating Discrimination and Hatred	Federal Decree Law No. 2 of 2015 on Combating Discrimination and Hatred
3.1	The State of Qatar	Law No. 14/2014 on Combatting Electronic Crimes	Law No. 14 of 2014 Promulgating Cybercrime Prevention Law
3.2		Decree Law No. 16/2010 on Electronic Transactions and Commerce	Decree Law No. 16 of 2010 Promulgating the Electronic Transactions and Commerce Law
3.3		Decree-Law No 34/2006 on Communications	Decree-Law No 34 of 2006 Promulgating the Telecommunications Law
4.1	The Sultanate of Oman	Royal Decree No. 12/2011 on Combatting Information Technology Crimes	Royal Decree 12/2011 Issuing the Cybercrime Law
4.2		Royal Decree No. 69/2008 on Electronic Data	Royal Decree 69/2008 Issuing the Electronic Transactions Law of the Sultanate of Oman
4.3		Royal Decree No. 30/2002 on the Telecommunications Regulatory	Telecommunications Regulatory Act
4.4		Royal Decree No. 6/2022 on Personal Data	Royal Decree 6/2022 Promulgating the Personal Data Protection Law
5.1	The State of Kuwait	Law No. 63/2015 on Combating Information Technology Crimes	Law No. (63) for the year 2015 on Combating Information Technology Crimes
5.2		Law No. 37/2014 Establishing the Communication and Information Technology Authority	Law No. 37 of 2014 on the Establishment of Communication and Information Technology Regulatory Authority
6.1	The Kingdom of Bahrain	Law No. 60/2014 on Information Technology Crimes	Law No. 60 of 2014 on Information Technology Crimes

6.2		Decree-Law No. 54/2018 on Electronic Communications and Transactions	Legislative Decree No. (54) of 2018 Promulgating the Electronic Communications and Transactions Law

Table 3 – Comparison of Official Translation in English and Author's Translation from Arabic (Authentic Text)

The conflict of laws may arise, enlisting, for instance, AML acts. For instance, Article 43 of the Kingdom of Saudi Arabia's Regulation dated 03.04.2012 on combating terrorist crimes and its financing criminalizes the terroristic activity and its financing by a computer or electronic device, electronic site or program, but it also constitutes crime under 2007 KSA Regulation. Such a similar situation occurs also in the UAE.

The Kingdom of Saudi Arabia

The Regulation dated 27.03.2007 on combatting crimes in informatics (2007 KSA Regulation) covers the following crimes: interception of data (art. 3, para. 1), encroachment on electronic data and information (art. 3, para. 3 and art. 5, para. 2), encroachment on an information system (art. 2 art. 7), illegal access (art. 3, para. 2, art. 4, para. 2, art. 5, para. 1), violation of privacy (art. 3, para. 4), cyberterrorism (art. 7, para. 1), attacks on public order and morals (art. 6, paras. 1, 2, 3, 4). Art. 23 of the Regulation dated 27.03.2007 on electronic transactions criminalizes the following acts: service provider activities without a license, abuse and misuse of information without consent (disclosure without consent, misleading and false information), fraud, forgery of electronic records, signatures and digital certificates, identity theft and illegal access to the system.

In Saudi doctrine the basis for classification is the target of the attack: persons, property and the state (Alabdulatif A., 2018). The first category includes email spoofing, spam, phishing, cyberstalking, defamation, spying, pornography-related crimes; the second includes financial card skimming, attacks on intellectual property rights, software piracy, domain infringement, and identity theft. Crimes against the state are sometimes lumped together under the concept of cyberterrorism, which includes hacking, DoS-attacks, logic bomb, email bombs, data manipulation, the illegal sale of items whose circulation is restricted or prohibited, and propaganda aimed at undermining the constitutional order (Amrutha A., 2017).

ç

In Arab legal doctrine, cybercrime is regarded as a subspecies of economic crime (Imranuddin M., 2017). A similar approach is implemented in Law of the

State of Qatar No. 11 of 10.05.2004 on Penalties (the Qatari Criminal Code): Chapter 5 Computer crimes (Arabic "جرائم الحاسب الآلي") is placed in Part 3 Crimes against maalun (Masadeh A. M. S.). The term "maalun" (Arabic "مال") is translated as money, wealth, property, capital, or finance, depending on the context. Nevertheless, it seems too narrow. Firstly, the Qatari Criminal Code is not the only legal regulator, which makes it impossible to fully use this example as an argument. Secondly, the motive for acquisitive crimes is material or other gain, which does not always relate to cybercrimes. Thirdly, maalun is not the only object of cybercrime.

The UAE

The doctrine proposes a classification in relation to the computer: criminal activity is either directly aimed at it, or it may be used as the object of an attack. The former includes unauthorized access, malicious codes, disruption of electronic sites and services, theft or abuse of data or information, while the latter involves content-related violations, unauthorized modification of data, software and improper use of telecommunications networks.

Nevertheless, one should understand that information technology is the broadest term and can be used like an umbrella notion. It means any type of technology used to create, process, store, exchange and use electronic information systems, software, electronic sites (websites), information networks and any other means of information technology (see Art. 1 of the UAE FDL No. 34/2021). Therefore, a better classification of punishable acts seems to be based on the ethics of information technology use: against privacy and confidentiality, and against the values of society (Aissani R., 2022). Emirati law enforcers take a broader approach and distinguish four types of cybercrime: acts committed against reputation and honor, against privacy and confidentiality, financial offenses and fraudulent attacks (Salem F., Fiscbach T., 2017).

Typicality

Riyadh document as a uniform regulation on combating information technology crimes for the Gulf Cooperation Council (the GCC Model Law) and most of the legislation of the Arab states under consideration define two types of cybercrime as the most typical: information or electronic fraud and hacking. In the 2010s, the most common electronic security incidents were recognized as hacking of computers and electronic accounts of a specific person, company, as well as identity theft, hacking of an electronic website with fake or distorted content, viruses and malicious software, attacks on email (fraud, phishing, spam, attacks on honor and human dignity), misleading advertising and broadcasting inappropriate content (Mishaal Abdullah bin Hussein, 2009). As current trends show, electronic piracy, child pornography, electronic harassment, cyberattacks

with viruses and malware, and credit (financial) card abuse are the most typical, indicating the persistence of threats from cyberspace (General Directorate of Anti-Corruption and Economic and Electronic Security of the Kingdom of Bahrain).

Challenges

Bahrain's Law No. 60/2014 on information technology crimes distinguishes three groups of encroachments, Qatar's Law No. 14/2014 on combatting electronic crimes and Sultan of Oman's Decree No. 12-2011 on combatting information technology crimes have five groups, but different structures, while the 2007 KSA Regulation and Kuwait's Law No. 63-2015 on combating information technology crimes have no divisions at all.

№	State	Offences	Legislative types
1	The Kingdom of Saudi Arabia	Crimes in Sphere of Computer Science (Informatics)	—
2	The United Arab Emirates	Electronic Crimes	IT Offences
			Content Offences
			Crimes Related to Spreading Rumors and Fake News
3	The State of Qatar	Electronic Crimes	Forgery and Electronic Fraud
			Encroachments on Information Systems, Software, Information Networks and Electronic Sites
			IPR Infringements
			Electronic Transactions Crimes
			Content Offences
4	The Sultanate of Oman	IT Crimes	Violation of Confidentiality, Integrity and Availability of Electronic Data, Information and Information System
			Content Offences
			Illegal Use of a Financial Card
			Misuse of IT Tools
			Data Forgery and Fraud
5	The State of Kuwait	IT Crimes	—
6	The Kingdom of Bahrain	IT Crimes	IT and Data Related Crimes
			Crimes Related to IT Tools
			Content Offences

Table 4 – Categories of Cybercrimes under Arab Legislative View

CONCLUSION

One should note that a number of Arab states have developed their own conceptual apparatus: electronic crimes, information technology crimes, computer crimes, information crimes, crimes in computer science (informatics), but the structure and types of the acts differs. Official translations of documents into English uniformly use the term cybercrime.

One may conclude that there are different bases for the classification of cybercrimes in the Arab countries from the perspective of either legislator, law enforcement or researcher, although they are not perfect. In Arab legal doctrine, cybercrime itself is regarded as a subtype of economic crimes, which is reflected in the Qatari legislation. Nevertheless, this approach narrows the phenomenon in question.

The Arab Convention and the GCC Model Law reflect a slightly outdated but classic approach, which is based on the 2007 KSA Regulation and UAE Federal Law No. 2/2006 on combatting with IT crimes. They have influenced the legal framework of Oman and Bahrain. Nevertheless, it is broader than the Budapest Convention. The UAE FDZ No. 34/2021 is the most progressive approach, but it is sometimes criticized due to its too broad interpretation of the concept in question. The generic notion is electronic crime, which often includes, among other things, IT wrongdoing.

Along with the object of encroachment, the ethics of the IT use, the legal acts criminalizing wrongful behavior, and the optional elements of the objective side are identified as the grounds for categorizing cybercrimes. Nevertheless, due to the specificity of the offence, the division of acts based on the object, purpose and means of infringement does not seem to be successful.

Classifying acts based on the legal framework results in the issue related to an overlap. The separate laws are special to the Penal Codes and do not take precedence, thus creating a conflict of laws. Still, they can be divided into Acts on data protection, electronic transactions, counterterrorism, anti-money laundering, freedom of speech, telecommunications and information technology regulation.

Some researchers state that the scope of restricting free speech, including combating rumors and fake news, goes beyond cybercrime and violates human rights. However, this approach has in fact been previously implemented in many Criminal Codes in Arab states. The clauses on *lèse majesté* and respectful behavior have long been applicable to comments on social networks while discussing moral, family and religious topics. the Bahraini Criminal Code is an

example in such a case. Therefore, the cyberlaws of individual Arab states have similar provisions.

Moreover, it is worth mentioning that the regulation of illegal content and fake news entails not only criminal responsibility, but also the application of administrative measures to prevent illegal activities (e.g., Ar. 62 of the UAE FDL 34/2021 and Art. 38 of the KSA Regulation dated 29.11.2000 on press and publications). This demonstrates a comprehensive approach of lawmakers. Nevertheless, in the Arab countries there is an ambiguous interpretation of cybercrime (sometimes even within a single act), so it is recommended to develop a single definition and a uniform classification at the regional level in order to harmonize legislation. This would facilitate international cooperation in fighting crime and ease compliance with the principle of dual criminality for sake of extradition and mutual legal assistance in criminal matters.

REFERENCES

Aissani R. (2022). Anti-Cyber and information technology crimes laws and legislation in the GCC countries: A comparative analysis study of the laws of the UAE, Saudi Arabia and Kuwait. *Journal of Legal, Ethical and Regulatory Issues*, 25(1), 1–14.

Al Amir S. (2022). *Sharjah records 70 per cent rise in cyber crime in two years.* https://www.thenationalnews.com/uae/2022/07/22/sharjah-records-70-per-cent-rise-in-cybercrime-in-two-years/.

Al Amir S. (2022). *More than 25,000 cybercrimes reported last year, say Dubai Police.* https://www.thenationalnews.com/uae/2022/08/24/more-than-25000-cybercrimes-reported-last-year-say-dubai-police.

Al-Assoumi N.A. *Crime and Punishment under the Criminal Law of Bahrain and the United Arab Emirates* [Doctoral dissertation, RUDN University]. RUDN repository. https://repository.rudn.ru/ru/records/dissertation/record/46031/.

Alabdulatif A. (2018). *Cybercrime and analysis of laws in Kingdome of Saudi Arabia: Science in Information System Security* [Master's thesis, University of Houston]. Houston Repository. https://uh-ir.tdl.org/bitstream/handle/10657/3107/ALABDULATIF-THESIS-2018.pdf?sequence=1.

Altaher N. (2016). *UAE a target of 5 per cent of global cyber attacks.* https://gulfnews.com/uae/crime/uae-a-target-of-5-per-cent-of-global-cyber-attacks-1.1826610.

Amrutha A. (2017). *ATT(H)ack-Anti-Cyber Crime Law in Saudi Arabia*. https://www.stalawfirm.com/en/blogs/view/atthack-anti-cyber-crime-law-in-saudi-arabia.html.

Billah M. M. (2018). Sufficiency of Omani Laws to Suppress Cybercrimes in Light of the un Comprehensive Study on Cybercrimes. *Arab Law Quarterly*, 32(2), 158–184. https://doi.org/10.1163/15730255-12321010.

Elmasry T., Benni E., Patel J., aus dem Moore J.P. (2016). *Digital Middle East: Transforming the region into a leading digital economy*. https://www.mckinsey.com/featured-insights/middle-east-and-africa/digital-middle-east-transforming-the-region-into-a-leading-digital-economy.

General Directorate of Anti-Corruption and Economic and Electronic Security of the Kingdom of Bahrain.أنواع الجرائم الإلكتروني [Types of electronic crimes]. https://www.acees.gov.bh/cyber-crime/types-of-cybercrime/.

Imranuddin M. (2017). *A Study of Cyber Laws in the United Arab Emirates* [Master's thesis, Rochester Institute of Technology (Dubai Campus)]. Rochester Institute of Technology Repository. https://scholarworks.rit.edu/cgi/viewcontent.cgi?article=10766&context=theses.

ITU. (2020). *Global Cybersecurity Index 2020*. https://www.itu.int/dms_pub/itud/opb/str/D-STR-GCI.01-2021-PDF-E.pdf.

Masadeh A. M. S. *Combating Cyber Crimes — Legislative Approach — A comparative Study (Qatar, UAE, UK).* https://www.almeezan.qa/ReferenceFiles.aspx?id=54&type=doc&language=en.

Mathias Rohe. (2009). *Das islamische Recht: Geschichte und Gegenwart*. C.H. Beck.

Mishaal Abdullah bin Hussein. (2009). Special Report of the Computer Incident Response Center on Information Technology Crimes 2008-2009. https://elaws.moj.gov.ae/UAE-MOJ_Fokeh/15_الرابع%20العدد/UAE-MOJ_2%تقرير%20مركز%20الإستجابة%20لطوارئ%20الحاسب%20الآلي%20المعلومات%20تقنية%20لجرائم0.html?val=UAE-FokehAA1.

Salem F., Fiscbach T. (2017). *Cybercrime and the Digital Economy in the GCC Countries.* Chatham House.

The Gulf Centre for Human Rights. (2018). *Mapping Cybercrime Laws and Violations of Digital Rights in the Gulf and Neighbouring Countries*. https://www.gc4hr.org/report/download/78.

The Law, State and Telecommunications Review / Revista de Direito, Estado e Telecomunicações

Contact:
Universidade de Brasília - Faculdade de Direito - Núcleo de Direito Setorial e Regulatório
Campus Universitário de Brasília
Brasília, DF, CEP 70919-970
Caixa Postal 04413

Phone: +55(61)3107-2683/2688

E-mail: getel@unb.br

Submissions are welcome at: https://periodicos.unb.br/index.php/RDET