Anti-Cybercrime legislation in the Kingdom of Saudi Arabia: An analysis and evaluation of the KSA criminal procedure approach to cybercrime with reference to England and Wales.

Abdulmajeed Kuwayran H Alsulami

Submitted in accordance with the requirements for the degree of
Doctor of Philosophy

The University of Leeds
School of Law

January 2022

The candidate confirms that the work submitted is his own and that appropriate credit has been given where reference has been made to the work of others.

Acknowledgments

First and foremost, I am deeply grateful to my supervisors, Professor Clive Walker and Professor David Wall for their invaluable advice, continuous support, and patience during my PhD study. Their immense knowledge, plentiful experience, and caring direction have encouraged me throughout the period in which I undertook my academic research project and in many aspects of daily life.

For the memory of my late parents who dedicated their lives to the happiness and success of their children, I would love to pay them all my respect and appreciation for their untold and unknown sacrifices. Also, I would like to express my gratitude to my compass in life, my wife, who continually helps, supports and directs me towards being a better version of myself. Finally, I would love to thank all my friends and family for their encouragement and prayers, especially my brother Ibrahim. Without their tremendous understanding and encouragement over the past few years, it would be not possible for me to complete my studies.

Abstract

The Kingdom of Saudi Arabia (KSA) is in danger of falling behind other nations in combatting cybercrime as it becomes more technologically sophisticated. This raises important questions over whether the difficulties faced reflect the state's desired approach toward tackling cybercrime or the underlying nature of the criminal procedure in the KSA. The problem does not just relate to effectiveness but also raises the relevant question of whether the KSA's approach toward the criminal procedure in dealing with cybercrime is fair. In answering these major questions, the thesis investigates the shortcomings and factors holding the KSA back from tackling cybercrime in procedural terms. Amongst the factors identified are the reliance on the Islamic Sharia and the KSA's legislative frameworks, including the Basic Law of Governance 1992 (BLG) and the Criminal Procedure Law 2013 (CPL). Both of these features are crucial when evaluating the KSA's response to cybercrime from a procedural perspective. It is generally possible to say that the KSA does not differentiate between the criminal procedure of cybercrime and Non-Cyber Crime (NCC), which impairs the effectiveness and fairness of its approach to the former. Even though the KSA claims to be modernising society through its strategic plan, *Vision* 2030, it continues to depend on the pre-modern traditions found within the teachings of the Islamic Sharia to deal with cyberspace, which is a late modern phenomenon. Besides identifying the factors which have led to deficiencies in the KSA's approach toward the criminal procedure of cybercrime, the thesis focuses on the why the KSA criminal procedure of cybercrime remains indistinct from NCCs, even though it has passed multiple pieces of legislation which distinguish cybercrime from NCCs at the substantive level. Reforms will be suggested to produce more effective and fairer approaches to the criminal procedure that is applied to cybercrime, particularly in the light of lessons that can be gleaned from the experiences and legal accomplishments of England and Wales.

Table of Contents

List of Tables

List of figures

List of Abbreviations

ACL (Anti Cybercrime Law 2007)
ACFL (Anti Commercial Fraud Law 2008)
BIPP (Bureau of Investigation and Public Prosecution)
BIPPL (Bureau of Investigation and Public Prosecution Law 1989)
BLG (Basic Law of Governance 1992)
CA (Court of Appeal)
CC (Criminal Court)
CCJ (Criminal Court Judge)
CIC (Centre for International Communication)
CITC (Communication and Information Technology Commission)
CPL (Criminal Procedure Law)
CPLER (Criminal Procedure Law Executive Regulation 2015)
CPS (Crown Prosecution Service)
CSP (Communication Service Provider)
DNS (Internet Domain Name System)
DRM (Digital Rights Movement)
EEPU (Electronic Extortion Prevention Unit)
ETPL (Electronic Transection Protection Law 2007)
GCC (Gulf Cooperation Council)
GCHQ (Government Communications Headquarters)
GDI (General Directorate of Investigation)
GDNC General Directorate of Narcotic Control)
GPPVPV (General Presidency for Promotion of Virtue and Prevention of Vice)
HRW (Human Rights Watch)
IAB (Internet Architecture Board)
ICANN (Internet Corporation for Assigned Names and Numbers)
ICCPR (International Covenant on Civil and Political Rights 1966)
IETF (Internet Engineering Task Force)
IPA (Investigatory Powers Act 2016)
IPCO (Investigatory Powers Commissioners Office)
ISOC (Internet Society)
ISP (Internet Service Provider)
JA (Judge of Appeal)
JSL (Judiciary System Law 2007)
KACST (King Abdul-Aziz City for Science and Technology)
KSA (Kingdom of Saudi Arabia)
MEPPB (Members and Employees of the Public Prosecution Bylaw 2016)
MCIT (Ministry of Communication and Information Technology)
MoI (Ministry of Interior)
MoJ (Ministry of Justice)
NCA (National Cybercrime Authority)
NCC (Non-Cyber Crime)
NCSC (National Cyber Security Centre)
NCSS (National Cyber Security Strategy 2016-2021)
NISS (National Information Security Strategy 2013)
NPCC (UK National Police Chief's Council)

PACE (Police and Criminal Evidence Act 1984)
PF (Police Force)
PP (Public Prosecution)
PPL (Public Prosecution Law 1989)
PCIO (Preliminary Criminal Investigation Officer)
RCCP (Royal Commission on Criminal Procedure)
RIPA (Regulation of Investigatory Powers Act 2000)
SFCSP (Saudi Federation for Cyber Security and Programming)
SFO (Serious Fraud Office)
SJC (Supreme Judicial Council)
SS (UK Security Service)
UCHR (European Convention on Human Rights 1950)
UDHR (Universal Declaration of Human Rights 1948)
UK (United Kingdom)
UK NCA (National Crime Agency)

List of Arabic Terms

Aqidah (Islamic Doctrine)
Diyya (compensation or blood money)
Fiqh (Jurisprudence)
Halal (Allowed)
Haram (Prohibited or Forbidden)
Hudud (Class of punishment fixed in Qur'an)
Ijtihad (Personal judgment passed by Ulema)
Ulema (Sharia Scholars)
Ummah (Muslim Population)
Qathf (Defamation, used in relation to accusations of fornication)
Qisas (Class of punishment determined by retribution)
Ridah (Apostasy)
Sahwah (An Islamic and a Saudi fundamentalist movement that inspired social and political aspects)
Shura (Consultation)
Ta'zir (Class of punishment determined by Ijtihad)
Ta'zir be Alshubhah (Punishment based on suspicion)
Tafsir (Interpretation of the *Quran*)
Walee alamer (Muslim Guardian)
Zina (Fornication)

Chapter 1

Introduction

1.1 Background of the study

In recent years, the Kingdom of Saudi Arabia (KSA) has been confronted by a significant increase in cybercrime cases.[1] According to Norton Symantec, a US security software provider, 6.5 million people in the KSA were affected by cyberattacks and cybercrimes in 2016, and the cost to the KSA is almost SR 2.8 billion annually.[2] Moreover, this number has escalated since 2016, according to Kaspersky's 2021 report, in the first 2 months of 2021 there were 7 million cyberattacks which targeted the KSA, causing significant financial losses.[3] Aside from these financial losses, many of these attacks had a major impact upon components of the national infrastructure. However, the KSA seems to lack appropriate criminal procedures to tackle the threat of cybercrime.[4] One broad explanation is that cybercrime is the product of late modernity, while the KSA depends on pre-modern traditions, most notably its reliance on *Sharia* which is considered to be the supreme law of the land.[5]

The landscape of cyberattacks and cybercrime involves a threat to both people and governments as they include unique criminal activities such as hacking,[6] ransomware or "blackmail viruses"[7] and denial of service attacks. This threat landscape is very broad and therefore many elements of it are beyond the scope of this thesis, which will focus only on cybercrime from a procedural standpoint and will focus on *cybercrime* rather than *cyberattacks*. Cybercrime mostly involves domestic law violations committed in cyberspace,

[1] Alamro (2017) 36
[2] *Ibid* 40
[3] Obaid (2021)
[4] Hakmeh (2017)
[5] Algarni (2010)
[6] Wall (2018) 7-26
[7] *Ibid* 14

while cyberattacks might involve international violations committed in cyberspace, especially in the context of cyberwarfare[8] which is beyond the focus of this thesis. In Chapter 2, both cybercrime and cyberspace will be discussed in relation to the aims and objectives of this thesis.

1.2 Thesis statement

This thesis sets forth the proposition that the current procedural law and enforcement approaches in the KSA have become insufficient to tackle cybercrime. This thesis will examine the legal system in the KSA and investigate the proposition in order to indicate what factors have led to such deficiencies. It will demonstrate the flaws in the KSA's legal system through an examination of the current policies, laws, and regulations, and how they are applied to cybercrime, especially in regard to the law of criminal procedure. An examination and evaluation of procedural law related to cybercrime will be the main focus of the thesis. Furthermore, as the KSA is a Muslim country, an investigation into the influence of Islamic teachings and *Sharia* on cybercrime in terms of enforcement, practice and legislation will be undertaken in order to gain an understanding of how the KSA's legal system works and the limits it engenders in the response to cybercrime. The thesis will make the proposition that, through the reliance on the current understandings of *Sharia* and the current array of laws, further reforms are required to effectively and fairly address the challenges of cybercrime.[9]

This thesis will also evaluate attempts at combating cybercrime procedurally in the KSA using an analytical approach by comparing it with UK's[10] experience of tackling cybercrime procedurally for the following two reasons. Firstly, the researcher has conducted his research in England which provides an opportunity for the researcher to access a great

[8] Schmitt (Ed) (2017) 107-110
[9] See subsection 2.2.1
[10] Whenever the thesis refers to the (UK), it refers mainly to England and Wales only unless stated otherwise.

deal of material on the subject in UK libraries. It also provides a rare opportunity for the researcher to discuss his research with experts on the subject of his thesis and obtain criticism which will aid the development of the research. Secondly, the UK is one of the most highly developed countries in the world and boasts some of the most sophisticated laws and legal experts regarding cybercrime.[11] As a result, being in such an environment enhances the findings of the thesis and certainly helps the researcher in seeking a more advanced perspective than available solely in the KSA.

Therefore, regarding the study of cybercrime from a procedural standpoint, there are two jurisdictions which are studied in this research. The first and primary jurisdiction is that of the KSA. The research is mainly built on studying the KSA's application of both *Sharia* and national legislation and how they deal with the problems arising from cybercrime. The second is that of the UK. The researcher has stated the reasons for choosing this jurisdiction and why it is important for the research. However, comparing the KSA's approach with the UK's experience of combatting cybercrime is not as easy because the two jurisdictions are very different in terms of the structure and content of their laws and in their political and social structures. Yet, it is possible to explore the possibility of transferring policy ideas regarding the criminal procedure of cybercrime from the UK to the KSA as common ground to base the transfer on is found, such as the common aim of both jurisdictions to protect people from being subject to cybercrime and to prevent cybercrimes. Thus, it may also be claimed that the nature and experiences of cybercrimes overlap to some extent, though not as a whole. Therefore, it is possible to say that the KSA could learn lessons for combating cybercrime, not just from its neighbouring Muslim countries, but also from the UK because "most different countries offer the maximum of fresh insights into the public policy."[12]

[11] Ibekwe (2015) 8
[12] Rose (2005) 48

Overall, the key issue which this thesis covers is the KSA law of criminal procedure as it relates to cybercrime. The thesis will focus on the four stages of criminal procedure, namely policing, investigation, prosecution and trial, and will test whether they are fair and effective based on measurements set out in Chapter 2. It is clear that fundamental and detailed reform is needed to improve the criminal procedure relating to cybercrimes in the KSA. Nevertheless, there is some hope that reform is possible, and a recent radical example concerns the changes to the role of *Sharia*. In recent years, reforms have been made to the Criminal Procedure Law (CPL) 2013.[13] On 3 January 2019, the KSA Minister of Justice and the president of the Supreme Judicial Council (SJC) issued an executive order that aimed to apply provisions of Article 3 of the CPL 2013 with no regard to *Sharia* interpretation on the matter.[14] The order abolished what *Sharia* experts termed the *Ta'zir be Alshubhah* (punishment based on suspicion). This concept is supposedly inspired by the *Sharia* and gives Criminal Court Judges (CCJ) authority to punish when they do not have enough evidence to convict suspects under formal legislative rules of evidence, including in cybercrimes cases,[15] as will be discussed in Chapter 7. Abolishing *Sharia* experts' interpretation of Article 3 would an important step towards reforming the criminal justice system in the KSA, because this interpretation of the Article was being acted on by CCJs based on old interpretations of the *Sharia*[16] which most of them support. However, the majority of CCJs are experts only in *Sharia*[17] and have little knowledge regarding cyberlaw more broadly, as will be addressed in Chapter 7.

Before the abolition of this interpretation of Article 3, there were many lawyers and law experts who strongly disagreed with the concept of *Ta'zir be Alshubhah* as it clearly

[13] KSA CPL 2013, promulgated by a Royal Decree No. M/2
[14] Ministry of Justice (2019)
<https://www.moj.gov.sa/ar/MediaCenter/News/Pages/NewsDetails.aspx?itemId=707>
[15] CPL 2013 Article 3
[16] Alhifnawi (1986) 575
[17] Interview with Criminal Court Judge CJ1

contradicts the said Article, but their voice was not heard as it was argued that "their claim contradicts the *Sharia*."[18] However, neither the *Quran* nor the *Sunnah*, which are the two primary sources of *Sharia*,[19] support the *Ta'zir be Alshubhah*. In fact, both sources advise against it. For example, the Prophet Muhammed is reported to have said, "Suspend applying *al-hudud* on cases of suspicion."[20] *Al-hudud*, which will be covered in Chapter 7, are punishments which are fixed in the *Quran* for particular crimes[21]. However, CCJs in the KSA supported the interpretation of the Article, not because it is *Sharia* based, but because it gave them more power, and the abolition of this Article's interpretation limits their already extensive power. Also, the abolition demonstrates that the KSA is letting go of some strict applications of *Sharia* because of the KSA *Vision 2030*[22] which seeks to modernise the country,[23] as will be addressed in Chapter 2. Thus, depending only on *Sharia* would be an obstacle to the modernization of the country and to cooperation with the international community which strongly opposes many of *Sharia* principles.[24] While some reform of the KSA's law of criminal procedure regarding criminal cases has thus occurred, many other aspects of criminal procedure regarding cybercrime, such as policing, investigation, prosecution and trial require further attention.

1.3 Research aims, objectives and questions

The main distinction between research objectives and research aims is that research aims describe what the research is meant to achieve,[25] while the research objectives describe

[18] Interview with Criminal defence Lawyer CL2
[19] BLG Article 7
[20] Altermithi 824-892 AD (No 1344)
[21] Udah (2009) 243
[22] KSA Vision 2030 <https://vision2030.gov.sa/en>
[23] *Ibid* <http://vision2030.gov.sa/en/node/9>
[24] Emon et al. (2012)
[25] Thomas and Hodges (2010) 38-47

how the researcher is going to achieve the aims of the research.[26] Therefore, each will be addressed separately in order to comprehensively draw out the main lines of the thesis. In addition, research questions which are derived from the aims and objectives of the research will be addressed in a separate subheading to distinguish further their derivation.

1.3.1 Research aims

This thesis aims to evaluate cyberspace as a phenomenon in the KSA, and to assess how the KSA deals with such phenomenon. The phenomenon of cyberspace outside the KSA has been already analysed by many distinguished scholars,[27] however, it has not been fully covered in relation to the KSA's jurisdiction, especially in regard to criminal procedure. Additionally, the thesis will evaluate how cyberspace generates or permits cybercrime in the KSA, and how the KSA responds to cybercrime, whether through legal, social, or political measures. Here, the researcher will explore the background occurrence of cybercrime in the KSA and will evaluate the role of *Sharia*, legislation and other measures for regulating cybercrime and cyberspace, and how this very modern phenomenon is being addressed within the very traditional culture of the KSA (including the ways in which it utilises the *Sharia).* This aim will be further pursued through analysing relevant policies, including *Vision 2030*[28] which seeks to drive the KSA's political and social systems toward modernity, or even late modernity.

Secondly, the thesis aims to evaluate the impact of *Sharia* on the field of cybercrime by analysing and evaluating the provisions of the criminal procedure that are related to cybercrime that exist in *Sharia* and how they compare with both the KSA's criminal procedure legislation and with international standards such as the Convention on Cybercrime

[26] *Ibid*
[27] See Section1.5
[28] KSA Vision 2030 <http://vision2030.gov.sa/en/node/9>

2001[29] (as implemented in the UK). Moreover, the research will test whether the responses in the KSA are fair and effective. The tests of fairness and effectiveness will be drawn out through both theoretical (document analysis) and empirical (interviews) approaches. It is important to know whether KSA law is fair and effective, in order to know whether or not the KSA has failed in combating cybercrime from a procedural perspective. It is especially significant for this thesis to know whether the KSA's law of criminal procedure regarding cybercrime is fair and effective in order to explain its operation and to suggest reforms.

Thirdly, the research aims to evaluate the policy approaches that the government of the KSA implements to tackle cybercrime procedurally. In other words, the research will study the domestic response to cybercrime at a procedural level. This will be done through the description and evaluation of official institutions and private entities involved in the implementation of activity against cybercrime in the KSA, including the development of strategies, operational measures, and coordination mechanisms. In terms of detailed implementation, the thesis analyses and evaluates cybercrime in relation to the attendant CPLs in the KSA. In addition, with regard to the evaluation and analysis of the criminal procedure of cybercrime in the KSA, the thesis aims to identify changes which are necessary to improve procedural protection against cybercrimes in line with values of effectiveness, fairness and whether they can or should be made in the light of the precepts of *Sharia* law.

Lastly, the research considers the transfer of policy from other jurisdictions, specifically that of the UK. Here, it will be explained how the UK performs better than the KSA in combating cybercrime procedurally and regulating the use of cyberspace.

[29] Convention on Cybercrime 2001

1.3.2 Research objectives

The overall approach of this thesis is divided into doctrinal and empirical methods in order to achieve the research aims, as will be explained later in the Methodology Chapter (Chapter 3). For the most part, the theoretical explanations will be mainly based on documents and literature in English and Arabic accessed while studying in Leeds and Riyadh respectively. Those materials involve primary and secondary sources, and they are available in libraries and online. These resources allow the researcher to evaluate the nature of cybercrime and the KSA's attempts to combat cybercrime procedurally by using an analytical approach and by comparing the UK's experience. At the same time, the empirical approach was mainly conducted using online communications platforms in the middle of 2020, due to restrictions and social distancing rules put in place as a result of the COVID-19 pandemic. Through this platform, the researcher interviewed KSA citizens who possess expert information related to the criminal procedure of cybercrime in the KSA and which is relevant to the subject matter of the research. Here, it will be demonstrated how cybercrime and the responses in process in the KSA operate in practice. To do this, the researcher has chosen to conduct multiple interviews with expert government officials, lawyers and private sector employees to collect data related to cybercrime and the responses in process in the KSA. To pursue that objective, the researcher excluded both general public and cybercrime victims.

This thesis seeks to determine how best to tackle cybercrime in terms of criminal procedure and to test how far it is possible to do so by relying on *Sharia* as well as modern legislation. There will need to be four aspects to the analysis of whether current models of law comply with *Sharia* and whether further changes are needed which can remain compliant. The first of these is the analysis of laws of the KSA, including those directly related to *Sharia* and the institutional laws that are derived from *Sharia*. These aspects will, secondly, include the legislation about criminal processes (including policing and judicial

interventions). The first aspect is more general and abstract, while the second aspect is more specialist and detailed. This means that the research is focused more on the second aspect as more relevant to the thesis. The research will, thirdly, test the measures by referencing their conformity with both international standards of fairness and effectiveness, including the Council of Europe Convention on Cybercrime 2001 the International Covenant on Civil and Political Rights 1966 (ICCPR),[30] the Universal Declaration of Human Rights 1948 (UDHR),[31] as well as standards in KSA law. The research will, fourthly, test measures by referencing their conformity to other domestic standards of fairness and effectiveness, such as the laws in the UK, for the purpose of policy transfer.

1.3.3 Research questions

1. What is the role of both *Sharia* and the KSA legislation (the KSA law) in combating cybercrime procedurally? (Chapters 2, 4, 5, 6 and 7)
    a. Where does *Sharia* stand with regard to cybercrime and procedures to deal with the phenomenon? (Chapters 2 and 4)
    b. What is the current legislation related to the processes of policing investigation, prosecution, and trial to deal with cybercrime in the KSA? (Chapters 4, 5, 6 and 7)
    c. How does the CPL 2013 work with regard to criminal procedures in response to cybercrimes? (Chapters 4, 5 and 6)
    d. What other instruments of governance might be used to deal with cybercrime and what processes do they imply? (Chapters 4, 5, 6 and 7)
2. Is the KSA law of criminal procedure that relates to cybercrime fair and effective? (Chapters 4, 5, 6, and 7)

[30] ICCPR 1966
[31] UDHR 1948

a. What is meant by fair and effective? (Chapter 2)
b. What are the international standards of fairness and effectiveness? (Chapter 2)
c. Is *Sharia* fair and effective? (Chapter 4)
d. Is the KSA legislation fair and effective? (Chapters 5, 6, and 7)

3. How does the UK deal with cybercrime, and how can the KSA best benefit from this experience? (Chapter 7)
    a. Is it possible to transfer policies from the UK to the KSA? (Chapters 3, 4, 5 ,6 and 7)
    b. What specific lessons can policy transfer draw upon to make criminal procedures in regard to cybercrimes fairer and more effective? (Chapters 4, 5, 6, and 7)

1.3.4 Structure

This thesis is divided into 8 chapters, as the diagram in 1.1 shows. The following paragraphs will demonstrate how each chapter of the research is structured.

To start with, Chapter 1 (Introduction) introduces the thesis by setting out the thesis statement, the research questions and the research aims and objectives. It will also explain the originality of the research. Moreover, it introduces useful works in the Literature Review section that will be discussed in later chapters. Also, Chapter 1 includes the outline of the research and how it is structured.

Chapter 2 (thesis background) explores the background of the researched phenomenon and how to understand it as a matter of policy and law. In terms of the latter, this chapter shows how the legal system of the KSA works overall, including the roles of *Sharia* and modern legislation. Looking forward, this chapter addresses the policy shift that the government is working on through *Vision 2030*; then it will apply these changes to the phenomenon studies in the thesis. This chapter also addresses the meaning of values of

fairness and effectiveness which are used in later chapters as an instrument of analysis, particularly in Chapters 4, 5, 6 and 7.

Chapter 3 (Methodology) is about the methodologies that the researcher uses. This research involves both documentary and fieldwork (qualitative) research in which the researcher utilises an empirical study to gather and evaluate data collected mainly from experts through interviews with them. It will also discuss how field work data are obtained and processed. Finally, this chapter suggests lessons that can be learned from the UK using the policy transfer method.

Chapter 4 (Assessment of cybercrime law of procedure in the KSA) explores the current legislation on cybercrime in the KSA related to the law of criminal procedure. It explains and assesses it in terms of the effectiveness and fairness of the KSA's cybercrime procedural response. It examines the current legislation about cybercrime in the KSA, and also the operation of *Sharia* law in so far as it affects legislation and as a source in its own right. Moreover, the *Sharia,* as applied in the KSA, will be tested for its fairness and effectiveness using instruments of analysis introduced in Chapter 2. Furthermore, a Model Code of the KSA's approach to the criminal procedure of cybercrime is suggested to illuminate the main institutions and operations involved in the process in order to identify what has been done and what has yet to be done by the KSA in regard to the criminal procedure of cybercrime.

Chapter 5 (Policing or initial investigation of cybercrime in the KSA) explains the current legislation on cybercrime in the KSA regarding the law of criminal procedure as it applies to policing and initial investigation. It addresses the policing of cyberspace within the boundaries of the KSA and how the police initially investigate cybercrime in the KSA. It also explains how policing authorities in the KSA deal with cybercrime suspects; how they are investigated and then subjected to formal policing powers such as arrest and search. This

chapter explains who polices the use of the internet in the KSA. It will be demonstrated that policing cybercrime is very complex, because there are multiple authorities, aside from the Police, that have both policing and investigative authorities. The data collected from the fieldwork will be used as a main source to inform the discussion about policing cybercrime in the KSA. Moreover, a test of fairness and effectiveness of the KSA's policing will be tested in regard to the related institutions and operations that are introduced in the same chapter. Also, lessons from the UK in regard to the matters discussed in the chapter are drawn as an objective of this thesis.

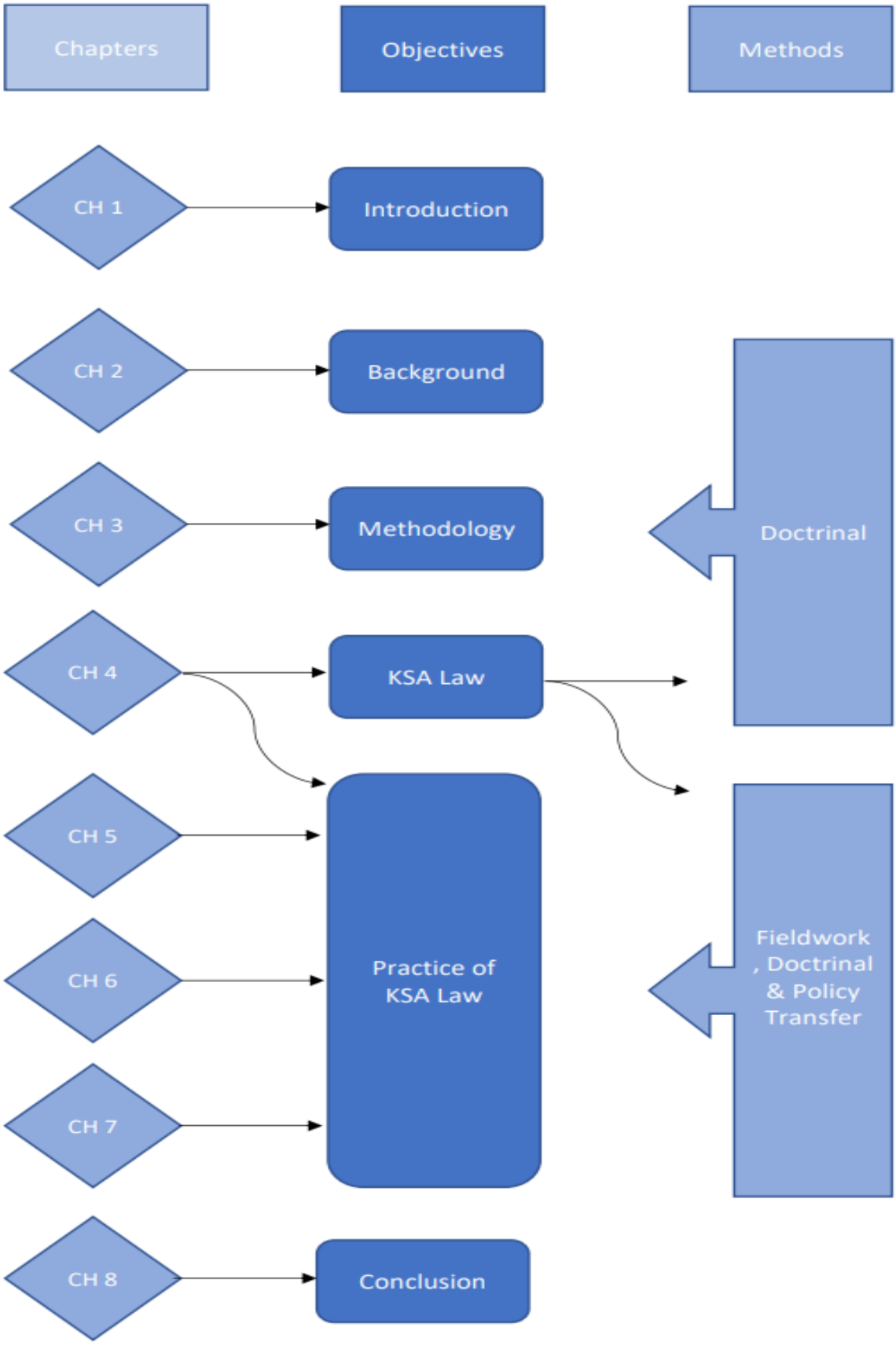
Chapter 6 (Preliminary investigation of cybercrime in the KSA) explores the KSA's legislation related to the criminal procedure for the investigation of cybercrime. In this chapter, the Public Prosecutor (PP) is introduced as the main investigatory entity in the KSA as outlined in the CPL, along with the powers they exercise related to the criminal investigation of cybercrime. Interview data will be employed in this Chapter as there is a lack of sources regarding investigation of cybercrime in the KSA. Moreover, this chapter tests this institution and how it operates for both fairness and effectiveness, based on the values of fairness and effectiveness introduced in Chapter 2. Next, it mentions the UK's experience of the criminal investigation of cybercrime in order to learn lessons from its experience.

Chapter 7 (Prosecution and trial for cybercrime in the KSA) answers the question, "what is the current legislation on cybercrime in the KSA regarding the law of criminal procedure as it applies to prosecution and trial?" It evaluates criminal justice in the KSA through analysing the process of prosecuting and seeking court decisions on cybercrime offences. The chapter discusses how prosecution works in the KSA, both institutionally and operationally. In regard to the process of investigation and prosecution, this chapter will also explain the process of trial in courts and the presentation of cyber evidence and how the trial of cybercrime is conducted in light of both institutional and operational aspects. In this Chapter,

collected data from interviews will be used as a crucial source of data about the prosecution and trial of cybercrime in the KSA. Moreover, this chapter aims to test the fairness and effectiveness of both the prosecution and trial of cybercrimes in the KSA to satisfy the thesis' aims and objectives.

Lastly, Chapter 8 (Conclusion) will conclude the thesis. This chapter will be comprised of a presentation of the findings, limitations and recommendations of the thesis.

Figure 1.1 Thesis structure related to objectives and methodologies



1.4 Originality of the thesis

This thesis evaluates a topic that has not been fully addressed yet by other researchers, namely, the evaluation of whether the KSA's CPL (in *Sharia* and national legislation) fairly and effectively combats cybercrime. Some studies have briefly mentioned this issue, such as Alqarni's PhD thesis, *Policing the Internet Fraud in Saudi Arabia: The Mediation of Risk in a Theoretic Society.*[32] However, Alqarni's paper and other similar studies neither detail nor evaluate the law of criminal process in the KSA regarding cybercrime. Moreover, even recent works which address substantive cybercrime, such as the PhD thesis *Legal Responses to Cybercrime in Saudi Arabia with Special Reference to the Council of Europe Convention on Cybercrime and the Law of the United Kingdom* that was submitted in 2016 by Suhail Almerdas, do not address criminal procedure regarding cybercrime.[33] The same point applies to Bushra Muhammed's work.[34] In addition, her study focuses more on cybercrime in the field of cybersecurity. Fahad Moafa also takes a similar approach to that of Muhammed, but he refers to the UK.[35] Next, Flaeh Alqahtani researched cybercrime in the KSA with reference to the UAE.[36] However, the present thesis will not have as its primary focus the substance of cybercrime, and it will refer to the UK. In addition, this thesis will not just consider the technical details of the criminal procedure related to cybercrime but will also assess how policy such as *Vision 2030* can influence future legal developments. Finally, most of the foregoing texts are entirely doctrinal, with a few exceptions such as Almerdas and Algarni, whereas this thesis is socio-legal.

The leading textbooks on criminal law in the KSA do not deal with cybercrime substantively or procedurally. Even though Usama Abdula'al's book, *Explaining the General*

[32] Algarni (2012)
[33] Almerdas (2016)
[34] Elnaim, (2013)
[35] Moafa (2014)
[36] Alqahtani (2017a)

Principles of Criminal Law; *Analytical Study Compares Between Provisions of Sharia and Legislation,*[37] is recent, it does not deal with cybercrime. Similarly, *The Coded Ta'zir Crimes in the KSA* by Futuh Alshatheli[38] does not mention cybercrime at all, even though this book was updated in 2015. Both of these books, which are used by students, deal primarily with substantive criminal law and lack attention to criminal procedural law. Within books more related to criminal procedure, Al Said Shareef's *Brief on Explaining the KSA Criminal Procedural Law*[39] does not cover the criminal procedure of cybercrime even though it is the leading textbook about criminal procedure in the KSA. The same applies to Abudlfattah Saifi's *General Principles of Criminal Law in Sharia and Legislation,*[40] which is taught to prosecutors and detectives.[41]

In fact, most judges, lawyers, policemen, detectives, prosecutors and law researchers, including law professors in the KSA, deal with cybercrime in the same way as more traditional forms of crime due to the limited training and textual sources.[42] The leading source of criminal law in the KSA and many Arab countries which discusses criminal law in accordance with the *Sharia* in depth is *Islamic Criminal Law with Comparison to Legislation* by Abdulqader Udah.[43] It was written around 1940 and does not, therefore, mention cybercrime at all. Yet judges in the KSA still depend on it along with other books that were written between the 13th and the 14th century, by such scholars as Ibn al-Qayyim and Ibn Taymiyah.[44]

Therefore, the researcher can claim originality in this subject area of research by going into more depth in evaluating the ability of the KSA's law of criminal process to combat

[37] Abdula'al (2015)
[38] Alshatheli (2015)
[39] Shareef (2016)
[40] Saifi (2013)
[41] Interview with Detective of the PP D1
[42] 18 out 21 interviewees think there is no need to distinguish between cybercrime and traditional crimes, because they are all crime and therefore essentially the same.
[43] Udah (2009)
[44] Interview with Criminal Defence Lawyer CL2

cybercrime and test whether it is fair and effective using mixed methods, which are comprised of doctrinal analysis, policy transfer and interviews. Moreover, due to the unique nature of the KSA's legal and social system, this thesis will be a socio-legal study, investigating the KSA's legal system in regard to the area of research with reference to the views of professional experts and the policies set forth in *Vision 2030*.

1.5 Literature review

There are many scholarly sources that address issues surrounding cybercrimes which originate from countries beyond the KSA, especially the UK and USA. First, conceptual literature which may be helpful to the thesis will be considered and, second, more detailed and technical literature will also be considered. As one aim of this thesis is to analyse the KSA's response to the criminal procedure of cybercrime and one objective is to reference the UK jurisdiction to inform suggested policy transfer, conceptual literature helps in understanding the cyber phenomena and its relationship to law – criminal law in particular – in order to ascertain how the KSA should operate. Moreover, detailed and technical literature helps in the overall analysis of the KSA's response and how it should benefit from the UK.

Amongst the leading conceptual literature, Lawrence Lessig wrote a series of books on the governance of cyberspace, including *The Future of Ideas; The Fate of The Commons in Connected World*[45] and *Code and Other Laws of Cyberspace*.[46] Lessig's work will be examined in Chapter 2 along with Ayres and Braithwaite's book, *Responsive Regulation Transcending the Deregulation Debate*,[47] which helps in drawing a picture of how the use of cyberspace could be regulated in the KSA.

[45] Lessig (1999)
[46] Lessig (2006)
[47] Ayres and Braithwaite (1992)

As well as addressing the conceptual literature on cybercrime and cyberspace, the researcher will address the more detailed and technical literature on cybercrime and cyberspace. To start with, Majid Yar and Yvonne Jewkes' book *Handbook of Internet Crime*[48] explains cybercrime features.[49] It is very informative in analysing the UK's Computer Misuse Act 1990,[50] which will be compared with cybercrime legislation in the KSA in order to draw out the stated research objectives of this thesis. Criminal justice is an essential aspect of this research, and this book covers the impact of internet technologies in criminal justice.[51] Other books which aid the technical analysis of cybercrime and related procedures include Stefan Fafinski's *Computer Misuse; Response, Regulation, and The Law*[52] which explains the distinctions between civil wrongdoing and criminal actions that constitute cybercrime, and the jurisdiction of the misuse of the internet within the UK.[53] He also demonstrates the concept of risk, the risk society and risk in criminal law which links into the concept of modernity.[54] Furthermore, on the subject of cybercrime, *Information Technology Law; The Law of Society* by Andrew Murray[55] illustrates the concept of the network of the networks (the internet) and the cross-border challenges that it faces.[56] This book also considers both the UK and the global standards of internet pornography.[57] Another book edited by Andrew Murray, along with Mathias Klang, is *Human Rights in the Digital Age*.[58] This book is valuable to the research because it discusses issues, with reference to the value of fairness, such as internet firewalls and the censorship of the internet; filtering and

[48] Yar and Jewkes (2010)
[49] *Ibid* 44 & 89
[50] *Ibid* 404
[51] *Ibid* 582
[52] Fafinski (2009)
[53] *Ibid.* 119-123
[54] *Ibid* 133, 151-157 and 180
[55] Murray (2019)
[56] *Ibid* 15 & 49
[57] *Ibid* 355 & 359
[58] Murray and Klang (2005)

blocking.[59] For instance, this book explains which websites are being blocked by the KSA authorities.[60] Finally, *Law, Policy and the Internet*, edited by Lilian Edwards, also discusses the regulation of the internet along with Lessig's theory.[61] This book will be helpful when addressing topics around the UK's polices regarding cyberspace, such as internet censorship,[62] including their effectiveness.

More policy orientated books which were relied on for this thesis included those from David Wall who shows how the law in the UK operates in regard to cybercrime. *Crime and Deviance in Cyberspace*, which he edited, explains the concepts of cyberspace and cybercrime, and gives definitions of such terms.[63] The book also helps in identifying cybercrime targets through measurements that are included in the law and norms.[64] It also helps in understanding cybercrime related subjects such as codes, cyberspace governance, and cyberspace policing.[65] Another important book is *Crime and The Internet*[66] which facilitates the notion that the internet is not a lawless place; harmful and illegal contents should be controlled, and order and law should be applicable in cyberspace.[67] Additionally, his book *Cybercrime; The Transformation of Crime in the Information Age*,[68] gives more detail about what to consider as cybercrime in the UK. It also explains some of the procedural aspects in the UK's laws regarding cybercrime. Consequently, the researcher will consider these ideas in this thesis when either referring to cyberspace or cybercrime within the UK jurisdiction.

[59] *Ibid* 111
[60] *Ibid* 122
[61] Edwards (2019) 4-8 and 15
[62] *Ibid* 291
[63] Wall *(*2009) 5
[64] *Ibid.15-18*
[65] *Ibid.* 117, 165, 168, 379, & 451
[66] Wall (2001)
[67] *Ibid* 114-120 & 169-170
[68] Wall (2007a)

The researcher also sought out literature regarding the enforcement of law in cyberspace within the UK's jurisdiction, such as Graham Smith's *Internet Law and Regulation* which focuses in part on enforcement and jurisdiction.[69] Other books such as Walden's *Computer Crime and Digital Investigation* explore issue like policing cyberspace, computer and network forensics, monitoring or surveillance of cyberspace, and seizing data.[70] In the same regard, Peter Grabosky's book, *Electronic Crime,* deals with the procedural issues regarding cybercrime within the US perspective, especially when it comes to investigation.[71] However, the US's jurisdiction is not generally included in the scope of this thesis because of the constraints of space and time.

In contrast to UK literature, there are very few published sources that address the Saudi approach to cybercrime, both at substantive and procedural levels, especially in the English language. Some of these sources take the form of academic research and articles, but only a few of them are conducted within the area of law. The first relevant source is the PhD by Suhail Almerdas. The areas that he has covered should be updated and developed by the researcher because, since 2016, there have been various changes, both in the area of law, such as the amendments to anti-cybercrime laws and in the area of politics. In subsequent years, the KSA has established two government entities to enhance and strengthen cybersecurity in the Kingdom, the first of which is the Saudi Federation for Cyber Security and Programming (SFCSP),[72] which was formed in January 2018.[73] The second entity is the NCA which was established in October 2017.[74] As mentioned previously, Almerdas' PhD thesis mainly

[69] Smith (2002) 241
[70] Walden (2007) 48, 205, 214, 222, 276, and 391
[71] Grabosky (2007a) 69
[72] Saudi Federation For cybersecurity and Programming <https://safcsp.org.sa/en>
[73] Saudi Press Agency (SPA) (2018) <https://www.spa.gov.sa/1706467>
[74] Saudi Gazette <http://saudigazette.com.sa/article/520782/SAUDI-ARABIA/King-orders-setting-up-of-National-Cyber-Security-Authority>

concentrates on the technical concept of cybercrime and not procedure, or how offences are enforced in law and implemented in practice.

Additionally, unlike Almerdas' PhD thesis, this thesis will show in depth how the *Sharia* affects legislation in the KSA, especially on criminal procedure of cybercrime. The general effect of the *Sharia* on legislation in the KSA has been addressed by numerous scholars, such as Jan Michiel Otto who argues that, as the KSA criminal law still relies on *Sharia* Criminal Law, the country has not implemented modern criminal codes.[75] Another scholar who addresses the effect of *Sharia* over the KSA's criminal law is Rudolph Peters who says that the legal system in the KSA is exceptional and different from other Islamic countries because it makes *Sharia* the ultimate source of legislation, yet the KSA's legislators have not codified the rules of *Sharia* in criminal law.[76] These arguments will be addressed throughout the thesis in the context of cybercrime in the KSA, especially in Chapters 2, 4, 5, 6, and 7.

In contrast, studies exist that detail KSA's Anti Cybercrime Law 2007 (ACL),[77] such as Abdullah Algarni's PhD thesis on *Policing the Internet Fraud in Saudi Arabia: The Mediation of Risk in a Theoretic Society*.[78] Therefore, the evaluation of criminal law offences in this thesis will be confined mainly to one chapter only (Chapter 4), and it will also consider the impact of Islamic law – how it has shaped offences or determined the legislative agenda.

Leaving aside doctrinal literature, this research also adopts a socio-legal approach. In comparison, there have been some studies that are similar in terms of methodology but not in terms of subject. For example, Nurah Qaisi has written about the socio-logical reasons that drive offenders to commit cybercrimes, and what should the government do to prevent

[75] Otto (2010) 19
[76] Peters (2005) 148
[77] ACL, promulgated by Royal Decree No. M/17
[78] Algarni (2012)

cybercrime by strengthening the ACL.[79] Finally, this research will discuss the later socio-legal and political variables that led the Government of the KSA to devise the KSA's *Vision 2030* and how such changes will have impact on cybercrime.

1.6 Conclusion

Until recently, especially before the launch of the KSA *Vision2030* in 2016, the KSA showed limited interest in the rising threats from cybercrime and cybersecurity.[80] As noted by Yar et al, "'Cyberspace', the realm of computerised interactions and exchanges, seems to offer a vast range of new opportunities for criminal and deviant activities."[81] Such "criminal and deviant activities" attack infrastructure and citizens alike and need to be tackled by appropriate legal measures on both substantive and procedural levels.[82] The KSA's approach to tackling cybercrimes is insufficient, especially with regard to criminal procedure which this research highlights. The KSA equally struggles in dealing with substantive crimes within cyberspace. Although the KSA has passed the ACL,[83] cybercrime in the KSA is still being dealt with in the same way as more traditional forms of crime, yet it is argued that it should be dealt with distinctly as will be discussed in the next chapter. Both legislation and *Sharia* say almost nothing about the criminal procedure in regard cybercrimes. Moreover, cybercrime is not a subject of study in law schools in the KSA, whether on the substantive or procedural level. The leading textbooks in the KSA on criminal law do not deal with cybercrime; they are either from the classical era of Islam[84] and therefore hundreds of years old, or they view cybercrimes as being the same as traditional forms of crime. Furthermore,

[79] Qaisi (2010)
[80] Yar and Steinmetz (2019) 1-11
[81] *Ibid* 2
[82] *Ibid* 1-11
[83] ACL, promulgated by Royal Decree No. M/17
[84] Otto (2010) in p.25, he says "the corpus of rules, principles, and cases that were drawn up by fiqh-scholars in the first two centuries after the Prophet Muhammad. Sharia"

there are only a few PhD researchers who have discussed cybercrimes within the context of the KSA, and they have focused on substance not procedure. Therefore, this research provides an original and comprehensive analysis and critique of cybercrimes in the KSA in terms of the CPL. Most importantly, it does so with the benefit of a socio-legal approach and with the benefit of policy transfer from the UK.

Chapter 2

Background of the Study

2.1 Introduction

This chapter reflects the thesis aim of evaluating the KSA's approach to the cyberspace in order to build a basis for understanding its approach to the criminal procedures relating to cybercrime, which is the main focus of this thesis. Moreover, it reflects the aim of assessing *Sharia's* impact on the KSA's approach and the impact of *Vision 2030* on present and future changes. Moreover, as an aim of this thesis is to test the KSA's approach to the criminal procedure of cybercrime, this chapter introduces standards of fairness and effectiveness to be later applied in Chapters 4, 5, 6 and 7.

This chapter introduces the background phenomena shaping cybercrime processes in the KSA and provides an in-depth explanation of why and how cybercrime constitutes a problem within the jurisdiction of the KSA. It includes an in-depth introduction to some key concepts, such as cyberspace, effectiveness, fairness, *Sharia*, and *Vision 2030.* Thereafter, it will explain how the legal system in the KSA currently works in relation to cybercrime in order to test the ability of the KSA's legal system to tackle cybercrime from a procedural perspective. In addition, measurements of both fairness and effectiveness will be set out in this chapter to be used in the analysis of the KSA's laws. In order to pursue such analysis, tests for fairness and effectiveness to assess the KSA's law will be examined in order to achieve one of the objectives of this research which is to test the ability of the KSA's law of criminal process to combat cybercrime. Therefore, this chapter explains the instruments that will be used for these tests in further analysis, particularly in Chapters 4, 5, 6, and 7. Also, the chapter introduces the complexities of KSA law, which is crucial to understanding the current approach of the KSA's criminal procedure in relation to cybercrime, and further analysis in

Chapters 4, 5, 6 and 7 are made based on such understanding. Also, this chapter will show how *Vision 2030,* the KSA's reform blueprint, might have an impact on tackling cybercrime from a procedural perspective.

2.2 The meaning of cyberspace with regard to the KSA's jurisdiction

In order to fully understand the concept of cybercrime as a main focus in this research, the meaning of cyberspace will be explored and clarified. According to Darrel Menthe, "cyberspace is a place outside national boundaries: taken together, these tools constitute a unique medium – known to its users as 'cyberspace' – located in no particular geographical location but available to anyone, anywhere in the world, with access to the internet."[85] The internet makes it possible for users to communicate data throughout the network of computers using telephonic wires and Wi-Fi connections.[86] So, even though cyberspace has no single physical or geographical existence, all states must deal with it within their own jurisdiction;[87] however, no single national authority controls the internet.[88] In other words, there are no exclusively sovereign laws that regulate comprehensively the design of the internet,[89] and there is no single international law authority related to it.[90] The transnational authorities, such as they are, are mainly private bodies such as the Internet Corporation for Assigned Names and Numbers (ICANN)[91] and the Internet Society (ISOC),[92] as will be discussed later in the next subsection. Nevertheless, sovereign countries can seek to impose rules that are deemed to be important to their own society, whether by criminal law or

[85] Menthe (1998)
[86] Walker (1998) 3
[87] Zekos (2007)
[88] Loader (1997) 1
[89] Akdeniz, Walker, and Wall (2000) 6
[90] Murray (2019) 56 & 61-65
[91] See <https://www.icann.org>
[92] See <https://www.internetsociety.org/about-internet-society/>

civil law or other governance mechanisms.[93] Therefore, the Saudi authorities and officials have national powers to regulate, enforce and establish the necessary rules and means in order to control its own citizens' use of cyberspace, but they cannot control it entirely because most of the internet servers and private rule-makers are located in the United States of America (USA) or elsewhere outside of the KSA.

Issues of effectiveness and fairness inevitably arise because cyberspace is different from previous communications activities which the KSA and other countries have regulated by law because it is a development of late modernity.[94] Thus, this causes questions of effectiveness and fairness to arise about the value of the internet and whether it is desirable, proper, and fair for the state to interfere in cyberspace, as well as whether such interference might conflict with other national values or contravene international norms of fairness. Questions related to effectiveness involve whether states have the capacity to do something at all to achieve an objective, and, if so, how best to do it in terms of the use of utilising resources. Fairness is different from effectiveness, although both ask factual questions about whether states achieve something and both involve values and facts, yet effectiveness is about achievement and fairness is about the values and interests that are affected by such achievements, as will be addressed in Section 2.4.

2.2.1 Jurisdiction and expertise of the KSA over the Internet

Lessig argues that code is the ultimate architect of cyberspace, and it is also the only form of law which is made by common people through norms, so those people would either have an influence to code cyberspace in order to maintain the fundamental principles of liberality or to allow these principles to disappear.[95] He contends that, for the coming

[93] Akdeniz, Walker, and Wall (2000) 13
[94] Murray (2007)
[95] Lessig (2006) 6, 83-85 & 121-123

generation to enjoy their second life in cyberspace, it should be regulated.[96] He also argues that the Internet makes people's life easier, but it does not make it different, while cyberspace does because there are people who live in it throughout internet communication.[97] The Internet operates in cyberspace but it is distinguished from cyberspace, and it is important to know the distinction in order to know what to regulate.[98]

According to Lessig, there are two ways to regulate cyberspace.[99] One way is to regulate cyberspace through hard law (the *direct* approach), and the other way is to regulate cyberspace through soft law (the *indirect* approach). The first way means that cyberspace can be regulated directly by national governments, which in itself is a threat to liberty as well as cyberspace itself. The other approach means that cyberspace can be regulated indirectly by social norms or the internal rules of private corporations or even the laws of computing coding that operate in cyberspace. Therefore, lawmakers can employ all these techniques in order to regulate cyberspace.

Lessig argues that the internet consists of three layers; physical, codes, and content and, as such, is similar to other communication systems like telephone and cable television. In this regard, he argues that all of these layers can be controlled, but what should really be controlled is the layer of digital data or, as he refers to it, content which can be controlled by laws and codes.[100] When it comes to contents, not all of its contents are free.[101] He says that "free" does not mean "zero cost"[102] because it is related to both contract law and copyright law. "Free" in this sense means that the internet should be a platform which is open to the

[96] *Ibid* 9 and 23
[97] *Ibid* 23
[98] *Ibid*.111
[99] *Ibid.* 111
[100] *Ibid.* 132
[101] Lessig (1999) 23 and 25
[102] *Ibid* 255

public.[103] Nonetheless, Lessig argues that less control of the layer of code or the internet protocol increases the chance of its development. This development of codes would help in controlling contents.[104] An example of controlling contents through codes lies in Digital Rights Movement (DRM) technology that uses computer codes in order to restrict access to entertainment content via the Internet to those who are authorized by payment.[105]

As is shown in Figure 2.1, Lessig mainly talks about the U.S, and does not mention the KSA. Therefore, the researcher will seek to apply Lessig's approach within the context of the KSA. Lessig emphasises that cyberspace can be governed through two different methods.[106] The first of these methods is what he calls "east coast law" or formal laws that strive to catch up with the fast development of the internet. The second is "west coast law", or codes that are more fluid than the laws themselves. By saying "east coast law", he indicates formal laws that are created by legislators in Washington, and by saying "west coast law", he indicates the companies that are located in California, specifically in Silicon Valley, which have an influence over cyberspace through codes. According to Lessig, "codes" in this latter sense mean either soft law applied to users or computer coding. For instance, digital content can be protected by codes, which DRM technology uses to restrict access.[107]

As shown in Figure 2.2, the environment for regulation has an even more complex position when it comes to the KSA because the branch of law known as *Sharia* is very old and vague, and even the more modern branch, legislation, is still struggling to catch up with cybercrime. Thus, when it comes to codes in the KSA, there is less difference between the two types outlined by Lessig. The softer codes in the KSA can be broken into two categories. The first is the actual computer coding, such as virus protection programmes and firewalls

[103] *Ibid* 58
[104] *Ibid.* 72
[105] Esanu and Uhlir (2003) 109
[106] Lessig (2006) 132
[107] *Ibid.* 116

that are controlled by the government. The second category of softer governance of cyberspace in the KSA includes the internet polices made by government institutions such as National Cybersecurity Authority (NCA)[108] that work with the Communication Service Providers (CSPs), such as Saudi Telecom Company, to monitor internet content.

Figure 2.1 Lessig's approach to the regulation of cyberspace

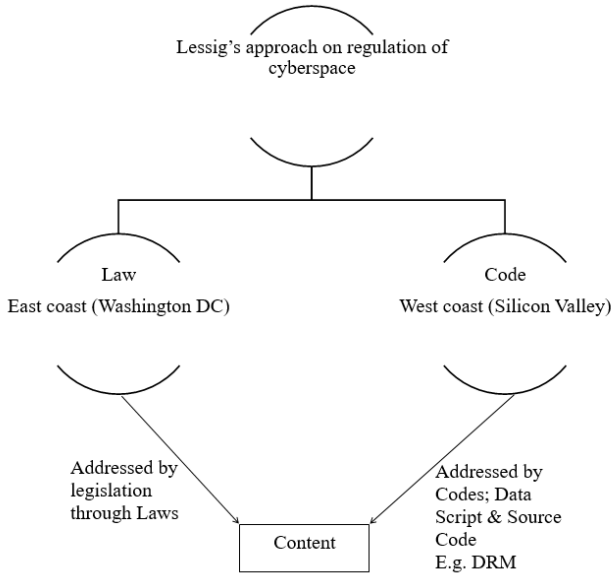
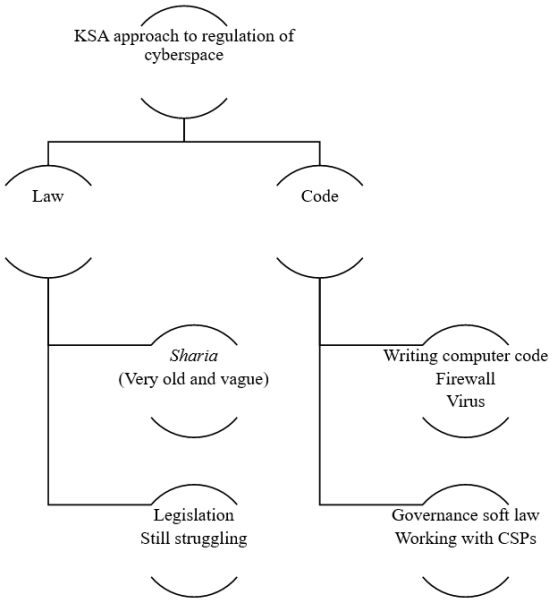


Figure 2.2 KSA's approach to the regulation of cyberspace



[108] KSA NCA <https://nca.gov.sa/en/index.html>

Lessig's analysis is criticised by some authors. Andrew Murray states that even though music industries have applied their own "code" into the music files to inhibit illegal sharing, "all attempts to use design modalities to engineer music files which could not be copied have failed."[109] This argument might indicate that Lessig's theory about code does not work in practice because of the open texture of coding.[110] Declan McCullagh criticises Lessig on his idea for a greater role for the government in enforcing the architecture of the Net, or it will suffer from "loss of sovereignty" in favour of the Net companies.[111] McCullagh says that "These are not exactly libertarian sentiments," and "Internet companies have proven to be flexible and responsible in crafting code in a way that benefits their users."[112] The dangers of the intervention of governments in internet usage can be shown by the EU proposals to seek to regulate internet content regarding terrorism[113] which resulted in the EU paper, Digital Services Act and Digital Markets Act in 2020.[114] According to critics, those proposed Acts might pay insufficient regard to effectiveness or for fundamental rights.[115] Paul M. Schwartz,[116] Roger Brownsword,[117] and Viktor Mayer-Schonberger[118] have also criticised Lessig. Schonberger says that Lessig overvalues democracy and transparency when he suggested that the "choice" is given to the person in cyberspace as a practice of freedom of speech, yet this might not be the case as people have less choice when it comes to privacy in cyberspace.[119] Moreover, Brownsword adds that, as a practice of democracy in the East Coast approach, regulators give reasons to the "regulatees" for their decisions, which is in contrast

[109] Murray (2019) 71
[110] *Ibid*
[111] McCullagh (2009)
[112] *Ibid*
[113] European Commission (2018) <https://ec.europa.eu/commission/sites/beta-political/files/soteu2018-preventing-terrorist-content-online-swd-408_en.pdf>
[114] European Commission (2021) <https://digital-strategy.ec.europa.eu/en/policies/digital-services-act-package>
[115] Broadbent (2020) 1
[116] Schwartz (2000)
[117] Brownsword (2005) 1
[118] Schonberger (2008) 713
[119] *Ibid* 728-729

to the regulators in the West Coast approach who might not share such reasoning which, it can be argued, conflicts with the principles of democracy.[120] In the same regard, Schwartz argues that in a democratic society, privacy is a value that should safeguard and shape the community, and the law should therefore intervene in order to protect privacy, especially information privacy, because it only can be protected by the law and not by codes.[121]

Clearly, the arguments of Lessig have their shortcomings, so, some other relevant works will be examined in order to enrich the present research agenda. For instance, Ian Ayres and John Braithwaite's book, *Responsive Regulation Transcending the Deregulation Debate,* explains how regulation in a late modern system can be enforced through cooperation between the state and corporations for the benefit of all stakeholders.[122] One popular idea that this book discusses is the regulatory pyramid, which puts the criminal law at the top of the pyramid and the broader techniques of governance at the bottom.[123] This model could be applied to the regulation of cybercrime in the KSA. Figure 2.3 explains how cybercrime in the KSA can be regulated in cyberspace based on the regulatory pyramid model. Firstly, on the top of the pyramid comes criminal law as the narrowest tool of regulation because it can only regulate crimes which are committed within the KSA jurisdiction effectively. Secondly, civil law comes after criminal law in the regulation of cyberspace. It is broader, but still limited. One popular example of using civil law as a tool of regulating cyberspace is contract law. Many of the internet web-sites have their own contract terms that people must agree to in order to access those web-sites.[124] Thirdly, formal regulation is a broader tool than both criminal law and civil law to regulate cyberspace because it allows or denies access to those who want to use the internet. For instance, the

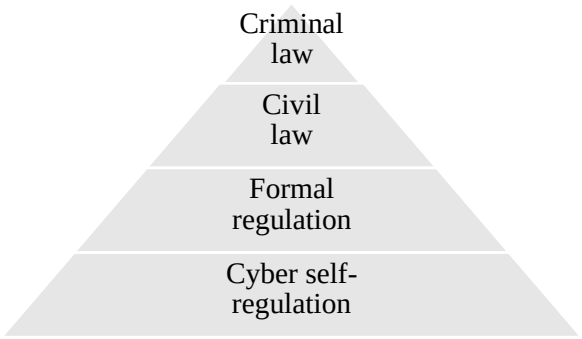
[120] Brownsword (2005) 3-4
[121] Schwartz (2000) 762
[122] Ayres and Braithwaite (1992) 35
[123] *Ibid*
[124] HRW (1999a) <https://www.hrw.org/legacy/advocacy/internet/mena/saudi.htm#TopOfPage>

firewall in the KSA denies access to pornography for people within the KSA jurisdiction.[125] In late modern jurisdiction such as the UK, pornography or "the production of sexually explicit imagery"[126] is a target for censorship or prosecution only where it involves illicit materials such as child pornography.[127] On the contrary, in the KSA, all pornographic materials are censored and accessing them might call for prosecution, as will be discussed in Chapter 7. In addition, politically sensitive material and materials contrary to Muslim or Saudi Arabian beliefs may be blocked.[128] This firewall is formal since it is controlled by the government of the KSA and will be discussed later in this Subsection. Lastly, private corporations have the most significant role in regulating cyberspace in the KSA. For instance, there may be guidelines and terms of usage applied by the Internet Service Provider (ISP) on its customers or by social media platforms. The private sector's design of hardware and software can also regulate what is allowed and not allowed. Therefore, state and private corporations must all play a role in handling cybercrimes for the benefit of all stakeholders.

The works of both Lessig and Ayers and Braithwaite are useful to the thesis and, when applied to the KSA, they help build an understanding of how the KSA's law functions in cyberspace, especially when it comes to self-regulation, as will be discussed in Chapters 4, 5, 6, and 7.

[125] HRW (1999a) <https://www.hrw.org/legacy/advocacy/internet/mena/saudi.htm#TopOfPage>
[126] Yar and Steinmetz (2019) 236
[127] *Ibid* 266
[128] See Freedom House on the KSA in 2020 <https://freedomhouse.org/country/saudi-arabia/freedom-net/2020>

Figure 2.3 Regulatory pyramid for cybercrime in the KSA



As mentioned above, no single transnational authority controls the internet.[129] Yet, the non-profit organization the ICANN controls the Internet Domain Name System (DNS).[130] In fact, ICANN "takes responsibility for several key areas of internet stability and governance."[131] Even though ICANN has authority over some aspects of the cyberspace regulation, it cannot regulate cyberspace entirely.[132] The same goes for the Internet Architecture Board (IAB),[133] which is a committee of the Internet Engineering Task Force (IETF)[134] and an advisory body of the ISOC. The IAB ensures that the internet would not be subject to any kind of localised technical codes[135] and controls the technological design of the internet.[136] Therefore, it can be said that these two organisations, along with other non-profit organisations, control the essence of the internet,[137] yet they are not sovereign authorities. For instance, ISOC is based in Virginia US,[138] and it is subject to the US law, but their regulations are not the product of the US law or the US governmental authorities.[139]

[129] Yar and Steinmetz (2019) 227
[130] See <https://www.icann.org/resources/pages/dns-2014-03-19-en>
[131] Murray (2019) 424
[132] Murray (2007) 99
[133] See <https://www.iab.org/about/iab-overview/>
[134] See <https://www.ietf.org/about/>
[135] Morgan (2016)
[136] Murray (2007) 92
[137] *Ibid* 99
[138] See <https://www.internetsociety.org/contact-us/>
[139] Murray (2007) 89-94

Furthermore, countries can impose local rules if they are prepared to severely restrict access to the internet and set up their own network.[140] China is the closest to this position.[141]

Like most countries, the KSA has made several attempts to regulate the use of the internet since it became available to the public in the late nineties. [142] The King Abdul-Aziz City for Science and Technology (KACST),[143] which is established and funded by the government of the KSA,[144] has played a major role in regulating access to the internet since they have the technology to monitor its use.[145] The KACST's mission has been to keep track of the unlawful use of the internet and to investigate cases that were referred to them by other government entities; they consequently block pornography and anti-government websites as much as possible.[146] Many Saudi people encounter the KACST because they are prevented from gaining access to specified websites by KACST, and attempts to access them causes a notification about it to appear on the computer screen, especially in the case of pornographic sites or, as it has been called by the KACST, "inappropriate information".[147] In the beginning of 2003, based on Royal Decree No. 133 dated 21/7/3, KACST shared their role with the Ministry of Communication and Information Technology (MCIT).[148] In 2006, the role monitoring the use of the internet transferred[149] to the Saudi Communication and Information Technology Commission (CITC).[150] However, even though these three government entities exercised authority over internet use, no laws were passed to govern internet use before 2007.

It would seem clear that cyberspace is intrinsically different from physical space, but the question arises is how and why cyberspace is different from other forms of

[140] Weber and Jia (2007) 772–789
[141] Karagiannopoulos (2012) 150–172
[142] HRW (1999b) <https://www.hrw.org/legacy/advocacy/internet/mena/int-mena.htm>
[143] KACST <https://www.kacst.edu.sa/eng/about/Pages/WhoWeAre.aspx>
[144] *Ibid*
[145] HRW (1999a) <https://www.hrw.org/legacy/advocacy/internet/mena/saudi.htm#TopOfPage>
[146] *Ibid*
[147] *Ibid*
[148] KSA MCIT <https://www.mcit.gov.sa/en/our-mission>
[149] See <https://internet.sa/en/internet-in-ksa/>
[150] KSA CITC. http://www.citc.gov.sa/en/AboutUs/Pages/History.aspx>

communication which are electronic (such as television and radio) in the context of the application of the legal system? There are four problems that arise from the distinctiveness of cyberspace that will be covered throughout this thesis. The first problem is the problem of complexity and the need for expertise. Cyberspace is a new area of social interaction and is based on complicated mathematical considerations that require experts to understand and subsequently work on.[151] This is not a unique problem, because humans have faced similar problems with other inventions such as the motorcar and television. However, cyberspace has a different level of complexity that causes new challenges to arise. Although people still live in the real world (physical space), they now use tools such as computers to access the virtual world (cyberspace). In the physical world, people are more easily aware of boundaries, such as those of their houses, proprieties, and countries, and consequently they know what is theirs and what is not, both physically and ethically. Besides, the physical world is easier to control and regulate. On the other hand, the virtual world knows no boundaries and is harder to regulate or control due to the massive flow of information and data across jurisdictions.[152] Comparison of television, as another instrument going beyond the physical world, might briefly be noted. Television is still very different to the internet since (1) there are limited international links because the signal does not go far and can be easily blocked, unless TV is transmitted via the internet which complicates its reach and regulation;[153] (2) it has always been subject to national licensing even in Europe and the US;[154] and (3) it has long been subject to international regulation.[155]

[151] Bandler and Merzon (2020) 27
[152] Smith (2002) 241
[153] Madiega (2019)
[154] The first such license (for radio) was the BBC (Royal Charter 1927) and users (Wireless Telegraphy Act 1923) see <https://www.bbc.com/historyofthebbc/research/royal-charter>
[155] Salomon (2008) 1

The second problem is that it involves multijurisdictional operation.[156] The Internet inevitably crosses boundaries and jurisdictions which makes it harder to regulate and control than physical space, especially when it involves sovereignty and human rights.[157] The third problem is that of private ownership and who runs the internet. A simplistic answer would be private operators do so, not sovereign states. It is apparent that internet companies and non-profit institutions run the internet in the most part, and such organisations control it, especially those that are located in the US.[158] However, this private ownership does not mean that sovereign states have no authority in this virtual space, but that their authority is limited to protect and regulate its subjects as users, rather than regulating the space.[159] The fourth problem is identity and users. The problem is that, on the internet, people can pretend to be someone, even something else, and can also easily pretend to be somewhere else. Realities and identities in the virtual world are multiple.[160] In the real world, a person generally has only one identity by which he/she is recognised, which means that it is easier to identify people in the real world than it is in the virtual world.

2.2.2 The KSA and values within cyberspace

In recent years, universities in the KSA have begun to teach cybersecurity as part of the curriculum for computer science courses,[161] which shows that the KSA is interested in becoming involved with innovation related to cyberspace and differentiating it from physical space. Yet, major universities in the KSA, such as the KSU, do not include cybercrime, cyber

[156] Katyal (2001) 1029
[157] Murray and Klang (2005) 1
[158] Murray (2007) 89-94
[159] *Ibid*
[160] Katyal (2001) 1032
[161] Alsmadi and Zarour (2018)

law, or any other aspect of the law related to them in their syllabuses,[162] a failure which indicates that the KSA's universities have an outdated approach toward cybercrime.

In contrast, the KSA seems to have arrived at a similar conclusion insofar as it relates to other late-modern phenomenon such as warfare, whereby the KSA has bought some of the most sophisticated and up-to-date weapons from late-modern states, such as the US and the UK.[163] This fortification is clearly necessary in order to go to war, or defend against invasive military attack, in the modern world because weapons from pre-modern times, such as swords and arrows, are not likely be effective when coming up against late modern weapons, such as missiles, fighter jets, drones and nuclear weapons. Moreover, the KSA benefits from late modern states' expertise on how to engage in war and uses logistical support from countries such as the US to protect its interests.[164] The same logic has been applied to attacks committed in cyberspace – or cyberwarfare and cyberattacks as they are known.[165] The KSA established the NCA in 2017 for the purpose of tackling and responding to cyberattacks,[166] equipping it with the most recent and sophisticated tools and minds to protect its interests within cyberspace.[167] Even though the KSA is categorised as a pre-modern state, it can deal with such late-modern issues, which it mostly does by importing solutions from late-modern states and benefitting from their expertise. Yet it still adopts only pre-modern tools for the criminal procedure of cybercrime. Thus, it might be said that the KSA does not prioritise the issues related to those aspects of late-modern technology, which is perhaps because officials

[162] Interviews with LP1, LP2 and LP3
[163] Smith and Brook-Holland (2021) 5
[164] *Ibid*
[165] See <https://www.gov.uk/government/statistics/uk-defence-and-security-export-statistics-for-2019/uk-defence-and-security-export-statistics-for-2019>
[166] KSA NCA <https://nca.gov.sa/en/pages/strategic.html>
[167] See <https://www.gov.uk/government/statistics/uk-defence-and-security-export-statistics-for-2019/uk-defence-and-security-export-statistics-for-2019>

perceive that it does not constitute an immediate threat to its vital security interests and there is a belief that such matters can be dealt with internally.[168]

However, similar to warlike cyberattacks, cybercrime is complex and threatening. For instance, it generates the issue of transnationality whereby power over the internet is diffused and not held within the KSA alone. As discussed in the previous subsection, one characterisation of cybercrime is that it is multijurisdictional which means that one single cybercrime might involve more than one jurisdiction. Therefore, to overcome such an issue, there is a need for international cooperation. Although international cooperation is not a focus of this thesis, it may be a factor that will eventually lead the KSA to change its approach toward the criminal procedure of cybercrime as more effective and fairer sovereignties excise international pressure on the KSA to take on key values which are thought of as fair and democratic, such as freedom of expression, as the internet can be used to support democracy[169]

Such views would lead to a cultural problem which lies at the heart of cyberspace, which is that its private controllers mainly adhere to Western liberal values, as most Internet companies such as Google[170] and Facebook (now Meta)[171] are physically located in California, one of the most liberal states within the US, which also reflects democratic values.[172] However, more recently, they are being challenged by alternative cultural and political conceptions from places such as China[173] and the EU.[174] Yet, the KSA – and more generally Arab and Islamic – values are not significantly reflected in the internet.[175] The

[168]Algarni (2012) 199-201
[169] Kahn R et al (1997) 129-151
[170] see <https://about.google/contact-google/>
[171] See <https://about.facebook.com/company-info>
[172] Schrag (2016) 11
[173] Segal (2020)
[174] See European Parliament study of 2016: <http://publications.europa.eu/resource/cellar/2e35913c-1d03-11e8-ac73-01aa75ed71a1.0001.01/DOC_1>
[175] Wheeler (2002) 2- 3

cyber-libertarian slogan, "information wants to be free",[176] reflects the Western liberal values of free expression within cyberspace. Freedom of expression as exercised in Western countries is not adopted within Muslim countries' legal systems in general, including that of the KSA.[177] Thus, Muslim countries, especially those governed by authoritarian regimes,[178] are put between the hammer and the anvil because they are not able to indoctrinate their population as they had previously been able to, and they are no longer in control of mainstream ideologies due to the access of their populations to cyberspace and the values of liberal democracies such as freedom of expression.[179] This lack of ideological control is, for the most part, due to their lack of the control of cyberspace.

Thus, the Arab Spring revolutions of 2011,[180] which ostensibly aimed to overturn dictatorships and replace them with mildly Islamised democracies,[181] came about as a consequence of the authoritarian regimes' lack of control over the minds of their youth. One major factor in the organisation of these revolutions and the dissemination of ideas was the Internet, as it facilitates the free expression of individual and collective desires.[182] This would indicate that the Internet is underpinned by Western liberal values rather than Islamic values as commonly exercised by Muslim and Arab countries. Therefore, it might be possible to say that cyberspace has contributed to liberating the social fabric of Muslim countries and, in turn, could lead to liberating their political structures, as a considerable number of individuals within Arab countries, including the KSA, have been inspired by Western liberal values such as freedom of expression and democracy. These patterns have been identified in almost all

[176] People attribute this expression to Stewart Brand (a computer expert) at conference in 1984. See Wagner (2003) Footnote 14
[177] Alhargan (2012) 133-134
[178] See discussion in 4.4.1
[179] Alhargan (2012) 127 and 133
[180] "The "Arab Spring" is what many international commentators are calling the cascading popular democracy movements that began in Tunisia, inspired Egypt, and consequently animated other movements across the region" see Howard and Hussain (2013) 1
[181] Howard and Hussain (2013) 1-20
[182] *Ibid* 2

Arab populations, and even though they have not yet been widely put into practice, they could be when the time is right. Fukuyama predicts the spread of liberal democracies as being the last socio-cultural evolution of forms of government because, as he argues, it is the fittest form of self-governance in human history.[183] Even though he was the first to criticise it himself,[184] his theory might become reality, as most humans who live under non-democratic states have touched in one way or another the practices of liberal democracies as spread in cyberspace.[185] However, it can be said that the internet alone is not enough to deliver these values. For instance, Egypt, Syria, and even Tunisia, where the idea of an Arab Spring started, have not turned into liberal democracies. Moreover, there is a dark side to cultural changes which may not be so popular or desirable, including disinformation,[186] exploitation[187] and cybercrimes.

Countries such as the KSA, whose law is built upon pre-modern traditions, have struggled to combat late modern problems like cybercrime as effectively as other countries, such as the UK, on both substantive and procedural levels. Even though the KSA passed the ACL in 2007 as a substantive response to cybercrime, that Law falls short of addressing procedural aspects. Thus, the KSA depends mainly on the CPL 2001[188] and its 2013 successor to combat cybercrime in a procedural sense. However, neither version addresses cybercrime and cyber evidence. Therefore, it is apparent that the KSA makes no distinction between the criminal procedure of cybercrime and that of NCCs.

[183] Fukuyama (1992)
[184] First criticism to his theory is related to the economic aspects and sociocultural evolution and one cannot be separated from the other in the context of evolution. See Fukuyama (1995)
[185] Howard and Hussain (2013) 1-20
[186] Schiffrin (2017) 117-126
[187] Bjola (2017) 189-191
[188] CPL 2001, Promulgated by Royal Decree No. M/39

These issues will be considered throughout different parts of this thesis. Also, they should be considered by lawmakers and legal scholars in the KSA when addressing the issue of cybercrime, in order to ensure that the law is effective.

2.3 Legal problems in the KSA's legal system regarding cybercrime

The KSA's legal system is mainly founded on *Sharia,*[189] which makes it difficult to categorise the nature of the KSA legal system, as being either adversarial or inquisitorial.[190] Thus, it can be said that it is a combination of the two, whilst being supervised by *Sharia,*[191] because it allows criminal courts to reinvestigate all crimes including cybercrime,[192] as will be discussed in Chapter 7. Yet, it might be possible to say that the KSA leans towards being inquisitorial due to the Egyptian influence that itself was influenced by France,[193] but no single system is formally adopted. Even though the KSA's legal system consists of formal (legislation) and informal sources (*Sharia*), the informal sources override aspects of both the formal legal system of the KSA and many aspects of inquisitorial or adversarial doctrinal approaches.

A key question is whether or not the cybercrime agenda is affected by the prioritisation of *Sharia* or whether other factors are holding back its necessary development. Concerns have been raised over the ability of the *Sharia* to allow for policies that can address cybercrime.[194] For instance, scholars such as Algarni have raised concerns over the ability of *Sharia* to allow for policies that can address cybercrime because it allows judges to employ *Ijtihad* in their verdict.[195]

[189] Vogel (2000) 3
[190] Baderin (2006) 241-284
[191] Esmaeli (2009) 12
[192] Reichel (2018) 130
[193] Hanson (1987) 272-291
[194] Colarik (2006) 33-53
[195] Algarni (2010) 8

Ijtihad can be defined as the use of *Fiqh* (jurisprudence) by the *Ulama* (Islamic scholars) in interpreting the Islamic texts such as the *Quran* and *Sunnah* (Prophet Mohammed's traditions).[196] There are two main eras of *Ijtihad*.[197] The first is the classical period which is the period immediately after the Prophet Mohammed's death and lasted around 250 years.[198] In this era, the main parameters of *Sharia* were rooted based on *Fiqh* by the *Ulama*.[199] This has led to mistrust and questions regarding the ability of Islamic governments to legislate and stand on their own in creating laws that are not based on *Sharia*.[200] The second era of *Ijtihad* is contemporary *ijtihad* which is the period after the classical period which stretches up to the current era and which reshapes the formulation of classical *Ijtihad* to "reflect contemporary political, legal, and economic realities."[201] For this reason, the judicial branch in the KSA relies on contemporary *Ijtihad* in the main.

The KSA is the only Muslim country that states in its constitution, which mainly resides in its Basic Law of Governance (BLG) 1992,[202] that the *Quran* and *Sunnah* form the base of its constitution.[203] That makes the constitution of the KSA vulnerable to falling behind technological innovation, especially when Article 38 states that no crimes or penalty can exist except in accordance with texts inspired by *Sharia* or the legislator.[204] That sounds like a clear direction, but many judges and prosecutors rely on their own perspectives of *Sharia* and enforce them as unwritten law under the umbrella of *Ijtihad*, [205] with no regard to Article 38.

[196] Khan & Ramadan (2011) 1-2.
[197] *Ibid*
[198] *Ibid*14
[199] *Ibid* 14-15
[200] *Ibid* 35
[201] *Ibid* 126
[202] BLG was promulgated by the Royal Decree No. A/90 1992
[203] *Ibid* Article 1
[204] *Ibid* Article 38.
[205] Vogel (2000) 3

Ijtihad operates with the approval of the government.[206] The reason why the government approves this doctrine is, as previously mentioned, that the constitution of the KSA is based on the *Quran* and *Sunnah*, which allows *Ijtihad*.[207] By comparison, other Muslim countries that have written constitutions mention that *Sharia* is only one of the primary sources of legislation, but not the dominant one.[208] This kind of flexibility does not apply in the KSA due to the restrictions that *Sharia* puts upon legislators who are obligated to devise laws that are based on the *Sharia*.[209] Even when legislators pass a law that adheres to the Islamic principles, say the ACL of 2007, it is vulnerable to being disregarded by judges, as will be addressed in Chapter 7 because it is seen as un-Islamic, based on Article 46 of BLG. This Article states that the Judiciary shall be an independent authority, and there shall be no power over judges in their judicial function other than the *Sharia* itself.[210] Therefore, even though the ACL came into force in 2007, judges still make their own disparate rulings that are inspired by *Sharia*[211] and that discretion may negatively affect the handling of cybercrime.

2.3.1 The role of *Sharia* and complexity of cybercrime within the KSA jurisdiction

As already noted, *Sharia* is the primary legal code in the KSA,[212] and it influences civil and criminal law in the KSA.[213] This point is stated in the BLG of the KSA in Article 1:

> "The kingdom of Saudi Arabia is a sovereign Arab Islamic state. Its religion is Islam, and its constitution is the Holy *Quran* and the Prophet's (peace be

[206] *Ibid*
[207] *Ibid*
[208] See UAE Constitution 1996 art.7
[209] Shalhoob (1999) 10
[210] BLG Article 46
[211] This will be covered in chapter 7
[212] Vogel (2000) 3
[213] Shalhoob (1999) 10

upon him) *Sunnah* (traditions). Its language is the Arabic language, and its capital city is Riyadh."[214]

Moreover, Article 7 emphasises that *Quran* and *Sunnah* are the primary sources of legislation and no law can conflict with or contradict them.[215] This shows that the main principles of Islam are the dominant authority over Saudi legislature, including that related to criminal law and criminal procedure. Although *Sharia* continues to evolve with time, most of the provisions that are still in use date from the 7th and 10th Centuries of the Gregorian calendar.[216] There have been some attempts to codify these rules,[217] but these attempts are not comprehensive.[218] This makes it rather difficult to determine the rules of *Sharia*, and so an individual has to interpret complex texts written by jurists. One major criticism of *Sharia* is its inability to evolve and accommodate the changing global situation,[219] such as how to deal with cybercrime.

According to Maghaireh, computer security currently represents a growing concern for Saudi society.[220] The general provisions of the *Sharia* are to protect the five indispensables in Islam: life, religion, intellect, property, and offspring.[221] Its precepts are thus very broad but also rather indistinct and subject to many variant interpretations, especially when dealing with a new phenomenon such as cyberspace.[222]

It is posited in this thesis that the KSA law requires more detailed technical and internationally acceptable solutions for dealing with cybercrimes than available by reliance on *Sharia* alone or as a dominant consideration. It is further argued that the lack of effective private and public policing and forensic facilities for investigation of cybercrimes compounds

[214] BLG Article 1
[215] *Ibid* Article 7
[216] Bassiouni (2012)
[217] Zada and Zada (2016) 163
[218] *Ibid*
[219] Colarik (2006) 33-53
[220] Maghaireh (2008) 337-345
[221] *Ibid* 341
[222] *Ibid*

the ineffectiveness of the KSA's implementation of *Sharia* in dealing with cybercrime, as will be discussed in Chapters 5 and 6.

Amongst ideas for reform, Ala`ali proposes that all computer crime laws in Muslim majority countries, including the KSA, should be developed further to protect the people in those countries.[223] Ala`ali underscores that the new update should respect individuals' privacy by ensuring that access to personal information is controlled.[224] Moreover, trust should be maintained as suggested by the *Quran*.[225] Similarly, theft of material things and personal information should be punished as specified by the *Quran* and *Sunnah.*[226] For instance, it is been suggested that in order to criminalise any action that happens in cyberspace, lawmakers should look into the equivalent to such criminalised action in the primary sources of *Sharia* (*Quran* and *Sunnah*) in order to link to crimes such as theft[227] and internet fraud.[228] Consequently, the criminalisation of acquiring private data without permission should be based on comparing that action with theft which is been criminalised in the *Quran* and *Sunnah*.[229] Additionally, the notion of promise emphasises the need to eliminate unauthorised access to any information.[230] All the laws must be based on all these aspects to protect people living in Muslim majority countries, including the KSA.[231] Thus, Ala'ali focuses on how the law should operate in accordance to *Sharia* principles, but seeks to draw out more specific rules that are derived directly from *Quran* and *Sunnah*, such as the prohibition of accessing houses without permission and prohibition of espionage.[232] He posits that even though these rules are for physical space, they could be applicable to cyberspace as

[223] Ala'ali (2007) 1-12
[224] *Ibid 9*
[225] *Ibid* 8-9
[226] *Ibid* 9.
[227] *Ibid* 5-7 and 9
[228] Algarni (2010) 1-2
[229] *Ibid* 3
[230] Ala'li (2007) 9
[231] *Ibid 10*
[232] *Ibid* 5-9

there is a clear similarity.[233] However, his proposal seems unlikely to lead to reform as he claims, because his position is already very similar to the KSA's approach to cybercrime in general.

This approach is based on the fact that the KSA legal system depends on the general principles of *Sharia*. However, *Sharia* does not directly or specifically address cybercrime and cyberspace. Therefore, the KSA's legal scholars should note that the rules of cyberspace must be distinct from the rules of physical space because the nature of both spaces is different.[234] Therefore, it may be possible to say that, if they noted the differences between the two, they would direct the KSA toward a more effective and fairer approach to the criminal procedure of cybercrime.

2.3.2 The problem of judicial personnel

Another issue affecting the effectiveness and fairness of the treatment of cyberspace in the KSA is the quality of judicial personnel. Even though the judicial personnel or other public law enforcement personnel are trained to deal with traditional crimes, they lack the relevant knowledge and training to deal with cybercrimes, as will be thoroughly addressed throughout Chapters 6 and 7. Other officials who are supposed to deliver and ensure justice, such as police and prosecutors, also suffer from a relative ignorance of cybercrime.[235] It may be said that developed countries such as the UK suffer from the same issue.[236] However, unlike the KSA, the UK deals with those issues more professionally, seriously, efficiently, and fairly, as will be addressed in Chapter 4.

[233] *Ibid* 6
[234] Alanazi et al (2018) 7
[235] Hakmeh (2018) 10
[236] Walden (2007) 205

2.3.3 The problem of codification

Another reason why cybercrime constitutes a problem in the KSA is that there is no penal code in the KSA.[237] Even though there are many legislative provisions about crimes, they are limited and sometimes inconsistent. For instance, the ACL does not talk about the dismissal of public employees who commit a relevant crime whereas other criminal laws punish public employees by firing them from their public office if they commit one of the listed crimes. However, in some cases, public employees who commit some of the crimes listed in the ACL have been fired, even though this punishment is not listed in the law. This problem and others arise because the KSA has no comprehensive criminal code, as will be discussed in Chapter 4. Therefore, there are often disputes between judicial decisions, the written scholarly sources (*Ulama*) and the legislation.[238]

Yet, codification does not alone determine the ability of the country's legal system to deliver justice and prevent its citizens' rights from being violated.[239] For instance, the UK, which is a common law country, also does not have a criminal code, but its criminal law is made accessible and available to the ordinary person.[240] For example, the website, www.legislation.gov.uk,[241] which contains almost all UK legislation, is available for everyone whether or not they are UK citizens. More importantly, the website provides explanatory notes for legislation which help to make the UK law more accessible. However, in the KSA, the criminal code is not accessible to the ordinary person,[242] either in terms of mechanical accessibility or in terms of its substantive meaning. The criminal code of the KSA is also not so accessible because, during enactment, legislation is not discussed with, or

[237] Alathli (2015) 9
[238] Chapter 7 will address this issue when discussing cybercrime cases
[239] Walden (2007) 205
[240] *Ibid* 42-43 & 395
[241] UK GOV <http://www.legislation.gov.uk/>
[242] Interviews with LP2 and CL1

explained to, the public. Even though the KSA's Shura Council and Council of Ministers discuss such laws, their sessions are not public, and, by law, deliberations are kept secret.[243]

2.4 The values of effectiveness and fairness

In this section, the values of effectiveness and fairness will be addressed in order to further analyse the ability of the KSA's criminal law of process to tackle cybercrime. The values in each concept will be defined in three senses: their conceptual meaning, their comparative and international meaning, and their national meaning. Later, a link between the two different concepts will be discussed in order to indicate that even though effectiveness and fairness are from different spectrums, they interact with each other in relation to their impact on law and policy.[244]

2.4.1 The meanings of effectiveness

To fully test the effectiveness of the KSA criminal process law regarding cybercrime and to pursue the objectives of this research, one should have a comprehensive understanding of the word "effectiveness" in order to accurately evaluate the ability of the KSA's procedural law to tackle cybercrime. The meanings of this word will be referred to in later chapters when analysing the KSA law, particularly when answering one of the research questions in Chapters 4, 5, 6 and 7 about whether the KSA law criminal process regarding cybercrime is effective. Therefore, as has been discussed, three aspects of effectiveness will be defined respectively.

[243] See Council of Ministers Law 1993 (Promulgated by Royal Decree 13/A 1993) Article 16
[244] Beetham (1991)

2.4.1.1 The conceptual meaning of effectiveness

In order to test the effectiveness of the KSA's law of criminal procedure regarding cybercrime, three points need to be considered regarding the meanings of the word "effectiveness". The first important aspect of effectiveness is the conceptual meaning of the word. Generally, effectiveness means "the degree to which something is successful in producing a desired result; success."[245] In accordance with this definition, it is possible to say that the first step to test whether the KSA's cyber laws are effective is it to look at their success in tackling cybercrimes from a procedural perspective.

However, what is more pertinent to this study is the meaning of effectiveness in a legal sense. Xanthaki asserts that "effectiveness is defined as the capacity of the legislative text to contribute to regulatory efficacy."[246] In addition, Blanc clarifies that "effective regulation can be understood as regulations and a regulatory system that achieve their objectives."[247] There are three elements that help in making the law effective; clarity, precision, and unambiguity regarding objectives, context, results and the content of the law.[248] These elements constitute an instrument which can be used to test whether the law is effective, and they could be applied on any stage of the process of making laws.[249] Therefore, if the law lacks any of these elements in terms of objectives, content, context and results of the law,[250] it is likely to be ineffective.

[245] Oxford Dictionaries <https://en.oxforddictionaries.com/definition/effectiveness>
[246] Xanthaki (2018) 433
[247] Blanc (2018) 465
[248] Xanthaki (2018) 434
[249] *Ibid*
[250] Mousmouti (2018) 445

2.4.1.2 The comparative meaning of effectiveness

Another way to assess the meaning of effectiveness in the field of cyberspace is to compare effectiveness in the KSA law with that of other jurisdictions. In the UK, John Stuart Mill's[251] utilitarianism theory posits one meaning of effectiveness that can be applied to the UK's legal provisions, particularly its cybercrime process laws. In brief, utilitarianism is about ensuring and achieving the greatest level of happiness for the greatest number of people possible.[252] Therefore, the state is neutral and does not intervene in people's choices that do not harm others,[253] but rather the state provides facilities, such as the internet, to ensure its citizens have a good life. Therefore, unlike the *Sharia*, it can be said that a utilitarian approach to law is not concerned with tempering immorality and applying moral codes that encourage people to approach life with probity and consciousness of the Divine.

The UK has a more efficient and successful approach to cybercrime than the KSA as it provides more sophisticated and extensive models.[254] It is considered to be a leader in dealing with cyberspace and cybercrime, having many strategic polices and detailed laws. The UK's policymakers decided that they were in need of legislation to criminalise some actions that happen on the internet ever since 1984 when Stephan Gold and his associate Robert Schifreen unlawfully accessed BT Prestel's computer.[255] There was no direct law that criminalised such an action and, therefore, the UK had to respond to the unauthorised access to the computer by attempting to criminalise it indirectly, resulting in failure.[256] In *R v Gold and Shifreen*,[257] it was decided to charge the accused pair under Section 1 of the Forgery and Counterfeiting Act 1981, with defrauding BT by manufacturing a "false instrument," namely

[251] See <https://plato.stanford.edu/archives/spr2017/entries/mill/>
[252] Mill (2009 copy) 2
[253] *Ibid* 8
[254] Long et al (2011) Vol 2
[255] Murray (2019) 357
[256] *Ibid* 360
[257] *R v Gold and Shifreen* [1988] 1 AC 1063

the internal condition of BT's equipment after it had processed Gold's eavesdropped password.[258] They were convicted on specimen charges, and they appealed to the Court of Appeal.[259] Their counsel cited the lack of evidence showing the two had attempted to obtain material gain from their exploits, and claimed the Forgery and Counterfeiting Act had been misapplied to their conduct. Thus, they were acquitted, and the prosecution appealed to the House of Lords.[260] However, the Lords upheld the acquittal.[261] Lord Brandon said:

> "We have accordingly come to the conclusion that the language of the Act was not intended to apply to the situation which was shown to exist in this case. The submissions at the close of the prosecution case should have succeeded. It is a conclusion which we reach without regret. The Procrustean attempt to force these facts into the language of an Act not designed to fit them produced grave difficulties for both judge and jury which we would not wish to see repeated. The appellants' conduct amounted in essence, as already stated, to dishonestly gaining access to the relevant Prestel data bank by a trick. That is not a criminal offence. If it is thought desirable to make it so, that is a matter for the legislature rather than the courts."[262]

It follows that one major response to cybercrime in the UK has been legislative in nature and is comprised of laws such as the Computer Misuse Act 1990,[263] Electronic Communication Act 2000,[264] Regulation of Investigatory Powers Act 2000,[265] Investigatory Powers Act 2016 (IPA)[266] and Digital Economy Act 2017[267] and the ratification of the provisions of the Convention on Cybercrime 2001. Even though the Computer Misuse Act

[258] *Ibid*
[259] Murray (2019) 357-360
[260] *Ibid*
[261] *Ibid*
[262] R v Gold and Shifreen [1988] 1 AC 1063
[263] UK Computer Misuse Act 1990
[264] UK Electronic Communication Act 2000
[265] UK Regulation of Investigatory Powers Act 2000
[266] UK Investigatory Powers Act 2016
[267] UK Digital Economy Act 2017

1990 comprehensively covers aspects of computer crimes, it has been criticised for its limitations, particularly because it has not kept up which rapid technological variables.[268] The second type of response is institutional and includes the establishment of specialist units in the National Crime Agency (NCA),[269] the Government Communications Headquarters (GCHQ)[270] and the National Cyber Security Centre (NCSC)[271] that monitor the internet and conduct investigation not just for cybercrime, but also for the purposes of national security threats.[272] More relevant to this thesis, the UK law of process regarding cybercrime is constantly evolving, dealing with cybercrime as having its own special features[273] which are distinct from traditional forms of crime. Walden notes that, in the UK, "the process of law reform has been considerably more vigorous and comprehensive in respect of criminal procedure than the area of substantive offences."[274] The meaning of effectiveness as understood within the context of the UK and its effective approach to the criminal process of cybercrime will be used as an instrument of analysis in Chapters 4 to 7 to test whether the KSA has an effective approach to the matter. Perhaps *Sharia* can also be described as Procrustean[275] too as it applies premodern tradition on late modern phenomena.

2.4.1.3 The national meaning of effectiveness

The third aspect of the meaning of effectiveness looks towards the KSA's law. The current approach of KSA law to the criminal procedure of cybercrime can be considered as being unsuccessful when compared to the UK due to the complexities of the KSA's criminal

[268] UK Home Office (2021) <https://www.gov.uk/government/consultations/computer-misuse-act-1990-call-for-information>
[269] UK NCA <http://www.nationalcrimeagency.gov.uk/about-us>
[270] UK GCHQ <https://www.gchq.gov.uk/what-we-do>
[271] UK NCSC
[272] *Ibid*
[273] UK National Cyber Security Strategy 2016-2021. 13
[274] Walden (2007) 48
[275] Lord Brandon refers to the classical myth of Procrustes, who would stretch his victims to fit a bed for which they were not suited for. See Graves (2017)

justice system that relies mainly on *Ijtihad* to interpret of *Sharia*.[276] As will be discussed in Chapter 4, the KSA claims that the constitution of the KSA is *Quran* and *Sunnah*[277] which are the main sources of *Sharia* and cybercrime and, therefore, its related laws of process are modern issues which the *Sharia* does not discuss explicitly. In the KSA, legislation must be compatible with *Sharia;* otherwise, it will not be passed.[278]

The measurements for effectiveness of the law in the KSA can be found in the BLG. In order for the legislation to be effective, it must comply with the principles of *Sharia,* especially the provisions in the *Quran* and *Sunnah*.[279] Measurements for effectiveness can be found in the *Quran* and *Sunnah* which Muslims are commanded to follow.[280] Therefore, it can be said that any legislation that opposes *Sharia* in the KSA could be seen as ineffective, and judges can decline to apply it.[281] However, the question arises as to whether or not the *Sharia* is itself effective. There is a tendency among people to defend their beliefs, whether or not they are religious in nature.[282] However, analysis of the legal effectiveness of *Sharia* cannot be based on personal belief; rather it should be based on the capability of the *Sharia* to contribute to delivering just and effective legislation. From the perspective of a country whose legal system has elements which contradict the *Sharia,* such as the UK, it is not likely that the *Sharia* will be seen as being effective in terms of its legal provisions, because it could conflict with the essence of democracy and individual rights.[283]

Even in the KSA, a country whose legal system is entirely dependent upon *Sharia,* the current applications of *Sharia* have been shown to be partially ineffective, especially when

[276] Vogel (2000) 3
[277] BLG Article 1
[278] Shalhoob (1999) 17
[279] BLG Articles 1 and 7
[280] Udah (2009) 19
[281] BLG Article 46
[282] Hoffer (2002 copy)
[283] Udah (2009) 24 and 25

they contradict the basic human rights that the KSA claims to protect in its constitution.[284] Also, the false application of *Sharia* and the passing of inefficient legislation under the name of *Sharia* (where *Sharia* has no relation to the subject matter)[285] increase the criticism regarding the *Sharia's* ability to regulate. An example of the false applications of *Sharia* in the KSA can be seen in the provision of Article 3 of the CPL 2013 which was recently abolished because it was deemed incompatible with *Sharia* and the fundamental human rights which apply to those who are being accused of crime.[286] This rule was passed after having been assessed as being compatible with the *Sharia,* however, the *Sharia* doctrine has nothing to do with this in practice. This example, along with other similar examples, will be addressed in Chapters 4 to 7 when testing the effectiveness of the KSA's law of criminal process with regard to cybercrime based on the national measurement.

2.4.2 Meanings of fairness

In order to pursue the research objectives further, fairness will be assessed in a similar manner to the way that effectiveness was above. This thesis measures the fairness of the country's criminal process regarding cybercrime and, in order to do so, three levels will be outlined in order to explain the concept.

2.4.2.1 The conceptual meaning of fairness

The first point is the abstract concept of fairness. A dictionary meaning of fairness is the "impartial and just treatment or behaviour without favouritisms or discrimination."[287] This definition could be applied to the legal aspect of the word. Therefore, for the law to be

[284] BLG Article 26
[285] Almibrad et al (2015) 2
[286] SPA (2019)
[287] Oxford Dictionaries <https://en.oxforddictionaries.com/definition/fairness>

fair, it must be just by not discriminating and not favouring any person over another.[288] In other words, the law must treat those who are subject to it with equity and equality.[289] Thomas Frank sees fairness in the law as being twofold; first it must be just in the eyes of a community by using the proper process to reaching fair decisions (procedural fairness), and second it must be just in the eyes of a community by reaching fair results (substantive fairness).[290] This dual meaning of fairness will be chosen for further analysis in the next chapters, especially in regard to procedural fairness, which complements the overall focus of the thesis. Moreover, Mill's harm principle[291] will be added to the measurement of conceptual fairness and applied to the legitimacy of official instruments. Since this thesis is limited to the criminal procedure of cybercrime, only a brief introduction to Mill's harm principle will be given here. Thus, it can be said that generally Mill's harm principle is to restrict people, "individually or collectively [authority]"[292], to cause harm to others unless it is for the rightful purpose which is self-protection.[293] Therefore, the test for conceptual fairness test will include this test for whether the means adopted in the criminal process of cybercrime are legitimate.

2.4.2.2 The comparative meaning of fairness

The conceptual meaning leads to the second point which is the meaning of fairness in international law which is, nowadays, mainly located in the precept that basic human rights must be protected.[294] Therefore, it is possible to say that major international human rights treaties address procedural fairness, and they take their enforcement from the international

[288] Hart (1994) 162
[289] *Ibid* 191
[290] Franck (1995) 6–9 and 47
[291] Mill (2017 copy)
[292] Mill (2003 copy) 94
[293] *Ibid*
[294] Chayes and Chayes (2007) 77-84

norm *pacta sunt servanda* (treaties are to be obeyed).[295] All major human rights are found in the ICCPR and UDHR.[296] For instance, in regard to criminal law and criminal procedure, both Article 6 of the ICCPR[297] and Article 5 of the UDHR[298] forbid any cruel or unusual punishment. Moreover, Article 10 of the UDHR protects the basic human rights in having a fair trial,[299] and Articles 9 and 11 of UDHR draw up the main principles of criminal procedure which signatory countries must not violate.[300] Similarly, the ICCPR secures basic human rights.[301] In regard to the criminal provisions, Articles 9 and 14 of the ICCPR illustrate the main principles of criminal procedure that member states must follow.[302] With regard to Article 5 of the UDHR and Article 6 of the ICCPR, the KSA has not applied the death penalty for any cybercrime. But does that mean the KSA law is fair with regard to all the general principles of fairness in International Law? The apparent answer is "no".[303] Within criminal process, it can be said that, with regards to the discussed Articles within international human rights law, the international concept of due process comprises four main principles which are: the right for the accused to be presumed innocent until proven otherwise, the right for an attorney or legal representation, the right for knowing the reason of detention, and the right for a unbiased and open trial.[304] Another question arises in regard to the fairness of the KSA law which is whether those principles of due process can be found in *Sharia*, as discussed next. These questions will be answered throughout Chapters 4 to 7 when testing the fairness of the KSA's approach to the criminal process of cybercrime.

[295] *Ibid* 75
[296] Henkin (1990)
[297] ICCPR Article 6
[298] UDHR Article 5
[299] *Ibid* Article 10
[300] *Ibid* Articles 9 and 11
[301] ICCPR Article 5
[302] *Ibid* Articles 9 and 14
[303] See Universal Periodic Reports from the UN and UNESCO reports <https://en.unesco.org/countries/saudi-arabia>
[304] Trechsel & Summers (2005) 81, 153, 192 and 242

2.4.2.3 The national meaning of fairness

The third point is the meaning of fairness in the KSA's law of criminal process regarding cybercrime. Its BLG specifies the principles of fairness in general and fairness in the criminal procedure in particular. Article 7 indicates that for any legislation to be fair, it must follow *Quran* and *Sunnah*.[305] Therefore, the KSA is obligated to protect basic human rights as long they do not conflict with the *Sharia*.[306] In terms of the main principles of fairness regarding criminal procedure, Article 36 prohibits unlawful detention, Article 37 prohibits unlawful search and seizure and Article 38 prohibits unlawful punishment.[307] Additionally, Article 54 underlines the role of the independent Public Prosecution.[308] These principles of fairness are applied generally to the criminal process in the KSA, and it deals with cybercrime in the same way it deals with traditional crimes. Even though there is mutual ground between KSA law and international law in regard to human rights within the law of criminal process (due process), such as the right for fair trial, the right for an attorney, the right to know the reason of detention and the right for an unbiased judge, the KSA's laws are nevertheless incompatible with many of the basic human rights in this regard – not just because the law itself, but also because, on many occasions, the application of these aspects of the law have been compromised.[309] For instance, in 2017 and 2018 the authorities conducted arbitrary arrests and detentions for multiple suspects without charging them or fairly trying them, resulting in multiple violations of basic human rights.[310] Even though, Article 26 of the KSA BLG states that the KSA protects human rights, it is possible to say that the KSA law of criminal process has failed to deliver a just system in practice. All of

[305] BLG Article 7
[306] *Ibid* Article 26
[307] *Ibid* Articles 36, 37, 38
[308] *Ibid* Article 54
[309] US Department of State, 9-15 <https://www.state.gov/documents/organization/277507.pdf>
[310] Amnesty International, Saudi Arabia 2017-2018 <https://www.amnesty.org/en/countries/middle-east-and-north-africa/saudi-arabia/report-saudi-arabia/>

these measures will be used as instruments of analysis for testing whether the KSA's cyber process law is fair and effective in detail in Chapters 4, 5, 6, and 7.

2.4.3 Linking fairness with effectiveness.

As has been shown earlier, effectiveness is different from fairness, but the question which arises from such differentiation is whether there is any link between the two of them. It is possible to link effectiveness with fairness through the notion of legitimacy, which is "the property that a regime's procedures for making and enforcing laws are acceptable to its subjects."[311] According to Beetham, legitimacy is an ongoing process that gives authority and power to the law as has been accepted by people (both subordinate and dominant), especially in securing rights for the subordinates.[312] Therefore, it could be said that "when power is acquired and exercised according to justifiable roles, and with evidence of consent, we call it rightful or legitimate."[313]

Both effectiveness and fairness each play an essential role in legitimatising the law.[314] Effectiveness is ultimately about the achievement of objectives, and it tends to be policy orientated and measure whether the policy objectives have been achieved;[315] fairness considers the acceptability of policy goals or outcomes or the processes by which they are secured and how they affect people.[316] Therefore, it could be said that fairness is a people-orientated measurement.

However, both effectiveness and fairness could work in conjunction to legitimatise the law.[317] According to Dworkin, fairness should apply over and above effectiveness

[311] Brown et al (2018)
[312] Beetham (1991) 6, 98 and 103
[313] *Ibid* 3
[314] *Ibid*
[315] Blanc (2018) 465
[316] Lloyd (1981 copy) 117-120
[317] Beetham (1991)

because the objectives that effectiveness seeks to achieve must be fair.[318] In other words, fundamental human rights override or "trump" any law or political decision that conflicts with them.[319]

In the KSA all legislation must be combatable with the *Sharia,* and any legislation that contradicts the *Sharia* will be abolished.[320] Therefore, with regard to Dworkin's notion, it is possible to say that *Sharia* is the KSA's trump card, which, as discussed earlier is significantly different from international notions of fairness.

2.5 Political and social changes in the KSA and Vision 2030

Because the legal system in the KSA is based on the teachings of Islam,[321] it is posited that the origins and rigidity of *Sharia* limit the potential of the KSA to handle issues of late modernity[322] such as cybercrime. The KSA can be categorised as a pre-modern state because it still relies ultimately and profoundly on a religion and its enforcement through the personal authority of the Royal Family.[323] Therefore, it can be said that the KSA is categorised as a premodern state because Islam has affected the KSA in many aspects of life including the legal system, and also because it has a political and cultural system which relies on personal authority and kinship,[324] rather than developed bureaucracies and universal social development, citizenship and emancipation.[325] Giddens explains that even though religion is one of the main parameters of pre-modernity or pre-modern society, it provides security among believers.[326] The society of the KSA is not an industrial society but remains closely

[318] Dworkin (1977) 191-200
[319] *Ibid*
[320] Alroways and Alrayees (2019) 92
[321] *Ibid* 89-90
[322] Yazbeck et al (2004) 4
[323] *Ibid* 4
[324] *Ibid*167
[325] Kaminski (2013) 1–10
[326] Giddens (1990) 103

linked to religion as an organising foundation.[327] However, it can be said that the KSA is moving toward modernity through *Vision 2030* which is a strategic transition plan that the Crown Prince Mohammed Bin Salman announced in 2016 and which began to be implemented from 2017.[328] Giddens says that "we live in a period of evident transition; 'we' here refers not only to the West but to the world as whole."[329] One element of the *Vision 2030* is to anticipate the danger of depending only on oil as the main resource of the country.[330] The *Vision 2030* comes up with solutions for not relying solely on oil and increasing national income by investing money internationally, establishing other industries such as solar energy.[331] These plans and others besides are risky. O'Malley mentions that:

> "Uncertainty, then, is to be the fluid art of the possible. It involves techniques of flexibility and adaptability, requires a certain kind of 'vision' that may be thought of as intuition but is nevertheless capable of being explicated at great length in terms such as 'anticipatory government' and 'governing with foresight'."[332]

Therefore, it can be argued that uncertainty is one inevitable aspect of the risk society,[333] and, if the KSA is on its way to becoming a late modern society and MBS's vision achieves its aims, the KSA should more actively deal with the risks of late modernity, including cybercrime. The transition to a late modern society must be reflexive.[334] Reflexive modernisation is to transit from an industrial society to a risk society;[335] this societal transition is, more likely than not, inevitable and is not something which comes about

[327] Yazbeck et al (2004) 43
[328] *Vision 2030* <http://vision2030.gov.sa/en>
[329] Beck et al (1994) 56
[330] *Vision 2030* <http://vision2030.gov.sa/en>
[331] *Ibid*
[332] O'Malley (2004) 5
[333] *Ibid*
[334] Lash et al (1996) 28
[335] *Ibid*

through choice, whether that transition is constructive or destructive overall.[336] Therefore it is better for the KSA to direct this coming transition to ensure it is constructive as it is beneficial to society. At the same time, it will have to handle expressly the new risks created by late modern society.

Even though the KSA is transforming into what seems a more progressive modern version of itself, it must take into its consideration that, historically, these types of transformations have caused conflict and risk that resulted from a variety of factors, including reflexive modernisation.[337] For instance, in 1989, the world witnessed the collapse of communism in Europe.[338] This collapse led Western Europe to rethink their success in modernising their own industrial society.[339] Beck states that "reflexive modernisation means the possibility of a creative self-destruction for an entire epoch that of industrial society. The subject of this creative destruction is not the revolution, not the crisis, but the victory of Western modernization."[340] Reflexive modernisation dis-embeds and then re-embeds social norms, leading to another aspect of modernity, or what Beck calls "a modernisation of modernisation" that is needed for the sustainability of society.[341]

However, the KSA's existing culture is, on the most part, based on traditional, pre-modern norms. As a result, for the KSA to become a late modern state, it must loosen those traditions that hold it back from societal change,[342] many of which are deeply honoured, as modernity itself has "always stood in opposition to tradition".[343] Since the beginning of 2005, there has been some social shifts throughout Saudi society.[344] One reason is that access to the

[336] Beck et al (1994) 6
[337] *Ibid* 1
[338] *Ibid* 1
[339] *Ibid* 1
[340] *Ibid* 2
[341] *Ibid 2-5*
[342] Giddens (1990) 37
[343] *Ibid* 56
[344] Alhussein (2019) 4

internet has become widespread, opening the society up to the world.[345] The internet is not the only factor to have this effect; travel, TV channels and overseas educational study have also influenced Saudi citizens. By the beginning of 2018, there were almost two hundred thousand Saudi citizens who were awarded a full scholarship by the KSA government for the purpose of studying abroad.[346]

Consequently, these changes have led to the erosion of various elements of what were seen as being the essence of its culture, such as a women's constrained role in Saudi society.[347] Women in the KSA were deprived of many privileges, but since King Salman came to the throne, women have been given access to greater freedoms.[348] For instance, in 24 July 2018, he allowed women to drive cars.[349] Part of the KSA *Vision 2030* vision is to enhance women's role in society.[350] For example, not very long ago, Saudi women were unlikely to hold position in government entities.[351] However, there are currently many women who hold high position in Saudi government.[352] For instance, the *Al Shura* Council, which is the second house of legislation in the KSA, used to be formed entirely of male citizens, but in recent years women have been able to participate in the decision making process.[353] Also, women had not previously been allowed to practice law, but in 2013 they have been given the permission to do so by an executive order from the Minster of Justice.[354] Moreover, it could be argued that even though the KSA has granted certain privileges to its female citizens, their basic human rights must be granted and secured along with such privileges. According to the Human Right Watch (HRW), male guardianship over adult

[345] See <https://www.internetsociety.org/contact-us/>
[346] Alshaikhi (2017).
[347] Ahmed and Elmulthum (2016) 42716-42726
[348] *Ibid*
[349] Damanhouri (2018)
[350] Ahmed and Elmulthum (2016) 42716-42726
[351] *Ibid*
[352] *Ibid*
[353] Radwan (2018)
[354] Hyde (2014)

women in the KSA violates fundamental human rights.[355] Those guarded women cannot make their own decisions over important matters, such as marriage, without the approval of their male guardians who control their lives.[356] However, this emphasis on male guardianship over women is slowly fading, and many relevant KSA laws have been either altered or abolished.[357]

Nowadays, it could be argued that Saudi citizens have a greater understanding of other cultures than previous generations who adhered closely to their own culture and values, with less exposure and regard to other cultures. Therefore, in light of what has been discussed, it can be said that the shift towards modernity is inevitable and is being encouraged nationally and internationally. More importantly, the KSA is seeking various other changes to push the country forward towards modernity. Muhammed Bin Salman states in his *Vision 2030* "we will continue modernising our social welfare system to make it more efficient, empowering and just."[358]

In the national transformation programme, 26 government entities were involved in the *Vision 2030*.[359] One of these entities is the Ministry of Media that established the Saudi Centre for International Communication (CIC) in 2016 to help reinforce the relationships between Saudi Arabia and the global media community.[360] The CIC serves as the central source of information about Saudi Arabia including government statistics and objectives.[361] Consequently, the CIC's website is an important source of information, especially regarding *Vision 2030* and how it would improve cyber security to prevent cybercrimes.[362] The CIC notes that technology will play an important role in facilitating the *Vision*, but the digitisation

[355] HRW (2016) <https://www.hrw.org/report/2016/07/16/boxed/women-and-saudi-arabias-male-guardianship-system>
[356] *Ibid*
[357] HRW (2019) <https://www.hrw.org/news/2019/08/02/saudi-arabia-important-advances-saudi-women>
[358] *Vision 2030* <http://vision2030.gov.sa/en/node/9>
[359] *Ibid* <https://vision2030.gov.sa/en/ntp>
[360] KSA CIC <https://cic.org.sa/about-cic>/
[361] *Ibid*
[362] *Ibid*

of public and private data will unavoidably become vulnerable to cybercriminals.[363] Consequently, *Vision 2030* leverages national cyber security bodies to develop and safeguard the Kingdom's cyberspace. Also, CIC states that part of *Vision 2030* is about having reliable data regarding incidences of cybercrime within the region because computer security currently represents a growing concern for Saudi society.[364]

This kind of transformation would have a positive effect on tackling cybercrime substantively and procedurally. For example, on 31 October 2017, and with accordance to *Vision 2030*, the KSA established the NCA, which was formed as a result of various cyber-attacks that targeted the KSA's official websites.[365] This authority was established to combat and anticipate cyberattacks before they happen.[366] This is a crucial step toward the country's development goals. However, as will be discussed in later chapters, particularly Chapters 4, 5, 6 and 7, the KSA lacks other suitable institutions to combat cybercrime procedurally.

2.6 Conclusion

Concerns arising in the pursuit of late modernity, such as the fairness and effectiveness of the KSA criminal process law, have been covered in this chapter in terms of the meanings and measurements of fairness and effectiveness. The chapter began by finding the meaning of both words linguistically and legally, and also finding international and national measurements in order to comprehensively test the ability of the KSA criminal process law to combat cybercrime. The measurements that have been established will be valuable in further analyses of the KSA's law in this thesis.

[363] *Ibid*
[364] CIC (2017) <https://cic.org.sa/2017/11/saudi-arabia-sets-up-cyber-security-authority-to-boost-national-security/>
[365] KSA NCA <https://nca.gov.sa/en/pages/strategic.html>
[366] *Ibid*

Even though the KSA has responded to cybercrime by passing legislation, and by establishing relevant institutions, it will be shown in this thesis that both responses lack effectiveness. The legislation is poorly written because it does not deal with key provisions such as jurisdiction and the process of cybercrime. It only refers to the Public Prosecution (PP),[367] which does not deal with cybercrime as being distinct in the processual problem it raises from traditional forms of crime, as will be discussed later in Chapter 6. Additionally, criminal procedure regrading cybercrime seems to be challenged by the complexities of the KSA's legal system that arise because the *Sharia* dominates the law. However, the KSA has begun to modernise itself by launching *Vision 2030* that still values the role of the *Sharia* within the community. The contemporary applications of *Vision 2030* show that the *Sharia* remains an important source of legislation in the country, yet not the only one. Therefore, there have been reforms of the legal system, but these reforms do not rise to the level of late modernity. For instance, legislation related to the criminal law of process remains stagnant and does not include the elaboration of criminal process regarding cybercrime.

It has been shown that effectiveness means achievement of goals and, in legal terms, effectiveness means meeting the objectives of a legal policy. On the one hand, comparative effectiveness is here described within the UK legal system as the application of utilitarianism, which means ensuring the greatest happiness to the greatest number of people regardless of their religions or traditions. On the other hand, the KSA's view of effectiveness is based predominantly on *Sharia*. Therefore, in the KSA, for the law to successful and meet the objective of policy it must be compatible with *Sharia*. These meanings of effectiveness will be considered as mechanisms for evaluating whether or not the KSA's criminal process of cybercrime is effective .

[367] PP <https://pp.gov.sa/ar/node/146>

In addition to effectiveness, fairness has been conceptually defined as for something to be just and indiscriminate in order to ensure equity and equality. In legal terms, it means achieving fair results by using proper processes. Also, fairness has been defined internationally as the requirement for processes that protect human rights. Similarly, the KSA's standard of fairness is to protect basic human rights. However, this is balanced by the need for those rights to be implemented in accordance with *Sharia*. This complicates the issue of fairness within the KSA because human rights in *Sharia* are broad and vague and dependent on personal views and interpretation, as will be discussed in Chapter 4. Standards of fairness in both international law and national law (KSA law) have been set out in order to test in Chapters 4, 5, 6 and 7 whether the KSA's approach toward the criminal process of cybercrime is fair.

Chapter 3

Methodology

3.1 Introduction

In Chapter 1, Section 1.3, it was stated that this thesis aims to analyse and test the KSA's approach to the criminal procedure of cybercrime using documentary and fieldwork data collection methods and also to make comparisons with the UK for the purpose of suggesting policy transfer. Thus, the present Chapter discusses the methods for achieving these aims.

Legal researchers adopt a socio-legal approach when they wish to understand the law as a broad phenomenon, and social or political socio-legal research is differentiated from traditional legal research approaches, such as black letter research.[368] Legal phenomena are not purely "black letter" laws for lawyers alone because they operate also within society and for society.[369] However, researchers use the doctrinal method, when conducting textual analysis,[370] as used extensively in this thesis. Texts will also form the basis for the policy transfer method to be used by the researcher. By contrast, in order to pursue changes in law or to seek resolutions for the current applications of law, it is better to study them within their sociological context.[371] Therefore, this thesis is socio-legal in nature because it also analyses the societal and empirical factors that prevent the KSA's cybercrime laws from tackling cybercrime procedurally.[372] Both qualitative and quantitative approaches could be used as methods in this research. However, the researcher chose qualitative over quantitative because the fieldwork and the empirical data gathering must be in depth and flexible to capture the

[368] Blandy (2014) 169
[369] *Ibid*
[370] Knight (2008) 29
[371] Blandy (2014) 170
[372] *Ibid* 168

data about the complex and exceptional criminal processes which deal with cybercrimes.[373] The empirical findings include an examination of how the legal system of the KSA operates in practice with regard to the criminal procedure of cybercrime. This examination seeks to indicate the social and political variables within the KSA and their correlation to the operation of cybercrime and cyberspace and the relevant criminal processes in response.

Overall, since the researcher will use doctrinal and fieldwork approaches, this thesis will utilise a "mixed methods" approach whereby the researcher uses more than one method for the purpose of generating and analysing data.[374]

3.2 Doctrinal Analysis

Doctrinal (or documentary) analysis comprises the methodology of analysing primary legal documents as well as the secondary legal literature based on meaning derived from the text and the history of the text. This approach has been selected because it helps the researcher to compile a comprehensive analysis of and comparison between the criminal procedure of cybercrime in the KSA and that of other countries. There are two sources to be analysed. There are primary sources which includes statutes and the *Quran* and *Sunnah* when it comes to *Sharia*. Secondary sources include books, articles, and other scholarly sources, such as explanations of *Quran* and *Sunnah*.

The researcher undertook the doctrinal aspects of the research mainly within the University of Leeds libraries and also online due to the lockdown which took place in the years 2020 and 2021 as a result of the COVID-19 pandemic. Since the body of literature is one the main areas to be analysed, the researcher also accessed online libraries both within the UK such as University of Leeds library[375] and outside the UK, such as online Egyptian

[373] Mack et al (2005) 3
[374] Bryman (2006) 97-113
[375] See <https://library.leeds.ac.uk/>

libraries,[376] the KSA Naif University for Political Sciences online library[377] and a range of public libraries in the KSA such as Saudi Digital Library.[378] Moreover, the researcher accessed UK official governmental websites that publish laws related to the criminal procedure of cybercrime in the UK and official reports related to it, such as GOV.UK,[379] for the purpose of informing policy transfer. For the KSA, the researcher accessed the Expert Authority website where most KSA laws are published in the Arabic language,[380] but most other governmental sources are not available to the public, or to researchers, whether on paper or online. This severe limitation hampered the research and is another reason why the fieldwork was undertaken as an important and original component.

3.3 Policy transfer

Policy transfer allows the researcher to make use of other countries' experiences in order to learn lessons from them.[381] It is important to acknowledge that policy transfer does not mean copying other countries' polices, but rather to learn from them and to adapt them if appropriate.[382] Policy transfer is different from the broader comparison method because the policy transfer aims to suggest changes by adapting other countries' polices,[383] while the comparison method aims to compare the countries' experiences in order to understand more clearly.[384] Thus, the comparison method aims more broadly to provide both the researcher

[376] See Hindawi non-profit online library <https://www.hindawi.org/>
[377] See <https://library.nauss.edu.sa/>
[378] See <https://sdl.edu.sa/SDLPortal/Publishers.aspx>
[379] See <https://www.gov.uk/>
[380] See Saudi Laws Collection on the Expert Authority website <https://laws.boe.gov.sa/BoeLaws/Laws/>
[381] Benson and Jordan (2011) 365
[382] Rose (2005) 1 and 22.
[383] Benson and Jordan (2011) 366
[384] Hoecke (2015)

and their audience with more in depth knowledge and understanding over the issues discussed in the research.[385] Therefore, this thesis is confined to policy transfer.

Using policy transfer will answer the research questions and help in suggesting solutions for the problems encountered within the criminal procedure of cybercrime in the KSA. Almost all sovereign countries use "foreign models" to improve their national policies.[386] Therefore, the researcher chose to use this technique with reference to the UK. Transferring polices from the UK to the KSA might sound impossible due the differences in the legislation, legal system and social life. It is also noted that transferring policies from other jurisdictions might cause unexpected changes which might negatively affect society.[387] Nonetheless, this unexpected change could be anticipated and limited.[388] In the KSA's case, policy transfer is not such a huge problem because the KSA has, for decades, already been implementing legal measures from Egypt.[389] Furthermore, the KSA has employed many legal experts from different nationalities including the UK in the field of cybersecurity in order to overcome cybercrime in the KSA.[390] This means that policies could be imported from all countries to the KSA as long as they do not contradict the supreme law of the land, namely, *Sharia.*

In the UK, there are multiple types of national agents who might assist in the transfer of policies from other jurisdictions, such as: "elected officials; political parties; bureaucrats/civil servants; pressure groups; policy entrepreneurs/experts; and supra-national institutions."[391/392] However, in the KSA, policy transfer is only vested in the legislative

[385] *Ibid* 2
[386] Dolowitz et al (2000) 1
[387] Benson and Jordan (2011) 367
[388] Rose (2005) 134
[389] See 4.4
[390] See United Kingdom-Saudi Arabia Joint Communiqué (2018) <https://www.gov.uk/government/news/united-kingdom-saudi-arabia-joint-communique>
[391] Benson and Jordan (2011) 369

branch particularly in the Council of Ministers,[393] where ministers of the KSA participate in passing and executing laws within their ministries. This practice is questionable in terms of fairness (because of its attendant secrecy), yet it does not invalidate the potential value of policy transfer from the UK into the KSA throughout this thesis.

3.4 Fieldwork Methodology

Aside from the use of numerical data, the major distinctions between qualitative and quantitative approaches lie in their purpose, focus, methods, and criteria for truth. Firstly, in terms of the purpose, the qualitative approach is less descriptive and explores the question of why, whereas the quantitative approach is based on prediction and does not answer the question of why. Secondly, in terms of focus, the qualitative approach focuses on the voice of participants even if it is not the common experience of all, while the quantitative approach focuses on what can be generalized to most of the population. Thirdly, in terms of methods, "most research methods can be used on either qualitative or quantitative methodologies."[394] However, the qualitative approach utilises inductive analysis for text data, while the quantitative approach uses deductive analysis of units of data. Lastly, in terms of criteria for truth, the distinction here lies in the proof of the study. In the qualitative approach, proof is based on faithfulness to data, while proof is based on statistical analysis and replication in the quantitative approach. Therefore, it is better suited to the nature of this research to use the qualitative approach. Although the researcher will employ numerical data in the research such as statistics and percentages when available from published sources, he will not generate new quantitative data.

---

[392] Parliament is also an agent of policy transfer as when it looks at what is happening overseas for inspiration. See House of Lords Select Committee on Communications, Regulating in a digital world (2017-19 HL Paper 299)
[393] Shalhoob (1999) 83
[394] Silverman (2005) 110

In terms of choice within qualitative research, various methods are possible according to Webley:

> "In qualitative research, the data are usually collected through three main methods, used singly or in combination: direct observation, in-depth interviews and analysis of documents."[395]

In order to more fully pursue the stated objectives of the thesis, a qualitative method of collecting and analysing data is conducted which allows a deeper and more flexible form of engagement with experts as participants.[396] Thus, the researcher chose in-depth interviews as the main method of collecting qualitative data because this method best enables the exploration of expertise within a complex and undocumented phenomenon.[397] Moreover, the researcher chose this method because, as already mentioned, there are limited public documentary sources in the KSA that relate to the subject under investigation. In 2020, the researcher was granted approval by the Ethics Committee of the University of Leeds to undertake the fieldwork interviews with elite experts from the KSA who have intimate knowledge of the subject matter.

3.4.1 Interviews

In depth semi-structured interviews are employed as the primary data collection method since they provide a personal and interactive approach to identifying the participant's opinions, feelings, and emotions regarding the research subject.[398] The distinction between

[395] Webley (2010) 2
[396] Taylor et al (2015)
[397] Opdenakker (2006) 2-4
[398] Juanena & Smith (2009)

semi-structured and unstructured interviews lies in the control imposed on the interviews.[399] Semi-structured interviews are more directed in terms of preparing the questions and shaping the interview, while an unstructured interview leaves the style much more open. Therefore, semi-structured interviews were preferred by the researcher because they draw the main lines of the interviews. As been noted by Juanena and Smith, the questions in semi-structured interviews must be derived from the chapters of the research before conducting the interviews and these questions must be relevant to the issues of the research and must be direct and precise.[400] Semi-structured interviews act as the primary tool for data collection.[401]

The researcher conducted 32 interviews, with no more than 3 people from each cohort stratum. However, of these, only 21 interviews were chosen for analysis and citation in this thesis because the other 11 interviews did not sign the consent form, which is a major ethical requirement. The several sub-populations that the researcher selected are as Table 3.1 shows.

[399] *Ibid* 315
[400] *Ibid*
[401] Opdenakker (2006) 3-4

Table 3.1 Fieldwork subpopulation data

Subpopulation	Total interviews sought	Total interviews achieved	Variation in numbers
The police	3	4	One member did not sign the consent form, so his data was destroyed and not used for the thesis.
The Public Prosecutor office	6	7	One member did not sign the consent form, so his data was destroyed and not used for the thesis.
The criminal court	3	3	
Sharia experts (*Ulama*)	3	4	One interviewee did not sign the consent form, so his data was destroyed and not used for the thesis
Private lawyers	3	5	Two lawyers did not sign the consent form, his data was destroyed and not used for the thesis
Law professors	3	4	One Professor did not sign the consent form, his data was destroyed and not used for the thesis
Government employees in related areas of cybercrime	6	3	Three interviews were conducted with: one Ministry official and two expert authority officials. All 3 failed to sign the consent form, so their data were destroyed and not used for the thesis.
Private sector employees in areas related to cybercrime	3	2	Two interviews were conducted with telecoms industry officials. Interviews were not fruitful, so their data were destroyed and not used for the thesis.
Total	30	32	11

One reason that the researcher chose these particular sub-populations and limited number of participants is that they can contribute in depth to the aims of the research due to their knowledge and expertise that fit with the research objectives. Some of them have participated in passing the laws that are related to the criminal procedure of cybercrime, whilst others have made judicial or other professional decisions on the criminal procedure of

cybercrime. Another reason is that stratification or dividing the participants into groups and then choosing samples of each group will make the data more precise than choosing random samples.[402]

The time that the researcher allocated to collect the data from all the various sources, including interviews, was limited to 3 months. The interviews were planned to take place in the KSA because it is the main focus of the research. However, they were actually conducted online due to the Covid-19 pandemic, after first formally receiving permission from the University of Leeds to allow the researcher to conduct his fieldwork online.

Lo Iacono et al argue that using VoIP (Voice over Internet Protocol) technologies might be as effective as face to face interviews.[403] Yet, one disadvantage is that the internet connection might be lost during the interview.[404] In her paper about conducting interviews with Saudi individuals, AlKhateeb addresses the same concern as well as poor internet connection.[405] Also, she adds that even though anonymity was ensured to participants, they prefer to have face to face interviews because they are unfamiliar with conducting online interviews.[406]

However, due the Coronavirus pandemic, many people in the KSA have become familiar with conducting online video meetings because during the lockdown and the curfew in the KSA which took place from March, April until May of 2020 almost all work meetings have been conducted online.[407] Moreover, the Internet connection in the KSA is now as good as in a developed countries such as the UK, and all major cities (where the participants live)

[402] *Ibid*
[403] Lo Iacono et al (2016) 103–117
[404] *Ibid*
[405] AlKhateeb (2018) 2253–2260
[406] *Ibid*
[407] Nurunnabi (2021) 127–128

in the KSA has a good internet connection.[408] Thus, during most interviews, the internet connection was good, and interactions were not affected by conducting interviews online. As experienced by Lo Iacono et al, they were as effective as face to face interview.[409] Therefore, all interviews were conducted only within three channels; Google Duo, Microsoft Teams, and Face Time, with Skype being avoided for security reasons.[410]

Ahead of each interview, an interview guide was provided for the interviewee, and a schedule of questions worked out.[411] Thereafter, the researcher spent around 5 months conducting the interviews, even though the initial plan was to take only 3 months, as some interviewees kept putting off the interviews beyond the scheduled dates within the given period. The researcher conducted one interview of around an hour and half with each participant.

The interviews are limited to expert professionals – hence they can be called "elite interviews".[412] One definition of professional elites might be broken down into two categories: ultra-elites and general elites. The ultra-elites are "the most highly placed members of an elite," and general elites are people who possess "the ability to exert influence" by "social networks, social capital and strategic position within social structures."[413] Interviews were held with elites in the sense of established professionals and officials. Therefore, the research excludes certain groups of people from being interviewed such as the general public and victims of cybercrime. Excluding the general public is due to their lack of expertise on the subject matter and the complex ethical concerns which would arise.

[408] Yamin and Mattar (2016) 944
[409] Lo Iacono et al (2016) 103–117
[410] *Ibid*
[411] See appendix
[412] Harvey (2011) 433
[413] *Ibid*

3.4.1.1 Identifying, approaching and recruiting participants.

The participant interviewees were identified based on their work status or their experience within the fields of the criminal procedure related to crimes in general and cybercrime in particular, Saudi criminal law and *Sharia*. The snowballing technique[414] is a common method to identify participants, but before using this technique, the researcher identified the initial people (the initial small snowball) who expanded the circle and led to the others (the bigger snowball). These first people were identified through common channels, such as webpages where CVs or publications are provided, such as Academia.com, Researchgate.net, and Linkedin.com, as well as social media, especially official Twitter accounts.

The participants who work within the government were approached through official channels, such as work email, administrative letters, and work phone. There is no law in the KSA which prevents public employees from conducting interviews or participating in any study or which requires a researcher to obtain clearance to interview public employees. The participants who are not government officials were approached through their personal email, personal phone, or work phone. The researcher avoided approaching participants through informal methods such as social media accounts or seeking to meet participants with no appointment to avoid falling into any ethical infraction.

Participants were given a summary of the research and information sheet, and they were provided with general information about what they are going to be asked and why they were chosen and approached along with the consent form.[415] Therefore, each participant knew what they will go through. Moreover, they were given the chance to withdraw from the

[414] See Mack et al (2005) 5-6
[415] See appendix A, B and C

research within two weeks. The participants had two weeks to decide whether they were going to take part in the research or not. The reason why 14 days was the chosen period is that the researcher would then be able to approach other participants who have similar characteristics to the participant who decided not to take part in the research. Since all the interviewees are Saudi nationals, the researcher translated all the provided materials into the Arabic language, so that the participants would have a comprehensive understanding about what they were going to participate in.

3.4.1.2 The purposive sampling method

The purposive sampling method was used to develop the sampled population. This is a non-probability sampling technique; thus, the sample members were selected based on their knowledge, expertise or relationships with the research subject. The sample members selected for the study have relevant and sufficient work experience within the field of cybercrime and have actively engaged in it. Within this context, the selection of study participants focused on professionals in the private and public sectors.

Also, when addressing the issue of criminal procedure on cybercrime in the KSA as the main aspect of this research, judiciary members and personnel were selected to contribute towards illustrating the considerable power that the judiciary branch has. In addition, a handful of judges, prosecutors and other judiciary personnel, such as criminal investigation officers, were selected and interviewed to investigate *Ijtihad* and other procedural issues that the judiciary based their decisions of cybercrime rulings on. People from the private sector were also selected due to their expertise.

3.4.1.3 Interview preparation

The researcher compiled various questions in order to collect data from interviewees. According to Opdenakker, this data should be derived from the participants own experiences and information about the subject matter.[416] Additionally, according to the University of Leeds ethical policies,[417] the researcher must have the interviewees' formal consent before starting the interview.[418] Moreover, the researcher should also prepare his questions before conducting the interview by beginning with general and broad questions and follow them up with more specific and detailed questions.[419] Therefore, the researcher asked both open-ended and close-ended questions. Open-ended questions, which are commonly used in qualitative approaches, allow the participant to answer more thoroughly in their own words, while close-ended questions, which are mostly used in quantitative approaches, limit the answer to words such as yes or no.[420] The questions were designed to fulfil the research objectives and were available to the interviewees before conducting the interview. Moreover, the researcher took into his consideration that he must pay full attention when he conducts the interview, taking notes and asking probing questions, especially when the interviewee's answer is brief or vague.[421] Moreover, the researcher made voice recordings of the interviews after gaining the interviewees' consent. However, most interviewees preferred not to be recorded. In that case, written notes were made. Both records were uploaded onto the researcher's private computer immediately after each interview. The data were stored in a secure place: they were uploaded onto the internet cloud that Leeds University provides to its students (OneDrive). One reason why the data was stored onto this cloud rather than the students' private internet cloud is that

[416] *Ibid*
[417] University of Leeds Research ethics and integrity (UoLRE). see <https://ris.leeds.ac.uk/research-ethics-and-integrity/>
[418] *Ibid*
[419] Mack et al (2005) 42
[420] Opdenakker (2006) 3-4
[421] Mack et al (2005) 43

the University's cloud is well protected for the sake of safety and the secrecy of the data as well as compliance with data protection laws, especially the UK Data Protection Act 2018.[422] Also, the data were encrypted using an encryption a programme that is approved by the University of Leeds called *Cryptainer* before uploading them onto the cloud, and only the researcher has the password for the encrypted files. The voice data is already digital, but any handwritten data was digitised by taking pictures of them or scanning them onto the researcher's computer allowing them to be encrypted and uploaded to the cloud. All paper copies were destroyed.[423]

The questions in the interviews were derived mainly from issues raised in Chapters 4, 5, 6 and 7. The researcher only asked about the related subjects such as polices, laws, and regulations, so that the questions benefit the research regarding how the system works in practice through people's experience.[424] The researcher then undertook the analysis of the data.

3.4.1.4 Analysis of data

The researcher listened and read through the interview data, developing and reflecting on key words that are directly related to cybercrime and its processes. Collected data must be analysed in order to obtain insights from it, so it was the researcher's duty to derive from these data evidence that which is relevant to his argument. Therefore, the researcher used an analytical technique which, as noted by Taylor et al, aims to identify themes or develop the concepts and ideas based on deep reflection on the raw data collected.[425] Then, the researcher took into consideration that he is going to review and compare the data and try to link them

[422] UK Data Protection Act 2018
[423] For the data management plan, see appendix D
[424] See appendix E
[425] Taylor et al (2015) 165

with other additional data that might be beneficial.[426] Moreover, as Taylor et al suggest, the researcher elaborated themes, concepts, or ideas to come up with findings that relate to the data.[427] Finally, the researcher considered the use the computer programme known as NVivo for data analysis. It is recommended for qualitative researchers who have a lot of data to use NVivo because "researchers can feel completely free to modify their documents, and to code them while writing them up."[428] However, since the researcher conducted the interviews mainly in Arabic, the use of NVivo would be of limited utility because the programme is designed to help in analysing data in English language only.

Next, it is important to ensure that issues of authenticity, generalisability and comparability are considered for better analysis. In short, authenticity is related to ensuring the interview data is truthful, and mainly considers how is it known whether the interviewees are telling the truth.[429] One test was that the researcher was able to compare answers within the sub-populations. Also, interviews were conducted online, so the researcher was able to see whether they were comfortable or not with their answers such as from tone of voice or non-verbal signals. Moreover, the project was conducted on a professional and rational basis which the interviewees would appreciate and was designed to trigger professional responses by them.

Generalisability relates to the extent to which the participants' responses can be ascribed to a wider population.[430] Limited claims can be made here. The sample was a low proportion of the whole population, so the researcher cannot be sure that the views expressed are the majority view or not. However, interviewees were experienced professionals, so they were less likely to be as variable as, say, the general population.

---

[426] *Ibid*
[427] *Ibid*
[428] Richards & Richards (2003)
[429] Kenyon and Stansfield (1992) 347-64
[430] Leung (2015) 324-27

Comparability is related to how one sub-population is compared to another.[431] The same questions were basically asked repeatedly because of the use of an interview schedule,[432] and all interviews were semi-structured. Thus, there was not much variation in answers, especially when it comes to technical issues related to the criminal procedure such as who investigate and prosecute cybercrimes.

The researcher will keep the data stored for 3 years after being awarded the degree. There are two reasons why the researcher needs to keep the data. The first is that the research in part or in whole might be published and the researcher might therefore go back and review the data before the publication because he might need to correct some errors if any are noticed by examiners.

3.5 Ethical issues and principal considerations

The main ethical issues with this research arise in connection with the fieldwork because the fieldwork deals with human participants. When conducting the research, the researcher must consider the ethical issues and deal with them professionally.[433] These issues include confidentiality, in accordance with the University of Leeds Research Ethics Policy,[434] the UK Data Protection Act 2018, the Human Rights Act 1998[435] and the University of Leeds Code of Practice on Data Protection.[436] The research must comply with all polices mentioned.

The researcher is also obligated to seek the participants' informed consent, ensure the safety of participants, inform participants of their right to withdraw within 2 weeks and to avoid influencing the participants.[437] The consent form is obtained on the basis that, first, the

[431] Kenyon and Stansfield (1992) 347-64
[432] See appendix E
[433] UoLRE <https://ris.leeds.ac.uk/research-ethics-and-integrity/>
[434] *Ibid*
[435] UK Human Rights Act 1998
[436] UoLRE <https://ris.leeds.ac.uk/research-ethics-and-integrity/>
[437] *Ibid*

researcher provided the participants with information sheets about the research and their involvement in it. Second, participants must be ensured anonymity, and both the researcher and the participants should be sure that identities will not be revealed, either directly by name or by implying something which leads to them being identified, such as their initials or their status.[438] Thus, the researcher has been careful when quoting interviewees; he did not quote too much, being selective and brief whenever he quotes any participants.

There are two forms of informed consent used in this research: one in English and the other one in Arabic.[439] Participants signed one in order to fully cooperate. Information about their participation was provided to them along with the option to withdraw at any time before the interviews take place and within 2 weeks after the interviews. Participants were informed that their data is interpreted by the researcher, and that the research will be published as a thesis and an academic paper. However, the researcher faced some difficulties regarding confidentiality when it comes to high ranked government officials who want to stay anonymous due to sensitivities related to their position. Most of them have taken an oath not to reveal any secret or sensitive information to the public. To overcome this issue, the researcher provided participants with a copy of the research objectives, so they can fully understand the nature of their participation, a copy of the informed consent form and advised them to call the numbers provided in the form.[440] Additionally, the researcher informed the participants that they have the right to withdraw from participation within a reasonable period of time (no more than two weeks). Also, the researcher informed the participants that both the University and he are obligated and bound by the UK data protection laws to not reveal any data.[441] Additionally, the researcher chose a safe and secure online application to conduct the interviews. There are some risks that might arise during the interviews, such as mention of

[438] *Ibid*
[439] See appendix C
[440] Mack et al (2005) 31
[441] UoLRE <https://ris.leeds.ac.uk/research-ethics-and-integrity/>

specific offences and offenders. In response, the researcher avoided talking about individual cases and dealing with highly sensitive data as they could have constituted a possible risk to confidentiality and were not relevant to the research aims and objectives, so he politely stopped the participants from bringing them up.

One issue which was being accounted for is that KSA does not have a specific law on data protection. However, there are various provisions in multiple laws in KSA that protect data, such as the BLG, the Electronic Transection Protection Law 2007 (ETPL),[442] and the ACL. Article 17 of the BLG states that:

> "Ownership, capital and labour are basic fundamentals of the kingdom's economic and social entity. They are private rights that perform a social function in conformity with Islamic Shari'ah."[443]

Also, Article 40 of the same law states that:

> "Correspondence by telegraph and mail, telephone conversations, and other means of communication shall be protected. They may not be seized, delayed, viewed, or listened to except in cases set forth in the Law."[444]

These two articles thus protect the right of ownership and privacy. Furthermore, the KSA is bound by *Sharia* which prohibits the invasion of privacy.[445] In the same regard, both the ACL[446] and the ETPL[447] prohibit and incriminate the unlawful accesses of data. Therefore, even though there is no single data protection law in KSA, the researcher is obligated to comply with what has been stated within the law regarding data protection. It is the

[442] ETPL, promulgated by Royal Decree No. M/8 of 8 Rabi' I 1428H (March 18, 2007)
[443] KSA BLG Article 17
[444] *Ibid* Article 40
[445] Ala'li (2007) 9
[446] ACL Articles 4 and 5
[447] ETPL Article 23

researcher's obligation to ensure the anonymity and the safety for both the participants and the researcher. All interviews are about policy law and general practice. Therefore, sensitive data and individual cases are avoided during the interviews to ensure the level of generality which guarantees the safety of the interview parties. The researcher utilised two techniques to ensure that sensitive data is not discussed. First, the researcher provided participants with an information sheet that says sensitive data will not be discussed because it is not relevant to the thesis. Second, the researcher interrupted participants who brought up sensitive data in live interviews and moved to other points and questions.

3.5.1 Risk assessment

The researcher was given formal approval in May 2020 by the University of Leeds to conduct the fieldwork. Due to the high risk of conducting face-to-face interviews during 2020 because of the Covid-19 pandemic, the researcher conducted all his fieldwork interviews online after receiving permission from the University in order to adhere to social distancing rules that were in place during the specified period using Microsoft Teams.

In order to ensure all risks are minimised, the researcher is obligated to fill in a risk assessment form that is provided by the University of Leeds and to obtain approval before conducting the fieldwork to evaluate whether it is safe for both the researcher and the participants to conduct the interviews.[448]

[448] UoLRE <https://ris.leeds.ac.uk/research-ethics-and-integrity/ >

3.6 Conclusion

This research involved a socio-legal study that uses documentary analysis allied with a qualitative approach as well as policy transfer.

These methods satisfy the research aims and objectives as the researcher accessed the data he desired especially during the first two years of the thesis and before the spread of Covid-19 in the year 2020. After the outbreak of the virus, physical access to library was not possible, but the researcher managed to access online libraries, and he managed to collect data from interviews by conducting online interviews which were surprisingly fruitful as most participants were at home most of the time during lockdown in 2020.

Chapter 4

Law of Criminal Procedure Applied to Cybercrime in the KSA

4.1 Introduction

The KSA has passed various laws, as mentioned in Chapter 2,[449] on cyber related crimes. However, articles in this body of legislation concentrate more on substantive crimes than on process.[450] Generally, the KSA's CPL 2103 is applied to the criminalisation of cybercrime, yet no single Article specifically addresses cybercrime.[451] This chapter focuses on legislation related to the criminal procedure applied to cybercrime in the KSA. It evaluates the effectiveness and fairness of those laws in regard to the standards that are set out in Chapter 2. Moreover, it analyses the effect of *Sharia* on legislation and evaluates whether *Sharia* is fair and effective in this context. As well as evaluating the KSA law with the standards of fairness and effectiveness, reference to the UK jurisdiction will be conducted in order to answer the research questions and objectives of whether the KSA law is fair and effective and how the UK jurisdiction deal differently with the criminal procedure of cybercrime.

It is an aim of this thesis to evaluate the KSA's approach toward criminal process, test whether it is effective and fair, and analyse whether it is has been adequate in dealing with cybercrime. The evaluation and analysis will be carried out in accordance with the research objectives to set forth the standards for effectiveness and fairness, which has been done in Chapter 2.[452] Now, these standards will be applied to the KSA law, both with regard to *Sharia* and legislation.

[449] See Section 2.2
[450] Hakmeh (2018) 9
[451] Abdulaziz (2018) 27-76
[452] See 2.4

Therefore, it can be said that this chapter will reflect three of the main research objectives set out in Chapter 1.[453] The first objective is exposition; setting out the KSA laws and regulations on criminal procedure regarding cybercrime, the second objective is assessment; providing critique to those laws and regulations, and the third objective is reflecting on the KSA's laws and regulations with a view to policy transfer.

In order to fulfil the agenda of the thesis, a critique of what the KSA has done in terms of tackling cybercrime in a procedural sense will be provided along with what the KSA has yet to do in light of tackling cybercrime in procedural sense throughout this chapter. This chapter will address the legislation that has been passed regarding cybercrime and the attendant criminal process, as well as the role of *Sharia* in regard to the criminal process of cybercrime to demonstrate the correlation between KSA law and *Sharia* and its effect on the criminal procedure applied to cybercrime. Additionally, a test for both the fairness and effectiveness of *Sharia* will be examined to investigate what holds the KSA back from efficiently tackling cybercrime from a procedural perspective. Furthermore, the UK laws on criminal procedure regarding cybercrime will be addressed to take lessons from other jurisdictions on the matter. In addition, a proposed Model Code will be used as a heuristic device in order to illustrate what has been done and what has yet to be done by the KSA in order to combat cybercrime procedurally. Finally, the chapter will conclude by outlining its main findings and criticisms.

4.2 Legislation related to the criminal process of cybercrime in the KSA

This section will introduce current cybercrime related legislation in KSA. It will make the point that most of the legislation related to cybercrime in KSA is substantive rather than procedural. It includes the ACL, Anti Commercial Fraud Law 2008 (ACFL),[454] and ETPL.

[453] See 1.3
[454] ACFL, promulgated by Royal Decree No. M/19 23 Rabi II 1429H / 29 April 2008

These laws barely mention policing and other criminal procedures. Only the CPL 2013 has been introduced in the light of the requirements of procedure for crimes.[455] One issue that arises from the KSA's law in general, and this legislation specifically, is that there is a lack of resources in regard to official published documentary history related to them. Therefore, based on the limited published history and facts in relation to this legislation, speculation about why specific legislation has been passed will be made along with an analysis of the role of each in combating cybercrime from a procedural perspective.

4.2.1 Anti Cybercrime Law 2007

In February 2007, new legislation about cybercrime was introduced owing to mounting pressure on the government which was applied by various individuals and corporations.[456] The ACL[457] was passed by the Council of Ministers to protect Saudi society from the rising threat of internet fraud around the nation.[458] The legislation that was introduced is primarily based on *Sharia* and derived from Article 7 of the BLG.[459] As discussed in Chapter 2, any legislation in the KSA must comply with *Sharia*.[460] The ACL was issued under the Council of Ministers resolution and approved under the Royal Decree.[461] This was the first legislation designed by the government to combat cybercrime.[462] The KSA became aware that the UAE was coping better in many aspects of technology including the new phenomena of cybercrime.[463] Therefore, the KSA passed this legislation one year after the issuance of UAE law on cybercrime.[464] Before the introduction of ACL, all

[455] Alali (2016) 33
[456] Alghamdi (2017) 80-81.
[457] ACL, promulgated by Royal Decree No. M/17
[458] Alqahtani (2016)
[459] BLG Article 7
[460] See 2.2
[461] Kshetri (2010)
[462] Bakhsh (2016) 9-15
[463] Alali (2016) 33
[464] UAE Federal Law No 5, 2006

judgments and cases regarding cybercrime were left to the discretion of the presiding judges under *Sharia.*[465]

Most judges prior to the ACL had limited knowledge about technology, computers and electronic devices in general, except for mobile phones.[466] As their knowledge of technology was poor, they struggled with handling computer crimes[467] which could lead to miscarriages of justice taking place, where offenders could avoid justice, and others might be wrongfully convicted of computer crimes.[468] Alongside the judicial branch, both executive and legislative branches had similar misapprehensions over computer crimes in the absence of comprehensive legislation on the matter.[469] Another complication was the role of religious police or the General Presidency for the Promotion of Virtue and the Prevention of Vice (GPPVPV)[470] which had intervened.[471] Before 2007, the religious police had repeatedly been invading people's privacy by unlawfully searching and seizing their phones, often based on unreasonable suspicion such as simply displaying westernised haircuts or clothes.[472] Some of these unlawful searches resulted in finding evidence that criminalised people, such as pictures of friends of the opposite sex at private parties, enabling PP to build a case based on this incriminating evidence.[473] Consequently, regardless of how the evidence was obtained, CCJs might end up dealing with people who committed what they used to describe as technology crimes.[474]

[465] Interview with CCJ CJ1
[466] Alshathri (2015) 60
[467] *Ibid*
[468] Gulf Centre for Human Rights (2018) 12-13
[469] Algarni (2015) 124
[470] GPPVPV <https://www.pv.gov.sa/Eservices/AGEN/Pages/Dashboard.aspx>
[471] Alhomodi (2009) 71
[472] Aldhuhaian (2014)
[473] Alali (2016) 90
[474] *Ibid*

The foregoing situation indicates the three main reasons that led both the *Al Shura* Council and CITC to suggest ACL to the KSA cabinet.[475] The first reason is the lack of knowledge about technology from all government branches.[476] The second is the absence of any legislation related to computer crimes.[477] The third is misconduct by police and misjudgements by PP and CCJs in cases that involved computer crimes.[478] Since they are *Sharia* diploma holders, it was up to CCJs and prosecutors to use *Ijtihad* in order to deal with cybercrime with their own interpretation of *Sharia.*[479] In general, this was not an effective measure to develop computer crimes. ACL might also satisfy some human rights advocates and political reformers because it lists with greater certainty what it considers as computer crimes.[480] However, the legislation says almost nothing about criminal procedure which remains a major problem associated with regulating the use of cyberspace in the KSA.

ACL contains a total of 16 Articles.[481] Article 1 provides the definition of terms that are applied to all the subsequent Articles.[482] Article 2 lists the aims sought through the enactment of the legislation, which is to combat information, internet and computer crimes through determining each crime and the punitive action required to punish those crimes.[483] Articles 3 through to 13 identify specific cybercrimes and indicate the specific penalty for each offense.[484] Next, Articles 14 through to 16 state the duties of the agencies tasked with execution of the Law.[485] The ACL provides a broad definition of internet crime, thus offering a response to any new form of internet crime that may arise in the future. This legislation

[475] ACL
[476] Interview with Law Professor LP2
[477] *Ibid*
[478] *Ibid*
[479] Interviews Detective of the PP D1 and CJ2
[480] Finlay (2009) 194-197
[481] ACL
[482] *Ibid* Article 1
[483] *Ibid* Article 2
[484] *Ibid* Articles 3-13
[485] *Ibid* Articles 14-16

covers several crimes, and other cybercrime related laws cover some other offences,[486] but others are ignored, such as sexual harassment in cyberspace. Additionally, some of the ACL provisions seem impossible to apply. For instance, most people can gain access to pornography websites in the KSA[487] even though watching pornographic content is a violation that is punishable with imprisonment or fine under Article 6 sections 1 and 2.[488]

Overall, the ACL is outdated, and it needs to be updated. As Wall noted, "The technological transformation is an ongoing process,"[489] which means that legal responses should be updated with this transformation. The ACL has not been updated to reflect technological changes such as cloud computing and social media. Moreover, Algarni notes that the CITC emphasised the weakness of the ACL and how it fails to cover completely the issues of spam,[490] or unsolicited commercial messages.[491] However, not every solution is to be found in the criminal law. In Chapter 1, it was illustrated that criminal law is at the top of the regulatory pyramid, followed by civil law and then formal regulation.[492] At the base of the pyramid is cyber self-regulation. Therefore, it should be noted that there are various alternative measures which could be at least as effective as criminal measures. For instance, compensation for people affected by cybercrime could be a civil solution, and censorship of the Internet and filtering content within the KSA jurisdiction could be used as a tool of formal regulation. Furthermore, ISPs can prevent violators, who commit cybercrime, from accessing the Internet, and would therefore provide a solution based on self-regulation.

[486] Alabdulatif (2018) 6
[487] Henry (2009) 311
[488] ACL Article 6
[489] Wall (2007a) 2
[490] Algarni (2010) 1-17
[491] *Ibid.* 10-12
[492] See figure 2.3

The criminal procedural law in the KSA is contained in the ACL only to a very limited extent. Article 14 states that the CITC shall provide support to detectives,[493] while Article 15 states that the Bureau of Investigation and Public Prosecution (BIPP)[494] shall carry out investigations and prosecutions.[495] These need to be researched further, so Chapters 6 and 7 will be dedicated to both investigation and prosecution. In addition, court processes for cybercrime will also be assessed in Chapter 6. It has been suggested that there is a lack of effective policing and forensic facilities for investigation in the KSA.[496] Almutairi notes that almost all forensic examiners are police officers who do not hold a bachelor's degree in biology, Chemistry, or Physics, as is required for forensic examiners, and they are unlikely to hold any cybersecurity qualifications about how to deal with cyber evidence.[497] He doubts whether forensic science in the KSA is fair and effective in its delivery.[498]

In greater detail, Article 14 of the ACL states that:

> "The Communication and Information Technology Commission, pursuant to its power, shall provide the assistance and technological support to competent security agencies during the investigation stages of such crimes and during trial."[499]

Even though this Article mentions policing, investigation, and trial for cybercrimes, it does so only by assisting and supporting existing structures. Articles 14 and 15 do not specify the competent security agencies in terms of policing. However, Article 15 specifies the relevant public authority for investigating and prosecuting:

[493] ACL art.14
[494] Now the PP.
[495] ACL Article 15
[496] Kshetri (2010)
[497] Almutairi (2013) 106
[498] *Ibid*
[499] ACL Article 14

"The Bureau of Investigation and Public Persecution shall carry out the investigation and public persecution of crimes stipulated in this law."[500]

Although this thesis is not about the doctrine of the separation of powers, it should be said that, in other countries, such as the UK, investigation and prosecution are generally separated and not vested in one authority. Otherwise, one authority would have too much power and could abuse that power too easily.[501] However, this principle of separation of power can be overridden in specialist cases such as the case of the UK Serious Fraud Office (SFO)[502] that investigates and prosecutes "the top level of serious or complex fraud, bribery and corruption"[503] including some cybercrimes.[504] Yet, investigation is generally separated from prosecution in the UK in contrast to the KSA, as will be addressed in Chapters 6 and 7. Aside from combining investigation and prosecution in one authority in the KSA, Article 15 needs to be updated is because, in the middle of 2017, King Salman Bin Abdulaziz ordered a change to the name of the bureau from BIPP to the PP.[505]

As has been discussed in Chapter 2, there is no criminal code in KSA,[506] so each substantive criminal law should define its own rules and procedures.[507] It appears from the ACL that this law states the crimes and their penalties, but it does not deal with procedural aspects. It only states broad Articles about the process which are not sufficient.[508] The ACL relies almost completely on the CPL.[509] The CPL has a limited impact because the KSA choses to deal with cybercrimes as not being distinct from NNCs, whereas those crimes are

[500] *Ibid* Article 15
[501] Iyer (2018) 507-528
[502] SFO <About us. https://www.sfo.gov.uk/about-us/>
[503] *Ibid*
[504] *Ibid*
[505] KSA Royal Decree No. A/240 of 2017.
[506] See 2.3.2
[507] Abdula'al (2015) 42
[508] Interview with Law Professor LP1
[509] *Ibid*

significantly different in nature.[510] One major difference is that NCCs are perpetrated in physical space while cybercrimes are mostly limited in non-physical space.[511] Consequently, this difference should lead to the design of specialist procedural law provisions for cybercrimes to cover issues such as jurisdiction, evidence gathering, evidence storage and evidence presentation in courts.[512] The distinction here lies in the possibility that cybercrime and its evidence cross national boundaries and jurisdictions in a very complex way, and it requires people with expertise to deal with it.[513] An underlying reason why the KSA struggles with cyberspace is because of the lack of expertise on cyberspace and cybercrime.[514] Casey suggests the need to "keep in mind that a procedure cannot cover all eventualities and individuals handling digital evidence may need to deal with unforeseeable situations. Therefore, all individuals handling evidence should have sufficient training and expertise to implement procedures and deal with situations that are not covered by procedures."[515] Also, differences between physical space and cyberspace raise a problem in the KSA regarding the transborder aspects of cybercrime. Cyberspace crosses boundaries and jurisdictions almost inevitably,[516] yet the KSA still treats the criminal process of cybercrime as equivalent to NCCs.

Additionally, differentiating cyberspace from physical space in the KSA raises the problem of the private ownership of cyberspace. Most of the internet is owned by private companies and organisations, many of which are located in the US[517] where the KSA has no jurisdiction. Even though the US has passed the CLOUD Act 2018,[518] which allows other countries to obtain evidence from internet companies in cybercrime cases, the KSA is most

[510] Hakmeh (2018) 10
[511] Sandywell in Yar and Jewkes (2011) 46-54
[512] *Ibid*
[513] Casey (2011) 179
[514] Alali (2016) 2
[515] Casey (2011) 229
[516] See 2.2.2
[517] *Ibid*
[518] USA Cloud Act 2018

unlikely to meet the requirement for recognition under this Act.[519] Finally, identity is the last main problem which results from the differentiation between cyberspace and physical space in the KSA. Unlike identity in physical space, identity on the Internet is surrounded by anonymity; "On the Internet, nobody knows you're a dog."[520] In this regard, the ACL only criminalises using false identity for the purpose of financial fraud.[521]

A more comprehensive procedural approach has not been undertaken within KSA law. For instance, there is no law in KSA that distinctly engages with cybercrime evidence law and forensic processes,[522] and both are treated as if they are NCCs. Moreover, the ACL does not talk about the jurisdiction of cybercrime, which means that it is left to the CPL to determine jurisdiction, taking into consideration that there are neither specific provisions for cybercrimes in the CPL nor any later update in this law regarding cybercrime. In fact, the only update regarding cybercrimes within the KSA laws was a substantive crimes update. In 2015, the Saudi government updated the ACL to include a further offence of naming and shaming perpetrators by publishing their name and the details of the criminal offense that they have committed.[523]

4.2.2 Electronic Transactions Protection Law 2007

The ETPL was passed based on recommendations made by the *Al Shura* Council and the CTIC on the basis that a large percentage of the KSA population use technology on a daily basis in commercial transactions.[524] Consequently, this piece of legislation was passed in order to protect these consumers.[525] The number of people who are involved in e-

[519] *Ibid*
[520] Fleishman (2000)
[521] ACL Article 4
[522] Interview with Detectives of the PP D1 and D2
[523] Al Shura Council (2015)
[524] ETPL.
[525] *Ibid* Article 2

commerce in the country has increased considerably since 2006.[526] Prior to 2007, there was insufficient legal protection offered to them.[527] This situation has encouraged the KSA government to pass this legislation in order to protect both KSA citizens and investors, whether they are locals or foreigners.[528] Similar to the ACL, the KSA passed this legislation one year after the UAE introduced their own Federal Law No 1 on Electronic Transactions and Electronic Commerce in 2006,[529] which makes it apparent that the KSA was following the steps of the UAE.

The ETPL unifies regulatory standards on the use of electronic transactions and signatures.[530] Also, it underscores the modes of existing cooperation between the KSA and other countries in relation to cybercrime, since it aims to increase the overall safety and confidentiality of electronic trading, records, and signatures.[531] The ETPL seeks to eliminate electronic fraud and promotes local and international operations in fields such as trading, medicine, e-payments, e-government and education. It provides protection against various forms of crime such as impersonation of an individual's identity, forgery of digital certificates and electronic signatures.[532] Additionally, it provides punishment for such crimes (not exceeding 5 million Riyals or five years imprisonment, or both).[533] This legislation includes two procedural articles; Article 25 is about policing the violation of this legislation,[534] while Article 26 is about investigating and prosecuting violators.[535]

Article 25 states that:

[526] CITC (2017)
[527] Alghamdi (2011)
[528] ETPL Article 2
[529] UAE Federal Law No 1 2006 on Electronic Transactions and Electronic Commerce
[530] ETPL Article 5
[531] *Ibid* Article 28
[532] *Ibid* Article 23
[533] *Ibid* Article 25
[534] *Ibid* Article 25
[535] *Ibid* Article 26

> "The Commission, in cooperation and coordination with competent authorities, shall be in charge of recording and inspecting violations set forth in Article (23) of this Law and making a record thereof. The Commission may seize equipment, systems and programs used in committing the violation until such violation is decided. The Governor shall issue a decision naming employees for the task and setting procedures for recording and inspection."[536]

This article gives the CITC the authority to act like a judicial officer by recording and inspecting violations. Therefore, because some of the violations for this legislation will be committed in cyberspace, the CITC can exercise policing functions in cyberspace in light of the provisions of this legislation but only for the violations listed in Article 23.[537] According to the criminal justice process in the KSA, the criminal investigation process goes through four stages; arresting, investigating, prosecuting, and trying suspects.[538] Therefore, it is possible to say that, by giving the CITC the authority to act like judicial officers, this legislation is the first to identify the stages of the criminal process for cybercrimes in the KSA as it begins to address the investigation and prosecution for these violations:

> "The violation record set forth in Article (25) of this Law shall, upon the Commission's completion of its task, be referred to the Bureau of Investigation and Public Prosecution to undertake, in accordance with its law, the investigation and prosecution thereof before the competent judicial authority."[539]

[536] *Ibid* Article 25
[537] *Ibid* Article 23
[538] Shareef (2016) 36
[539] ETPL Article 26

The ETPL does not focus on what makes a good investigation, including, first competence regarding skills, priority, and motivation, and second, independence and no conflict of interests.[540]

4.2.3 Anti Commercial Fraud Law 2008

Another Law that works in conjunction with the ACL is the ACFL.[541] This legislation demands the conduct of business with due diligence and the avoidance of engaging in activities that involve any form of cheating, misleading or scamming of the consumer.[542] This legislation provides the Ministry of Commerce with the tools for tackling consumer-related retail fraud.[543]

Because of the ongoing use of technology in commerce, especially the internet, crimes listed in this legislation which are similar to the ACL can be committed in cyberspace.[544] Therefore, this legislation is useful when addressing the issue of cyberspace, especially in terms of criminal procedure. This legislation does not include electronic commercial fraud, mentioning only traditional forms of commercial fraud. Moreover, as has been mentioned in Chapter 2, the KSA generally deals with physical space in the same way it deals with virtual space in its legal response to cybercrime.[545] Therefore, this legislation can be applied to commercial electronic fraud.

The ACFL led to the distribution of commissioners who constitute, as Article 6 calls them, "judicial recording officers" across the Kingdom for the enforcement of this Law.[546] According to Article 5:

---

[540] Lyman (2011) 21-23
[541] ACFL
[542] Clyde (2014)
[543] ACFL Article 1
[544] Algarni (2012) 124-123.
[545] See Section 2.2
[546] Obeidat and Zaza (2017)

> "Officials from the Ministry, the Ministry of Municipalities and Rural Affairs, and the Saudi Food and Drug Authority, appointed pursuant to a decision by the Minister after obtaining the approval of their relevant authorities, shall be liable, jointly or severally, for recording and establishing violations of the provisions of this Law and shall be considered judicial recording officers. The mentioned officials shall be under the liability and supervision of the Ministry."[547]

This Article addresses the policing of commercial fraud. It allows the Minister of Commerce to appoint judicial recording officers from three different public entities (the Ministry of Commerce, the Ministry of Municipalities and Rural Affairs, and the Saudi Food and Drug Authority) to report crimes committed in light of this Law.[548] This means that these officers can exercise their authority of policing commercial fraud within cyberspace which means that they are officers who police a part of cyberspace in the KSA.

Articles 5 to 14 are about the procedures relevant to this Law in terms of policing, investigation, prosecution, and trial. Article 6 demonstrates how the officers can conduct their investigation of commercial fraud:

> "If the judicial recording officer has compelling grounds to believe that the provisions of this Law are being violated, he may collect samples of the suspected product for analysis and file a report on the incident. Said report shall include all data necessary to verify the samples and the product in accordance with the regulations." [549]

According to Article 6, they can, without notice or warrant, search and seize any product that they suspect to be a subject of commercial fraud in order to withdraw a sample

[547] ACFL Article 5.
[548] *Ibid* Article 6.
[549] *Ibid*

of the product to examine it.[550] The only requirement that the officer needs to execute his authority is to have suspicion, or as the Article describes it "compelling grounds" to search and seize.[551]

Similar to Article 6, Article 9 supports what could be viewed as general search and seizure powers when stating that:

> "It shall be prohibited to prevent the judicial recording officers from performing their duties in inspecting and recording violations, accessing factories, stores, shops or others, or obtaining samples of the suspected products. The judicial recording officers shall provide proof of their identity as recording officers. They may close down a shop until the retailer informs the owner of the shop and grants them access to the shop." [552]

Aside from the broad authority that Article 6 gives to officers, this Article is excessive because of the measure that people whose private premises are subject to investigation cannot refuse the search of their premises.[553] Additionally, the only permission that officers need for conducting investigation and searching premises is to provide a valid ID which proves their appointment to office.[554]

Even though the measures in Articles 6 and 9 might be seen as an effective way to catch violators, they are not fair because they may be arranged to violate the KSA law regarding criminal procedure as will be addressed in Chapter 5. These Articles contradict the standards of fairness in the KSA BLG and *Sharia* itself which both prohibit searching private premises with no further notice.[555] Article 36 of the KSA BLG indicates that a legal officer

[550] *Ibid*
[551] *Ibid*
[552] *Ibid* Article 9
[553] *Ibid* Article 6
[554] *Ibid* Article 9
[555] BLG Article 36

must have the permission for the search and seizure of private residences with the consent of the owner.[556] In the same regard, *Quran* states:

> "And it is not righteousness to enter houses from the back, but righteousness is [in] one who fears Allah. And enter houses from their doors."[557]

This is not only applicable for private residences, but also for all private premises as the KSA CPL indicates. Article 42 of the KSA's CPL 2013 states that:

> "A criminal investigation officer may not enter or search any private houses except in the cases provided for in the laws, pursuant to a search warrant specifying the reasons for the search, issued by the Bureau of Investigation and Prosecution. However, other private premises may be searched pursuant to a search warrant, specifying the reasons, issued by the Investigator. If the proprietor or the occupant of a dwelling refuses to allow the criminal investigation officer free access, or resists such entry, he may use all lawful means, as may be required in the circumstances, to enter that dwelling. A dwelling may be entered in case of a request for help from within, or in case of a demolition, drowning, fire, or the like, or in hot pursuit of a perpetrator."[558]

Under this measure, officers cannot search private premises without reasoned permission from the BIPP (the PP now). This provides a clear condition for searching private premises, which is having permission from PP when searching private houses and having permission from detectives when searching other private premises.[559]

However, vesting such power alongside the powers of investigation and prosecution in the PP might lead to their abuse. The reason why developed countries such as the UK do

[556] *Ibid*
[557] Holy Quran Chapter 2 Verse 189
[558] CPL 2013 Article 42
[559] This point will be discussed later in chapters 5 and 6 regarding powers of policing and investigation.

not vest the power of search and seizure in regard to issuing warrants in the hands of prosecutors, as the UK Police and Criminal Evidence Act 1984 (PACE)[560] indicates, is to secure the rights of accused and ensure that the state would not have too much power vested in one entity.

Moreover, Article 12 needs to be updated because it states that the BIPP investigates and prosecutes violations whereas, as has been discussed, the name has been changed to PP rather than BIPP.[561]

4.2.4 Civil or criminal violations?

It might be argued that violations listed in both the ACFL and the ETPL might be better handled as civil law than as criminal law matters. What gives rise to this argument is that those violations will be tried before civil committees not before the criminal court.[562] Even though the violators of these two statutes will not be tried before the CC, it is possible to say that the violations listed in these two statutes are treated like crimes, not as civil violations for two reasons. The first is that the investigation and prosecution of violators will take place in the office of the PP which only process crimes.[563] The second reason is that the punishment for such violations includes imprisonment which is usually a punishment for crimes not for civil violations.[564] This reflects the seriousness of the wrongdoing as it is viewed in the KSA.

[560] See PACE sections 8, 9
[561] KSA Royal Decree No. A/240 of 2017
[562] See ETPL Article 26 & ACFL Article 21
[563] Both Laws refer to the PP for investigation and prosecution.
[564] Wilson (2017) 50-66

4.2.5 Criminal Procedure Law 2013 – "CPL 2013"

All the specialist legislation that has been discussed up to this point refers to both the police force and the PP when it comes to investigating and prosecuting crimes. Therefore, since these legal provisions are related to the law of criminal procedure in KSA, the CPL 2013, which is general rather than specialist, will be evaluated in light of its ability to cope with cybercrime in terms of policing cybercrime and cyberspace, investigating, prosecuting, and trying cybercrime suspects. This Law does not include any provisions specifically related to cybercrime,[565] and only details the criminal procedures for NCCs. However, due to the absence of any legal provisions that deal with the special issue of cybercrime procedure, it can be said that cybercrimes in KSA are treated the same as NCCs in terms of procedure. It has already been indicated that the three forgoing measures – ACL, ACFL, and ETPL– refer to the BIPP (or as it has been officially renamed the Public Prosecution – "PP").[566] In fact, almost half of the 222 articles of the CPL are about the PP. This indicates that the PP plays the main role in dealing with crimes, including cybercrimes.

The CPL 2013 is not the first legislation that the KSA has passed in regard to criminal procedure, having passed another piece of legislation in 2001.[567] The CPL 2001 version had many flaws and breaches which its 2013 successor aimed to solve.[568] Most of the changes in the CPL 2013 are related to the language it uses, and there is little change regarding its fundamental flaws, such as technological and legal redundancy law.[569] Moreover, the CPL 2013 has proved to be disappointing in substance, since changes were not fundamental because both laws lack explicit recognition of the accused's rights for proper due process and

[565] See 2.2
[566] KSA Royal Decree No. A/240 of 2017
[567] CPL 2001
[568] Shareef (2016) 10.
[569] *Ibid*

the power of investigation and prosecution is vested in a single unspecialized governmental entity, which is the PP.

The CPL 2013 does imply the right to due process, but does not say so directly,[570] giving rise to the prospect of unfair practices. For instance, the first paragraph of Article 4 has directly recognized the right for the accused to legal representation and legal counsel during the whole criminal procedure.[571] However, the second paragraph of Article 4 says: "The regulations of this Legislation shall specify the rights of the accused to be defined."[572] Even though this might be effective from the perspective of law makers in the KSA,[573] it might not be in practice because it is vague and could be considered to be misleading. When laws are vague, their interpretations and applications are likely to reflect this vagueness.

One major factor where this vagueness can be demonstrated is the transference of legal models from other jurisdictions with insufficient regard to the major differences between them, especially the social and political differences.[574] The KSA transferred most of its legislation from Egypt in the second half of the 20th Century.[575] This pathway might have been effective for a particular period of time, especially during the establishment of the KSA as a state after 1932.[576] At the time of the establishment of the KSA, most of the KSA population were illiterate and knew little about legislation, and that is why the KSA needed help from Egypt.[577] Many Gulf Cooperation Council (GCC)[578] universities' academic staff, including in the KSA, in 1980s came from Egypt.[579] The Imam Muhammed Bin Saud Islamic University, which is one of the KSA's main universities, was founded in 1953 by

[570] Interview with Law Professor LP1
[571] CPL 2013 Article 4, Paragraph A
[572] *Ibid* Article 4 Paragraph B
[573] Interview with Law Professor LP2
[574] *Ibid*
[575] Interview with Law Professor LP1
[576] *Ibid*
[577] *Ibid*
[578] GCC <https://www.gcc-sg.org/en-us/AboutGCC/MemberStates/pages/Home.aspx>
[579] Mazawi (2003) 253-254

Egyptians.[580] This dependence on Egyptian education and legislation remains until today, as both of the Laws enacted in 2001 and 2013 respectively were inspired by Egyptian law.[581]

However, even though the Egyptian influence over the KSA has been strong, the Egyptian jurisdiction has not been analysed and compared to that of the KSA in this thesis for two reasons. The first is that Egypt has been governed by successive dictatorships that pass unfair laws regarding the criminal process of cybercrime, often because of political and security considerations;[582] the result of this is the establishment of an unjust system that limits the freedoms of Egyptian citizens within cyberspace and beyond.[583] In July 2018, the HRW noted that the Egyptian government had detained peaceful activists, including online activists, by applying Egypt's Counterterrorism Law 2015.[584] In addition to this measure, Egypt passed a new cybercrime law in 2018 to deal with online activists who are accused of serious cybercrimes, which in effect increases the ability of the government to censor internet services in Egypt, undermining the freedom of people to use it.[585] According the United Nations' Periodic Review of 2019, Egypt has violated international law and human rights by torturing prisoners until death and depriving them of due process.[586] Some of those prisoners have been arrested based on committing serious cybercrimes, as mentioned in the Counterterrorism Law 2015.[587] Ironically, some cybercrimes that are considered to be serious are simply criticism of the Egyptian government which, in more modern countries, would be viewed as a basic right and fall under the categories of freedom of speech and freedom of expression.[588] Egypt has been accused of arbitrarily arresting and imprisoning many people

[580] Lacroix (2011)
[581] Interview with Law Professor LP2
[582] York & Hunasikatti (2018)
[583] HRW (2018)
[584] *Ibid*
[585] York & Hunasikatti (2018)
[586] UN High Commissioner Office for Human Rights (OHCHR). Compilation on Egypt A/HRC/WG.6/34/EGY. 2019. 4
[587] *Ibid* 5
[588] *Ibid* 5

for committing cybercrimes without due process since the 2011 Revolution.[589] Although the current Egyptian approach toward cybercrime might be effective for the Egyptian government, it should not be viewed as a fair precedent for others because it violates international human rights.[590] Moreover, Egypt is neither a world leader in its approach to criminal procedure regarding cybercrime compared to, say, the UK,[591] nor an Arab leader in its approach to criminal process regarding cybercrime.

Nevertheless, one main reason that the CPL says nothing about cybercrime is that the Egyptian CPL does not say anything about it either.[592] What is noticeable is that the KSA began to show interest in cyberspace and cybercrime in 2007, when it passed the ACL and the ETPL, which was around the time. Similarly, there was growing interest in the laws in the GCC States[593] and in Western countries such as the UK and US.[594] Thus, in 2005 the King Abdullah scholarship program for studying abroad began and many of the KSA population have had very good education in leading countries such as the US and the UK in most disciplines[595] as a result, including cybercrime and cybersecurity. This experience is likely to have a positive impact on the KSA's approach to cybercrime in the future. However, even though studying abroad in developed countries is helpful for increasing the legal knowledge of the KSA citizens, it is necessary to have proper consideration of the social and political differences that prevail in the KSA.[596] One aim of the present thesis is to transfer policy from the UK's jurisdiction by following two steps. The first is to find common ground to base the transfer on and the second is to learn lessons through policy transfer from the UK and not to just copy and paste policy.

[589] Alexander & Aouragh (2014) 894-895
[590] York & Hunasikatti (2018)
[591] See Subsection 1.1; reasons for choosing the UK
[592] Egyptian Criminal Procedure Law No. 150 of 1950
[593] Hakmeh (2018)
[594] Wall (2007a)
[595] Interview with Law Professor LP3
[596] Alkhrashi (2005)

The CPL 2013 is the default legislation when dealing with the criminal procedure of crimes[597] including cybercrime in the KSA which will be addressed thoroughly throughout this thesis in Chapters 5, 6 and 7. The CPL introduces public provisions for criminal procedure and also delineates the stages of criminal prosecutions from criminal charges being brought forward to trial.[598] The process seems reasonable, and it specifies the role of criminal case officials and the rights of the accused.[599] However, this does not mean that the CPL has met the values of fairness and effectiveness when it comes to cybercrime because it fails to provide comprehensive solutions for the field of cybercrime, as will be discussed in the next subheadings.

4.2.6 Effectiveness and fairness of the KSA Criminal process legislation regarding cybercrime

As has been highlighted, the KSA treats the criminal process regarding cybercrime as being no different to traditional crimes.[600] The ACL, the ETPL, and the ACFL all have referred to the BIPP for criminal procedure even though the BIPP was renamed the PP in 2017,[601] and these pieces of legislation have not yet been changed accordingly, which presents a clear picture of the necessity of updating the KSA's legislation. The PP executes the CPL 2013 for all crimes whether they be NCCs or cybercrimes. This legislation has no mention of cybercrime in it, as has been discussed in Subsection 4.2.5. Therefore, an assessment of both effectiveness and fairness in regard to the CPL 2013 will be conducted, and the other legislation will be excluded from the assessment because they are more focused on substantive criminal law rather than procedural criminal law. The test for both fairness and

[597] Shareef (2016) 9
[598] *Ibid*
[599] *Ibid*
[600] See Section 2.2
[601] KSA Royal Decree No. A/240 of 2017

effectiveness of the CPL 2013 will cover three matters: uncertainty, design, and delivery. This will be done on three different levels: conceptual, international or comparative, and national levels. The measurements of each were set out in Chapter 2.[602]

4.2.6.1 Effectiveness of the KSA Criminal process in dealing with cybercrime

According to the conceptual meaning discussed in Chapter 2,[603] effective law means that the law is successful in achieving its objectives.[604] Therefore, the question remaining here is whether or not the criminal procedure regarding cybercrime successfully achieves its objectives. In achieving its objectives, a law must be characterised as being clear, precise and unambiguous regarding its objectives, context, results and the content of the law.[605] Before jumping to any conclusion, in testing the success of the criminal procedure when dealing with cybercrimes, it is essential to demonstrate what objectives this law seeks. Therefore, the objectives of the CPL 2013 will be illustrated in order to test whether this legislation has been successful in achieving its drawn objectives.

Since there is no official published record regarding the objectives that the CPL 2013 seeks to achieve,[606] it is better to look into the literature to discover the CPL 2013's objectives. The first objective of the CPL 2013 is ensuring that justice is fairly delivered by utilising a fair process.[607] The second objective is to guarantee the rights of the accused and protect those rights from being violated.[608] The third objective is to protect human rights from being violated.[609] The fourth objective is to speed up the criminal process.[610] Based on these

[602] See Section 2.4
[603] See Subsection 2.4.1.1
[604] *Ibid*
[605] *Ibid*
[606] Khalifa (2019) 14-15
[607] *Ibid* 14-15
[608] *Ibid* 14-15
[609] *Ibid*
[610] *Ibid*

objectives, it is possible to say that the CPL 2013 seeks to deliver justice by punishing the criminal, exonerating the accused innocent, protecting the rights of the accused, and ensuring justice is delivered without delay. Therefore, the question arising from those objectives is whether or not the CPL 2013 successfully achieves its objectives.

In practice, the criminal procedure legislation has achieved positive results regarding all objectives, mainly because it has limited the extensive powers that the PF had before issuing CPL 2001[611] (the CPL 2013's predecessor). Before 2001, the KSA police used to wield the powers of investigation and prosecution alongside their policing power which has, as would perhaps be expected, caused miscarriages of justice due to the violation of the principle of the Separation of Powers.[612] After passing the CPL 2001, investigation and prosecution powers were passed to the new established entity; the BIPP,[613] which has been renamed PP in 2017.[614] As discussed in Subsection 4.2.5, the CPL 2001 is similar in content to the CPL 2013, and there were no significant changes made by the KSA by the passing of this new Law. Therefore, it can be said that the objectives of both pieces of legislation are identical. The reason the CPL has successfully achieved its objectives is that, before CPL 2001, there were no recognition for the rights of the accused except for basic standards known between police officers,[615] who were investigators and prosecutor in the same time,[616] such as providing detainees with food and drink, so they do not suffer from deprivation.[617] Also, there were instances of torturing detainees in order to obtain confessions.[618] This could be the practice before the separation of policing, investigation and prosecution powers in

[611] Interview with Detective of the PP D1
[612] Alshathri (2015) 19
[613] Aldosari (2019) 75
[614] KSA Royal Decree No. A/240 of 2017
[615] Interviews with Police Officers PO1, PO2 and PO3
[616] *Ibid*
[617] Interview with Police Officer PO2
[618] Interview with Police Officer PO1

2001.[619] Therefore, in comparing between the police practices before 2001 and afterwards, particularly after the transference of the powers of investigation and prosecution to the BIPP in 2001 and specifying its role in CPL 2001, it can be seen that a higher degree of justice has been ensured, more rights have been recognised and protected, and a more fair criminal procedure has been implemented and followed. This change occurred after 2001, and it enhanced the rule of law in the KSA, even though the CPLs of 2001 and 2013 fall short of the international standards of fairness, as will be addressed later in this section.

Nonetheless, 20 years after the CPL 2001, the legislation remains basically the same, despite some minor changes that are neither fundamental nor noticeable – even to law experts.[620] The need for changing or modifying the CPL 2013 comes from the KSA's desire to modernise the country. As the KSA progresses toward this goal, it can be said that the CPL 2013 fails to achieve effectiveness in tackling crime generally – particularly cybercrime – because the CPL 2013 aims to deliver fairness. However, it failed to reach international standards of fairness as will be discussed later in this section.

Moreover, based on comparative standards of effectiveness, as addressed in Chapter 2,[621] the CPL 2013 has not managed to comply with the comparative concept of effectiveness in combating cybercrime procedurally. Unlike the UK,[622] the KSA does not differentiate between cybercrime and NCCs in terms of the criminal procedure, even though there are multiple differences between the two which have been introduced in Chapter 2[623] and section 4.1 of this chapter. No single article in the KSA CPL 2013 mentions cybercrime. This undifferentiation between the two types of crimes in terms of procedures might cause

[619] Interviews with Police Officers PO1, PO2 and PO3
[620] Interviews with Law Professors LP1 and LP2
[621] See Subsection 2.4.1.2
[622] UK NCSS 2016-2021
[623] See Subsection 2.2.2

violations of the human rights, especially privacy, which would result in greater unhappiness and, therefore, conflict with the comparative standards of effectiveness.

In contrast, the KSA CPL 2013 seems to be in line with the KSA's standards of effectiveness, which is introduced in Chapter 2.[624] In the KSA, the most essential characteristic for a law to be considered as being effective is full compliance with the principles of *Sharia,* as understood and applied in the KSA;[625] if a law conflicts with these principles, it will not be considered to be effective.[626] Based on the KSA's standard of effectiveness, it is possible to say that the KSA CPL 2013 is compatible with *Sharia*, so it is nationally considered to be effective.[627] Moreover, based on the objectives of the CPL 2013 mentioned in this section, the KSA state seems to claim that the CPL 2013 is effective because it has delivered a higher degree of justice and better protected the rights of the accused than was the case before 2001. Nevertheless, in Chapter 2, the link between effectiveness and fairness of the law has been identified as a "trump card."[628] This means that it not enough for the law to be effective because fairness "trumps" effectiveness.[629] In other words, the law must respect and be in line with concepts of individual rights, irrespective of how effective is the outcome.

4.2.6.2 Fairness of the KSA Criminal process regarding cybercrime

A test of fairness of the KSA criminal procedure regarding cybercrime will be conducted based on the standards of fairness mentioned in Chapter 2.[630] As has been discussed in that chapter, according to the conceptual standard of fairness, "fair law" means a

[624] See Subsection 2.4.1.3
[625] *Ibid*
[626] BLG Article 7
[627] Interviews with all Police officers PO1, 2 and 3, Detectives and Prosecutors of the PP D1, 2 and 3, PP1 2 and 3, Criminal Defence Lawyers CL1, 2 and 3, CCJs 1, 2 and 3, Law Professors 1, 2 and 3
[628] See Subsection 2.4.3
[629] *Ibid*
[630] See Subsection 2.4.2

just law which does not favour one group over another or discriminate between them.[631] It must be just in the eyes of the community by using an appropriate and proper process to reach fair decisions (procedural fairness), and it must be just in the eyes of a community by reaching fair results (substantive fairness).[632] The CPL 2013 does not favour or discriminate, yet when applying the standards of fairness of international law, it is possible to observe its injustice.[633] This could give rise to the problem of uncertainty because the CPL 2013 does not give much attention to basic human rights in relation to due process. There are four human rights regarding due process, as discussed in Chapter 2; the reasoned and justified basis for detention and trial, the right to an attorney, the right to an unbiased judge, and the right to a fair trial.[634]

Beginning with arrest and detention, there is no single clear article in the CPL 2013 which prevents arbitrary arrest or prevents detention without reason. Although the CPL 2013 does not allow arbitrary arrest, it is not precise. Article 2 of the CPL 2013 says:

> "No person shall be arrested, searched, detained, or imprisoned except in cases specified by the law. Detention or imprisonment shall be carried out only in the places designated for such purposes and shall be for the period prescribed by the competent authority. A person under arrest shall not be subjected to any bodily or moral harm. Similarly, he shall not be subjected to any torture or degrading treatment."[635]

The beginning of the article seems promising, but when it says, "specified by the law", it does not mention which laws allow detention and arrest. Similarly, Article 36

[631] ICCPR Article 2
[632] Franck (1995) 6–9, 47
[633] The CPL does not favour or indiscriminate in general yet that might be wrong because the executive regulation for the criminal procedure law 2015 does not allow arresting ministers or former ministers.
[634] See subsection 2.4.2
[635] CPL 2013 Article 2

recognises the right for the detainee to know why they are being detained.[636] In practice, police officers have abused their power by arresting and detaining people without a proper reason and based on what they consider to be a crime, often for grounds which are not clearly forbidden by law but which may infringe morality.[637] Similarly, detectives have kept many people detained for more than 5 days – which is the maximum period specified by Article 20 of the CPL 2013[638] – because those suspects have committed activities that are thought to be crimes based on *Sharia*,[639] even though Article 3 of the CPL 2013 forbids punishing people without 'texts' founded in legislation and *Sharia*.[640] One such example of this contravention of human rights is being punished for playing music in public restaurants using electronic devices, which could be punishable as a cybercrime.[641]

Next, even though the CPL 2013 recognises the right to an attorney or legal representation during the criminal process,[642] many accused of committing a cybercrime do not hire a lawyer, often because they cannot afford it, or for other reasons that will be addressed fully in Chapter 6. In order to avoid miscarriages of justice, more developed countries such as the UK provide a legal counsel for those who cannot afford it in order to protect their right for an attorney.[643] The KSA does not fully secure this important right within its CPL that only allows for legal aid during the trial stage but not during other stages,[644] as will be addressed in Chapter 7. Therefore, it could be possible to say that having legal texts that mention the human rights regarding due process would not be fair if the State does not take all measures necessary to secure those rights in practice.

---

[636] *Ibid* Article 36 Paragraph 1
[637] Alshathri (2015) 22-23
[638] CPL 2013 Article 20
[639] Alshathri (2015) 23
[640] CPL 2013 Article 3
[641] Alali (2016) 33
[642] CPL 2013 Article 4 Paragraph 1
[643] UK Government <https://www.gov.uk/arrested-your-rights/legal-advice-at-the-police-station>
[644] CPL 2013 Article 139

Moreover, the right to due process through unbiased judges is not completely protected under the CPL 2013, because Article 146 says:

> "Subject to the provisions of Section 3 herein relating to order and control over hearings, the refusal and dismissal of judges shall be subject to the provisions of Sharia Procedure Law. A judge shall be precluded to try the case if the crime has been committed against him at times other than court hearings."[645]

Even though this Article seems to secure the right for an unbiased judge, it only refers to civil legislation, which stipulates that judges should be stood down whenever there is a conflict of interest.[646] The KSA seems to secure this right, however, judges in the KSA only need to be *Sharia* certificate holders, and often know little about the law which they claim to protect alongside *Sharia*.[647] Therefore, as long as judges in the KSA only hold *Sharia* certificates, the right for an unbiased judge is in jeopardy because law certificate holders have greater expertise in law than *Sharia* certificate holders.[648] This practice by the State is more likely to lead to unfair trial and consequently deliver injustice, especially when knowing that judges can, in accordance to the CPL 2013, reinvestigate the accused with less regard to the initial investigation done by the PF or the preliminary investigation done by the PP.[649] However, this argument might not be water-tight because many States with a fair approach are inquisitorial and allow judges to investigate, such as in France.[650] Even though such jurisdictions do not fall under the scope of this thesis, it worth mentioning that those

[645] CPL 2013 Article 146
[646] Sharia Procedure Law 2013 Article 94
[647] This will be addressed fully in Chapter 7 when discussing judicial institutions related to the trial of cybercrime.
[648] Interviews with Law Professors LP1, LP2 and LP3 and Criminal Defence Lawyer CL3
[649] Alshathri (2015) 30
[650] Aldosari (2019) 17-50

States do not allow for the vague powers allowed by *Sharia*[651] to accompany investigation, and they mostly specify judges as being in charge of investigation[652] (roughly equivalent to the PP in the KSA).[653] Moreover, to be unbiased, judges should first be independent, second allow for opportunities for defence representations, and third give open reasoning for decisions.[654] Beside judges, the law should allow for the appeal and correction of miscarriages of justice.[655] In contrast, judges in the KSA have an enormous amount of power given by the law. As discussed in Section 4.3.3 of this chapter, judges can overrule legislation with *Sharia* being a trump card. Additionally, they can reinvestigate the accused, determine whether the accused is guilty or not and, finally, they can determine a suitable punishment for each crime.[656] Having such judicial powers vested in one person could result in injustice, yet these excessive powers are approved by the CPL 2013, as will be discussed in Chapter 7.

At the international level, the KSA's CPL 2013 seems to fail in terms of fairness, but when applying the national standards of fairness,[657] the CPL 2013 seems to meet those standards which mainly lie in complying with *Sharia* as stipulated by the BLG. However, the test for fairness has been here conducted based on international human rights standards, and not national standards alone.[658]

[651] See Subsection 7.4.2
[652] Aldosari (2019) 17-50
[653] The PP considered as a judicial authority. See 7.2.1
[654] Shaman (1996) 618 and 622
[655] *Ibid* 618
[656] Alshathri (2015) 30
[657] See Subsection 2.4.2.3
[658] See four rights specified in p 121

4.3 The Role of *Sharia* with regard to the criminal process legislation in the KSA concerning cybercrime

As has been shown in Chapter 2,[659] according to Article 1 of the KSA BLG, *Sharia,* which is mainly rooted in *Quran* and *Sunnah,* is the supreme law of the land.[660] Additionally, in accordance with Article 7 of the same law, all legislation in the KSA must be issued in compliance with *Sharia*.[661] This hypothetical compliance in the BLG includes the legislation about the criminal procedure as it relates to cybercrime in the KSA. Therefore, based on the BLG, it is arguably true when assuming that all legislation in the KSA is in line with *Sharia.*

However, it could be argued that it is unfair to apply the very traditional rules of *Sharia* to very modern phenomena taking into consideration that it mentions nothing in regard to those phenomena, such as cybercrime and cyberspace.[662] In response to such concerns, it could be possible to say that even though *Sharia* does not regulate any of the modern phenomena including cybercrime and cyberspace, it is within the texts of the *Quran* and *Sunnah* to allow the regulatory power to be shared between the *Walee alamer* (Guardian) and the Muslim *Ummah* (nation).[663]

In this section, an evaluation of the influence of *Sharia* over the KSA's legal system, especially in regard to criminal procedure of cybercrime, will be addressed in order to fulfil the aims of this thesis. To reiterate, it is an aim of this thesis to analyse the deficiencies of the KSA's CPL regarding cybercrime. Also, it is an aim to test whether the KSA's law of criminal procedure is fair and effective. These aims cannot be comprehensively met without evaluating the correlation between *Sharia* and the KSA law. Therefore, this section will draw

[659] See Section 2.2
[660] BLG Article 1
[661] *Ibid* Article 7
[662] Haddad & Stowasser (2004)
[663] Naseeb et al (2011) 500-502

the main features of the correlation between the KSA law and the *Sharia*, by beginning with the main principles that the *Sharia* provides the KSA's CPL to deal with cybercrime.

4.3.1 The principle of obeying the *Walee alamer*

One of the basic principles of *Sharia* is to obey the *Walee alamer* of the *Ummah.*[664] Both *Quran* and *Sunnah* encourage Muslims to have absolute obedience to their *guardian* unless they are being directly ordered to oppose *Sharia*.[665] The Quran explains the hierarchy of such obedience.

> "O you who have believed, obey Allah and obey the Messenger and those Guardians among you. And if you disagree over anything, refer it to Allah and the Messenger, if you should believe in Allah and the Last Day. That is the best [way] and best in result."[666]

The Prophet Muhammed says:

> "A Muslim must hear and obey the guardian of the Muslims in what is pleasant and unpleasant, unless ordered to commit a sin and, if to be ordered to commit a sin, then neither hearing nor obedience [is permitted]."[667]

Aside from his commands to obey *guardians*, he says, "There is no obedience to the creation when it entails disobedience to the Creator."[668]

The KSA views its King and higher authorities as *Walee alamer*.[669] Its BLG states that:

> "Citizens shall pledge allegiance to the King on the basis of the Holy Quran and the prophet's Sunnah, as well as on the principle of hearing and obeying

[664] *Ibid*
[665] Udah (2009) 100
[666] Holy Quran Chapter 4 Verse 59
[667] Albukhari 810-870 AD (Vol. 9, Book 89, Hadith 258)
[668] Alsuuti 849-911 AD (No 7520).
[669] *Ibid*

both in straitened circumstances and prosperity and in pleasant and unpleasant times.[670]"

Additionally, it states:

"The King shall run the affairs of the nation in accordance with the dictates of Islam. He shall supervise the implementation of Sharia and the general policies of the State, and the protection and defense of the country."[671]

In compliance with the principle of Obedience for *Walee alamer* and the BLG, Kings of the KSA have been issuing legislation in response to modern phenomena,[672] including cyberspace and cybercrime (as already indicated). Therefore, it is possible to say that, even though *Sharia* does not explicitly say anything regarding cybercrime or cyberspace, it allows the *Imam* (governor) of a Muslim population to determine, on their behalf, what is in their best interests as long as it does not conflict with the *Quran* and *Sunnah.*[673]

4.3.2 The Principle of *Shura*

Another principle of governance within *Sharia* is the principle of *Shura* (consultation).[674] The *Quran* encourages both a leader of Muslims and their Muslim subjects to consult one another in all matters in order to reach resolutions.[675] In the *Al Shura* chapter, the *Quran* says:

"…and those who answer the call of their Lord, pray regularly, conduct their affairs by mutual consultation and give of what We have provided them..."[676]

Furthermore, it says in another chapter:

[670] BLG Article 6
[671] BLG Article 55
[672] Shalhoob (1999) 30
[673] Udah (2009) 80-81
[674] BinAbdulaziz (2002) 198-209
[675] *Ibid*
[676] Holy Quran Chapter 42 Verse 38

> "So by a mercy from Allah, [O Muhammad], you were lenient with them. And if you had been rude [in speech] and harsh in heart, they would have disbanded from about you. So pardon them and ask forgiveness for them and consult them in the matter. And when you have decided, then rely upon Allah. Indeed, Allah loves those who rely [upon Him]."[677]

For the purpose of complying with the principle of *Shura*, the KSA founded the *Shura* Council in 1992.[678] The role of the *Shura* Council has been identified in the BLG as a legislative branch of the government, along with the KSA cabinet (Council of Ministers)[679] in Articles 8, 67, 68, 69 respectively.[680] Article 8 of the BLG recognises the principle of *Shura*:

> "The system of governance in the kingdom of Saudi Arabia is based on justice, consultation (Shura) and equality according to the Islamic Sharia."[681]

Additionally, Article 67 states:

> "The Regulatory Authority shall be concerned with the making of laws and regulations which will safeguard all interests and remove evil from the State's affairs, according to Sharia. Its powers shall be exercised according to provisions of this Law, the Law of the Council of Ministers and the Law of the Shura Council."[682]

Furthermore, Article 68 says:

---

[677] Holy Quran Chapter 3 Verse 159
[678] Al Shura Council. Shura in the KSA <https://shura.gov.sa/wps/wcm/connect/ShuraEn/internet/Historical+BG/>
[679] Shalhoob (1999) 81
[680] BLG Articles 8, 67, 68 and 69
[681] *Ibid* Article 8
[682] *Ibid* Article 67

> "The Shura Council shall be established. Its Law shall specify the details of its formation, powers and selection of members. The King may dissolve and reconstitute the Shura Council."[683]

Lastly, Article 69 mentions:

> "The King may summon the Shura Council and the Council of Ministers for a joint session. He may summon others whom he deems necessary to attend the meeting and discuss whatever affairs he considers fit."[684]

Therefore, *Shura* is an Islamic principle for making legislation,[685] and it is thus possible to say that *Sharia* has left the decision to the *Ummah* along with the *Walee alamer*, which they would ideally arrive at through mutual consultation.[686] Therefore, the KSA can combat cybercrime in a procedural sense through the power of legislation is shared between King and the *Shura* members, as the *Al Shura* Council Law 1992 indicates.[687] For instance, the ACL was issued after it had been passed and approved by (68/43) resolution of the *Shura* Council in 2006.[688] Another example is that the CPL 2013 was passed based on the resolutions of the *Shura* Council (96/68) 2010 and (139/59) 2012.[689]

The *Sharia* scholar *Udah* has compared the principle of *Shura* as being equivalent to democracy in so far as it allows the people to choose their own fate.[690] He even goes further and states it is better than democracy because, unlike democracy, *Shura* is an old principle which continues to be applied throughout the centuries within Muslim countries.[691] However, this comparison could seem to lack credibility because it seems to be based on defending a belief that he, as is the case with many other *Sharia* Scholars, is religiously obligated to

[683] *Ibid* Article 68
[684] *Ibid* Article 69
[685] Shalhoob (1999) 83
[686] BinAbdulaziz (2002) 198-209
[687] Al Shura Council Law 1992
[688] ACL
[689] CPL 2013
[690] Udah (2009) 37-41
[691] *Ibid*

protect and apply *Sharia* to every aspect of life,[692] including modern phenomena in politics and law. Those previous discussions ultimately lead to the question: is *Sharia* fair and effective?

4.4 Fairness and Effectiveness of *Sharia*

Is *Sharia* fair and effective as applied to KSA criminal procedure? The measurements for such analysis have been introduced in Chapter 2,[693] and are comprised of a conceptual measurement, an international and comparative measurement and a national (KSA) measurement.

At this outset, it might be argued that this discussion will be biased because the researcher, as a Muslim and a citizen of the KSA, will be sympathetic to the applications of *Sharia* to the KSA CPL regarding cybercrime. It is a religious obligation for the researcher to defend his own belief as *Sharia* dictates.[694] In order to combat bias, a critique for the current approach of Muslim countries especially the KSA in light of applying *Sharia* to the criminal procedure regarding cybercrime will be provided based on academic literature rather than overt subjective beliefs.

4.4.1 Effectiveness of *Sharia*

It has been said in Chapter 2 that effectiveness in a legal sense means clear, precise and unambiguous policy in its contexts, results and contents which successfully achieves its objectives.[695] This broad definition for effectiveness gives a clear vision of what the law

[692] Alshwaeer (2008) Vol 6 page 31
[693] See chapter 2 section 2.4
[694] Alshwaeer (2008) Vol 6 page 31
[695] See chapter 2 subsection 2.4.1.1

should be in order to be considered as effective. In order to test whether *Sharia* is effective, the ability for *Sharia* to regulate should be tested in the first place.

Sharia is a system that Muslims believe they must obey and apply at all times.[696] It has within it many principles that could have affect the law[697] as well as culture.[698] Therefore, it is possible to say that *Sharia* is a fundamental part of Muslim identity.[699] Most Muslims understand the inherent tolerance of Islam and take it as their underlying approach.[700] However, some Muslims apply *Sharia* to the law in a wrongful way;[701] *Sharia* has been intentionally misinterpreted and applied by some authoritarian rulers.[702]

However, *Sharia* might have a greater ability to regulate and help in delivering a just system, only if interpreted by *Sharia* experts who have a great knowledge of law, including both *Sharia* and secular legal systems, in order to cope with the current international laws and human rights.[703] Many of the *Sharia* principles have striking similarities to international laws and human rights laws,[704] which provides evidence that *Sharia* could regulate affairs effectively.

4.4.1.1 The effectiveness of *Sharia* from a conceptual perspective

When measuring the precision and clarity of *Sharia*, it can be said that *Sharia* is broad, flexible and open to interpretation[705] which can also make it imprecise, unclear and ambiguous compared to the laws of modern societies. Due to its imprecise, unclear and ambiguous contents, some might argue that it is unable to achieve its broader objectives that

[696] Hallaq (2009)
[697] Udah (2009) 30.
[698] Hoffer (2002 copy)
[699] Hallaq (2009) 22
[700] Udah (2009) 10
[701] Alsulami (2014) 142
[702] Smock (2002) 3-7
[703] Taha (2009) 1-8
[704] *Ibid*
[705] Alsulami (2014) 1-37

lie in helping to fight the evil within one's own soul and replacing it with good qualities of character in order to protect the five necessities; life, religion, intellect, property, and offspring.[706] *Sharia*, especially as represented by the *Quran*, could be understood inaccurately by ordinary Muslims or non-Muslims alike.[707]

It is possible to say that whosoever wants to interpret *Sharia* correctly must have an adequate knowledge of classical Arabic, history of Quranic verses, jurisprudence of *Sharia* and prophet Muhammed's *Sunnah*.[708] Unfortunately, most people, including KSA citizens, have an inadequate knowledge about *Sharia* because of its ancient language.[709] Therefore, it can be said that most of the recent criticisms for *Sharia* have been made by people who have limited knowledge,[710] and they have used this limited knowledge to challenge the ability of the *Sharia* to deliver a just system. In contrast, skilled experts who possess adequate knowledge of *Sharia* and Arabic, would not view *Sharia* as imprecise, unclear and ambiguous.[711]

However, even if well understood, it can be said that *Sharia* is not law in the way people understand that term in modern times, and there are various major differences between *Sharia* and law. The first difference is the content. *Sharia* contains many provisions that regulate life.[712] However, many of those provisions are only guidance for Muslim individuals to practice their religion, control their behaviour and strengthen their relationship with *Allah*.[713] In fact, less than 100 out 6,236 verses in *Quran* are about actual legal issues including family law, contact law and criminal law.[714] In contrast, the content of modern laws

[706] Maghaireh (2008) 341
[707] Alsulami (2014) 140-160
[708] Udah (2009) 40
[709] Alsulami (2014) 140-160
[710] *Ibid* (2014) 140-160
[711] Interview with Sharia Expert SE1
[712] Hellman A (2016)
[713] *Ibid*
[714] *Ibid*

is more precise in dealing with legal issues.[715] Secondly, the source (authority) of where *Sharia* comes from – Allah as Muslims normatively believe[716] – which is different from what people know of as law in the modern world, whereby people expect national sovereigns to produce laws, not God.[717] Thirdly, *Sharia* is not systematic in the same way that modern law is. In a legal system, people expect laws to cover a comprehensive range of issues[718] which *Sharia* does not. Lastly, there are many interpretations and schools that have produced different versions of *Sharia*,[719] whereas the clarity and preciseness of modern laws limit such differences.[720] Therefore, *Sharia* is better viewed as a source of law, but not the law in itself, as is the case in some Muslim countries such as the UAE,[721] Egypt[722] and Kuwait.[723]

In regard to the relationship between criminal procedure and *Sharia*, the KSA BLG States that:

> "The Judiciary is an independent authority. The decisions of judges shall not be subject to any authority other than the authority of the Islamic Sharia."[724]

This means that judges in the KSA can overrule any legislation that they view as incompatible with *Sharia* using their right of exercising *Ijtihad*,[725] which will be addressed fully in Chapter 7. CCJs have overruled Article 3 of the CPL 2013, which stipulates that no person shall be punished unless they have been convicted of a crime punishable in *Sharia* or in the legislation[726] by employing their own interpretation of *Sharia* for punishing but not

[715] Lloyd (1981 copy) 7-10
[716] Udah (2009) 11
[717] Lloyd (1981 copy) 44-45
[718] *Ibid*
[719] Udah (2009) 19
[720] Lloyd (1981 copy) 7-10
[721] UAE Constitution
[722] Egypt Constitution Article 3
[723] Kuwait Constitution Article 2
[724] BLG Article 46
[725] See Section 2.3
[726] CPL 2013 Article 3

convicting accused people whose criminal cases lack evidence.[727] The result appears to be arbitrary.[728]

In summary, as has been discussed earlier, *Sharia* sets up a number of principles for Muslim states to consider with regard to governance, such as the principle of *Shura*.[729] Therefore, deciding upon legislation for combating cybercrime in a procedural sense is up to the state and not to *Sharia*, which has no precedents to draw upon that can be directly related to modern phenomena such as cybercrime. One of the reasons some Muslim countries have more effective laws than others in combating crimes (including cybercrime) is that those which have more effective laws treat *Sharia* as being a source of legal guidance, but not the only one.

4.4.1.2 The effectiveness of *Sharia* from a comparative perspective

It has been stated in Chapter 2 that one of the main comparative measurements for testing the effectiveness of laws is what the UK considers within its legal system.[730] The idea of utilitarianism, or John Stuart Mill's "greatest happiness principle"[731] can be used for measuring the effectiveness of UK laws, including procedural law related to cybercrime.

As in Chapter 2, in general, utilitarianism is about ensuring and achieving the greatest happiness for the greatest number of people.[732] Therefore, the state should be neutral and not intervene in people's choices,[733] yet the state can still provide facilities such as the internet to ensure more prosperity for its citizens. Therefore, it can be said that utilitarianism is not about

[727] See Subsection 7.5.1.1
[728] By contrast, judges in the UAE bound by legislation and, with the exception of judges in the Supreme Court, they cannot overrule existing legislation. See UAE Constitution. Article 99
[729] See subsections 4.3.1 and 4.3.2
[730] See Subsection 2.4.1.2
[731] Mill (2009 copy) 2
[732] *Ibid* 8 and 43
[733] *Ibid*

eradicating moral wickedness and applying moral codes to make people good, unlike the *Sharia* that seeks to achieve these aims among Muslims.

Similar to utilitarianism, *Sharia* ensures happiness to its followers. For instance, *Sharia* did not view the internet and its use when it first became public, as being immoral.[734] In fact, based on the principle that the *Ulama* (*Sharia* scholars) have agreed on "All things are permissible [Halal] unless it has been directly prohibited [becomes Haram] by texts of Quran and Sunnah";[735] so the internet is not prohibited by *Quran* and *Sunnah*, and Muslims can enjoy it along with all other things that are not *Haram*. However, strict Muslims have other views based on another principle from *Ulama*: "Ward off harms before bringing interests."[736] They have viewed the use of the internet as *Haram* due to illogical reasons which are not based on reality or *Sharia*, such as the notion that the internet has been created by infidels who want to undermine Islam and brainwash Muslim youths with atheistic materialistic ideologies.[737] This strictness cannot be justified by *Sharia*, but many Muslims have followed this misinterpretation and others similar to it.[738] This view of *Sharia* cannot be easily changed and replaced with the true view on *Sharia* which ensures happiness to its followers if followed correctly.[739]

When applying the UK's measurement of effectiveness to the laws of many Muslim countries which are inspired by *Sharia*, it would be possible to say that those laws, including the laws of criminal procedure regarding cybercrime, are ineffective because they achieve neither *Sharia's* objectives nor the objectives of legislation. Consequently, it is the predictable tendency for people to blame *Sharia* for such ineffectiveness since *Sharia* is the

[734] Some of modern western innovations have been viewed as evil tools by Ulema such as TV, Smartphones, and the Internet. See Alatawneh (2008) 117-119
[735] Abo Zaid (2010) 247
[736] *Ibid*. 247
[737] Alatawneh (2008) 118-119
[738] *Ibid*
[739] Alghazali (1910 translation)

clearest common link between Muslim countries.[740] Moreover, many of those countries lack the expertise to devise effective laws that are equally compatible with *Sharia* and international laws and human rights.[741] Even though some Muslim countries have a great number of experts who could come up with effective criminal procedural laws regarding cybercrime, they are being ruled by less expert authorities.[742]

Therefore, it could be possible to say that *Sharia* does not fail in delivering effective legislation to tackle cybercrime in a procedural sense. It is Muslims alone who fail to deliver effective laws because they have been blinded by the strictness of *Walee alamer*. Therefore, it can be true to say that if *Sharia* is applied carefully and precisely, it could ensure the greatest happiness for the greatest number of people,[743] and it could be consistent with comparative standards of effectiveness.

4.4.1.3 The effectiveness of *Sharia* from a national perspective

The national measurement for the effectiveness of law has been introduced in Chapter 2.[744] As the BLG states, in order for the legislation to be effective, it must comply with the principles of *Sharia*, especially the provisions in the *Quran* and *Sunnah*.[745] This measurement is for legislation made by the KSA, but the question arises as to what the measurements for the effectiveness of *Sharia* are as found in *Quran* and *Sunnah.* Many Quranic verses and statements of the Prophet Muhammed show that *Sharia* is effective when applied because it entails obedience to the commands of *Allah*.[746] This is a broad measurement which seems difficult to apply. Therefore, in order for this broad measurement to be applicable, it should

[740] Taha (2009) 8
[741] Interview with Law Professor LP1
[742] Feldman (2008)
[743] Alghazali (1910 translation)
[744] See Subsection 2.4.1.3
[745] BLG Article 7
[746] Udah (2009) 50

be narrowed down to the application of the main rules of governance found in the *Quran* and *Sunnah* to Muslim states.

In order to achieve such effectiveness, *Sharia* should be codified so that it is not viewed as being a vague, traditional or outdated system.[747] There have been many attempts by jurists to codify *Sharia* within Muslim countries, including the KSA.[748] However, none of those codification attempts have been adopted due to power struggles between jurists who want to modernise *Sharia* and zealots who see law experts as being the enemy of religion and the rule of *Sharia*.[749] Consequently, they have opposed the codification project in every instance, usually with the support of authoritarian governments and an indoctrinated public.

In the KSA, an era of ultra-literal and strict Islam began following Muhammed Bin Abdulwahab's crusade (after whom the subsequent movement Wahhabism was named) in the middle of the 18th Century in Najd (the centre of the Arabic peninsula).[750] Wahhabism's main purpose is to spread what he considered the true massage of Islam, emphasising the worship of the One God – *Allah* – and loyalty to the Muslims and disloyalty to non-Muslim.[751] Abdulwahab's religious movement constituted rebellion against the *Caliph* (successor of the Prophet) and it was joined with a political agenda.[752] He agreed with Muhammed Bin Saud (the first ruler of House of Saud which constitutes the Royal family in the KSA) that the House of Saud should take over the political power of the Arabic peninsula, and he (the House of Sheik) should take over the religious power.[753] The movement succeeded, and the two houses have been honouring their agreement ever since.[754] His strict view of Islam resulted years later in the phenomenon of strict dissenters within Muslim countries, especially

[747] Abdulaati (2019) 1-3
[748] Aljare'e (2010)
[749] Alajloni (2004)
[750] Alfahad (2004) 488
[751] *Ibid* 490
[752] Aldakheel (2013) 52
[753] *Ibid*
[754] Alatawneh (2009) 721

the KSA.[755] An example is the *Juhayman* incident, which involved the invasion of the Holy Mosque in Makkah in 1979, and which caused the infamous *Sahwah* (awakening) movement in 1979 within the KSA,[756] and which was inspired by Wahhabism.[757]

Sahwah's main objective is to reform people whom they see as being morally corrupted by leading them to the "correct" Islam.[758] The *Sahwah* movement eventually weakened after 2007 until it is faded out in 2017.[759] Yet still, *Sahwah* has had an enormous impact on almost all domains within the KSA, including law and policy.[760] Many of the strict *Sahwah* members wield power and influence and were able to influence the public with their ideology in a way which was completely unprecedented, especially during its peak, from 1979 to approximately 2007.[761] Also, during those years, many official authorities changed their policies to cope with the new idea that the government must only apply *Sharia* and nothing but *Sharia*.[762] Many of influential *Ulama* at that time opposed laws even though they do not conflict with *Sharia* because they view the modern concept of law as contradicting with *Allah's* commands and prohibitions as it is inspired by non-Muslim foreigners whose minds are corrupted by Satan.[763] They have wielded a huge amount of influence over the KSA, including on one of the main KSA legal instruments, namely the BLG.[764] That is why it states that *Sharia* is the supreme law of the land and its constitution.[765]

In 2017, Crown Prince Muhammed Bin Salman promised to free the KSA from *Sahwah*.[766] This promise is being integrated into the KSA's laws and policies in accordance

[755] Alatawneh (2008) 11
[756] Lacroix (2011) 133
[757] Alrasheed (2002) 139-143
[758] *Ibid* 138-139
[759] Interviews with Law Professors LP1 and LP2
[760] Lacroix (2011)
[761] Interview with Sharia Expert SE2
[762] Feldman (2008)
[763] Alajloni (2004)
[764] BLG was passed in 1992
[765] Interview with Law Professor LP1
[766] Almuhaini (2017)

to KSA's *Vison 2030* where many rights and privileges have been granted for citizens, most notably women who constituted the section of society most negatively affected by *Sahwah.*[767] In accordance with KSA *Vision 2030,* a code of the provisions of *Sharia* would be finally released.[768] This will help in measuring the effectiveness of *Sharia* based on accessible codes not false interpretations. Moreover, it is an achievable goal of the KSA *Vision 2030* to eliminate the strict concept of *Sharia* alongside eliminating strictness within the KSA by "fostering Islamic values of moderation & tolerance."[769] In his speech about *Sahwah* in 2017, Mohammed Bin Salman stated:

> "We are returning to what we were before – meaning before the *Sahwah* movement in 1979 –; a country of moderate Islam that is open to all religions and to the world. We will not spend the next 30 years of our lives dealing with destructive ideas. We will destroy them today."[770]

This speech indicates that the KSA is determined to let go of strict applications of *Sharia* that were dominant during the era of *Sahwah* in the KSA.[771]

The reason that the KSA law of criminal procedure regarding cybercrime is considered to be ineffective is that the KSA is still recovering from the aftermath of this false concept of *Sharia* that lies in *Sahwah*. The KSA's legislative branch is still under the influence of the notion that any law or policy must be compatible with *Sharia* and there must be some provisions in the sacred texts which say something about what they desire to legislate.[772] Complete compatibility with *Sharia* might be considered as a false measurement

[767] Saudi Embassy in the US (2019)
[768] KSA MoJ. (2019a)
[769] KSA Vision 2030. Strategic Objectives and Vision Realization Programs <https://vision2030.gov.sa/sites/default/files/vision/Vision%20Realization%20Programs%20Overview.pdf>
[770] Sanchez (2017)
[771] Interview with Law Professor LP2
[772] Naseeb et al (2011) 161-192

for effectiveness of law.[773] Unfortunately, that is what the KSA still takes as its main approach within its legal system.

4.4.2 Fairness of *Sharia*

Fairness has been defined in Chapter 2[774] as being twofold. First, a law must be just in the eyes of a community by using an appropriate process to reach fair decisions (procedural fairness), and second it must be just in the eyes of a community by obtaining fair results (substantive fairness).[775] Fairness of *Sharia* could be tested based on this definition along with the international standards for fairness and the national standards for fairness discussed in Chapter 2.

4.4.2.1 The fairness of *Sharia* from a conceptual perspective

There have been many concerns about *Sharia* regarding fairness, whether they be from a substantive or procedural point of view.[776] Most of those concerns are based on biased perspectives that see *Sharia* as a system which allows inequality for women, cruel punishments, war on infidels, and other human rights violations based on *Quranic* texts.[777] These criticisms, whether they emanate from Muslims or not, may be questioned.[778]

Before addressing those concerns, it better to say that *Sharia* does not endorse the violation of basic human rights.[779] In fact, *Sharia* identified many of the basic human rights from the beginning of its existence, such as the right for life, the right to liberty, the right to

[773] *Ibid*
[774] See Subsection 2.3.2.1
[775] Franck (1995) 6–9, 47
[776] Smock (2002) 3-7
[777] Udah (2009) 30
[778] Smock (2002) 3-7
[779] Udah (2009) 32

fair trial, the right to propriety, the right to travel and the right to inheritance.[780] Those human rights and others found in *Sharia* would indicate that *Sharia* has within it many just principles.[781]

However, as discussed earlier, that strictness, authoritarianism and ignorance have led to the misinterpretation of *Quran* and *Sunnah.*[782] As a result, corrections to these inaccuracies are required. For instance, in the KSA, the issue of strictness that causes women's inequality has been identified, and the combating of *Sahwah* has led to limiting some of what is being viewed as cruel punishments, such as cutting off the thieves' hands and lashing consumers of alcohol or those convicted of cybercrimes.[783]

Not every single text in *Quran* or *Sunnah* constitutes a law or a command which Muslims must follow.[784] In fact, *Sharia* texts are mostly about spiritual guidance, historical stories, exceptional circumstances or special cases.[785] Thus, they are not applicable as laws.[786] For instance Verse 33 of Chapter 33 indicates that women should stay home and never wear alluring clothing.[787] This rule was revealed as an exception to the general rule because the Prophet Muhammed wives asked to participate in military campaigns during a period of intense hostility, so the *Quran* commanded them to stay in their houses and, if they were to leave, they should wear clothes which would prevent them becoming the victims of sexual assault.[788] Now, due to their ignorance of the matter, many Muslims believe that women should not be allowed to work, drive cars, or go out for entertainment.[789] This and

[780] *Ibid* 31
[781] Taha (2009) 8-9
[782] See subsection 4.4.1
[783] Supreme Judicial Council Order No 1492/T Dated 25/09/1441 Ah (18/05/2020) ordered to stop sentencing convicts to lashing punishment
[784] Hellman (2016)
[785] Interviews with Sharia Experts SE1 and SE2 and CCJs CJ2 and CJ3
[786] *Ibid*
[787] Holly Quran Chapter 33 Verse 33
[788] Ibn Kather (2016 copy) Vol (4), 422
[789] Alqurtubi 1214- 1273 AD (2006 copy) Vol (14) 163

many other false practices toward Muslim women are based on an incorrect understanding of *Sharia* and not because *Sharia* is not fair in and of itself.

4.4.2.2 The fairness of *Sharia* from an international perspective

International standards of fairness regarding criminal procedure has been defined in Chapter 2 as being based on compliance with international human rights laws.[790] Therefore, in order to test the fairness of criminal procedure under *Sharia*, it must compared to the international laws of human rights as they relate to international standards of criminal procedure. The standards found within the international law are mainly related to due process and acceptable punishments.

Unlike the direct and precise modern international laws, *Sharia* does not say how to deal with issues of criminal procedure in cases of cybercrime. However, it guides Muslims to conduct their own affairs by using the principle of *Shura*, to reach fair rules about the proper criminal procedure for cybercrime. Therefore, it can be said that *Sharia* has left the choice of how to conduct such matters in a fair way to Muslim nations based on following the provisions found within *Quran* and *Sunnah*, or other doctrines under the condition that those doctrines must not conflict with *Sharia.*[791] Indeed, this happened during the Prophet Muhammed's time when approval was given to rules that had been applied before the coming into being of Islam which, although they are not found in *Quran*, they do not conflict with it.

In regard to due process, international laws of human rights stipulates four foundational rights: the right of the accused to be presumed innocent until proven otherwise, the right for an attorney or legal representation, the right for knowing the reason of detention and accusations, the right for an unbiased judge and open participatory trials.[792] It can be

[790] See Subsection 2.4.2.2
[791] Taha (2009) 1-9
[792] See UDHR Articles 9-11

asserted that nothing found in *Sharia* opposes those features. Furthermore, many texts exist in the *Quran* and *Sunnah* that encourage having an attorney, presumption of innocence and the appointment of fair judges.[793] For instance, the Prophet Muhammed says:

> "Avoid condemning the Muslim to Hudud [punishment] whenever you can, and when you can find a way out for the Muslim then release him for it. If the Imam errs it is better that he errs in favour of innocence (pardon) than in favour of guilt (punishment)."[794]

Therefore, it is up to Muslim states to apply *Sharia* fairly to help overcome issues that are related to modernity, such as appropriately and adequately applying international human rights law to their own criminal procedure.

4.4.2.3 The fairness of *Sharia* from a national perspective

The KSA treats *Sharia* as the basic norm of the country.[795] In Article 1 of the BLG, it states that the *Quran* and *Sunnah* are the constitution of the KSA.[796] One major reason why the KSA chooses *Sharia* as its constitution is that, at time of issuing the BLG, *Sahwah* followers were in control of the public discourse and they strongly believed that the only way to establish a fair system is by basing it on *Sharia.*[797] This led them to ignore and oppose other non-*Sharia* based systems, even those which do not conflict with it,[798] and they placed pressure on the KSA's government to meet their demands.

In regard to the unfairness of the CPL on cybercrime in the KSA, *Sharia* – as applied by KSA – is one factor that causes such unfairness, especially in regard to due process and

[793] Udah (2009)
[794] Altermithi 824-892 AD (No 1424)

[795] See Section 2.3
[796] BLG Article 1
[797] Lacroix (2011)
[798] Alatawneh (2008) 35-54

cruel punishments. The KSA has not completely recognised all principles of due process found within S*haria* because they have not been directly and clearly mentioned in *Quran* and *Sunnah.*[799] Also, they have been applying *Sharia* exactly how it was applied centuries ago, including the use of severe punishments.[800] It is a mistake to look for law provisions about modern phenomena in an ancient doctrine which has not directly encountered modern phenomena,[801] such as cyberspace.[802] The KSA has apparently made this mistake which could be why its legal system is considered by many to be unfair.[803] In other words, the mistake has not been what has been applied (i.e. *Sharia*) but rather how it is applied.

Even though the KSA has many proficient *Sharia* scholars, they often do not have the adequate expertise related to the modern concept of law[804] and many scholars of law lack knowledge of *Sharia.*[805] The *Ulema* and law scholars always meet when regulating a new law,[806] but they rarely agree over matters, such as importing laws from more devolved countries because Saudi's *Sharia* scholars always oppose the importation of laws from non-Muslim countries[807] as they consider them to be against *Quran*.[808] Surprisingly, they always have public support,[809] apparently as a matter of national pride.[810]

Unfortunately, it might be said that those factors have negatively affected the fairness of the KSA's legal system, including that which is related to the CPL on cybercrime. This negative impact might make the KSA law of criminal procedure regarding cybercrime

[799] Interview with CCJ CJ2
[800] Amnesty International report 2020/2021. 311 <https://reliefweb.int/sites/reliefweb.int/files/resources/POL1032022021ENGLISH.PDF>
[801] Haddad & Stowasser (2004) 1-11
[802] *Ibid*
[803] Amnesty International report 2020/2021. 311 <https://reliefweb.int/sites/reliefweb.int/files/resources/POL1032022021ENGLISH.PDF>
[804] Alajloni (2004)
[805] Interviews with CCJs CJs, Sharia Experts SEs and Law Professor LP2
[806] Interviews with CCJ CJs and Law Professor LP2
[807] Interview with Law Professor LP2
[808] Almibrad et al (2015) 15-18
[809] Interview with Law Professor LP1
[810] *Ibid*

incapable of delivering fair decisions and fair results. Recently, with the promises of Muhammed Bin Salman, some CPL provisions which were based on wrong interpretations of *Sharia* have been either modified or abolished, despite the fact that many *Sharia* scholars were not convinced that it was appropriate to do so,[811] such as abolishing *Ta'zir be Alshubhah* based on Article 3 of the CPL 2013.[812] This proves that the KSA understands the importance of not always complying with *Sharia* scholars' interpretation of *Sharia*.[813] It is clear from this that the KSA *Vision 2030* is slowly driving the KSA towards modernity and fairness.[814]

One example of the KSA's efforts to avoid the misinterpretation of *Sharia* and deliver a fairer judicial system is the activation of an old project regarding the codification of provisions of *Sharia,*[815] which was pursued in 1972 by the *Islamic Researches Institution* with the support of several Muslim countries.[816] Following this effort, the KSA sought to unleash its own project.[817] In fact, there was an earlier attempt even before the unification of the KSA in 1927 by the order of King Abdul-Aziz (the first King of the KSA),[818] but it was stopped because many *Ulama* issued *Fatwas* (legal opinions) which viewed the project as *Haram* (prohibited).[819] Additionally, all other attempts since then have been fought and stopped by strict *Ulama* because, as Alshathri asserts, codification is *Haram* because it limits *Ijtihad* and consequently limits *Sharia* from being valid for all different times.[820] One of those contested attempts to codify *Sharia* was conducted in the mid-20th Century by the former judge and former Chief of the Makkah Courts, Ahmad Alqarri, when he, under his

[811] Interview with CCJ CJ3 and Sharia Expert SE2
[812] Supreme Judicial Council Order No 1492/T Dated 25/09/1441 Ah (18/05/2020)
[813] Interview with Criminal Defence Lawyer CL3
[814] See Section 2.3
[815] Rashad (2021)
[816] Committee for Codification (1972)
[817] Rashad (2021)
[818] Alashaik (2019)
[819] *Ibid*
[820] Alshathri (2007)

own a initiative, collected judicial precedents within the KSA, analysed them, and developed them into law provisions.[821] His personal effort was converted into a book called *Sharia Provisions Journal,* and it is considered to be the main reference that judges in the KSA including CCJs follow until recent days,[822] even though most of them oppose the codification of *Sharia*.[823] At the beginning of 2019, Crown Prince Muhammed Bin Salman initiated a *Sharia* codification project.[824] If this promise were to be delivered and the provisions of *Sharia* really were to be codified, it would help in making the laws more accessible, preventing both intentional and unintentional misinterpretation of *Sharia,* especially when it comes to cybercrime and the criminal procedure regarding cybercrime where there is no mention to them within any of the older codification projects. Codification of *Sharia* would limit *Ijtihad* and consequentially make judicial decisions fairer than the current ones, as will be analysed in Chapter 7.

4.5 Approaches to the cybercrime criminal process in the UK

As a leading country in the cybersecurity domain, the UK passed the five-year National Cyber Security Strategy (NCSS) in 2011 to enhance cybersecurity within the country.[825] The 2011, NCSS aimed to strengthen the UK's security within cyberspace.[826] As the 2011 NCSS achieved most of its objectives in terms of policies, institutions and initiatives which were developed during that period, another five-year NCSS has been passed to cover the period from 2016 to 2021.[827] For the implementation of its plan, NCSS states:

[821] Alqarri (1981) 1-3
[822] Alqarri (2015) 6-8
[823] Interview with Criminal Defence lawyer CL3 and Law Professor LP1
[824] Alashaik (2019)
[825] UK NCSS 2016-2021 (2016) 13
[826] *Ibid*
[827] *Ibid*

> "Our goals for the country's cyber security over the next five years are rightly ambitious. To achieve them will require us to act with consequence and determination across the digital landscape. Activity to deliver the Government's vision will advance the three primary objectives of the strategy: to DEFEND our cyberspace, to DETER our adversaries and to DEVELOP our capabilities, all underpinned by effective INTERNATIONAL ACTION."[828]

The UK has successfully been able to differentiate between cybercrime and traditional crime.[829] According to UK NCSS, cybercrime takes two interrelated forms: cyber-dependent crimes, and cyber-enabled crimes,[830] both of which have become more prevalent, especially during Covid-19, because of growing internet usage.[831]

Furthermore, the UK does not only respond to cyberspace through security measures, as there has also been a legal response to cyberspace and cybercrime, which is another reason why the UK is a world leading country in responding to cyberspace and cybercrime.[832] The absence of consolidated criminal code does not mean that the state cannot issue strong legislation that tackles cybercrime or crimes in particular.[833] The UK does not have a written Criminal Code, yet the UK Computer Misuse Act 1990 offers clear and comprehensive legislation on cybercrime.[834] What makes this legislation effective is that it does not only specify computer crimes, but it also specifies general and private principles of crimes and cybercrime that are related to the criminal process, such as jurisdiction.[835] The Computer Misuse Act 1990 mostly relates to the substance of crimes than the procedure of crimes.

[828] *Ibid* 30
[829] *Ibid*
[830] *Ibid* 17
[831] Buil-Gil et al (2020) S51
[832] UK NCSS 2016-2021 (2016) 13
[833] Walden (2007) 23
[834] *Ibid.* 48
[835] Fafinski (2009) 44

However, it was the first step toward recognising cybercrime and distinguishing it from traditional forms of crime in terms of substance and procedure.[836]

The UK Computer Misuse Act 1990 has opened the way for more recent and relevant UK laws which handle issues of criminal procedure regarding cyberspace and cybercrime. One of these laws is the Police Act 1997,[837] which specifies the role of police in policing crimes which includes cybercrime.[838] The second of these laws is the Regulation of Investigatory Powers Act 2000 (RIPA),[839] which specifies the situations where public bodies can intercept communications and carry out surveillance and investigation for crimes including cybercrime.[840] The third of these laws is the Criminal Justice and Police Act 2001 Part 2: Powers of Seizure,[841] which precisely mentions the conditions where proprieties can be subjected to the power of seizure for sizable objects, such as electronic devices used in cybercrime.[842] The fourth of these laws is the Justice and Security Act 2013.[843] The second part allows civil litigants to present sensitive evidence and to invoke closed material procedures in proceedings before the higher courts.[844] This Act is controversial especially among human rights lawyers and advocates within the UK because of the secrecy or "closed material proceedings" that the 2013 Act allows in respect to the national security interests.[845] The fifth of these laws is the Data Retention and Investigatory Powers Act 2014,[846] which has

[836] *Ibid.* 43-44
[837] UK Police Act 1997
[838] Fafinski (2009)
[839] UK Regulation of Investigatory Powers Act 2000
[840] *Ibid*
[841] UK Criminal Justice and Police Act 2001
[842] *Ibid* Article 50 Part 2
[843] UK Justice and Security Act 2013
[844] *Ibid* Part 2
[845] Tomkins (2014) 306 & 309
[846] UK Data Retention and Investigatory Powers Act 2014

been replaced by the IPA.[847] The 2014 Act deals with the retention of data acquired by the lawful interception of communications.[848]

The sixth of these specialist laws is the IPA.[849] It deals with acquiring evidence (data) that is sensitive due to its relationship with privacy, such as the interception of calls, the monitoring of communications, and other forms of electronic and physical surveillance.[850] This law was passed in 2016 to replace the Data Retention and Investigatory Powers Act 2014 and much of the RIPA.[851] The IPA includes 272 articles distributed across 9 sections which mostly deal with investigatory powers regarding lawful interception of communication data, and retention of communication data without violating the fundamental human right of privacy and takes into consideration that the issue of mass collection of communication data has not yet been comprehensively covered from both human rights and international law perspectives.[852] The IPA allows official authorities to seek evidence by issuing warrants to ISPs that hold communication data.[853] As has been noticed, "the Investigatory Powers Act establishes a legal basis for advanced modern surveillance techniques, and so provides an appropriate framework to address the issues under discussion, which involve the large-scale collection, retention and subsequent analysis of communications data,"[854] Therefore, it could be possible to say that, without the precise measurements of precaution that this Act follows, people's privacy would be at risk of being undermined by government surveillance.[855]

These laws will be used for policy transfer purposes in this thesis. They will be analysed when considering the possibility for policy transfer, especially in Chapters 5, 6 and 7 which address the issue of policing, investigation, prosecution and trial of cybercrime in the

[847] UK IPA
[848]UK Data Retention and Investigatory Powers Act 2014. Article 1
[849] UK IPA
[850] For implementation, see the reports of the Investigatory Powers Commissioner <https://www.ipco.org.uk/>
[851] McKay (2017)
[852] Murray and Fussey (2019) 32-33
[853] Cobbe (2018) 15
[854] Murray and Fussey (2019) 32 and 31
[855] *Ibid*

KSA. Moreover, the UK seems to deal more effectively with the four issues arising from the differentiation between cyberspace and space[856] than the KSA. These issues are: the physical complexity of cyberspace and the need for expertise, multijurisdictional operation, the private ownership of cyberspace, and identity and users in the internet.[857]

Through its response to cybercrime in policy, procedure and substance, the UK laws have been shown to be more able to adapt to the unique nature of cyberspace.[858] Therefore, it can be said that the UK has produced various effective and fair laws of criminal procured regarding cybercrime, and it deals with cybercrime as being very different to traditional crime, a standard which will be explored further in future chapters.[859]

4.6 Model code

In order to present a full picture of a truly effective agenda for the law of criminal procedure to be applied to cybercrime, a proposed model code can illustrate the agenda and thereby support the aims and objectives of the thesis.

The proposed model code provides a framework for the chapter and presents a clear guidance for the KSA legislation regarding the criminal procedure applied to cybercrime. A version of the Model of Code of Criminal Procedure in the KSA Regarding Cybercrime should contain the main principles and provisions for the criminal procedure of cybercrime to be set in the KSA laws. The proposed code should only cover procedural aspects and excluding substantive aspects as they are not within the scope of this thesis.

As shown in Figure 4.1, in the main construction of the Model Code, three hierarchal levels are identified in order to categorize the criminal procedure regarding cybercrime in the

[856] Saunders (2017) 6
[857] See Section 2.2
[858] Saunders (2017) 6-8
[859] *Ibid*

KSA, starting from general to specific. The first level is the strategy level, the second level is the functional level, and the third level is the agenda level.

4.6.1 Strategy level

In the first level (strategy), there are two main elements that are related to the law of criminal procedure as it relates to cybercrime in the KSA. The first element is the legal strategy, which is the focus of this thesis, and the second element is the security strategy, which is not. Therefore, even though the security strategy is as important as the law strategy, it is excluded as it does not fit the aims and objectives of this thesis which mainly lie in evaluating and analysing the KSA law of criminal procedure regarding cybercrime. Therefore, the proposed model code will focus on the KSA criminal law of procedure regarding cybercrime (legal strategy).

However, it is crucial to the thesis to have a general insight about the KSA's strategy regarding cybersecurity in terms of its institutional and policy responses to cybercrime. To start with, the KSA established the NCA in 2017 to fulfil the KSA strategy for cybersecurity.[860] According to the NCA, this institution has been established based on the KSA *Vision 2030*'s National Transformation Program, one aim of which is to transform the country toward better engagement with the digital world.[861] The NCA is working on the National Strategy for Cybersecurity[862] and updating the KSA National Information Security Strategy 2011 (NISS) released by the KSA MCIT.[863] One of the aims of the NISS is to "Transform the Kingdom of Saudi Arabia into an information-secure society, enabling information to be used and shared freely and securely."[864] Another aim is to "increase the

[860] KSA NCA <https://nca.gov.sa/en/pit ages/about.html>
[861] *Ibid*
[862] *ibid*
[863] See NISS on <https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map/strategies/national-cyber-security-strategy-of-saudi-arabia/view>
[864] KSA NISS

security, safety, and integrity of online information while promoting the increased use of information technology."[865] It appears that the KSA is seeking a more secure engagement with cyberspace by providing more strategies for cybersecurity.[866] Secure cyberspace would decrease the number of cybercrimes committed within the jurisdiction of KSA, and would protect both the country and its citizens from being exposed to cyberattack and cybercrime.[867]

4.6.2 Functional and feature levels

The legal strategy level branches out into four different elements which comprehensively complete the functional level of the proposed Model Code. The first element is policing. It can be said that policing the use of cyberspace in the KSA needs special powers and a set of supplementary features to address cybercrime (agenda level). The first of these is the power for police to obtain evidence, and includes the power to collect cyber evidence, whether in physical space or cyberspace, through searches (power of seizing). The second policing power is the power to process evidence, which includes powers of retaining, sifting and accessing encrypted data. In regard to institutional setting, there should be an assessment of the distribution of powers for surveillance in relation to institutions involved in policing the use of the internet and also whether the KSA needs a specialist law enforcement body for policing cyberspace?[868]

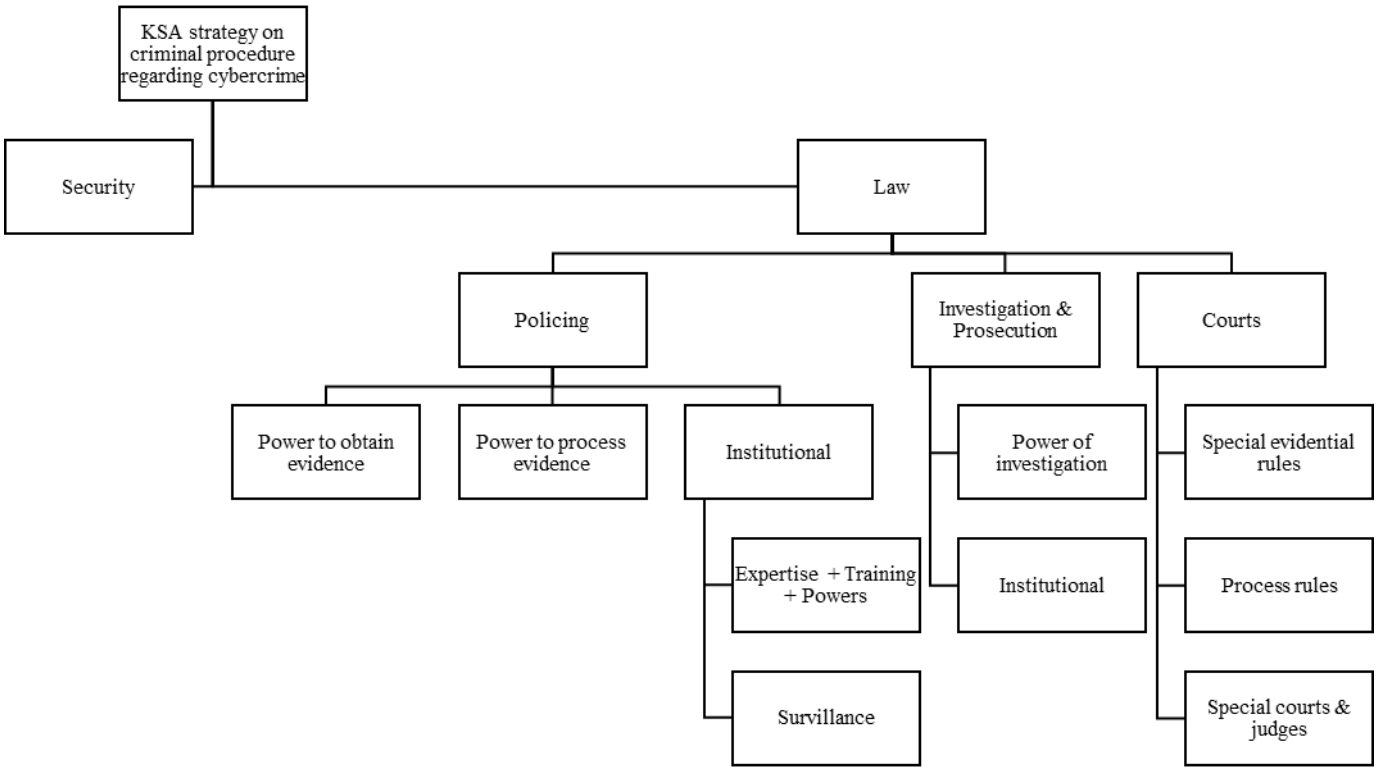
The second element is within the prosecution and investigating (process) features. In most developed countries such as the UK, due to the purpose of separation of powers, prosecution and investigation are generally separated to ensure the rule of the law.[869] However, in the KSA, the two powers are vested in one entity (the PP), which is the reason

[865] *Ibid*
[866] Alamro (2017) 35-37
[867] *Ibid* 37
[868] The UK has multiple agencies which police cybercrime crime such as NCA, ICPO, GCHQ and NCSC. See 5.3.1
[869] Iyer (2018) 513

they are included in one element. The first investigation and prosecution power (agenda) is the power to investigate cybercrime. The supplementary powers that occur here are powers of retaining, questioning, sifting, accessing encrypted data. The second investigation and prosecution feature is institutional. It raises the question of whether it is fair and effective to vest those two separate powers in one entity.

The third element is the court process which branches out into three agendas. The first agenda is special evidence rules; the laws of evidence regarding cybercrime. The second agenda is the court process rules regarding evidence; i.e. what the evidence is that can be presented in courts. The last agenda item is institutional features; are there courts and judges to rule over cybercrime?

Figure 4.1 Proposed Model Code for the CPL regarding cybercrime in the KSA.



4.6.3 A heuristic device

The proposed Model Code should be viewed as an instrument of analysis for what the KSA has done and what it lacks in regard to tackling cybercrime from procedural standpoint. From what has been discussed throughout this chapter, the KSA law of criminal procedure regarding cybercrime is insufficient in light of the proposed Model Code. The process of cybercrime in the KSA, in terms of policing, investigating, prosecuting, and trying cybercrime suspects, will be assessed in Chapters 5, 6 and 7 using this heuristic device as a tool of analysis. Even though the KSA has passed two major pieces of legislation regarding the criminal process of cybercrime, the CPL 2013 and the ACL, they have failed in combating cybercrime procedurally because they treat it the same they would an traditional crime. This delimitation of law will be discussed throughout Chapters 5, 6, and 7.

4.7 Conclusion

The KSA has passed various laws related to criminal procedure that deal with cybercrime which have not been effective for the following reasons. The most apparent is that the KSA still treats cybercrime as a non-distinctive crime, discarding the main four problems arising from this necessary differentiation which should be made: the complexity of cyberspace and the subsequent need for expertise, its multijurisdictional operation, the private ownership of cyberspace, and identity of users. Despite applying the CPL 2013 to cybercrime, this law makes no mention of cybercrime. Likewise, the ACL has just one Article related to the criminal procedure of cybercrime, which refers all cybercrime cases to the BIPP – which has been renamed *PP* in 2017,[870] although it remains BIPP in the ACL. This indicates that the KSA is not keeping up to date with its own laws, and the same applies to the ETPL and ACFL. Those Laws do not just become outdated when technological and

[870] KSA Royal Decree No. A/240 of 2017

legal changes happen, they have proven to be ineffective and unfair because they do not meet international and comparative standards of both fairness and effectiveness.

The role of *Sharia*, which is the main sources of legislation in the KSA,[871] has been identified as problematic in Sections 4.3 and 4.4 when it comes to the criminal process of combating cybercrime. *Sharia* gives two important principles to the KSA. The first is the principle of *Shura,* where Muslims are required to take consultation in their affairs and decide their own fate based on what they agree upon, which can include the removal of an unjust ruler. The second is the principle of obeying just rulers who can decide what is best for their own people after consulting with them. Therefore, *Sharia* gives Muslims the choice to find ways to combat cybercrime and to establish a robust criminal procedure, but *Sharia* has been misinterpreted by people in power, resulting in undue authoritarianism and conservatism. Otherwise, if those principles were actually to be applied, it is likely the KSA would use them to import, or at least learn from, effective laws from countries such as the UK.

As discussed in Section 4.5, the UK achieves better standards than the KSA in combating cybercrime procedurally. One key success of the UK's response is that it deals with the criminal procedure of cybercrime as being different from traditional crimes. The UK has passed many Acts that deal with cybercrime since 1990, and it keeps updating its laws in accordance to technological variables. Another key success for the UK is effective cooperation with other countries in regard to cybercrime. The UK is party of the Budapest Convention of Cybercrime 2001 and the CLOUD Act 2018 which the KSA cannot join because of its human rights record.

A heuristic device has been introduced as an element of analysis to what the KSA has done and what it is yet to be done, in terms of combating cybercrime procedurally. Therefore, the KSA has identified the issue of cybercrime in the Kingdom. In terms of security, the KSA

[871] BLG Articles 1 and 7

passed the NISS in 2011 to give a clear vision of how the KSA can deal with cyberspace.[872] This strategy is imminently likely to be updated by NCA in accordance with the KSA's *Vision 2030*,[873] as technology is increasingly evolving and the country is working toward modernisation.

In terms of law, the KSA has passed various pieces of legislation in regard to cybercrime. However, these barely mention the criminal procedure of cybercrime, only referring to the body of investigation in the KSA – the PP – vesting it with both investigation and prosecution powers. This governmental entity, along with CC and the PF, employs the KSA CPL 2013 in dealing with both traditional crime and cybercrime with no differentiation between them in terms of the criminal process, even though there are essential differences between the two.[874] Moreover, the legislation does not cover all aspects of due process which makes it open to criticism, especially in terms of its fairness.[875] Therefore it can be said that this Law does not meet the international human rights standards because it does not fully address the accused's rights of due process, such as the right for an attorney, the right for unbiased judges and the right to know the reason for detention. Some might attribute such unfairness to the country's interpretation of *Sharia*, as discussed earlier in this chapter. What the KSA needs is to provide more effective and fair legislation that meets the minimum standards of international effectiveness and fairness. Suitable designs will be discussed in Chapters 5, 6 and 7.

[872] European Union Agency for Cybersecurity. National Cyber Security Strategy of Saudi Arabia. <https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map/strategies/national-cyber-security-strategy-of-saudi-arabia/view>
[873] KSA NCA <https://nca.gov.sa/en/pit ages/about.html>
[874] See Section 2.2
[875] Alsubaie (2013) 131

Chapter 5

Policing cybercrime in the KSA (Criminal Investigation Initial Stage)

5.1 Introduction

This chapter aims to answer the following question: what is the current legislation on cybercrime in the KSA related to the law of criminal process as it applies to policing?[876] A key term used in this chapter is "policing". Therefore, in order to draw a firm basis for the argument, a clear definition is needed. It can be said that the terms "police" and "policing" refer to the maintenance of public order by civil (meaning non-military) law enforcement.[877] However, those terms constitute a broader concept which means exercising "broader 'social control' activities even those of a quite informal nature. 'Policing' activities in this sense are undertaken by parents, teachers, and a whole range of people, as well as members of police forces,"[878] and policing can be carried out be both public and private entities alike.[879] Public and private approaches are one distinction, formal legal and informal social approaches are another. The Chapter is mostly about public and formal approach not social approaches. This reflects reality in KSA in line with the nature of the political and cultural approach to governance. However, social forms of control might be relevant especially when involving *Sharia* sources, such as statements from *Imams* (leaders within a *Mosque*) which might be counted as social form. However, this chapter will focus only on policing carried out by the public and formal Police Force (PF) as it reflects aims and objectives of the thesis.

[876] See chapter 1 section 1.3
[877] Newburn and Jones (1998)
[878] *Ibid* 1
[879] *Ibid* 2

The concept of policing in a legal sense has both broad and narrow functions. The broad function of policing includes various entities which may exercise observational behaviour with limited authority on particular subjects and co-operate in policing societies[880] such as "neighbourhood watch, victims by reporting crimes, social workers engaged in child protection work,"[881] "traffic safety education, drug abuse prevention and search and rescue".[882] In cybercrime, police officers are sometimes referred to as "cybercops."[883] Moreover, such a conception gives rise to a very narrow concept of policing despite it including various entities such as the police themselves, ISPs and internet users.[884] This term constitutes the narrow function of police because it points to a specialism in policing even though it includes non-governmental organisation. As noted by Wall:

> "Although the non-governmental, non-police organisations are mainly private bodies, they often perform public functions and a growing concern is that they, as such, lack the formal structures of accountability normally associated with public organisations."[885]

The narrow function of the police includes the PF as a governmental entity that maintains law and order as expected by the public,[886] and this narrow function of the PF is mainly addressed by this chapter as it deals with policing crimes, including cybercrime. Taking into consideration that policing cybercrime can involve a broad array of actors in both the public and the private sectors, the main focus of this chapter is to thoroughly address governmental police organisations. Non-governmental and non-police organisations will only briefly be considered in relation to performing public functions. The reason that this chapter

[880] Mawby (2008)
[881] *Ibid*
[882] Cordner (2014)
[883] Yar and Jewkes (2008) 582
[884] *Ibid* 581 and 582
[885] Wall (2007b) 189
[886] *Ibid*

mainly reflects a narrow focus of policing is due the generally authoritarian nature of governance prevailing in the KSA.

The CPL 2013 is the main legislation which focuses on the narrow aspect of policing institutions and defines policing powers. As will be discussed later in this chapter, it vests investigatory powers in the hands of the PP and CC, rather than the PF because the KSA criminal procedure is a mixture of inquisitorial and adversarial systems,[887] and as addressed in Chapter 2, the KSA system is a system of formal (legislation) and informal sources (*Sharia*). As noted by Reichel:

> "Islamic procedural law is a mixed system combining adversarial and inquisitorial aspects. Because the Sharia is a religious law based on divine command and revelation, it did not develop through judicial precedent or legislative codification."[888]

Thus, a police investigation in the KSA is the initial investigation and is therefore different from prosecution and judicial investigations. Therefore, policing cybercrime in the KSA will be the main focus of this chapter, which branches out into two major aspects. The first aspect is institutional: who are the KSA PF and what affects their profile and structures? The second aspect is operational: what do they do and how do they do it? Therefore, it can be said that this chapter addresses the policing of cybercrime and how cybercrime is policed in the KSA. Additionally, it will explain how policing authorities in the KSA deal with cybercrime suspects or those accused of cybercrime; it will analyse how they are processed and then subjected to formal policing powers such as arrest, detention, surveillance, search and seizure. Furthermore, this chapter will explain who is responsible for policing the use of the internet and cybercrime in the KSA. Moreover, it will demonstrate that policing

[887] Reichel (2018) 130
[888] *Ibid*

cybercrime is very complex in the KSA because there are multiple official authorities, aside from the KSA PF and PP, which have both policing and investigative authority.

As the KSA deals with cybercrime in a way which is largely indistinct from NCCs in terms of criminal procedure, this chapter will begin by introducing the main provisions for policing of NCCs found in the main legislation on criminal procedure, the CPL 2013. Then, it will apply those provisions to policing cybercrime and analyse the KSA's response to policing cybercrime in depth, both institutionally and operationally.

Subsequently, an assessment based on both effectiveness and fairness of the KSA response to policing cybercrime will be conducted in order to meet the research objectives regrading identifying what is holding the KSA back from combating cybercrime in a procedural sense.

To meet the research objectives, this chapter will also reference the England and Wales jurisdiction and how it responds to policing and cybercrime in order to learn lessons for the KSA from that country's approach to cybercrime in a procedural sense.

Given the two foci of this chapter, it is useful to clearly state its aims. It can be said that the first aim is to identify the KSA's response to cybercrime in terms of criminal procedure, specifically with regard to what institutions police cybercrime and how they operate. The suggested Model Code[889] will be a checklist used to analyse the country's current approach to cybercrime in terms of policing. As outlined in Chapter 1,[890] this is the third main aim of the thesis as it is expected that it will contribute toward evaluating the current approach of the KSA's response to the modern phenomena of cyberspace in relation to the criminal process of cybercrime. Therefore, this chapter will evaluate the KSA's responses to cyberspace in terms of policing cybercrime. In order to clear the path for the

[889] See Chapter 4
[890] See Subsection 1.2.1

remainder of this chapter, an evaluation and analysis to the KSA's main legislation regarding policing cybercrime will be conducted in order to identify the KSA's approach to the criminal process of cybercrime. This includes the CPL 2013 and its Criminal Procedure Law Executive Regulation 2015 (CPLER).[891]

The second aim is to identify what is holding the KSA back from tackling cybercrime in a procedural sense, particularly those factors related to policing cybercrime; as listed in the ACL, the ETPL and the ACFL, which have been introduced in Chapter 4.[892] There is no doubt that the KSA's current approach to cybercrime, both substantively and procedurally, puts the country at risk and must overcome this risk before it becomes more difficult to do so. Therefore, as mentioned earlier in Chapter 2, the KSA is seeking reforms to modernise the state under the *Vision 2030* reforms in a time of risk and uncertainty,[893] so it can be said that the first step toward overcoming these risks is to identify them.[894] The KSA has to identify the legal risks regarding its legal system including the criminal procedure. *Vision 2030* has given the governmental entities, including ministries, the choice as to whether they want to join the *Vision* or not.[895] Even though the choice has been given to the ministries to join the *Vision* voluntarily, it is more realistic to say that they must join due to the nature of the ruling system in the KSA. As discussed in Chapter 4, *Sharia* dictates that people must obey the Islamic rulers unless those rulers ordered something that directly goes against the teachings of *Islam*.[896] Generally, *Vison 2030* does not conflict with *Sharia*,[897] and so, the MoJ began to

[891] The CPLER was passed in January 2015 by the KSA Council of Ministers (No 142) in order to clarify some Articles in the legislation. Executive regulation is a common official legal tool that the KSA uses to explain its legislation in detail. See Naseeb et al (2011)
[892] See Section 4.2
[893] See Section 2.5
[894] Berg (2010) 79-95. 83
[895] KSA Vision 2013, National Transformation Programme; Delivery Plan 2018-2020 (2017) <https://vision2030.gov.sa/sites/default/files/attachments/NTP%20English%20Public%20Document_2810.pdf>
[896] See Section 4.5
[897] See Section 2.5

implement the *Vision* in 2018 along with almost all other governmental entities.[898] One concern of the MoJ is therefore to reform the current laws on cybercrime.[899]

The third aim is to test both the effectiveness and the fairness of the KSA's approach to policing cybercrime. It will refer to the standards of effectiveness and fairness set out in Chapter 2.[900]

The fourth aim is to compare the KSA's approach regarding policing cybercrime with that of the UK jurisdiction in order to consider policy transfer and learn lessons from better approaches to cybercrime. Therefore, this chapter will investigate the relevant UK laws regarding policing cybercrime and compare them selectively with the KSA's legislation in order to learn lessons from them.

5.2 Policing NCCs in the KSA

The distinctions between NCCs and cybercrimes have been briefly outlined in Chapters 2[901] and 4,[902] focussing on the space where crimes are committed and the nature of the crimes themselves. One distinction is that cybercrime is more complex than NCC, and it often requires particular expertise to perpetrate (at the very least knowledge of how to access the cyber sphere) and therefore to investigate such crimes.[903] A second distinction is that cybercrime almost inevitably involves crime that crosses boundaries and jurisdictions.[904]

[898] KSA MoJ, National Transformation Plan Programme <https://www.moj.gov.sa/English/Ministry/vision2030/Pages/NationalTransformationProgram.aspx>
[899] KSA MoJ, MoJ's Initiatives <https://www.moj.gov.sa/English/Ministry/vision2030/Pages/MoJInitiatives.aspx>
[900] See Section 2.4.
[901] See Subsection 2.2.1
[902] See Section 4.5
[903] Bandler and Merzon (2020) 27
[904] Smith (2002) 241

The third distinction is related to the private ownership of the domain and the implications for policing.[905] In other words, the internet is run and governed mainly by private operators, not sovereign states, and this trait affects the balance of power within cyberspace.[906] For instance, ICANN, which controls internet domains, is an independent organisation, even though it was established by the US Department of Commerce in 1998.[907] This non-profit organisation remains private and self-regulated even though the international community, mainly European countries in this case, has unsuccessfully pressured the US to make this body part of international law structures.[908] Sarah Mainwaring emphasises that the internet is sometimes metaphorically called the "Wild West" because boundaries and authority barely exist within it.[909]

However, multiple attempts from nation states, such as Russia, America, China, and some Arab countries, seek to shape cyberspace.[910] For their part, countries such as China have to some extent controlled the cultural and political uses of the Internet within their jurisdictions but at the expense of closing off usage and opportunities for users.[911] By contrast, liberal countries, such as most European countries, including the UK, issue their own national cyber security strategies in order to protect cyberspace from some forms of harms but less so to control it for cultural and political reasons.[912] Therefore, it is possible to say that nation states aim to restore some domestic power under their vague understanding of cyberspace, or the "mysterious space,"[913] which is still highly privatised in terms of governance.[914] Thus, it has been posited that public-private partnership in cyberspace is the

[905] Murray (2007) 89-94
[906] *Ibid*
[907] Kleinwachter (2003) 1111
[908] *Ibid* 1111- 1116
[909] Mainwaring (2020) 215–232
[910] *Ibid*
[911] Wall (2007b) 189
[912] *Ibid*
[913] Mainwaring (2020) 215–232
[914] Kleinwachter (2003) 1111

solution to achieve governance so that both can work in harmony.[915] In addition, private ownership is not confined to the internet infrastructure, but is also evident in the mode and terms of access through contracts with CSPs.[916] Furthermore, private ownership affects usage because of major social media platforms and search engines, as well as commercial players like Amazon.[917]

A fourth distinction is identity and users.[918] The problem is that on the internet people can more easily pretend to be someone else or even something else, and also they can pretend to be somewhere else.[919] As discussed in Chapter 2 anonymity is one of the distinctions that exit between the two types crimes.[920] Therefore, there is a need for international cooperation especially in terms of collecting cyber evidence since it often involves other jurisdictions.[921] However, this aspect of policing activities is excluded from the thesis.[922]

Unlike many countries, such as the UK, which have taken those distinctions into consideration in terms of substance and procedure in policy, law, and practice,[923] the KSA still deals with cybercrime as being no different from NCCs in terms of the criminal process.[924] Therefore, this section will look into policing NCCs in the KSA as the first authoritative step of criminal process.

Since the KSA deals with NCCs as being indistinct from cybercrime, it applies the main institutional and operational principles of policing NCC to cybercrime. The KSA PF and other similar authorities such as the religious police or GPPVPV, the General Directorate

[915] Shore (2011) 4
[916] Kleinwachter (2003) 1111
[917] *Ibid*
[918] Smith in Yar and Jewkes (2011) 284
[919] *Ibid*
[920] See chapter 2 subsection 2.2.1
[921] Hakmeh (2016)
[922] However, it will be recommended for further research in the conclusion chapter of this thesis.
[923] UK NCSS 2016-2021
[924] Hakmeh (2018)

of Narcotic Control (GDNC),[925] and Interior Intelligence Agencies, such as the General Directorate of Investigation (GDI),[926] will be introduced as the policing institutions which the CPL 2013 recognises for the purposes of policing crimes.[927] Most of those institutions are supervised by the Ministry of Interior (MoI).[928] Some are listed in Article 26 of the CPL 2013, as will be discussed later in this section, and they can operate in cyberspace and physical space and so tackle both NCC and cybercrime. However, the GDNC and the GDI are not listed within the CPL 2013, yet they function as the KSA PF and exercise the policing powers recognised by the CPL 2013.[929]

The main operational issues incurred in practice by police institutions in the KSA concerning the policing of crimes are stopping, arresting, detaining, searching, and surveillance of suspects.[930] This section will cover the KSA's jurisdiction regarding policing crimes from these perspectives. Therefore, in Section 5.2, the main institutional and operational principles of policing crimes will be covered in order to apply them in the coming Section 5.3 about policing cybercrime in the KSA, which is the main focus of this thesis. Thus, it can be said that the main facets regarding policing crime in the KSA which are covered in this section relate to the KSA PF institutions (structures) and operations (powers).

5.2.1 Policing NCCs in the KSA: institutional aspects

Generally, policing means "maintaining public order and safety, enforcing the law, and preventing, detecting, and investigating criminal activities"[931] by the "body of officers

[925] KSA General Directorate of Narcotic Control
[926] KSA General Directorate of Investigation
[927] CPL 2013 Article 26
[928] KSA MoI. Sectors
[929] Interview with Police Officer PO1
[930] Those powers as will be addressed later in this chapter and in chapter 6 overlap with the operation of the PP.
[931] Police Foundation & Policy Studies Institute. (1996) xii

representing the civil authority of government"[932] (i.e. the Police). In modern societies, "the Police are identified primarily as a body of people patrolling public places in blue uniforms, with a broad mandate of crime control, order maintenance and some negotiable social service functions."[933]

Almost all countries, including the KSA, have their equivalent PF institution which follows a basic and historic common purpose, which is to maintain order.[934] However, KSA policing is distinctive in various ways. For example, the UK is known for its 'policing by consent'[935] which is based on the Peelian Principles, or Robert Peel's[936] nine principles of policing.[937] These principles were first introduced in 1829 by Robert Peel in order to draw up the policing roles within the society.[938] According to Peelian principles, the roles of the Police are as follows:

> "1. To prevent crime and disorder, as an alternative to their repression by military force and severity of legal punishment;
>
> 2. To recognize always that the power of the police to fulfil their functions and duties is dependent on public approval of their existence, actions and behaviour, and on their ability to secure and maintain public respect;
>
> 3. To recognize always that to secure and maintain the respect and approval of the public means also the securing of the willing cooperation of the public in the task of securing observance of the law;

[932] *Ibid* xii
[933] Reiner (2010) 3. See also Police (Northern Ireland) Act 2000. Part VI s.32
[934] Newburn (2012) 1-2
[935] Sheehy (1993)
[936] See Emsley (2009)
[937] Brown (2014) 10-14
[938] *Ibid* 10

4. To recognize always that the extent to which the cooperation of the public can be secured diminishes, proportionately, the necessity of the use of physical force and compulsion for achieving police objectives;

5. To seek and preserve public favour, not by pandering to public opinion, but by constantly demonstrating absolutely impartial service to law, in complete independence of policy, and without regard to the justice or injustice of the substance of individual laws, by ready offering of individual service and friendship to all members of the public without regard to their wealth or social standing; by ready exercise of courtesy and good humour; and by ready offering of individual sacrifice in protecting and preserving life;

6. To use physical force only when the exercise of persuasion, advice and warning is found to be insufficient to obtain public cooperation to an extent necessary to secure observance of law or restore order; and to use only the minimum degree of physical force which is necessary on any particular occasion for achieving a police objective;

7. To maintain at all times a relationship with the public that gives reality to the historic tradition that the police are the public and that the public are the police; the police being only members of the public who are paid to give full-time attention to duties which are incumbent on every citizen in the interests of community welfare and existence;

8. To recognize always the need for strict adherence to police-executive functions, and to refrain from even seeming to usurp the power of the judiciary of avenging individuals or the state, and authoritatively judging guilt and punishing the guilty;

9. To recognize always that the test of police efficiency is the absence of crime and disorder and not the visible evidence of police action in dealing with them."[939]

These principles are the essence of policing by consent in the UK, which means that policing should be broadly approved by the society being policed.[940] Most parts of UK society are satisfied with the work of the Police, but some are not.[941]According to statistics released by the UK government in 2020, 75% of citizens in England and Wales aged 16 and over had confidence in local police in 2019,[942] which is an increase by 14% from 2018.[943] There is no equivalent to data on confidence in the KSA PF, and the relationship between the PF and the KSA population involves "uncharted territories."[944] There is also no strong Peelian tradition in the KSA, though Peelian ideas may be more relevant than first appears to KSA since some KSA PF have been trained in the UK[945] and other developed countries.[946]

In the UK, policing crime is a task which is not unique to the Home Office funded PFs, as policing is also based on a "multi-agency" approach which allows public-private entities to be involved within policing.[947] The idea of corporatism (the control of an organisation by large interest groups) sometimes underpins this approach when applied to specialist sectors such as complex industries or sectors such as banking.[948] As for policing cybercrime in the UK, victims (by reporting crimes), national public policing agencies and

[939] Brown (2014) 13-14
[940] Tyler (2009) 307-359
[941] Sheehy (1993)
[942] UK Government (2020) <https://www.ethnicity-facts-figures.service.gov.uk/crime-justice-and-the-law/policing/confidence-in-the-local-police/latest>
[943] BMG Research (2019) <https://www.justiceinspectorates.gov.uk/hmicfrs/publications/public-perceptions-of-policing-in-england-and-wales-2018/>
[944] Sharaf (2009). See also Walsh (2020)
[945] UK IPAB (2016) <https://www.statewatch.org/media/documents/news/2016/jun/uk-ipab-saudi-forensics-partnership-torture.pdf >
[946] For history and training, see Alobeid (1987) 80, Sharaf (2009) and Nasasra (2021) 899.
[947] Crawford (1994) 497-519
[948] *Ibid*

third parties which include those in the internet business and also non-profit private organisations are all involved:[949]

> "The latter may or may not pursue their own investigations and sanctions approaches without law enforcement involvement such as the Federation Against Copyright Theft (FACT), Get Safe Online and Cifas (the UK's fraud prevention service). It also includes organisations that have regular contact with the public, such as Citizens Advice."[950]

This adaptation of corporatism within policing has helped the UK to tackle cybercrime more effectively than many other countries, such as the KSA.

In the KSA, the KSA PF is the institution that seeks to maintain order and one of their essential roles is to police crime.[951] However, there are various institutions that share this role with the KSA PF, so, as crimes are varied and have diversified, the responsibility for policing crimes is shared among other institutions aside from the KSA PF.[952] The Traffic Police, and the Special Forces of Roads and Security are under one directorate, the General Directorate of Public Security, which is supervised by the MoI.[953] Therefore, it can be said that, collectively, those institutions are the KSA PF.

As mentioned in Chapter 4, before 2001, the KSA PF practiced policing, investigation, and prosecution.[954] During that time and until the establishment of the BIPP in 1995,[955] there was no separate entity for investigation and prosecution,[956] so PF officers were the first authority to process crime by stopping, catching, detaining, interrogating,

[949] Wall et al (2015) 13
[950] *Ibid* 13
[951] KSA MoI. The Police of Riyadh Province
[952] Interviews with Police Officers PO1 and PO2
[953] KSA MoI. General Directorate of Public Security
[954] Aldosari (2019) 10
[955] *Ibid*
[956] Mohammed (2017) 20

investigating, and prosecuting suspects.[957] This extensive role led to the misuse of power.[958] For instance, the KSA PF officers from the rank of lieutenant and higher would cover for each other and were rarely questioned for their mistreatment of the public.[959] At that time, the KSA PF officers were highly respected within KSA society.[960] This respect for PF officers was not only out of what De Botton sees as a natural unconscious appreciation of status,[961] but also it was out of fear for being under their mercy because it appears that the collective consciousness of the KSA PF at that time was not always observant of the humanitarian treatment of the population.[962] Therefore, it can be said that the vast power they possessed, along with being highly respected within the society, led to the abuse of power by the KSA PF.[963]

Furthermore, this respect for PF officers is a result of various factors which go beyond the scope of this thesis, such as the culture and the nature of the KSA society. In brief, the tribal hierarchy within the KSA society has led the population to maintain a high degree respect to tribal status and powerful tribes and families.[964] Until recently, most PF officers would be hired from "noble" tribes.[965] This tribal respect and hierarchy has rendered PF officers less accountable when they abuse their power because they are protected by the status of their tribes. The second factor is that the social life in the KSA is ruled by *Sharia.*[966] The KSA PF officers claim to be the protectors of *Sharia*[967] even though they might abuse their power, and people, especially during the spread of the *Sahwah*, would fear questioning by them because they might be viewed as challenging the teachings of *Islam*

[957] *Ibid* 20
[958] Interview with Detective of the PP D1
[959] Mohammed (2017) 10
[960] *Ibid* 10 and 52
[961] De Botton (2004)
[962] Mohammed (2017) 12
[963] *Ibid* 12
[964] Siddique et al (2016) 44
[965] Interview with Police Officer PO1
[966] Siddique et al (2016) 44
[967] Jerichow (1997) 27-37

regarding obeying the authority,[968] which PF officers represent. Not only were Saudi nationals exposed to PF brutality, but also vulnerable migrant workers in the country who were often specifically targeted, especially those from Bangladesh, India, and the Philippines.[969]

After the KSA passed its first CPL 2001, the role of the KSA PF was specified by legislation, rather than *Sharia*, and was thereby limited to the exercise of more distinct and better defined policing functions only alongside other entities[970] whose investigatory powers are merely initial powers which do not rise to the level of the investigative powers given to the PP. Additionally, investigative powers given to the PF should generally be either under the supervision of PP or under their review.[971] Therefore, it can be said that after limiting the role of the KSA PF, the CPL 2001 has consequently resulted in limiting the abuse of power by the KSA PF. In comparison with the situation before 2001, passing and executing the CPL 2001 was a human rights advance for the KSA, even though it did not cover all aspect of due process.[972] This legislation was an important step towards recognising and implementing international standards of human rights within the KSA legal system.[973] Nevertheless, some of the CPL 2001 provisions were in breach of human rights, especially in terms of privacy,[974] but they have not been modified in the CPL 2013 version. Therefore, the KSA was still expected by the international community[975] to deliver more legal reforms that would demonstrate a stronger commitment to human rights.[976]

[968] Alatawneh (2009) 726
[969] Sherry (2004)
[970] CPL 2001 Article 26
[971] Shareef (2016) 159
[972] Alshathri (2015) 10
[973]Alsubaie (2013)
[974] *Ibid* 82
[975] Universal Periodic Review (UPR), Saudi Arabia 3rd cycle <https://www.ohchr.org/EN/HRBodies/UPR/Pages/SAindex.aspx>
[976] Alsubaie (2013)

Unfortunately, the CPL 2013 that replaced the CPL 2001 (in response to the ongoing international pressure) was identical to the CPL 2001 in most of its provisions,[977] especially with regard to the right to an attorney.[978] Human Rights Watch asserted that it is not just the law which needs to be modified but, more importantly, the practice of the KSA officials who often breach human rights during the criminal process.[979] These breaches include arbitrary arrests, coercion, torture and inhumane treatment in detention, and search and arrest without a warrant.[980]

There is no obvious reason why the KSA authorities passed the CPL 2013 when they could have more simply amended the CPL 2001, but it is not uncommon for the state to act in this way.[981] Perhaps the KSA is still struggling to gain a comprehensive understanding of modern CPL and the demands of international human rights law. There is also the struggle with the *Sahwah* movement, which rejects modern law as an infringement of *Sharia.*[982]

Another explanation may lie in legal education. Until recently, there were thousands of students who were admitted to the Schools of *Sharia* across the country after graduating from secondary schools especially in Riyadh,[983] whereas only hundreds of students graduated from the leading non-religious Law schools in the KSA.[984] However, thousands of students are now admitted to law schools and the most popular choice of secondary schools graduates is to major in Law,[985] replacing *Sharia*. The reason why this statistic matters is that, until the recent past, *Sharia* graduates, who have less knowledge and understanding of modern law, were in control of the country's legal system as the KSA BLG which gives *Sharia* supremacy

[977] Alshathri (2015) 10
[978] HRW (2008) <https://www.hrw.org/reports/2008/saudijustice0308/saudijustice0308webwcover.pdf >
[979] *Ibid*
[980] *Ibid*
[981] Shareef (2016) 6
[982] Almibrad et al (2015) 15-18
[983] Imam Saud Islamic University, General Statistics <https://imamu.edu.sa/about/Pages/statistics.aspx>
[984] KSU, Graduation yearbooks <https://dar.ksu.edu.sa/ar/grad_yearbooks>
[985] KSA Ministry of Education
<https://moe.gov.sa/ar/knowledgecenter/dataandstats/Pages/educationindicators.aspx>

over the law,[986] which is one major reason for the outdated legal approach in the KSA. As noticed by Salameh, "the law in Saudi Arabia can primarily be described as consolidation of both written and unwritten laws."[987] The written laws can be easily understood by Law students as they have been taught more modern legal studies than those found in *Sharia,* but the unwritten laws need a higher degree of understanding of *Sharia*.[988]

Some aspects of *Sharia* are taught in Law Schools due the education structure in the KSA that dictates that Higher Educational institutions in the KSA must teach *Sharia* as part of all majors, including art and science.[989] This indoctrinates students with the notion of the supremacy of *Sharia* over every other domain. However, not all major aspects of *Sharia* are taught in non-religious Law Schools, and is only taught in specialist *Sharia* Schools. For instance, in Law schools, *Sharia* is taught in regard to its relationship with the law under the condition that it must not exceed more than 15% of the degree credits,[990] but the most important aspects of *Sharia,* such as interpretation of the *Quran* (*Tafsir*), Islamic jurisprudence (*Fiqh*), *Sunnah,* and Islamic Doctrine (*Aqidah*) are exclusively taught in *Sharia* schools.[991] From the establishment of the KSA until the near past, many *Sharia* scholars have looked down on modern legislation,[992] even though it might be compatible with *Sharia*. This strict perspective of the *Sharia* scholars has had a negative impact on the KSA law, including both versions of the CPL 2001 and 2013 which have not being fully respected by CCJs in the KSA.[993] It has already been discussed that CCJs used to disregard provisions of Article 3 of

[986] Almehaimeed (1993) 36
[987] Salameh (2017) 290-302
[988] Interview with Sharia Expert SE3
[989] Smith and Abouammoh (2013) 3-5
[990] Salameh (2017) 299
[991] Imam Mohammed Bin Saud Islamic University, College of Sharia <https://units.imamu.edu.sa/colleges/sharia/Pages/tosifatnew.aspx>
[992] See Mohammed Bin Ibrahim 1893-1969 book (*Governance of modern Laws*) where he strongly opposes governance by modern law. He was the first to officially be announced the general *Mufti* (Sharia advisor) of the KSA in 1953.
[993] Interview with Law Professor LP1

the CPL 2013.[994] A more specific reason for such an attitude is that it has been believed by CCJs, especially during the peak of *Sahwah* in the KSA,[995] that modern laws were created by non-Muslims who have based them only on the sanctity of the concept of liberty which is driven by secular principles.[996] Although such strict views remain, they are slowly fading away as KSA society gradually turns towards modernity. Nevertheless, while CCJs are socially and politically forced to accept the rule of law and rights, they might not fully respect it, including the CPL 2013.[997]

Subject to the ongoing role of *Sharia*, both the CPL 2001 and the CPL 2013 constituted modernising reforms that implement the principle of separation of powers and some elements of human rights such as due process, especially with regard to limiting the role of the KSA PF and recognising the role of a separate PP.[998] The PP has its own law in regard to their administrative functions,[999] while their legal practices are covered by the CPL 2013.[1000]

The KSA CPL 2013 refers next to PF officers as Preliminary Criminal Investigation Officers (PCIO),[1001] who work alongside other policing institutions. Article 26 lists the PCIO, but there is no clear definition within the CPL 2013 or its CPLER of the roles of these officers. However, it is still possible to say in general that they exercise policing powers in order to prevent crime, protect the public, protect life and property, bring the violators before justice and, most of all, preserve the law and maintain order.[1002] These PCIOs have been specified in Article 26 of the CPL 2013:[1003]

---

[994] See Section 4.3
[995] *Ibid*
[996] Udah (2009) 30
[997] Interview with CCJ CL1
[998] Mohammed (2017) 3
[999] KSA Bureau of Investigation and Public Prosecution (Public Prosecution) Law 1989
[1000] KSA Public Prosecution <https://www.pp.gov.sa>
[1001] CPL 2013 Article 24
[1002] Interviews with Police Officers PO1, PO2 and PO3
[1003] CPL 2013 Article 26

"Proceedings relating to preliminary criminal investigation shall be conducted by the following persons, each within their jurisdiction:

1- Members of the Bureau of Investigation and Public Prosecution in their area of specialities;

2- Directors of Police stations and their assistants in cities, counties, and townships;

3- Officers across all military sectors, with respect to crimes falling within their respective jurisdictions;

4- Governors of counties and administrators of townships;

5- Captains of Saudi vessels and airplanes, with respect to crimes committed on board;

6- heads of centres of the General Presidency for the Promotion of Virtue and Prevention of Vice, with respect to matters falling within their jurisdictions;

7- Employees and other persons entrusted with the powers of preliminary criminal investigation pursuant to special regulations; and

8- Agencies, committees and persons assigned to conduct investigation pursuant to relevant laws."[1004]

Additionally, Article 13 of the CPLER adds that all of the above must:

"Carry out criminal arrest activities - according to the provisions of paragraph (2) of Article Twenty-Six of the Law - in addition to the directors of Police stations, individuals and persons assigned to assist them."[1005]

[1004] CPL 2013 Article 26
[1005] CPLER Article 13

These Articles specify the officers who carry out the function of policing crime within the KSA jurisdiction. Even this long list is not comprehensive because other institutions are not included, such as the Anti-Drug Enforcement and Interior Intelligence Agencies that also police crimes.[1006] Another complication is that not all of those listed practice general policing powers, such as employees and other persons entrusted with the powers of preliminary criminal investigation pursuant to special regulations, agencies, committees and persons assigned to conduct investigation pursuant to the relevant laws, and captains of Saudi vessels and airplanes. Yet, although such individuals may have the authority to maintain order and hold limited and specified policing powers in particular locations, they do not practice general policing powers.[1007]

Even though Article 26 limits the role of the KSA PF to that which was practiced before 2001, it has strengthened the role of PP (previously known as BIPP) and given those officers a policing power along with their investigation and prosecution powers, as will be discussed in Chapters 6 and 7. It seems likely that this substantial amount of power might lead to its abuse, and what the KSA had successfully moved away from by limiting the KSA PF powers, has been compromised with the conferment of broad powers on the PP. Even though the policing power that the PP has is limited to their own area of expertise ("their area of specialities" according to Article 26), this limitation of power is vague because neither the CPL 2013, nor its executive regulation, explain what the precise limitations are. Moreover, the Bureau of Investigation Public Prosecution Law 1989 (PPL)[1008] does not explain any further what policing power the Bureau has. Therefore, there is a need to update the CPL

[1006] Strobl (2016) 553
[1007] Shareef (2016) 149
[1008] The PPL was passed by Royal Decree No. M/56 (29 May 1989). It used to be called Bureau of Investigation and Public Prosecution Law until 2017 when the name of the establishment has been changed to Public Prosecution. See KSA Royal Decree No. A/240 of 2017. Even though this Law created the Bureau in 1989, it did not exercise neither investigation nor prosecution until the Criminal Prosecution Law 2001 was passed. See Aldosari (2019) 66

because it deals mostly with the BIPP, which was subsequently renamed the PP in 2017,[1009] and thereafter does not even refer to this public body by its correct name.

Moreover, Article 26(6) should also be updated to include the new role of GPPVPV. Its role was limited in 2016 to advising against committing sins which are not serious enough to be considered as a policing matter.[1010] Before 2016, and since the establishment of this institution in 1974,[1011] it exercises policing powers of stopping searching and detaining suspects.[1012] The role of the institution was to maintain order regarding violations of religious principles which might constitute crimes.[1013] However, the role of this institution was vague and unprecedented within the modern countries from which the KSA took inspiration for its modern administrative system, mainly France via Egypt.[1014] This anomaly has led the KSA to minimize the GPPVPV's role, especially after the country started to allow music concerts, cinemas, less gender segregation in public and more choice regarding how women may dress in public.[1015]

In summary, it is possible to say that the CPL 2013 gave specified policing institutions the authority to police crime, as will be discussed in the coming subsection. Thus, when referring to the (Police) within the context of the KSA, the term does not only refer to the KSA PF, but also refers to all institutions that have policing powers most of which are supervised by the MoI. The most relevant to cybercrime are the KSA PF and the GPPVPV as the latter has one of the most important cybercrime units in the KSA, namely, the Electronic Extortion Prevention Unit (EEPU).[1016]

[1009] CPL 2013 Chapter 4
[1010] Said-Moorhouse (2016). l
[1011] GPPVPV < https://www.pv.gov.sa/Pages/AboutAuthority.aspx>
[1012] Interviews with PO3 and LP1
[1013] *Ibid*
[1014] Brintion (1930 copy)
[1015] Alomran (2020) <https://www.ft.com/content/81a8267e-1cc9-11ea-97df-cc63de1d73f4>
[1016] GPPVPV, EEPU <https://www.pv.gov.sa/Eservices/Pages/AntiExtortionService.aspx>

One reason why this latter unit was established in the first place is that the GPPVPV consider themselves as guardians of honour.[1017] This kind of specialisation had the consent and support of both the public and the government during the period that was dominated by *Sahwah* indoctrination, especially from 1979 until 2016, after which the role of the GPPVPV was limited to just reporting crimes to the KSA PF,[1018] as ordered by the KSA government.[1019] During the period in which they had greater powers, most GPPVPV officers were *Sharia* graduates.[1020] Therefore, it can be said that because they are *Sharia* graduates, GPPVPV officers acquired both public and government consent to protect honour based on a *Sharia* principle that states:

> "No statement shall be attributed to a person who remains silent, but silence in circumstances requiring a statement shall be deemed an acceptance." [1021]

Both the public and the government were silent when the GPPVPV declared themselves as the guardians of honour, even though it might be considered that the GPPVPV often overstepped their powers.[1022] Arguably, GPPVPV officers mistakenly took this silence as an indicator of consent and encouragement.[1023] The silence of the public and the government might have been driven by the notion of shame, because they were influenced by the *Sahwah* movement itself to consider it shameful to criticise those who protect honour.[1024] As a result, even though the EEPU is now an official unit, it started as a voluntary unit[1025] out of a sense of duty to prevent crimes (especially sexual extortion) that could bring shame to a very conservative society.

[1017] Jerichow (1997) 27-37
[1018] Interviews with Police officers PO1 and PO3
[1019] KSA Council of Ministers order No (289) 2016
[1020] Interviews with Police officers PO1 and PO3
[1021] Alzuhaili (2006) 160
[1022] Interview with Police Officer PO3
[1023] *Ibid*
[1024] *Ibid*
[1025] Awwad (2020)

5.2.2 Policing NCCs in the KSA: operational aspects

As already explained, the CPL 2013 vests policing powers in the hands of specified entities, including the KSA PF, referred to in the CPL 2013 as PCIO.[1026] This reference is not accurate because their powers are initial rather than preliminary,[1027] because, as will be discussed later in this chapter, they are subject to approval and supervision of the PP. Initial policing powers are detailed in several parts of the CPL 2013, which involve powers of stopping, arresting, detaining, searching and surveillance, and some can also be found in the KSA BLG which affords them constitutional recognition. It is uncommon for a national constitution to address issues such as policing powers, but the reason in this case is as follows. The KSA BLG was passed in 1992, almost ten years before the first CPL 2001, and so it includes policing powers because there was no specialist legislation regarding policing powers. During the 1980s and the 1990s (after the outbreak of *Sahwah*), the KSA struggled to deal with strict religious activist groups that put pressure on the country by demanding legal reforms to implement a purely *Sharia* based legal system.[1028]

Consequently, the BLG was passed to satisfy those demands,[1029] but some of those activist groups were not content with this settlement,[1030] so they tried to overthrow the government in order to takeover and Islamise the whole country.[1031] This enmity was because they believed[1032] that the Royal Family had lost its legitimacy,[1033] particularly in 1991 when the KSA sought help from foreign non-Muslim troops (led by the US Operation Desert Storm[1034] and the UK Operation GRANBY[1035]) in their war with Iraq 1990-1991.[1036] Many

[1026] See previous subsection
[1027] Interviews with Detective of the PP D1 and Law Professor LP1
[1028] Lacroix (2011) 200
[1029] *Ibid*
[1030] *Ibid* 201
[1031] *Ibid* 204
[1032] See Section 4.4
[1033] Aba-Namay (1993) 298
[1034] Collins (2019)

Sahaween (members of *Sahwah*) were strongly against the KSA government's action,[1037] and engaged in protests.[1038] This led to the arrest of many of those *Sahawah*-driven protestors,[1039] but in order to do so, the government needed a legal foundation for their arrests. Therefore, the BLG was implemented in 1992[1040] to send a message to those groups (and the general population) that: here is a constitution that respects *Sharia* by requiring the authorities to follow *Sharia* in their governance,[1041] and here are the legal policing powers that do not conflict with *Sharia*. Thus, policing powers were mentioned in the BLG and later in both versions of the CPL.

5.2.2.1 Operational aspects of policing NCCs in the KSA: Powers of stopping, arresting, interrogating and detaining

The PF functions begin with the powers of stopping, arresting and detaining, which are found in Article 36 of the BLG:

> "The State shall provide security to all its citizens and residents. A person's actions may not be restricted [stopped], nor may he be arrested or detained, except under the provisions of the Law."[1042]

The BLG recognises those powers and leaves it to other laws to explain them in more detail. "Law" mainly refers to the CPL. According to the CPL 2013 and CPLER, PF officers can stop, arrest and detain a suspect or suspects in a case of *flagrante delicto*. It has been explained in Article 30 that:

[1035] UK Ministry of Defence, 1990/1991 Gulf Conflict <https://webarchive.nationalarchives.gov.uk/20120816163733/http://www.mod.uk/DefenceInternet/AboutDefence/WhatWeDo/HealthandSafety/GulfVeteransIllnesses/19901991GulfConflict.htm>
[1036] *Ibid*
[1037] Lacroix (2011) 208
[1038] *Ibid* 209
[1039] *Ibid* 209
[1040] Aba-Namay (1993) 298
[1041] Alatawneh (2009) 730
[1042] BLG Article 36

> "A crime shall be deemed *flagrante delicto* if the perpetrator is caught in the act of committing such a crime, or shortly thereafter. It shall also be deemed *flagrante delicto* if the victim or a shouting crowd is found pursuing another person subsequent to the commission of the crime, or when the perpetrator is found shortly thereafter in possession of tools, weapons, property, equipment, or other items indicating that he is the perpetrator or accomplice thereto, or if, at the time, marks or signs indicating the same are found on his person."[1043]

In the case of *flagrante delicto*, PF officers can stop, arrest and detain suspects without permission from a competent authority.[1044] Nonetheless,

> "In other than *flagrante delicto* cases, a person may not be arrested or detained without an order from the competent authority."[1045]

This Article makes it clear that PF officers have the powers of arresting and detaining, and their exercise is conditioned with obtaining permission from the competent authority.[1046] What makes this Article vague is that it does not mention the power of stopping, and it seems that it has left this aspect to customary practice,[1047] which is contradictory with the rule of law. Moreover, this Article does not specify which authority is considered competent to grant permission. It is arguable that competent authority might be explained in further or previous Articles in the CPL 2013. Article 25 of the CPL 2013 sates:

> "Preliminary criminal investigation officers shall, in conducting their duties as provided for in this Law, be subject to the supervision of the Bureau of Investigation and Public Prosecution. The Bureau may ask the competent

[1043] CPL 2013 Article 30
[1044] Shareef (2016) 121
[1045] CPL 2013 Article 35
[1046] Shareef (2016) 121-123
[1047] Interview with Police Officer PO3

> authority to consider any violation or omission by any officer and may request that disciplinary action be taken against him, without prejudice to the right to initiate criminal prosecution."[1048]

This Article implies that the BIPP (now the PP) might be the competent authority mentioned later in Article 35 and all other later Articles in the CPL 2013. However, Article 25 makes it clear that the role of the PP is only supervisory. Therefore, when looking into Article 12 of the CPLER, it is possible to say that competent authority is the "public body to which the Preliminary Criminal Investigation Officer belongs".[1049]

Next, the power of interrogation is recognised by the CPL for the PP not the PF. However, PF officers exercise this power as it is legitimate even though there is no mention of it in the CPLs. As will be addressed later in Chapters 6 and 7, the PP approves of the PF initial investigation and does not conduct their own. The PF starts the criminal case file (dossier)[1050] after charging suspects with committing crimes. This dossier is best known in inquisitorial systems such of that of France.[1051] As been addressed in Chapter 4, the KSA transferred policies from Egypt which in turn was inspired by France.[1052] While this practice is not approved by the CPL, it existed before 2001[1053] when the KSA PF used to have a monopoly over criminal cases. So, the dossier was effective during that time, but it might be considered ineffective after passing the first CPL in 2001 which placed investigative powers in the hand of the PP. Therefore, it can be possible to say that exercising interrogation as a policing power in the KSA overlaps with the PP power of interrogation. Yet, it is practiced because the PF should fill in the dossier with legitimate reasons for exercising other

[1048] *Ibid* Article 25
[1049] CPLER Article 13
[1050] The dossier might be an indirect adaptation of the French model of criminal procedure. See Hodgson (2005). 32, 146, 191, 246
[1051] *Ibid*
[1052] See subsection 4.2.5
[1053] Mohammed (2017) attachments

legitimate powers. Although the PF practices the power of interrogation, it will not be addressed in this section or the next because such a power will be addressed fully in the next Chapter as it is practiced by the PP.

5.2.2.2 Policing powers in the KSA: powers of search, seizure and surveillance

The powers of searching and surveillance are initially founded in the BLG.[1054] Article 37 prohibits unlawful search and seizure,[1055] and Article 40 prohibits viewing and listening, which are forms of surveillance, to correspondence by telegraph and mail, telephone conversations, and other means of communication "except in cases set forth in the Law".[1056] Therefore, the BLG recognises the powers of search and surveillance, and it leaves it to the "Law" to determine which cases are eligible for using exceptional surveillance powers. By the word, "Law", it mainly refers to the CPL.

Along with giving and explaining the powers of stopping arresting, and detaining to PF officers, the CPL 2013 also gives them the powers of search and seizure and surveillance and explains them in detail.[1057] Chapter 4 of the CPL 2013 consists of Articles 41 to 55, and relate to seizure, searching people and dwellings.[1058] Thus, all of the Articles contained in Chapter 4 have been specified for the purpose of identifying those powers. It begins with a reminder of the privacy of both body and dwellings,[1059] and subsequently prohibits PCIO from searching dwelling and seizing evidence without obtaining a search warrant.[1060] Since investigators (who are assigned detectives to the office of the PP)[1061] are considered as

[1054] Some has compared it to the US constitution of this regard. See Naseeb et al (2011) 183-186
[1055] BLG Article 37
[1056] *Ibid* Article 40
[1057] Shareef (2016) 121-123
[1058] CPL 2013 Chapter 4
[1059] *Ibid* Article 41
[1060] *Ibid* Article 42
[1061] Interviews with Police officers PO1, PO2 and PO3 and detectives of the PP D1 and D2

judicial officers,[1062] they can issue the warrant to the KSA PF authorising and stating the grounds the search and seizure.[1063] Furthermore, the CPL 2013 allows PCIO to search both body and belongings in cases of lawful stopping, and it details that, when suspects are women, a search must be conducted by a woman.[1064] Similarly, when a dwelling is only occupied by a woman, the search must be conducted by women too.[1065] Moreover, "In case of *flagrante delicto*, a preliminary criminal investigation officer may search the dwelling of the accused and seize any items" without a warrant.[1066]

Additionally, as Article 45 states, in case there is circumstantial evidence against the suspect or any other occupier during the search of the dwelling, subject to lawful research, PCIO may search those suspects and seize evidence even though they are not named in the search warrant.[1067]

Allowing the search and seizure of circumstantial evidence without a warrant might seem odd, and the CPL 2013 should have required reasonable doubt or probable cause rather than circumstantial evidence, because it is legally difficult to convict a suspect in this way, unless there is plenty of circumstantial evidence.[1068] For instance, in England and Wales stops and searches carried out by a constable (Police officer) can be conducted based on circumstantial evidence on the basis of reasonable suspicion without a warrant, but, even so:

> "This section does not give a constable power to search a person or vehicle or anything in or on a vehicle unless he has reasonable grounds for suspecting that he will find stolen or prohibited articles".[1069]

[1062] PPL Article 3 Paragraph 3
[1063] CPL 2013 Article 42
[1064] *Ibid* Article 43
[1065] *Ibid* Article 53
[1066] *Ibid* Article 44
[1067] *Ibid* Article 45
[1068] Interview with Law Professor LP1
[1069] PACE, s.1(3)

Reasonable suspicion is to be proven during the criminal investigation while, during criminal conviction, UK prosecutors have to prove searching without warrant is beyond reasonable doubt.[1070] Moreover, in developed countries such as the UK, Police officers must show "reasonableness" when they acted without a warrant.[1071] To obtain a warrant, the police must prove reasonable suspicion under PACE ss. 8, 9.[1072] Similarly, in the KSA, lawful search and seizure is only limited to the crime suspected, but PCIO may seize evidence found which might reveal another crime during the process of searching a dwelling.[1073] More importantly, searching dwellings must be conducted in the presence of the occupier, and when it is not possible, it must be in the presence of the mayor of the neighbourhood and two neutral eyewitnesses.[1074] Other Articles in the Chapter mention formalities of searching and seizing such as what is to be written in the search warrant, to whom the search warrant is addressed, and where to keep seized evidence.[1075]

Chapter Five of the CPL 2013 consists of Articles 56 to 62, and they relate to surveillance powers. To begin with, Article 56 of the CPL 2013 is a mere reflection of Article 40 of the BLG which states:

> "Correspondence by telegraph and mail, telephone conversations, and other means of communication shall be protected. They may not be seized, delayed, viewed, or listened to except in cases set forth in the Law."[1076]

It can be said that BLG allows surveillance in narrow cases.[1077] Before going into further evaluation, the term surveillance in this context means observing the means of communication in order to maintain law and order, whether people under surveillance know

[1070] *Woolmington v Director of Public Prosecutions* [1935] AC 462
[1071] *Fox, Campbell and Hartley v the United Kingdom* [1990] paras.32-36.
[1072] PACE, ss.8 and 9
[1073] CPL 2013 Article 46
[1074] *Ibid* Article 47
[1075] *Ibid* Chapter 4
[1076] BLG Article 40
[1077] Naseeb et al (2011) 186

(overt surveillance)[1078] or not (covert surveillance).[1079] Article 40 of the BLG refers to the Law to specify those cases, but there is no Law in the KSA which is equivalent to the very detailed measures found in the UK's Police Act 1997, RIPA, and IPA 2016,[1080] which has changed "the covert policing landscape beyond recognition."[1081] However, it is possible to say that the CPL 2013 is the law meant in Article 40 of the BLG as it states:

> "Mail, cables, telephone conversations and other means of communication shall be inviolable and, as such, may not be accessed or monitored except pursuant to a reasoned order and for a limited period as provided for in this Law."[1082]

This Article recognises the power of surveillance. However, the following Article 47 of the CPL 2013 says that the order of surveillance is vested in the hand of the Chairman of the BIPP (now PP), and the other Articles in the Chapter specify the role of detectives regarding these powers.[1083] Therefore, the power of surveillance is better viewed as an investigative power rather than policing power and will therefore be explained in Chapter 6.

As discussed in this chapter[1084] and Chapter 4,[1085] the KSA PF as an institution no longer investigates crimes preliminarily, ever since the first law of criminal procedure came into force in 2001. Even though the KSA PF exercises investigative powers such as arrest, search, seizure, and interrogation, these powers are just initial. Therefore, when arresting anyone, they should immediately report it to the PP in order to have their permission to detain and interrogate the suspects.[1086] Also, they are not authorised to conduct search and

[1078] McKay (2010) 166
[1079] *Ibid* 194
[1080] See chapter 4 section 4.5
[1081] McKay (2017) 1
[1082] CPL 2013 Article 56
[1083] CPL 2013 Article 47 and Chapter 4
[1084] See Subsection 5.2.1
[1085] See Section 4.3
[1086] Mohammed (2017) 87

seizure unless proven by the PP.[1087] Thus, it is possible to say that, although policing powers and investigative powers might overlap, PF officers in the KSA do not function as detectives, and detection is mainly a function of the PP as will be addressed in Chapter 6.

5.2.3 The Police Culture in the KSA

It has been observed that policing culture is changing around the world, especially in late modern societies,[1088] and changes to one culture will affect the change of another.[1089] One significant impact of changing the Police culture at the political level is the constant need for reforms,[1090] which often aim to make the Police increasingly independent from politics and more dependent on individual professionalism.[1091] Also, Police culture changes in order to adapt within other levels other than the political; among of all is the social level, such as to reflect diversity or new risks to the population such as cybercrimes.[1092]

Even though the KSA is not a late modern society (or as yet even a modern society),[1093] it seeks multiple reforms[1094] which both directly and indirectly relate to its policing culture. Therefore, during the analysis of policing cybercrime in the KSA, multiple practices would appear from such changes such as applying unwritten ethical codes within the policing practice which were influenced by individuals' own personal conception of *Sharia*, which is a result of the absence of a written detailed code of practice,[1095] such as those found in the England and Wales PACE 1984.[1096] The KSA PF culture has been continuously changing since the establishment of the first policing institution in the year

[1087] *Ibid*
[1088] Reiner (2010) 116.
[1089] Newburn and Peay (2012)
[1090] Chan (1997) 55
[1091] Reiner (2010)
[1092] *Ibid*
[1093] Haddad & Stowasser (2004) 62
[1094] See Section 2.5
[1095] Interviews with Police officers PO1, PO2 and PO3
[1096] PACE Part VI

1924, which was supervised directly by King Abdul-Aziz.[1097] Then, the KSA PF, by the order the King Abdul-Aziz, became supervised by the Crown Prince in 1930 until the KSA PF became linked to the MoI in 1950[1098] to the present time.[1099] The practice of the KSA PF between 1924 until 1950 followed the orders of supervisors, which mainly comprises the King and his most trusted son (the Crown Prince Faisal).[1100] Then, the KSA PF practice was covered by the General Security Law 1950,[1101] the procedural provisions of which were abolished by the CPL 2001. Based on the 1950 Law, the KSA PF were conferred with the powers of arrest, search, seizure, interrogation and investigation, and Chief Police officers were allowed to bring suspects before judges (prosecution).[1102] Therefore, it can be said that the KSA PF were policing, investigating and prosecuting crimes all at once.

It is possible to say that there have been three different stages through which the KSA's PF culture has evolved. The first stage is from 1924 to 1950. In this period of time, the whole country was newly established and most of the population were illiterate Bedouins[1103] who scarcely understood modern professional policing.[1104] Therefore, this stage is better described as informal, since the unification of the KSA happened during the first half of this stage. The unification of the KSA in 1932 enabled the migration of large numbers of people from the deserts to the small cities in the following years, which have since become the country's major cities. [1105] Most of that generation during that time were shaped by their pre-migration lifestyle which was primarily linked to a constant need to follow natural sources of

[1097] Alkharashi (2015) 198
[1098] Strobl (2016) 552-556
[1099] *Ibid* 552-556
[1100] *Ibid*
[1101] Khidher (2007) 60
[1102] *Ibid* 60
[1103] Harper (2007) 39
[1104] Strobl (2016) 552
[1105] Alrasheed (2002)

water. [1106] When this generation settled in places where they could find food and water, they paid less regard to the secondary issue of structure of the police and their powers.[1107]

The prevailing education was limited to *Sharia*, so their demands of the PF centred on not hurting and spying on people (as *Sharia* dictates) and to protect honour.[1108] Most of the population were indebted to the new King who helped in providing them with a drastically different lifestyle, and for that they were exceptionally loyal.[1109] Therefore, they did not think of questioning the role of his PF. But, after oil was discovered in the KSA in 1938,[1110] the revenue it generated helped in establishing educational institutions for the children of the first generation, and it helped shape government entities through the extensive help afforded by Egypt.[1111] The PF culture in the KSA began to change slowly, especially after the PF became linked to the MoI rather than directly to the King.[1112]

The second stage of changing PF culture in the KSA began in 1950 and ended in 2001. As the descendants of the first generation became more educated and less dependent on rulers in comparison to the first generation,[1113] they began to demand more political and social changes that would enhance the status of *Sharia* within the KSA.[1114] The constant demands for *Sharia* led to the *Sahwah* movement finally taking control as a dominant ideology within the KSA in 1979. [1115] That was one of the reasons why the KSA's PF officers, as individuals, applied their own *Sharia* moral codes[1116] rather than the limited written legislation which the KSA had passed over the years, which manifested as multiple failed attempts by the government to define the PF and their role, as expressed in the Public

[1106] Harper (2007)
[1107] Alrasheed (2002)
[1108] *Ibid* 547
[1109] Troeller (2013) 129-130
[1110] Bronson (2006) 18
[1111] See Chapter 4
[1112] Strobl (2016) 552-556
[1113] Alrasheed (2002). 12 and 49
[1114] Bronson (2006) 10
[1115] Alrasheed (2002). 12 and 49
[1116] Interviews with Police Officers PO1 and PO3

Security Directorate Law 1949, Princes Law 1959, Internal Security Forces Law 1965, and Imprisonment and Detention Law 1978.[1117] The underlying response of the Royal Family to the spread of *Sahwah* which threatened the Crown was to allow arbitrary arrests[1118] and to oppose all attempts to separate prosecution from policing.[1119] However, the game changer was not the domestic political and social pressure to reform the police, but the international pressure the Crown experienced after the 1950s,[1120] resulting in various reforms such as the BLG[1121] which began to restrict policing powers.[1122] Therefore, as international pressure escalated, the KSA had been forced to finally formalise and limit the role of PF by passing the CPL in 2001.[1123] This was the tipping point to direct the PF culture in the KSA towards being more balanced and fair.

The third stage began in 2001 and lasts up until the present day. The legal recognition that the CPL 2001 gave to the PP as the entity that preliminarily investigates and prosecutes crimes might be considered as a political reform which again changed the PF culture, and by withdrawing their judicial powers, the KSA PF found that their social status had decreased.[1124] Therefore, they had become in need of social respect or as the German philosopher Georg Hegel calls it, "struggle for recognition",[1125] and in order to restore their social position, they became less violent, more tolerant and proved themselves worthy by catching more suspects.[1126] Perhaps the first two changes in the PF culture could be considered positive, as they used to be more violent and less tolerant. However, the later change of emphasis to proving themselves worthy to the public led them to commit more

[1117] Khidher (2007) 60-62
[1118] Lacroix (2011) 301
[1119] Interview with Police Officer PO1
[1120] Nehme (1994) 930-943
[1121] HRW (2008) <https://www.hrw.org/reports/2008/saudijustice0308/saudijustice0308webwcover.pdf>
[1122] See <https://www.bbc.co.uk/news/stories-50852379>,
Alrasheed (2006); Haykel et al (2015)
[1123] UPR, Saudi Arabia 1st cycle <https://www.ohchr.org/EN/HRBodies/UPR/Pages/SAindex.aspx>
[1124] Mohammed (2017) 52
[1125] Hegel (2018)
[1126] Mohammed (2017) 52-53

violations of the principles of fairness found in *Sharia,* such as by spying on people and disregarding the word of the *Guardian of Muslim*s (the King) by committing procedural errors, such as searching and seizing without warrant.[1127]

As discussed in this section, that was the practice until the CPL 2001 was passed. It is possible to say that, from the year 1930 until recently, the KSA PF culture has been shaped to apply personal changing moral codes rather than outdated vaguely written codes. This practice has led to two different ways that high-ranked PF officers, who are under less obligation of accounting for their actions, can conceive of fairness and effectiveness.[1128]

The first way is applying fair processes based on officers' own understating of *Sharia,* such as prohibiting themselves from the invasion of the privacy of others, the torture of the accused, and any form of abuse of policing powers.[1129] The second way is applying effective yet not necessarily fair processes based on their own understanding of fairness.[1130] This was perhaps the most common practice of the KSA PF when they had both investigative[1131] and policing powers. However, they still apply this moral code when policing crimes – including cybercrimes.[1132] This practice can be called the "unwritten police code."[1133]

Moreover, it has been discussed by Chan that since technology (such as keeping video and voice records of police practice) entered the field of policing, police culture has become more "transparent."[1134] One considerable modern technological impact on policing culture in the KSA is the involvement of all people in the KSA in the act of policing. In 2016, the KSA the Directorate of Public Security launched an app called *Kulluna Amn* (we all are security) where people within the KSA can report crimes to all public security sectors including the

[1127] Interviews with Police officers PO1, PO2 and PO3
[1128] *Ibid* PO1
[1129] *Ibid*
[1130] *Ibid* PO2 and PO3
[1131] See sections 7.4 and 7.5
[1132] Interviews with Police officers PO1, PO2 and PO3
[1133] Chan (1997 46
[1134] *Ibid* 52

PF.[1135] This involvement is crucial for two reasons; first, it has led the KSA's PF officers to be more disciplined and considerate because of the danger of being reported through the same app.[1136] Second, it has helped the KSA PF to detect crimes in general, and cybercrime in particular, because the latter is not easy for the KSA PF to detect.[1137] Additionally, Lessig's idea of code as a way of regulating cyberspace through "soft law" or "codes",[1138] and the regulatory pyramid[1139] suggests that cyberspace would regulate itself out of necessity and in the absence of practicable legislation.[1140] Therefore, it is possible to say that this technological impact on policing culture is one possible example of cyberspace regulating itself leading to changes in the policing culture.

In the context of involving all people in policing through technology, the KSA might have noticed that people have a tendency to desire power,[1141] including policing power.[1142] Thus, KSA society is traditionally conservative and authoritarian, and so is receptive to strong policing.[1143] Policing in itself is appreciated even if it might restrict individual freedoms.[1144] In this way, the police are given powers which the population accept and which accords to their desires.[1145] Therefore, it might be said that strong police power is popular.[1146] In a more modern version of the KSA society, policing has become limited to the PF, leaving room for those with more authoritarian tendencies to volunteer to protect (society, religion, and homeland) through the channels available to them. For example, in the recent past, and before limiting the role of the Religious Police in the KSA in 2016, many of those with

[1135] Alarabiya (2016)
[1136] Interviews with Criminal Defence Lawyer CL1, Detective of the PP D1
[1137] Interviews Police Officers with PO1 and PO3
[1138] Lessig (2006) 132
[1139] Ayres and Braithwaite (1992) 35
[1140] See Subsection 2.2.1
[1141] Interview with Law Professor LP1
[1142] *Ibid*
[1143] *Ibid*
[1144] *Ibid*
[1145] *Ibid*
[1146] *Ibid*

authoritarian inclinations were keen to volunteer in the GPPVPV which has been created at first by volunteers (mutaṭawwiʿen) and based on their own understanding of the *Sharia* principle of *Hisba*.[1147]

Currently, in the KSA, the more authoritarian tend to volunteer and report through the "We are all security" app. This has led many violations reported through this app to be "malicious reports", especially when it comes to cybercrime.[1148] Therefore, it can be possible to say that technology has had a considerable impact on PF culture in the KSA. For example, it has seemingly led to a willingness for the PF to treat policing as a communal endeavour and not as something which is left for the PF themselves to engage in.[1149] Even though the public's involvement in policing NCCs in the KSA may be limited to reporting them to the police,[1150] it has been seen that they often go further than that.[1151] Unlike policing NCCs, the KSA PF are more accountable when policing a cybercrime reported by an app because the public can track their reports on the app and question the PF about procrastination and delays through the press, social media or foreign pressure groups, since national pressure groups are suppressed in the KSA.

5.3 Policing cybercrime in the KSA

The role of the KSA PF has been analysed in the previous section in relation to NCCs. The reason that the role of the KSA PF with regard to NCCs has been analysed is that the KSA deals with cybercrime as being indistinct from NCCs with regard to the criminal

[1147] Jorn T (2017)
[1148] Awwad (2020)
[1149] Interview with Law Professor LP1
[1150] Interview with Police officer PO2
[1151] Interview with Police officer PO1

process,[1152] which includes policing. Therefore, it is crucial to the thesis to explain policing of NCCs in order to analyse and evaluate how the KSA deals with policing cybercrime.

The KSA employs the CPL 2013 and CPLER 2015 to regulate the criminal procedure of cybercrime including policing. This section discusses two main aspects regarding policing cybercrime in the KSA. The first aspect is institutional and deals with the allocation of responsibilities to policing authorities for policing cybercrime in the KSA. The second aspect is operational and discusses what powers and means are given to the policing authorities regarding the criminal procedure of cybercrime in the KSA. Therefore, this section is split (as was the previous section) into two subsections: institutional and operational.

5.3.1 Policing cybercrime in the KSA: Institutions

In Section 5.2 of this chapter, the policing institutions outlined in Article 26 of the CPL 2013 and Article 13 of the CPLER 2015 are analysed. Those identified institutions are established by the KSA to police NCCs, and their members are called PCIO. Furthermore, as previously mentioned, there are other institutions which police crimes in the KSA, yet they are not recognised in the primary law of criminal procedure in the KSA.[1153] Moreover, those institutions are also active in policing cybercrime because, as mentioned above, the KSA deals with cybercrime as it deals with NCCs and does not differentiate between NCCs and cybercrime in terms of its criminal procedure.

In contrast, developed countries such as the UK deal with cybercrime as being distinct to some extent from NCCs in terms of procedure and substance.[1154] In terms of policing cybercrime the UK has established dedicated cybercrime teams or units which are meant to police cybercrime in the UK in most Police force in England and Wales, overseen by the

[1152] See Section 2.2
[1153] See Subsection 5.2.1
[1154] UK NCSS 2016-2021

National Police Chief's Council (NPCC)[1155] and operating in accordance with the UK 2025 Policing Vision.[1156] In addition to local policing of cybercrime, the UK NCA has a national role in policing cybercrime.[1157] The UK NCA assists the Police, and this partnership has led to catching a large number of cybercrime perpetrators.[1158] Another part of the structure in the UK is that the City of London Police Fraud Unit specialises in the policing of cyber fraud.[1159] Additionally, there is a partnership within the UK between the Government Communications Headquarters (GCHQ)[1160] and the UK National Cyber Security Centre (NCSC)[1161] which is part of the Security Service (SS)[1162] to increase cybercrime reporting and to help with detection.[1163] Moreover, the UK has partnerships with "international law enforcement such as Europol, the FBI and the US Secret Service to share intelligence and coordinate action."[1164]

Unlike the KSA, the UK NCA takes a major role in the UK regarding cybercrimes and cyberattacks along with other intelligence agencies, such as GCHQ, the SS and the NCSC.[1165] Dealing with major organised cybercrime and disruption to electronic systems are core parts of their work. They may be specialist intelligence institutions whose reliance on community support and consent is reduced compared to local policing, but they can be counted as policing institutions for these purposes.[1166] Most of them are recognised in law, for example the Security Service Act 1989[1167] and the Intelligence Services Act 1994,[1168]

[1155] UK National Police Chief's Council (2019) <https://news.npcc.police.uk/releases/dedicated-cybercrime-units-get-million-pound-cash-injection>
[1156] UK National Police Chief's Council, Policing Vision 2025 <https://www.npcc.police.uk/NPCCBusinessAreas/ReformandTransformation/PolicingVision2025.aspx>
[1157] UK NCS <https://www.nationalcrimeagency.gov.uk/what-we-do/crime-threats/cyber-crime>
[1158] Saunders (2017) 6
[1159] Wall and Williams (2013) 409
[1160] UK Government Communications Headquarters <https://www.gchq.gov.uk/information/cyber-threat> See also Intelligence Services Act 2004.
[1161] UK NCSC <https://www.ncsc.gov.uk/>
[1162] UK Security Service <https://www.mi5.gov.uk/cyber>
[1163] Saunders (2017) 8
[1164] UK NCA, What we do <https://www.nationalcrimeagency.gov.uk/what-we-do/crime-threats/cyber-crime>
[1165] UK NCSC <https://www.ncsc.gov.uk/>
[1166] Saunders (2017) 6
[1167] UK Security Service Act 1989
[1168] UK Intelligence Services Act 1994

with the exception of the NCSC, and these agencies are subject to oversight, especially by independent commissioners who produce reports about them.[1169] Within the context of addressing those intelligence institutions, the concepts of high policing and low policing, as explained by Brodeur, are helpful explanations.[1170] Generally, high policing or "policing political activities" or "political policing"[1171] is related to an element of "protection of the political regime"[1172] from internal threats. For instance, the UK SS and NCA are high policing; specialist and with political direction rather than community or semi-autonomous direction as occurs with UK local police forces (low policing). As noticed by Walker and Masferrer, high policing involves intelligence, terrorism, and security, and low policing involves crimes.[1173]

The KSA PF institutions use advanced technology to catch cybercrime,[1174] but the approach does not differentiate between NCCs and cybercrime in terms of policing in its CPL 2013 or any other legislation. At the same time, the KSA MoI, which is the Ministry that oversees the KSA PF, [1175] contains a cybercrime unit which assists the KSA PF,[1176] but this unit is not mentioned in the CPL 2013, making its operation questionable in terms of its legality.[1177] It might be argued that this cyber unit is an administrative entity only; therefore, there is no need to recognise it by law because it does not have a legal impact. Nevertheless, this entity does have a legal impact because it provides assistance to the KSA PF, processes the reported cybercrimes and, most importantly, intercepts communications.[1178] Therefore, it

[1169] Information Commissioner's Office <https://ico.org.uk/about-the-ico/>
[1170] Brodeur (1983) 508-520
[1171] *Ibid* 512
[1172] Brodeur (2011) 226
[1173] Walker and Staniforth (2013) 303
[1174] Alali (2016) 11
[1175] Strobl (2016) 555
[1176] Alali (2016) 1
[1177] Beetham (1991) 6
[1178] Interviews with Detective if the PP D1, Police Officers PO1, PO3 and Criminal Defence lawyer CL2

should be recognised by the law because it deals directly with the right of privacy and impacts on criminal procedure.

The same doubts about legality apply also to the GPPVPV which operates an EEPU[1179] that might be characterised as a policing cybercrime unit. Similarly, the Anti-Drug Enforcement has an Electronic Unit that detects drug trafficking on the internet.[1180] Even though those units use technology to assist in catching cybercrime, they still deal with cybercrime as NCCs in terms of the criminal procedure, especially in regard to operations as will be discussed under the next subheading.

Although the KSA PF might contain those fragments of cyber units within the KSA PF institutions, they are not developed sufficiently to be able to deal with cyber evidence effectively and efficiently;[1181] they cannot deal with them properly because the nature of cyber evidence is different from that which policing institutions commonly handle.[1182] In fact, cyber evidence collection techniques vary among these units.[1183] For instance, cyber evidence that can be found on smartphones is technologically different from cyber evidence found on laptops, which is in turn different from cyber evidence found on the internet.[1184] It can be said that having units or sub-departments within the policing authorities to assist the policing institutions by using advanced technology is not enough to distinguish cybercrime from NCCs procedurally. One other crucial aspect of policing cybercrime is to legally identify how the KSA PF functions or operates in cyberspace.

The KSA equivalents to the UK cybercrime policing institutions have been addressed in various sections of this research, such as the NCA, the MCIT, the CITC, and the KACST. However, unlike the UK, these KSA institutions are administrative, and their roles are

[1179] GPPVPV <https://www.pv.gov.sa/eservices/Pages/AntiExtortionServiceInfo.aspx>
[1180] Alali (2016) 63
[1181] Interview with Law Professor 01
[1182] Oparnica (2016) 143
[1183] *Ibid* 144
[1184] *Ibid* 144

fragmented and ambiguous. They seem to assist investigation more than taking part in actual policing because, in the KSA's inquisitorial system, policing is related to the executive branch, while investigation is related to the judicial branch.[1185] These institutions perhaps have less to offer regarding tackling cybercrime, but they are able to collaborate effectively to tackle cyberattacks because the KSA state gives high priority to external threats[1186] than internal threats.[1187]

5.3.2 Policing cybercrime in the KSA: Operations

Even though the KSA has its own specialist units to assist the KSA PF in catching cybercrime suspects, the KSA policing institutions' powers in cyberspace are not fully identified in the law. This shortcoming makes clear that the KSA is still struggling with the new phenomena of cybercrime and has failed to fully distinguish cybercrime from NCC in regard to policing. When looking into the powers that the CPL 2013 gives to the policing institutions – stopping, arresting, detaining, searching, seizing, and surveillance[1188] – the CPL 2013 does not distinguish between cybercrime and NCCs, and these powers are used by the policing institutions in regard to cybercrime and NCCs simultaneously. However, those powers should have been distinguished depending on whether it relates to cybercrime or NCCs due to the nature of cybercrime and the special problems which it poses for policing. For instance, surveillance of cybercrime within the KSA jurisdiction is not covered by any

[1185] Aldosari (2019) 81
[1186] External cyberattacks, or what the UK calls "hostile activity", might involve other sovereign States where they might be involved in an act of cyberwar (Stated sponsored cyberthreats). See Cornish et al (2009) This type of cyberattacks will not be addressed in this research because it does not often affect criminal procedures.
[1187] Alsowailm et al (2017) 10
[1188] Shareef (2016) 121-123

law, and it can be said that it is left up to the conscience of PCIO to evaluate whether they are invading privacy or not.[1189]

Therefore, for the KSA's approach to be comprehensive (effective) and also certain and clear (fair and legitimate), it should differentiate between the KSA PF operations in cyberspace and physical space. For instance, obtaining a warrant to search the premises and seize physical evidence related to NCCs is hardly applicable to cybercrime because cybercrime is perpetrated in virtual space which might make the specified policing powers for NCCs unsuitable for cyberspace.[1190] Therefore, in this sub-section, the policing powers suitable for dealing with cybercrime will be discussed.

5.3.2.1 Policing powers with regard to cybercrime in the KSA

In this sub-section, the operational steps which can be taken by the KSA PF within the virtual space will be discussed. This analysis will allow consideration of what operational laws exist (mainly highlighted in the CPL 2013 and related to NCCs) and what shortcomings remain.

5.3.2.2 Policing powers regarding stopping, arresting and detaining cybercrime suspects

The CPL 2013 allows PCIOs to stop, arrest and detain suspicious people.[1191] In NCCs, suspicious behaviour can often be reported by an average person or be spotted by a trained PCIO when viewing suspicious physical behaviour.[1192] Therefore, the CPL 2013 allows PCIO to stop, arrest and detain suspects.

In contrast, suspicious behaviour is not so easily detected in the context of cybercrime because it is done mostly without a recognisable change that can be observed in physical

[1189] Interviews with Police Officers PO1, PO2 and PO3 and Law Professor LP1
[1190] Bandler and Merzon (2020) 116-118
[1191] Shareef (2016) 121-123
[1192] *Ibid*

space.[1193] For instance, a person who bullies people on social media does not need to follow them physically or shout at them through direct contact.[1194] All they need is access to the internet.[1195] In this example, a bully could be sitting in a public place and cause people distress without any recognisable suspicious change to their facial expression or body gestures.[1196] They are even less detectable if the conduct arises in a private dwelling.[1197] Hence, the question which arises here is whether, due to the absence of special clauses within the CPL 2013 to afford policing powers over cybercrime, PCIOs can stop, arrest, and detain whomever they suspect of committing cybercrime based on suspicion of internet activities?

It is possible to say that PCIOs could stop, arrest, and detain whomever they suspect of committing cybercrime, regardless of whether it is allowed by the CPL 2013 or not.[1198] The powers given to the KSA PF to police cybercrime are the same powers given to them to police NCCs.[1199] As a result, there are two major flaws within the KSA's approach. The first flaw is that, even though the CPL 2013 allows for policing powers, it does not limit them properly, neither within the CPL 2013 itself nor within its executive regulations. The second major flaw is that the CPL 2013 does not allow for the dismissal of criminal cases that do not follow the legal criminal process within the law[1200] which might lead PCIOs to abuse their policing power.[1201] For instance, when a PCIO stops, arrests and detains a cybercrime suspect who is suspected of committing cybercrime which does not fall into the jurisdiction of PCIO, the criminal case will not be dismissed on the grounds that the process was not lawful.[1202]

[1193] Bandler and Merzon (2020) 285-292
[1194] *Ibid.* 105
[1195] *Ibid*
[1196] Interview with Detective of the PP D1
[1197] *Ibid*
[1198] Interviews with Police officers PO1, PO2 and PO3
[1199] See Subsection 5.2.2
[1200] See sub section 7.5.1.1
[1201] Interview with Detective of the PP D1
[1202] Interviews with Police officers PO1, PO2 and PO3 and Detective of the PP.

In practice, the PCIOs could be disciplined administratively for overstepping their authority, and the criminal case would take its course despite its initial unlawfulness.[1203] This practice is not exclusive to cybercrime as it is common across all areas of crime in the KSA.[1204] It has been argued that the CPL 2013 does not allow for dismissal of criminal cases on the ground of procedural errors because it is immoral to let criminals escape justice, which is unfair in the eyes of the *Sharia* as it strictly calls for justice.[1205] This is a popular argument among *Ulama* within the KSA[1206] whom may be said to be an unhelpful influence on the CPL 2013 in general due their lack of understanding of modern law and cyberspace.[1207]

Even though the principles found in *Sharia* are from the past, they can still provide guidance to the KSA regarding policing crime and cybercrime, especially in terms of respacing people's privacy. On one hand, spying (surveillance) is allowed for detectives to conduct, but not for the KSA PF under the CPL 2013 because the KSA detectives (who are part of the PP structure) have a judicial function rather than an executive function, as will be discussed later in Chapter 6 when addressing surveillance as an investigative power. On the other hand, *Sharia* has almost nothing to say about spying as a power.[1208] It encourages individuals not to engage in spying[1209] but does not explicitly mention the authorities in this regard. Therefore, spying is seen as a sin rather than a crime.[1210] In this context, *Sharia* leaves the regulation of spying as a power to the legislative authority through the principle of *Shura,*[1211] which in its turn has failed to deliver a comprehensive regulation and understanding of the relevant powers. The current CPL 2013 also does not comprehensively state what powers of surveillance may be used nor does it restrict unlawful search and

[1203] *Ibid*
[1204] *Ibid*
[1205] Mahdi (2013) 39
[1206] *Ibid*
[1207] Interviews with Law Professors LP1 and LP2.
[1208] Alqaysi (2019) 114-132
[1209] *Ibid*
[1210] *Ibid*
[1211] See Section 4.3

seizure.[1212] The powers of policing are mentioned within the CPL 2013, but there are not many safeguards to restrict the government from abusive policing by way of surveillance.[1213]

Both primary sources of *Sharia* (the *Quran* and the *Sunnah*)[1214] contain implied policing powers,[1215] and they allow for the dismissal of cases for errors in practice in order to restrict the authority from abusing its policing powers. The *Quran* says:

> "And it is not righteousness to enter houses from the back, but righteousness is [in] one who fears Allah. And enter houses from their doors."[1216]

Also, it says:

> "O you who have believed, do not enter houses other than your own houses until you ascertain, welcome and greet their inhabitants. That is best for you; perhaps you will be reminded."[1217]

It appears from these scriptures that it is not allowed to enter premises without obtaining permission from the residents; otherwise, it is to be considered as an invasion of people's privacy.[1218] This would be an obvious reason for CCJs, who claim to apply *Sharia* on criminal cases before them, to dismiss criminal cases based on procedural error. [1219] This is not to encourage Muslims to commit crimes and escape justice based on procedural error as some might argue,[1220] but to encourage the official authority in Muslim societies to respect privacy.

[1212] Interview with Law Professor LP1
[1213] See subsection 6.2.2.3
[1214] Saifi (2013) 33
[1215] Almuallami (2008) 7
[1216] Holy Quran Chapter 2 verse 189
[1217] Holy Quran Chapter 18 verse 27
[1218] Almuallami (2008) 11
[1219] Interview with Criminal defence Lawyer CL3
[1220] Mahdi (2013) 39-52

Similarly, the Prophet Muhammed rejected the confession of one of his companions when she admitted on multiple occasions having committed *Zina* (adultery),[1221] which is a crime mentioned in *Quran.*[1222] He implied by this rejection that the *Quran* conditioned applying the punishment for adultery with the testimony of four trustworthy eyewitnesses who must clearly see the sexual intercourse with their own eyes simultaneously.[1223]1400 years ago, the Police did not exist in contemporary form, but it can be said that some policing powers were shared between Prophet Muhammed's companions, such as stopping violators and reporting them to the Prophet.[1224]

Therefore, it can be said that when the woman confessed of committing adultery, Prophet Muhammed enacted what can be viewed in the modern era as a dismissal of the criminal case on the ground of a flawed procedure.[1225] This dismissal of adultery cases happened twice in the era of Prophet Muhammed,[1226] even though the strongest of all evidence – confession[1227] – was present.

Moreover, Prophet Muhammed says:

> "…so you must keep to my Sunnah and to the Sunnah of the *Khulafa Ar-Rashideen* (the rightly guided caliphs), those who guide to the right way. Cling to it stubbornly [literally: with your molar teeth]."[1228]

This textual guidance is a clear indication that Muslims must follow the Prophet Muhammad's successors [his Companions] in their interpretation and application of *Sharia.*[1229] One such successor of the Prophet Muhammad is Omar Bin Alkhatab.[1230] When

[1221] Alshubily (2005) 5
[1222] Udah (2009) 83
[1223] *Ibid* 600
[1224] Almuallami (2008) 7
[1225] Alqaysi (2019) 302
[1226] *Ibid*
[1227] Udah (2009) 600
[1228] Altermithi 824-892 AD (No 266)
[1229] Saifi (2013) 34
[1230] Almuallami (2008) 7-19

Omar ruled, four years after Prophet Muhammad's death, he was practicing *Assah,* which is known in the modern world as policing,[1231] one night when he heard a Muslim man singing inappropriate songs. Omar peaked through the window and saw a man drinking wine[1232] which is a crime mentioned in *Quran.*[1233] As the highest authority in town, he commanded the man to open the door to arrest him.[1234] However, the drunken man said:

> "O Omar! You want to punish me because I sinned once, but you sinned three times Allah says; "Do not spy", but you spied, and "Enter houses by their doors", but you entered by the window, and "Do not enter houses until you have been given permission, and greet the occupants with peace", but you did not seek permission, nor did you give the greeting of peace."[1235]

Omar laughed and walked away and did not catch the violator, knowing that he had committed what can be considered in modern language as a procedural error.[1236]

The KSA claims to comply fully with the principles of *Sharia,* yet it fails to deliver appropriate legislation that allows for dismissal of criminal cases on the ground of procedural errors.[1237] It is not only a failure at the legislative level, but also at the level of the judiciary.[1238] As explained in Chapter 2, judges in the KSA are only bound to the rule of *Sharia*,[1239] yet there only one published cybercrime case, in the KSA that has been dismissed on the grounds of a procedural error.[1240] For this reason, PPCIO have an operational policing flexibility in cases of cybercrimes committed within the KSA jurisdiction with regard to stopping, arresting, and detaining cybercrime suspects since they can commit procedural

[1231] *Ibid*
[1232] *Ibid*
[1233] Udah (2009) 83
[1234] Almuallami (2008) 7-19
[1235] Alsalabi (2003) 342-344
[1236] *Ibid*
[1237] Dismissal of criminal cases based on procedural error do exist in practice, yet they are only personal effort by CCJs and not binding by neither Sharia nor law as will be discussed in subsection 7.5.1.1
[1238] Interview with Law Professor LP1
[1239] See Section 2.3
[1240] See appendix F, No 1

errors without much consequence.[1241] Not only can they stop, arrest and detain cybercrime suspects, they can also search, seize, and observe cybercrime suspects with flexibility allowed indirectly by the KSA Law of 2013.[1242]

5.3.2.3 Policing powers of search, seizure and surveillance over cybercrime

Just as it recognises the operational policing powers for stopping, arresting and detaining cybercrime suspects, the CPL 2013 also permits the search, seizure and surveillance of cybercrime suspects.[1243] Those recognised powers within the CPL 2013 are intended by the KSA legislative branch to be applied to NCCs. However, since the KSA does not differentiate between cybercrime and NCCs in terms of criminal procedure, including the policing of cybercrime, those policing operational powers are applicable to cybercrime also.[1244]

5.3.2.3.1 Search and seizure

In NCCs, PCIOs can search and seize evidence by obtaining warrants and, in cases of *flagrante delicto*, without a warrant.[1245] Similarly, PCIOs can search and seize cyber evidence based on what the CPL 2013 allows in terms of policing powers.[1246] Therefore, it can be said that policing powers of searching and seizing NCCs evidence allowed by the CPL 2013 are the same that are applied for cybercrime evidence, so there are no experts and specialists to deal with such matters.[1247]

[1241] Interview with Law Professor LP1
[1242] Interviews with Police Officers PO1, PO2 and PO3
[1243] Shareef (2016) 121-123
[1244] See appendix F
[1245] Shareef (2016) 121-123
[1246] *Ibid*
[1247] Interviews with Police Officers PO1, PO2 and PO3

As noted by Casey, policing cybercrime should be undertaken by specialists.[1248] Since the CPL 2013 allows PCIOs to search and seize cyber evidence and treats them in a procedural sense the same way as NCCs evidence, the indication is that the KSA's approach is unfair and ineffective.[1249] It might be acceptable to search and seize cyber evidence by PCIOs when they obtain a warrant, however, it is not acceptable to search and seize cyber evidence without a warrant in cases of *flagrante delicto.* In the absence of any legislation that deals comprehensively with policing powers within cyberspace in the KSA, PCIOs would have to happen upon suspects of cybercrime in cases of *flagrante delicto*, [1250] which does not seem logical because such a criminal action does not happen in clear sight.[1251] There are three main reasons for why it is not acceptable to search and seize cyber evidence without a warrant in cases of *flagrante delicto*.

The first main reason that it is unacceptable for PCIOs to search and seize cyber evidence without a warrant is that it is difficult to detect cybercrime, even by a specialist in computer science.[1252] Regular PCIO officers are trained to deal with NCCs evidence; for cybercrimes, they lack training.[1253] One reason that they lack training is not because the training itself is wholly absent, but because the trainees, especially police officers, lack the appropriate background qualifications to improve from the training.[1254] Therefore, they are likely to lack the expertise to deal with cyber evidence even though they still have some relevant operational policing powers under the CPL 2013. The second major reason is that in many cybercrime cases, cyber evidence does not fall within the KSA's jurisdiction, making it unlawful for those officers to search and seize cyber evidence which involves another

[1248] Casey (2011) 179
[1249] Next Section
[1250] Interviews with Police Officers PO1, PO2 and PO3
[1251] Bandler and Merzon (2020) 230
[1252] Casey (2011) 229
[1253] Almutairi (2013) 103-119
[1254] *Ibid*

sovereign entity.[1255] Therefore, the complexity of cyberspace makes it impossible to apply traditional criminal procedure rules to the criminal procedure of cybercrime.[1256] The third reason is that those officers are uncertain about how to avoid being unfair by applying their own moral code of what is right or wrong.[1257] However, what the law dictates in regard to evidence-gathering in cyberspace is left uncertain.[1258] This indicates that the law of criminal procedure with regarding to cybercrime is neither effective nor fair.[1259]

5.3.2.3.2 Surveillance

As discussed in this chapter, policing authorities are allowed to intercept communications data under the CPL 2013 and the BLG.[1260] KSA law does not address surveillance in specific terms and therefore does not differentiate in its laws between content data and communications data, leaving open the possibility for privacy to be breached. A better approach to this can be seen within the UK IPA 2016 which distinguishes between communications data that is subject to interception and content data which is subject to retention.[1261] The UK draws such a distinction in order to protect privacy because content data constitutes private personal data.[1262] Because communications data constitutes a tool for the UK intelligence and security services to track perpetrators on the internet, interception of communication data and even bulk surveillance is allowed by the IPA.[1263] However, such interception can easily breach the human right for privacy, so there must be safeguards when allowing such spying.[1264]

[1255] See chapter 2 sections 2.2 and 2.3
[1256] *Ibid*
[1257] Algarni (2013) 511
[1258] Bandler and Merzon (2020) 269
[1259] Next Section.
[1260] See Section 5.2
[1261] Boukalas (2020) 5
[1262] *Ibid*
[1263] Murray & Fussey (2019) 31-60
[1264] *Ibid* 34-35

From the European Court of Human Rights' judgment in *Szabo and Vissy*,[1265] Murray and Fussey note two safeguards:

> "… first, the use of bulk techniques must be restricted to circumstances that are strictly necessary to safeguard democratic institutions. This indicates that powers may only be used in relation to certain categories of serious crime, although this requirement should perhaps be more appropriately read as safeguarding the components essential for a democratic society. Second, if such powers are appropriate as a general consideration, then the strict necessity test further requires that, at an operational level, powers must be 'vital' to an individual operation."[1266]

Therefore, it is possible to say that surveillance in the UK is likewise allowed, yet it is sufficiently regulated and restricted to be potentially fair even though there are some ongoing challenges related to it regarding the human right to privacy,[1267] especially after the Snowden[1268] revelation of the government spying on people using vague (or even non-existent) policing powers in cyberspace.[1269]

The interception of communications data in the KSA is a form of surveillance and is authorised by the investigative institution, the PP.[1270] Moreover, the power of surveillance in the KSA is better understood as an investigative power not a policing power, because it is authorised by the PP for the purposes of investigation.[1271] The purpose of making such distinction is to inform where to better control this power. It can be deduced that the CPL 2013 does not consider surveillance to be a precautionary measure that is authorised before

[1265] *Szabo and Vissy v Hungary* (n 5) para 73
[1266] Murray & Fussey (2019) 56
[1267] Hirst (2019) 403-421
[1268] See Greenwald (2014)
[1269] Hirst (2019) 403-421
[1270] CPL 2013 Chapter 6
[1271] *Ibid*

the crime is committed, rather, it is an instrument of investigation which is authorised after a crime is committed, which is likely to lead to many escaping justice.[1272] That is why the KSA PF conducts surveillance even though not expressly permitted to do so by the CPL 2013.[1273]

Despite this legal limitation, policing institutions in the KSA conduct surveillance within cyberspace in order to anticipate cybercrime without the authorization of PP and before the crime is committed.[1274] Therefore, the question that arises here is whether it is lawful for the KSA policing institutions to conduct unauthorised surveillance. In practice, it seems like the unwritten customary law (*Sharia*) does not rule out this type of surveillance because it serves a greater purpose.[1275] However, this is not how the CPL should work because, aside from their fairness and effectiveness, for the set of the rules to be considered as a law, they must be written and passed by a competent authority and there must be certainty about it.[1276] Similarly, the KSA BLG emphasises that legislation must be passed by Royal Decree and published in the Official Gazette.[1277] Therefore, policing institutions should not conduct surveillance for the purpose of policing because this kind of power does not exist in the written rules, even if officers within those institutions believe they exercise a moral underpinning to distinguish right from wrong.[1278] Nevertheless, the KSA legal system – especially when it comes to criminal cases – gives this kind of surveillance implied legitimacy because no procedural error clause is included within the CPL 2013.[1279]

[1272] Alqaysi (2019) 140
[1273] Interviews with Police Officers PO1 and PO2
[1274] *Ibid*
[1275] *Ibid*
[1276] Beetham (1991)
[1277] BLG Articles 70 and 71
[1278] Mahdi (2013) 39-52
[1279] *Ibid*

In the absence of clear direction in KSA law, reform models by way of policy transfer should be considered.[1280] The England and Wales PACE allows for the rejection of criminal evidence obtained unfairly[1281] and thus provides a more nuanced rule than that found within KSA legislation. Moreover, the UK seeks to avoid procedural error in regard to the criminal investigation of crimes, including cybercrime, utilising two main procedures. The first is that the UK tries to comply by specific legislation with international human rights law.[1282] Additionally, the UK passed the Human Rights Act 1998[1283] in order to make international human rights generally enforceable in the UK.[1284] The second is that England and Wales law limits errors in the criminal process by following highly bureaucratic procedures that tackle possible errors.[1285] One fair bureaucratic safeguard which the UK PACE ensures dismissal of evidence acquired in violation to the process; such exclusion is vested in the hands of criminal judges.[1286] Moreover, the bureaucratic procedure requires prosecutors to prove that evidence has been obtained legally.[1287] Therefore, the UK laws always tend to be intensive and comprehensive. For instance, when the European Court of Justice invalidated the European Data Retention Directive (2006/24/EC) by allowing 12 months of data retention in 2014, the UK passed Data Retention and Investigatory Powers Act 2014.[1288] However, the UK High Court found it was not to compatible with human rights requirements in EU law,[1289] which is one reason why the IPA 2016 was passed and then modified again.[1290]

[1280] The UAE exercises a different approach from the KSA which could be viewed as fairer. Article 228 of the UAE Criminal Federal Law No (35) 1992 about concerning criminal procedure says: "The voidance of the procedure shall entail the voidance of all preceding procedures and the following ones, if not based on it."
[1281] PACE Section 78
[1282] Hoffman and Rowe (2013) 63-92
[1283] UK Human Rights Act 1998
[1284] Hoffman and Rowe (2013) 63-92
[1285] *Ibid* 39-51
[1286] PACE ss.76, 78.
[1287] *Ibid*
[1288] UK Data Retention and Investigatory Powers Act 2014
[1289] *Liberty v Home Office* [2018] EWHC 957 (Admin)
[1290] Data Retention and Acquisition Regulations 2018, SI 2018/1123. See Boukalas (2020) 5

On the other hand, it is possible to say that the KSA legal system, as represented by the CPL 2013, affords PCIOs the space to commit procedural mistakes such as spying and conducting surveillance without permission because criminal cases continue on their legal course even though those criminal cases are procedurally flawed.[1291] This flexibility is argued by some to be ineffective because it causes uncertainty and is unfair because privacy is not fully protected.[1292]

A remedy for this found in the UK.[1293] Even though there may have been procedural mistakes committed by the UK Police, these mistakes can potentially be identified for two main reasons. First, the overseeing bureaucracy (within policing agencies themselves and through the ICPO) reduces the chance of procedural mistakes being committed.[1294] Second, the UK has produced a robust legislative codes related to it, namely, the PACE 1984, the IPA 2016, and also measures such as disclosure requirements,[1295] rather than broad and vague language, such as is employed in the KSA. This approach by the UK restricts the likelihood of procedural errors being committed and does not allow for personal interpretation to take place.[1296]

5.4 Effectiveness and fairness of the KSA's response to policing cybercrime

As a main objective of this research, the KSA's response to policing cybercrime will be tested for fairness and effectiveness in order to identify what holds the KSA back from tackling cybercrime procedurally.[1297] Instruments of such test are identified in Chapter 2.[1298]

[1291] Mahdi (2013) 39-52
[1292] *Ibid*
[1293] See also Section 6.5
[1294] Fleming and Rhodes (2005) 193-195
[1295] See Criminal Procedure and Investigations Act 1996.
[1296] *Ibid*
[1297] See Section 1.3
[1298] see Section 2.4

5.4.1 Effectiveness of Policing cybercrime in the KSA

To test whether the KSA's response to policing cybercrime in the KSA is effective, three main standards for such analysis will be applied: conceptual effectiveness, comparative effectiveness, and national effectiveness.[1299]

5.4.1.1 Conceptual effectiveness of policing cybercrime in the KSA

It has been mentioned in Chapter 2 that "*effective*" means achieving an objective successfully.[1300] Therefore, the question which arises is whether policing cybercrime in the KSA has successfully achieved its objectives. To answer this question, it is proposed to analyse further what has been discussed about both institutional and operational policing of cybercrime in the present Chapter. Also, in order to answer this question, it is crucial to know the objectives which the KSA seeks in policing cybercrime. There are no official published objectives that are linked directly to policing cybercrime in the KSA which of itself makes it possible to assert that the KSA overall approach regarding the matter tested is not effective.

Overall, the KSA has established cybercrime units to tackle cybercrime using traditional policing powers exercised by the KSA PF.[1301] Moreover, under the KSA's *Vision 2030,* there is an intention to reduce the increasing number of cybercrimes being committed within the KSA,[1302] which might be considered as an indirect objective with regard to cybercrime and may indicate the objective of the KSA in policing cybercrimes. Thus, it is possible to say that the KSA is attempting to keep pace with the rapid technological changes, yet this adaptation is happening very slowly.[1303] Hence, it seems more likely that policing

[1299] *Ibid*
[1300] See Subsection 2.4.1.1
[1301] See Subsection 5.3.2
[1302] Ouassini & Boynton (2021)
[1303] *Ibid*

cybercrime in the KSA is unsuccessful, because there are no directly drawn objectives to cover policing cybercrime and the existing general objectives of policing are not enough.

5.4.1.2 Comparative effectiveness of policing cybercrime in the KSA

The main aim here is not to test the UK response regarding policing cybercrime but to find insights from which to derive lessons for the KSA,[1304] given that the UK has a more effective response than the KSA.[1305] It has already been outlined that the UK's response consists of both legal and institutional aspects. [1306] With regard to the legal aspect, the UK has produced multiple Acts which have been addressed in this chapter, Chapter 4[1307] and Chapter 2,[1308] including the PACE Act 1984 and the IPA 2016.

Furthermore, the principle of Utilitarianism can be applied to test UK policing.[1309] Thus, the UK surveys whether its population are satisfied with the Police, and it finds that the majority are content with it.[1310] Moreover, it has published some of its objectives regarding policing cybercrime in its NCSS,[1311] which makes possible to measure effectiveness by testing whether drawn objectives have been achieved.

The UK's response to policing cybercrime also involves legally treating cybercrime as being distinct from NCCs in terms of the criminal process which aids effective policing. When looking to the UK Police Act 1997, the Regulation of Investigatory Powers Act 2000 and the IPA 2016, the policing of technology "is dealt with comprehensively"[1312] even

[1304] See Section 1.3
[1305] See Section 4.5
[1306] See Subsection 2.4.1.2
[1307] See Section 4.5
[1308] See Section 2.4
[1309] Alderson (1998 reprinted 2013) 31
[1310] UK Government (2020). https://www.ethnicity-facts-figures.service.gov.uk/crime-justice-and-the-law/policing/confidence-in-the-local-police/latest
[1311] UK NCSS 2016-2021
[1312] McKay (2010) 5

though there is room for further reforms to be made.[1313] This relatively successful approach can be attributed to clear plans, such as the NCSS, and detailed legislation, which seem to produce public contentment with the Police. On the contrary, KSA cybercrimes and NCCs are not distinct or developed, and no attention is paid to public opinions about the policing.

5.4.1.3 National effectiveness of policing cybercrime

The primary measurement of successfulness within KSA law is to produce a law which is compatible with *Sharia* as required by the BLG.[1314] The CPL is successful in this sense, yet, the CPL 2013 only briefly mentions the powers and institutions of the KSA PF; it says nothing about institutions and powers in regard to the criminal process cybercrime. However, when looking deeper, there the KSA has fragmented objectives which are indirectly related to policing cybercrime, found in both the KSA National Information Security Strategy 2013 (NISS)[1315] and *Vision 2030* to tackle cybercrime.[1316] Yet, those objectives are mainly based on distinguishing cybercrime from NCCs, so it can be said that the KSA fails to achieve this objective because it is still legally treating cybercrime in much the same way as it treats NCCs in terms of the criminal procedure. Also, the KSA's NISS aimed to develop information security (cybersecurity) unit by 2017 to avoid cybercrime and cyberattacks,[1317] and it has done it partially by establishing NCA. Although the KSA incorporates some institutional changes related to cybercrime in accordance with NISS objectives, such changes do not qualify for considering the KSA approach toward policing cybercrime successful because the NISS objectives are not related to aspects of policing

[1313] McKay (2017) 30
[1314] BLG Article 7
[1315] MCIT (2013)
[1316] Ouassini & Boynton (2021)
[1317] Alsowailm et al (2017) 9

cybercrime. Furthermore, the NISS objectives are outdated and have not been revised since 2013.

5.4.2 Fairness of Policing cybercrime in the KSA

Instruments for testing fairness of the KSA response to the criminal procedure of cybercrime in the KSA are found in Chapter 2.[1318] These instruments seek to define the meanings of fairness on three levels: conceptual, international and national.[1319]

5.4.2.1 Conceptual meaning of fairness in regard to policing cybercrime in the KSA

There are two main aspects of fairness, both of which were addressed thoroughly in Chapter 2.[1320] First is procedural fairness; the system must be just in the eyes of the community to which is applied by using proper processes. [1321] Second is substantive fairness; the system must be just in the eyes of the community by reaching fair results. [1322] The KSA has responded to policing cybercrime in the two aspects, and it has achieved multiple decisions and results in the matter. Therefore, the question here is whether those decisions and results are fair? The answer to this question is divided into two further perspectives; international and national.

5.4.2.2 International meaning of fairness in regard to policing cybercrime in the KSA

From an international perspective, international human rights law provides important measurements for fair criminal processes.[1323] The CPL 2013 complies with most of the

[1318] See Subsection 2.4.2
[1319] *Ibid*
[1320] *Ibid* 2.4.2.1
[1321] Franck (1995) 6–9, 47
[1322] *Ibid* 6–9, 47
[1323] See Subsection 2.4.2.2

international human rights provisions[1324] even though it is fragmented and unclear.[1325] However, this compliance is theoretical because, although the law stipulates fair policing measures, in practice, it has been observed that KSA PF uses force and coercion with cybercrime suspects, especially those who are accused of committing cybercrimes of a political nature.[1326] Also, they have been found to arbitrarily arrest people without letting them know what the reason for such arrest is.[1327] The person arrested is often expected to know what they are being arrested for, such as when police officers often tell individuals who are accused of cybercrimes "you know why we are arresting you."[1328] Thus, the accused must assume what their crime might be. [1329] Legal standards may not be entirely internalised by the police, as reflected in this observation by Police officer PO1:

> "It is bizarre that, whenever there is an error in the criminal procedure, police officers are the first ones to be blamed because they are in the public's plain sight"

and

> "Even though some low ranked police officers might not follow the law by not letting them know what a person's crime is or use violence against them [he means the accused], they are just being mildly disciplined by high ranking police officers while they should be punished for violating the law."[1330]

It is even possible to speak of brutality in cyberspace policing in the KSA. For instance, the KSA PF may track down someone who is accused of cyber-sexual harassment

[1324] Alqaysi (2019) 19
[1325] Interview with Law Professor LP3
[1326] HRW (2013) <https://www.hrw.org/report/2013/12/17/challenging-red-lines/stories-rights-activists-saudi-arabia>
[1327] *Ibid*
[1328] Interview with Criminal Lawyer CL1
[1329] Interview with Public Prosecution Officer PP1
[1330] Interview with Police Officer PO1

and cyber-sexual extortion, and subject them to brutality by, for example, hitting them and dragging them down the street.[1331] Therefore, it is possible to say that the KSA situation has shortcomings in terms of the fairness of its policing of cybercrime. Even though the thesis has been able to only acquire qualitative and not quantitative data in regard to policing cybercrime in the KSA due to the absence of any relevant qualitative data having been published, the laws, the police cultures, the data from fieldwork and some international non-government organizations point to inadequacies which find the KSA PF to have abused their operational powers. Not only have they overstepped in regard to arrest and detention, but they have also been found to abuse other powers such as surveillance, search, and seizure in policing cybercrime.[1332]

Those practices have a negative impact on the fairness of policing cybercrime in the KSA from an international perspective, and three observed unfair practices should be highlighted. First is lack of respect for human rights of expression.[1333] Second is lack of due process, involving delays in bringing to trial, secret trials, lack of representation,[1334] and lack of disclosure of the charges.[1335] Third is excessive and inhuman punishment which mainly is represented by whipping.[1336] Although the KSA promised in its latest periodic review that it would consider a fairer approach toward human rights by ratifying ICCPR,[1337] it has not yet so acted. Moreover, as has been addressed in this chapter,[1338] in the absence of clear human rights rules in the KSA, PF officers have applied unwritten moral codes[1339] which are not fair based on the international standards of fairness (especially certainty) even though those measures might be considered fair at a national level.

[1331] Interview with police officers PO2
[1332] Interviews Criminal defence Lawyers CL1 and CL3
[1333] UPR, Saudi Arabia 3rd cycle <https://www.ohchr.org/EN/HRBodies/UPR/Pages/SAindex.aspx>
[1334] Alhumodi (2014) 159
[1335] This will be addressed further in Chapters 6 and 7.
[1336] Chapter 7 will address the lashing punishment in relation to cybercrime.
[1337] UPR, Saudi Arabia 3rd cycle <https://www.ohchr.org/EN/HRBodies/UPR/Pages/SAindex.aspx>
[1338] See Subsection 5.2.3
[1339] Interviews with Police officers PO1, PO2 and PO3

5.4.2.3 National meaning of fairness in regard to policing cybercrime

Human rights are involved in policing cybercrime.[1340] According to the KSA's main domestic legislation, the KSA protects human rights in accordance with *Sharia.*[1341] Therefore, it is assumed that, since the KSA claims to protect human rights, there is legislation which specifies human rights in *Sharia*, but that is not the case. Nonetheless, the KSA has multiple applications of human rights within police practice and legislation related to policing,[1342] but ironically its main reference to human rights is international law[1343] which the country has not yet ratified.[1344] Moreover, the BLG contains human rights of relevance to criminal procedure, which might indicate the will of the KSA to be fair by setting out standards of fairness in its supreme legislation. However, as will be discussed in Chapters 6 and 7, and as has been discussed in this chapter[1345] those standards of fairness are related to physical space and are unclear;[1346] *Sharia* does not address late modern issues such as spying in cyberspace.

This confusion allows the majority of the KSA population, including PF officers and policy makers, to believe that the PF are protectors of human rights based on *Sharia*, even though international human rights are being violated by the KSA PF on an operational level, both in general and in regard to cybercrime specifically.[1347] As noted by Alain Supiot, having lesser acceptance of the Western view on human rights leads some Muslim societies into

[1340] Murray and Klang (2005) 10
[1341] BLG Article 16
[1342] See subsection 5.2.3
[1343] Main textbooks which explain human rights in the KSA refer to UDHR as source of establishing modern human rights. See Naseeb et al (2010) and Alroways and Alrayees (2019)
[1344] OHCHR, Human rights Bodies <https://tbinternet.ohchr.org/_layouts/15/TreatyBodyExternal/Treaty.aspx?CountryID=152&Lang=EN>
[1345] See 5.3.2
[1346] *Ibid*
[1347] HRW (2020) <https://www.hrw.org/world-report/2020/country-chapters/saudi-arabia>

authoritarianism.[1348] Therefore, it can be said that the KSA PF's approach to human rights is fair within the KSA as many Saudis might view the doctrine,[1349] and violation of international human rights, as justified under the concept of the greater good.[1350] However, this approach is not tolerated by the international community which has pressured the KSA to be more considerate of human rights.[1351]

5.5 Policy transfer lessons from the UK

Another objective of the thesis is to learn from other countries' approaches regarding the criminal process of cybercrime.[1352] Therefore, the UK response to policing cybercrime will be addressed in this section. Then, it will be compared with what the KSA has done and what the KSA has yet to do in order to learn lessons from better approaches.

Due to the early recognition of the differentiation between cybercrime and NCCs, the UK passed various Acts which specify the role of Police regarding cybercrime all of which has been addressed in Chapter 4.[1353] It appears that the UK has drawn clear lines for the Police to function in cyberspace and detect cybercrime using lawful powers.[1354] Moreover, the UK has regularly updated its law in accordance with technological developments,[1355] especially when it comes to basic human rights such as privacy.[1356] Besides, the UK has a long history of policing, which is perhaps one reason why it has successfully recognised and adapted the role of the police in cyberspace.[1357]

[1348] Supiot (2017).
[1349] All interviewees say that Sharia is fair and so legislation derived from it. In chapter 3 and 8 some of interview points were discussed especially in regard to transparency.
[1350] Interviews with Sharia Experts SE1, SE2 and SE3
[1351] Amnesty International Report 2017/18 the State of the World's Human Rights, 317 <https://www.amnesty.org.uk/files/2018-02/annualreport2017.pdf>
[1352] See Section 1.3
[1353] See Subsection 4.5.2
[1354] Bandler & Merzon (2020) 27
[1355] *Ibid*
[1356] McKay (2017)
[1357] McKay (2010)

As well as new powers and offences, the UK has established cyber units and cybercrime related agencies specifically to police cybercrime.[1358] Thus, the UK Police has specialized units to police cybercrime.[1359]

5.5.1 Redefining the function of the police in relation to cybercrime

Among the suggested reforms to policing cybercrime is that the KSA should be transparent and consistent about organisational structures assigned to cybercrime police.[1360] The current approach in the KSA in regard to policing cybercrime is not as successful as it could be, because there is no line drawn which demarcates where the KSA PF can intervene in policing cybercrime.[1361] The CPL 2013 should be updated in this regard in order to designate the institutions that police cybercrime.[1362] Even though the KSA passed the ACL in 2007 which recognises the different nature of cybercrime on the substantive level, it does not recognise the different nature of cybercrime on the procedural level which this thesis has argued is just as crucial as the substantive. It might be argued that such a differentiation would have some advantages which might be secured from this reform; first clearer purpose and priority, second resources and training and expertise can be concentrated, and third accountability could be secured.

In the UK, multiple laws that effectively recognise the different nature of cybercrime on both the substantive and – more importantly – procedural levels have been passed, beginning with the Computer Misuse Act 1989 through to the IPA 2016. This dedication to keeping the law up to date, which has spanned three decades, should be copied by the KSA. The UK has also continued to develop and execute its policy through the NCSS 2016-2021

[1358] Saunders (2017) 6-11
[1359] See Subsection 5.3.1
[1360] Interview with Law Professor LP1
[1361] Interview with Law Professor LP1
[1362] Interview with Criminal Lawyer CL1

which recognises the role of cybercrime policing agencies.[1363] Thus, it is possible to say that the UK government has mobilised policing to improve tackling cybercrime effectively and fairly.[1364] The KSA should benefit and learn from this attention by dedicating its resources to producing effective legislation as soon as possible (but without treating the issue as an emergency) and to continue to revise as necessary.

5.5.2 Reconsidering a fairer approach towards human rights

The UK does not just effectively police cybercrime; it also fairly polices cybercrime, because it always expressly takes into its consideration issues of human rights.[1365] One reason why the UK avoids the violation of human rights is that it has ratified multiple human rights treaties and has passed its own Human Rights Act 1998.[1366]

In cyberspace, issues of human rights in regard to policing cybercrime occur in both physical and virtual space.[1367] The UK has a comparatively good human rights record when it comes to policing cybercrime in both virtual and physical space.[1368] It might be argued that policing cyberspace is only done in virtual space and not in physical space.[1369] Nevertheless, the traditional powers of the police, such as arresting cybercrime suspects, detaining them and interrogating them, occurs in physical space.[1370] Therefore, the two spaces cannot be ignored when it comes to the police using their traditional powers in relation to cybercrime.[1371]

Therefore, it is important to consider whether the UK fairly exercises traditional policing powers in relation to cybercrime. However, some policing powers, such as

[1363] UK NCSS 2016 to 2021
[1364] McKay (2017) 24
[1365] Her Majesty's Inspectorate of Constabulary and Fire & Rescue Services (2019)
[1366] Hoffman and Rowe (2013) 63-92
[1367] Murray and Klang (2005) 10.
[1368] See league tables about the UK < https://ourworldindata.org/human-rights>
[1369] Wall (1997) 208-236
[1370] *Ibid*
[1371] *Ibid*

surveillance and acquiring cyber-evidence which are exercised in virtual space, are questionable in terms of whether they violate the human right of privacy, especially when it comes to bulk interception of communication which the IPA 2016 allows.[1372] The argument in this regard is that even though bulk interception of communication is legally allowed, human rights defenders in the UK argue that this might enable the government to spy on people and violate their human right of privacy.[1373] This argument is one reason that the UK Parliament passed the IPA 2016.[1374] In turn, human rights defenders are worried that the government has supported legislation affecting policing powers in regard to cybercrimes which is too permissive towards the police.[1375] At least through taking these arguments seriously and dealing with them through public discourse, the UK state shows its concern about protecting human rights.[1376] The UK's legislative development is well in advance of the KSA but is far from perfect and remains in need of ongoing reform.[1377]

Unlike the UK, the KSA has a much more tarnished human rights record, which includes the way it polices cyber related crimes.[1378] This record includes various violations in certain domains that are connected to one another, such as mistaken interpretations of *Sharia* and the underdeveloped system of governance. Although the KSA's record is not as strong as that of the UK, it has tried to improve its record, and "it is slowly making its legal system fairer than before."[1379] Nevertheless, to benefit from the UK's experience on policing cybercrime fairly, the KSA should first consider whether it can sign and ratify leading human rights treaties (such as the UN ICCPR) and then implement these treaties within its domestic legal framework. Thus, there may be various gains for fairness; first, it would set symbolic

[1372] Murray and Fussey (2019) 31-60
[1373] *Ibid*
[1374] McKay (2017) 24
[1375] Murray & Fussey (2019) 31-60
[1376] *Ibid*
[1377] See Case C-623/17, Privacy International *v Secretary of State for Foreign* and *Commonwealth Affairs*, ECLI:EU:C:2020:790, 6 October 2020
[1378] HRW (2020) <https://www.hrw.org/world-report/2020/country-chapters/saudi-arabia>
[1379] Interview with Law Professor LP1

standards, second it would require further detailed legislation which explains compliance and specifies sanctions for breaches, and third it would allow for better transparency and accountability.[1380]

Then, the KSA should define the functions of the police in accordance to the principles found in international human rights standards, such as universal due process in accordance with the ICCPR.[1381] Finally, it should make a clear distinction in its legislation between the criminal procedures related to cybercrime from criminal procedures related to NCCs, especially when it comes to the policing powers exercised in cyberspace. This reform would benefit the overall fairness of the KSA's approach to the criminal procedure of cybercrime, as there would be less abuse of vague policing powers and less dependence on personal moral codes of PF officers.

5.6 Conclusion

The findings of this chapter fall under two main categories. The first category is institutional and relates specifically to cybercrime policing institutions in the KSA. This has two branches; specialisation and breadth. Specialisation denotes that the KSA lacks specialisation in its institutions that address cybercrime compared to the UK that has specialised cyber institutions with a clear delineation of their functionality as specialist cyber policing authorities. Even though the KSA has cyber units supporting the PF, those units lack specialisation with regard to policing itself as a narrow concept that is vested to the police institutions, particularly related to policing cybercrime as these units are not recognised by the law of criminal procedure in the KSA. With regard to how broad institutions are, there is a need to move away from state domination and to allow public/private collaboration and

[1380] Alhargan (2012) 491
[1381] Henkin (1990)

user empowerment. Hence, even though there is the need for a specialist group, policing should not be exclusive to them and broader institutions should be included in the process. The regulatory pyramid addressed in Chapter 2[1382] suggested that every stakeholder should be involved in policing cybercrime as a form of self-regulation. Moreover, this notion is congruent with Lessig's theory, mentioned in Chapter 2,[1383] where private organisations such as ISPs could be involved in policing cybercrime as specialists who assist the PF in that endeavour.

The second category is operational, which indicates the policing powers related to cybercrime. The summary findings for powers of policing cybercrime also bear two branches: specialisation and breadth. In regard to specialisation, it has been noticed that the KSA PF has sufficient funds and an array of developed technology, yet it still lacks the legal training necessary to take advantage of the available funds and technology. As for breadth, even though regular people cannot be given policing powers such as those given to the PF, in the broader arrangements, ISPs and the general public (subject to safeguards) should at least be allowed to become involved in the overall process.[1384]

In terms of standards, this Chapter also found the KSA PF is neither fair not effective in policing cybercrime. It is not clear who exactly polices cybercrime in the KSA. Even though the CPL 2013 outlines who the PF are, it mixes them with detectives of the PP and calls their power preliminary. The power is "initial" because it is under the supervision of the PP that conducts preliminary criminal investigation as will be discussed in in Chapter 6. Also, those so-called PF and PCIOs were found by independent international human rights observers to be abusive of human rights in regard to cybercrime. Not only has the PF been found to be abusive by international human rights observers but – more importantly – it fails

[1382] See chapter 2 figure 2.3
[1383] *Ibid* section 2.2
[1384] Compare *Sutherland v HM Advocate* [2020] UKSC 22

to meet KSA's standards of fairness. As been pointed out in this Chapter in regard to PF, lack of laws, training, and a suitable culture are key contributory failures.[1385]

Moreover, as drawn by the Model Code in Chapter 4,[1386] and as mentioned in this chapter, the KSA PF needs to fill in gaps at both the strategy level and the institutional and operational levels. The most apparent gaps between what is happening in the KSA and what is yet to be done require differentiating laws between NCCs and cybercrimes in regard to the PF, which means that the KSA needs to update its CPL 2013 to include specialist policing powers and police structure in regard to cybercrime. Moreover, the KSA PF personnel need to be trained to deal with cybercrime fairly and effectively, and there needs to be better oversight to foster changes in policing culture.

[1385] Wehrey (2015) 71-85
[1386] See section 4.6

Chapter 6

Preliminary Investigation of cybercrime in the KSA

6.1 Introduction

This Chapter aims to answer the following questions: what is the KSA's approach to cybercrime in terms of its criminal process as it applies to investigation?; and, is this approach fair and effective? The main reason for separating this chapter from the previous one is that the KSA CPL 2013 vests the powers of what might be called "preliminary investigation" in the hands of the detectives of the Public Prosecution.[1387] Article 2 of the PPL states that:

> "First - the Public Prosecution shall have the competence, in accordance with the law and what is specified by the organizational bylaw, to:
>
> A – Investigate crimes.
>
> B - Act in the investigation by filing or dismissing the case in accordance with what the law specifies.
>
> C - Prosecute before the judicial authorities in accordance with the law…."[1388]

As explained in Chapter 5, the KSA PF opens a case file (dossier), from which detectives of the PP can follow up on what has been termed in this thesis the Police's "initial investigation".[1389] Therefore, it is possible to say that the KSA PF do not carry out detailed investigations, but act primarily as responders to the public and PP.[1390] At the same time, the

[1387] Shareef (2016) 107
[1388] PPL Article 2
[1389] See Section 5.2
[1390] Shareef (2016) 20, 64 and 101

KSA's legal system might not be merely categorised as either an inquisitorial or an adversarial system, due to the dominant informal source of the law – *Sharia*.[1391] However, when looking to the structure of the KSA's criminal justice system with regard to the criminal procedure, it is possible to note that it leans more towards being an inquisitorial system.[1392] In such a system, it is no wonder that the PP is involved in the preliminary investigation of cybercrime.[1393]

A key term used in this chapter is "investigation"; thus, a definition of investigation is required. Using a similar approach to that used in defining policing in the previous chapter, the concept of investigation in a legal sense contains both broad and narrow functions. The broad function of investigation might include multiple institutions which exercise limited investigative powers related to particular elements of policing.[1394] However, the narrow function of the term only includes the criminal investigation, usually held by the Police investigating officer;[1395] who is "an employee of a police authority, other than a constable, designated under s 38 of the Police Reform Act 2002 to investigate offences and have certain police powers in relation to such an investigation."[1396] Therefore, it is possible to say that police officers function as detectives within England and Wales. By comparison, for the purposes of disclosure, England and Wales law identifies the narrower concept of criminal investigation as "an investigation conducted by police officers with a view to it being ascertained whether a person should be charged with an offence, or whether a person charged with an offence is guilty of it."[1397]

[1391] Baderin (2006) 241-284
[1392] See chapter 2 section 2.3
[1393] Braum (2012) 69
[1394] Gehl & Plecas (2016) 25 and 121
[1395] Newburn et al (2009)
[1396] Gooch & Williams (2015)
[1397] UK MoJ (2020) 4

In the KSA, detectives (as identified in the CPL)[1398] are responsible for carrying out criminal investigations, so in the KSA the narrow function of investigation refers mostly to the PP as a governmental institution which practices both investigation and prosecution.[1399] Some adversarial systems, including the UK's criminal justice system, vest investigative powers in the hands of the police and separate investigation from prosecution. However, the KSA does not vest investigatory powers in the hands of the PF any longer, mainly because it looks upon criminal investigation as a judicial tool[1400] which should primarily be exercised by a judicial authority. Therefore, the KSA has passed changes in Article 1 of the PPL in 2020 to clearly state that "Public Prosecution is a part of the judicial branch..."[1401] This measure seems to have been passed because the KSA authorities desired to raise the salary of the PP members as will be discussed in Chapter 7, not because of a desire to lean toward inquisitorial approach which considers the PP as a part of the judiciary.

It is possible to assert that the KSA vests the preliminary investigatory powers in the hands of the PP instead of the PF for several other reasons. The first is that the KSA's legal system is influenced by Egyptian law,[1402] which vests investigatory powers in the hand of the PP[1403] and, as a result, the KSA tends to imitate it rather than deviate from its course.[1404] The second is that the KSA PF used to abuse its investigatory powers, and this deviance was made possible by sheer extent of their vested powers.[1405] Therefore, the KSA's lawmakers cut them down by giving preliminary investigatory powers to the PP, whose detectives are

[1398] CPL 2013 Articles 13 and 15.
[1399] Shareef (2016)
[1400] *Ibid*
[1401] See changes made on Article 1 of the PPL <https://laws.boe.gov.sa/BoeLaws/Laws/LawDetails/ac892eff-4aa4-4b26-b312-a9a700f2663d/2>
[1402] Interview with Law Professor LP2
[1403] AlGharib (2001) 501-514
[1404] Aldosari (2019) 63
[1405] The KSA PF used to exercise policing, investigative and prosecutorial powers before the issuance of the CPL 2001 that took away both investigative and prosecutorial powers as a sign of moving towards fairer approach. See Subsection 5.2.3

required to have majored in *Sharia* studies or law studies,[1406] based on the assumption that they therefore would have a deeper understanding of law and human rights.[1407] However, as will be discussed in this chapter, despite their technical knowledge, PP members still abuse their investigatory powers, especially when it comes to investigating cybercrime.

The focus of this chapter is on the narrow function of detectives as investigators of crime in the shape of cybercrime. The reason that this chapter selects the narrow function of detectives is because it aids the identification of the institutions and operations involved in investigating cybercrime in the KSA once criminal procedure is underway. The criminal procedure begins with a PF report (dossier) where it relates the initial investigation conducted by the PF (as covered in Chapter 5). [1408] Then, the PF report their suspicions to the detectives of the PP who are appointed to be stationed in police stations beside their main work position in the PP.[1409]

6.1.1 Aims of the chapter

The main focus of this chapter is to address governmental investigation organisations which are involved in the processing of cybercrimes. Non-governmental investigative institutions will be excluded as beyond the parameters of this thesis. Given the focus of this chapter, it is useful to clearly state its aims more fully.

The first aim is to identify the KSA's response to cybercrime in terms of criminal procedure, specifically with regard to which institutions investigate cybercrime and how they operate. The Model Code suggested in Chapter 4 will be the main instrument used to evaluate

[1406] Article 1 Paragraph 4 of the Members and Employees of the Public Prosecution Bylaw 2016 (MEPPB) issued by Royal Decree No. (406) 27/06/2016 states that appointed member (detective or prosecutor) "must have a *Sharia* college certificate [bachelor degree or higher], or another certificate equivalent to it, or he must be a have a certificate in law [bachelor degree or higher] from a university in the Kingdom, or another equivalent certificate, and in case of equivalence, he must pass a special examination held for this purpose."
[1407] Interviews with members of the PP D3 and PP2
[1408] See Subsection 5.2.2.1
[1409] Interviews with Police officers PO1, PO2 and PO3 and detectives of the PP D1 and D2.

the country's current approach to cybercrime in terms of investigation.[1410] As outlined in Chapter 1 Subsection 1.2.1, this is the third main aim of the thesis. Therefore, this chapter will evaluate the KSA's responses to cyberspace in terms of investigating cybercrime. In order to clear the path for the remainder of this chapter, an evaluation and analysis of the KSA's main legislation regarding cybercrime investigation will be conducted to identify the KSA's approach to the criminal process of cybercrime. The relevant legislation includes the CPL 2013 and its CPLER 2015, the evaluation of which leads to the fulfilment of the next aim of this chapter.

As was introduced in Chapter 4, the CPL 2013 is the main legislation which focuses on the narrow aspect of investigative institutions, defining investigatory powers.[1411] Additionally, as was addressed in the previous chapter, the CPL 2013 vests investigatory powers in the hands of the PP and the CC, rather than the PF, whose powers are preliminary, because the KSA's criminal procedure is a combination of inquisitorial and adversarial systems.[1412] Therefore, it is possible to say that this blend allows CCJs to reinvestigate crimes, including cybercrimes,[1413] because the KSA's system is made up of formal (legislation) and informal sources (*Sharia*)[1414] which can override any aspect of the formal legal system in the KSA.[1415]

This Chapter is centred on investigating cybercrime in the KSA, which branches out into two major aspects, reflecting the Model Code created in Chapter 4.[1416] The first aspect is institutional and relates to who are the investigatory entities in the KSA. The second aspect is operational which relates to what the relevant entities do, their legal powers, and how they

[1410] See Section 4.6
[1411] See Subsection 4.2.5
[1412] Esmaeli (2009) 12
[1413] Reichel (2018) 130
[1414] Baderin (2006) 267
[1415] See Section 2.3
[1416] See Section 4.6

exercise them. Therefore, it can be said that this Chapter addresses the investigation of cybercrime and how cybercrime is investigated in the KSA. Additionally, it will explain how investigatory authorities in the KSA deal with those accused of cybercrime; how they are investigated and then subjected to formal investigatory powers such as interrogation, surveillance, search and seizure.

This aim has been discussed fully in both the previous Chapter and will be repeated in this Chapter because both the KSA PF and the PP have the same investigatory powers in theory, yet, in practice, they adopt different roles. The distinction that should be highlighted here is that policing powers related to cybercrime can be said to be investigative in nature,[1417] yet, they are viewed as initial policing powers rather than investigative powers in the KSA law.[1418] This categorisation is adopted for two main reasons. The first is that the PF are involved in what might be called initial investigation, rather than the preliminary investigation, even though the KSA PF officers are identified in the KSA CPL 2013 as PCIOs.[1419] The second reason is that PF officers can conduct preliminary investigations into cybercrime only when they are supervised by detectives of the PP.[1420] Hence they are identified as PCIOs.

The chapter's second aim is to identify what is holding the KSA back from tackling the preliminary investigation of cybercrime in a procedural sense, particularly those factors related to the investigation of cybercrime as listed in the ACL, the ETPL and the ACFL, which are introduced in Chapter 4.[1421] There is no doubt that the KSA's current approach to cybercrime, both substantively and procedurally, puts the country at risk because of shortcomings. Therefore, as mentioned in Chapters 1 and 2, the KSA is seeking reforms to

[1417] Wall (1998) 210
[1418] See Subsections 5.2.2 and 5.2.3
[1419] CPL 2013. Article 26
[1420] Shareef (2016) 159
[1421] *Ibid* 4.2

modernise the state under the *Vision 2030*.[1422] It can be said that the first step toward overcoming these risks is to identify them.[1423]

Furthermore, this chapter will explain how investigation of cybercrime is performed within the jurisdiction of the KSA. Moreover, it will be demonstrated that investigating cybercrime is very complex because it involves multiple official authorities which have been afforded various investigatory powers, such as special committees, aside from the KSA PF who undertake the initial investigation, the PP, and the CCJ (who will be addressed in the next Chapter).

As the KSA deals with cybercrime in a way which is largely indistinct from NCC in terms of criminal procedure,[1424] this chapter will begin by introducing the main provisions for preliminary investigation of NCCs found in the main legislation (the CPL 2013). Then, it will apply those provisions to the investigation of cybercrime and analyse the KSA's response to the investigation of cybercrime in depth, both institutionally and operationally. Subsequently, both the effectiveness and the fairness of the KSA's response to investigating crimes, mainly cybercrime, will be assessed in order to meet the research objectives regarding identifying what is holding the KSA back from combating cybercrime from a procedural perspective.[1425]

The third aim of this chapter is to test both the effectiveness and the fairness of the KSA's approach to investigating cybercrime. This evaluation will refer to the standards of effectiveness and fairness set out in Chapter 2 Section 2.4.

The fourth aim is to improve the KSA's approach regarding policing and investigating cybercrime by drawing policy and regulatory lessons from England and Wales. Therefore, this chapter will investigate the relevant UK laws regarding investigating cybercrime and compare them with the KSA's legislation in order to learn lessons from them.

[1422] See Section 1.1 and Section 2.5
[1423] Lash et al (1996) 1-28
[1424] See Section 2.2
[1425] See Section 1.3

6.2 Investigating NCCs in the KSA

As a major step towards the elucidation of investigating crimes, the role of detectives, who are officers based in the BIPP (PP), will now be introduced in this section with reference to the investigative powers conferred by the CPL 2013 to investigate NCCs. Therefore, this section covers two main aspects regarding the investigation of NCCs in the KSA. The first aspect is institutional and aims to identify which entity investigates crimes. The second aspect is operational and aims to address investigation powers such as stop, arrest, interrogation, detention, search, seizure, and surveillance. Therefore, this section identifies the role of PP regarding criminal investigation within the KSA's jurisdiction and how they operate. Although the role of PP bares certain similarities to the function of the KSA PF,[1426] it is distinct because the PF operates differently from the PP in the KSA. The KSA's PF conducts its initial investigation and begins processing criminal cases by filing a report in a dossier which they give to the PP to continue working on. [1427]

As addressed in the introduction of this section, investigating crime in the KSA is a broad subject, so this section is narrowed to fit the research aims, objectives and questions. Moreover, the focus of this section is to identify the main principles of investigating crimes in the KSA in order to apply them to cybercrime. Since the KSA deals with cybercrime as being indistinct from NCC in terms of criminal procedure,[1428] there is a need to know how the KSA deals with NCCs in term of investigation. Therefore, this section will address both institutional and operational responses to the investigation of NCCs within the KSA.

[1426] Shareef (2016) 178
[1427] See Subsection 5.2.2.1
[1428] See Section 2.2

6.2.1 Investigation institutions in the KSA

As already mentioned, before 2001, the KSA PF was the institution responsible for policing, investigating, and prosecuting crimes.[1429] However, after the KSA passed the CPL 2001, both the investigation and prosecution of crimes became the exclusive responsibility of the BIPP (now PP).[1430] Therefore, it can be said that, according to the CPL 2001 and its successor, the CPL 2013, the responsibility of investigating crimes is only vested in detectives within the PP.[1431] Chapter 5 of the CPL 2013 specifies how detectives conduct their investigation,[1432] which will be covered when addressing investigation powers (operations).

One complicating factor is that, in some cases, PF officers within the policing institutions might act with preliminary investigative powers under the authorisation and supervision of PP detectives.[1433] Article 66 of the CPL 2013 says:

> "The investigator [detectives of the Public Prosecution] may assign in writing any of the preliminary criminal investigation officers to carry out one or more of the investigation proceedings save for the interrogation of the accused. The assigned officer shall have, within the scope of his assignment, the same powers as those of the investigator in carrying out such proceedings. If the circumstances of the case warrant that the investigator act beyond his jurisdiction, he may, as the case may be, assign the proceedings to an investigator or a preliminary criminal investigation officer from the

[1429] See Section 5.2
[1430] KSA Royal Decree No. A/240 of 2017
[1431] CPL 2001 and 2013 Chapters 5
[1432] CPL 2013 Chapter 5
[1433] *Ibid* Article 66

competent department. The investigator shall carry out such proceedings if deemed necessary for the investigation."[1434]

It appears from this Article that the assignment of the PCIOs must be in writing and limited to one assignment at a time.[1435] Moreover, aside from the PP and PCIOs, CCJs function as investigators in the criminal court.[1436] This role might seem inappropriate, because the CPL 2013 requires judges to be neutral.[1437] However, Article 162 of the CPL 2013 says:

> "If the accused denies the charges or refuses to respond, the court shall proceed to hear the evidence and take necessary action. It shall interrogate the accused in detail regarding the evidence and charges. Each of the parties may, with the permission of the court, cross-examine witnesses and evidence."[1438]

It appears from this Article that CCJs in the KSA can exercise investigation powers by interrogating the accused, and they can discard or repeat what has been investigated by the PP[1439] based on the case file presented to them.[1440] It might be argued that Article 162 indicates that CCJs in the KSA treat the fundamental procedural practice of the PP as evidence which needs to be examined rather than just examining the presented evidence by PP.[1441] Consequently, the fundamental procedural work of the PP could be disregarded, and CCJs could open a new criminal investigation.[1442] This judicial role could undermine the investigation conducted by detectives, because, if their efforts are disregarded by the CCJs, detectives would be likely to deliberately put minimum effort into their investigation.[1443]

[1434] *Ibid* Article 66
[1435] *Ibid*
[1436] Shareef (2016) 150 and 262
[1437] *Ibid* 262
[1438] CPL 2013 Article 162
[1439] Shareef (2016) 153
[1440] Interview with detective of the PP D1
[1441] *Ibid*
[1442] Shareef (2016) 153
[1443] Interviews with detectives of the PP D1 and D3.

Therefore, justice would be undermined. Thus, it can be said that CCJs in the KSA have the final say in the investigation not the PP.[1444] This relationship will be covered in further detail in Chapter 7 when addressing CC in the KSA as a further crucial element of the criminal procedure of cybercrime in the KSA. However, it should be understood that involvement of a judge in investigating the case is common in inquisitorial systems which the KSA resembles in some respects.[1445]

Similar to the potential practice of CCJs, the CPL 2013 indicates that detectives should not rely on the initial investigation held by PCIOs.[1446] As mentioned in Chapter 5, the KSA PF investigation is initial,[1447] and it should not to be treated as part of the preliminary investigation until the detectives of the PP are involved in the investigation and have considered it.[1448] Thus, in many cases, detectives of the PP do follow up the police report[1449] (arising from the initial investigation) or approve it all without carrying their own investigation.[1450] In some cases, they might disregard the initial investigation undertaken by the PF[1451] because some think that many PF officers lack the knowledge required to deal with the criminal procedure.[1452] This view is reinforced by the data obtained from the fieldwork interviews, where detectives claimed more understanding of criminal procedure than PF officers because "we studied the criminal procedure law academically twice, in the college and in the Academy."[1453] Nonetheless, one PF officer claimed that:

[1444] Shareef (2016) 153
[1445] Spencer (2016) 601-616
[1446] Interview with Public Prosecution Officer D1
[1447] See Subsections 5.2.1 and 5.3.1
[1448] *Ibid*
[1449] Shareef (2016) 60
[1450] See appendix F
[1451] Interview with Detectives of the PP D1, D2 and D3
[1452] Interview with Police officers PO1, PO2 and Detective o the PP D1
[1453] Interview with detective of the PP D2

> "Detectives do not respect us anymore because they think they are better than us; they think that, because they are more educated and well paid, they know better – whilst it is us who do all the investigative work."[1454]

Ultimately, the CPL 2013 vests the authority of investigation in the hands of the judicial branch (which includes the PP),[1455] not the executive branch,[1456] which is why detectives can discard the initial investigation done by PF officers, regardless of any personal opinions about the PF. Therefore, the question that should be asked is whether it is fair and effective to vest the primary authority of investigation in the hands of the PP, including duplication of earlier police work which may elongate the criminal process. Since this question is not within the scope of this thesis, it will not be answered fully.[1457]

As already mentioned, investigating crimes is primarily vested in the hands of the detectives of the PP, as legislated for by the CPL 2013. Other institutions are involved in investigating crimes, such as the PF in the initial investigation and CC in the final investigation, but they are not the main investigatory institutions.[1458] Therefore, they are not identified or discussed in this chapter as investigatory institutions in the KSA.

Finally, investigative bodies can be established for particular crimes in the KSA, which then self-dissolve after accomplishing their objectives. This kind of institution will be addressed in Section 6.4 regarding cybercrime because their main function is investigative and they have similar investigatory powers to detectives of the PP and are used for NCC purposes; the most well-known example is related to corruption.[1459]

[1454] Interview with Police Officer PO3
[1455] The KSA treats the PP as a judicial entity not an executive one. see PPL Art.1
[1456] Shareef (2016)
[1457] For discussion, see Aldosari (2019)
[1458] See Subsection 7.4.2.2
[1459] BBC News (2019)

6.2.2 Investigation powers (operations) in the KSA

In accordance with the CPL 2013, detectives within the KSA have three main functions: as PCIOs, detectives, and prosecutors or public defenders.[1460] In the first function, as discussed in Chapter 5, they are PCIOs and work in conjunction with the KSA PF, allowing them to exercise the policing powers discussed in Chapter 5.[1461] Most importantly, they also function as detectives of crime and public prosecutors which is their main function. Their function as detectives of crimes will be discussed in this sub-section, and their functional as public prosecutors will be discussed in Chapter 7 when addressing prosecution and courts in relation to the criminal procedure of cybercrime in the KSA.

To begin with, detectives of the PP have multiple functional powers under the CPL 2013. They can interrogate suspects and have been given the powers of search, seizure and surveillance. Although those powers are used by policing institutions, as addressed in Chapter 5, they are used mainly under the supervision of detectives or supervision of the MoI.[1462] There is no authority over members of the PP, including detectives, except for the authority of *Sharia;*

> "Members of the Bureau are totally independent, and they shall not be subject in conducting their work except to the provisions of Islamic Shari'ah and the relevant laws, and no one shall interfere in their work."[1463]

Therefore, they can practice investigatory powers more widely and less strictly since there is an absence of "officially recognized procedure"[1464] in the KSA in relation to cyber evidence and cybercrime.

[1460] Aldosari (2019) 30
[1461] See Section 5.2
[1462] *Ibid* Subsection 5.2.2
[1463] PPL Article 5
[1464] Alanazi et al (2018) 10

In the next set of subsections, powers of interrogation, search, seizure and surveillance will be discussed in relation to the NCCs. Then in 6.3, they will be applied to cybercrime.

6.2.2.1 Investigation powers (operations) in the KSA: the power of interrogation

The CPL 2013, Article 101, allows for the interrogation of suspects. Article 101 says:

> "When the accused appears for the first time for interrogation, the investigator shall record all his personal information, inform him of the charge against him and record any statements he makes regarding the accusation. The investigator may have the accused confront other accused persons or witnesses. The accused shall sign his statements after they are read to him. If he declines to sign, a note to that effect, along with the reasons, therefore, shall be entered into the report."[1465]

This Article gives the power of interrogation to the criminal detectives of the BIPP, taking into consideration that interrogation must not be conducted with coercion and violence.[1466] Even though the CPL 2013 allows suspects to hire an attorney to be present during all the criminal process,[1467] almost all suspects do not hire an attorney during the first stages of criminal process.[1468] Most of them hire an attorney only after the criminal case goes to trial.[1469] Not having an attorney present during interrogation may allow detectives to abuse their power.[1470] It has been reported that various detectives have treated suspects inhumanely

[1465] CPL 2013 Article 101
[1466] CPL 2013 Article 102
[1467] Shareef (2016) 23
[1468] Interview with Detective D1, and Criminal lawyer CL1
[1469] A point that all interviewees share
[1470] Interview with Law Professor LP1

either by torturing them or otherwise coercing them to obtain a confession[1471] even though it is prohibited by the CPL 2013 to torture or coerce suspects.[1472] The only mentioned safeguard within the CPL 2013 is the safeguard of allowing an attorney to be present.[1473] Other safeguards during the interrogation such as taping and recording the session, medically checking suspects or overseeing the process by supervisory officers do not exist within the CPL 2013 and the CPLER.[1474] However, detectives of the PP seem to agree that it is prohibited by the law and *Sharia* to harm others (suspects),[1475] but it doubted by international observers whether these safeguards are considered a priority in practice.[1476]

Moreover, national prevention mechanisms within the KSA criminal justice system, such as for the investigation of complaints against detectives, do not formally exist. Nor has he KSA ratified Optional Protocol to the Convention against Torture and Other Cruel, Inhuman or Degrading Treatment or Punishment 2006.[1477] Even though the KSA ratified the Convention Against Torture and Other Cruel, Inhuman or Degrading Treatment or Punishment 1984[1478] in 1997,[1479] taking this step alone is insufficient because the KSA has not implemented it fully within its national law.

In regard to the failure to ensure the presence of an attorney, criminal defence lawyers whom the researcher interviewed have suggested reasons why suspects do not hire an attorney. The first is that most detectives tend to be hostile towards them because they think that lawyers defend "criminals" not "innocents".[1480] The second reason is that some criminal

[1471] Amnesty International Report 2017/18, 317. <https://www.amnesty.org.uk/files/2018-02/annualreport2017.pdf>
[1472] CPL 2013 Article 2
[1473] *Ibid* Article 70
[1474] CPLER 2015
[1475] Interviews with detectives of the PP D1, D2 and D3
[1476] Amnesty International, Saudi Arabia 2017-2018. <https://www.amnesty.org/en/countries/middle-east-and-north-africa/saudi-arabia/report-saudi-arabia/>
[1477] UN OHCHR. <https://www.ohchr.org/en/hrbodies/opcat/pages/nationalpreventivemechanisms.aspx>
[1478] UN OHCHR. <https://www.ohchr.org/en/professionalinterest/pages/cat.aspx>
[1479] UN OHCHR. <https://indicators.ohchr.org/>
[1480] Interviews with Criminal defence Lawyers CL1 and CL2

defence lawyers avoid representing certain groups of people for discriminatory reasons, such as because they are foreigners, poor, females, tribeless or members of rival tribes or from a different religious sect.[1481] The third reason is that many suspects prefer not to hire an attorney during the early stages of the criminal process because they feel it might incriminate them or make them look guilty.[1482] The fourth reason is that criminal law is not a preferred area of practice among lawyers in the KSA because "it is a pain in the head, and not worth the money."[1483] Thus, there is a lack of specialist criminal defence lawyers in the KSA which makes it more difficult for an accused to hire a criminal lawyer, and they might hire less appropriate civil lawyers instead.[1484] The fifth reason is that it is part of the culture of the KSA for individuals to rely on their own "courage" to defend themselves, so they prefer not to hire an attorney, believing that they think they can handle the criminal procedure on their own.[1485] The sixth reason is that many suspects cannot afford to hire a defence attorney, and the state does not operate clear legal aid system to provide one for them even for those who cannot afford it,[1486] especially in pretrial stages.[1487] During trial stage, the KSA is obligated by the CPL 2013 to provide an attorney for those who cannot afford it as will be discussed in Chapter 7. However, neither the Judicial Aid Guide[1488] nor the non-profit Legal Clinic[1489] of the Saudi Bar Association (SBA)[1490] mention aid for attorney in pretrial stages. Detectives of the PP who participated in this study have not defended criminal cases which had been aided

[1481] *Ibid*
[1482] Interview with Criminal lawyer CL2
[1483] Interview with Criminal Lawyer CL1
[1484] *Ibid*
[1485] Interview with Criminal lawyer CL2.
[1486] There may be some firms willing to act pro bono. See British Embassy in Riyadh, List of lawyers in Saudi Arabia.
<https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/943729%2FLocal_Lawyers_List_2020_Saudi_Arabia.pdf>
Also see Latham & Watkins LLP (2019). <https://www.lw.com//admin/Upload/Documents/Global Pro Bono Survey/pro-bono-in-saudi-arabia-3.pdf>
[1487] Interviews with Detectives of the PP D1, D2 and D3
[1488] SBA (2018a). <https://sba.gov.sa/wp-content/uploads/2018/04/legal-aid-bylaw.pdf>
[1489] SBA (2018b). <https://sba.gov.sa/wp-content/uploads/2018/05/legal-clinic-bylaw.pdf>
[1490] SBA. <https://sba.gov.sa/>

by the SBA during investigation stage,[1491] which indicates that having an attorney during investigation stage is not common in the KSA. Lastly, a reason why the human right of legal representation is not secured is that criminal defence lawyering is not respected among official authorities and lawyers, as it is seen as aiding criminals and defending them, a perspective which assumes guilt rather than innocence.[1492] This biased perspective indirectly results in the violation of human rights by preventing suspects from finding proper legal counsel. The KSA criminal law itself appears to be an essential reason which enhances the perspective that suspects are mostly criminals because, as noted by Baderin, the principle of the presumption of innocence is not clearly adopted within the KSA criminal [1493] and constitutional law.

Despite these negative factors, the presumption of innocence appears to be implied within the KSA law, as both the BLG[1494] and CPL 2013[1495] prohibit punishing people who are not convicted with crimes mentioned in the KSA law or in *Sharia*. However, these are implied meanings and not a direct statement, which leaves them open to spurious interpretations by the judicial branch, including the PP, when they presume guilt rather than innocence before conviction. The danger remains that official KSA personnel who are involved within the criminal procedure of crimes may invoke personal morals in the absence of clear legal provisions.[1496]

Therefore, the human right for suspects to have an attorney present during the criminal procedure is far from secured in law or practice in the KSA, even though the CPL 2013 allows for it.[1497] Also, unlike other countries that have successfully secured this right,

[1491] Interviews with Detectives of the PP D1, D2 and D3
[1492] Interview with Law Professor LP1
[1493] Baderin (2006) 274
[1494] BLG Article 40
[1495] CPL 2013 Article 2-4
[1496] Algarni (2013) 511
[1497] CPL 2013 Article 139

pressure from civil society in the KSA is relatively weak, and state intervention is needed to enforce such reforms by formal means.[1498]

Not only is the right to have an attorney present not comprehensively secured during the investigation stage, but other rights also need to be addressed within the KSA law in order to ensure due process, such as access to medical checks, accurate records and notification of family members. Even though some detectives who allow medical checks and give detainees access to doctors and phone calls, detectives of the PP seem to rule it out of considerations of effectiveness,[1499] while the law itself says little about these issues.[1500] Thus, it is common among detectives not to record interrogation sessions,[1501] even though places of detention are equipped with both voice and video recorders.[1502]

Both the KSA BLG[1503] and the CPL 2013[1504] state that it is prohibited to punish a person until they are convicted with crimes found in *Sharia* or legislation. This is the closest that the KSA's legislation comes to the presumption of innocence. Therefore, if the KSA paid more effective attention to the principle and applied it clearly, more effective safeguards would be observed, such as the right to legal counsel.

As addressed in Chapter 2, the KSA has no written criminal code[1505] that states general principles such as the presumption of innocence. Therefore, it is useful to look into the CPL 2013 to see whether it reflects the principle. One tool of analysis that is used in this thesis is policy transfer, so looking into England and Wales's experience in the matter may be

[1498] Montagu (2015) 10-11
[1499] Interview with Sharia Expert SE1
[1500] Article 1 Paragraph 7 of the MEPPB requires that appointed members of the PP "must not have been convicted of crimes or a crime that violates honour or trust, or a disciplinary decision has been issued against him for dismissal from a public office…" The requirement related to crimes of honours and trust indicates that members of the PP should be morally disciplined, and it is to be believed that that is why they allow for access to doctors and phone calls for suspects
[1501] Interview with detective of the PP D1
[1502] *Ibid*
[1503] BLG Article 38
[1504] CPL 2013 Article 3
[1505] See Section 2.3

of benefit. In England and Wales, the presumption of innocence was stated in the common law (by judges),[1506] even before the creation of the European Convention on Human Rights (UCHR) 1950[1507] and the UDHR 1948.[1508] It arguably goes back to Magna Carta of 1215, which stipulated that "no free man is to be arrested, or imprisoned… or in any other way ruined, nor will we go against him or send against him, except by the lawful judgment of his peers or by the law of the land."[1509] In practice, Ferguson notes that the UK differentiates between broad and narrow adaptations of the principle.[1510] A broad adaptation indicates that it applies even before the commencement of a trial, while the narrow adaptation applies it only during the trial.[1511] For instance, English law puts the burden of proof on the prosecutor to prove guilt beyond reasonable doubt[1512] by following proper due process, which leads to the distinction between "legal guilt", that the accused actually did it, or "factual guilt."[1513] In contrast, if they do not prove guilt beyond reasonable doubt, then it is "factual and legal innocence."[1514] Similarly, the police must prove reasonable suspicion when exercising their policing powers or they would be violating the principle.[1515] Therefore, as a practice of the broader adaptation of the principle, it is arguably more important that, before the trial and during the investigation, it is acted on in practical ways, such as by providing legal aid and training for lawyers, their mandatory presence during interviews, video and audio records of interviews, access to medical checks, and access to phone calls.[1516] Most of these points are effectively covered by PACE Codes C and E in stark contrast to the position in the KSA.[1517]

[1506] *Woolmington v DPP* [1935] A.C 462
[1507] UCoHR Article 6 Paragraph 2
[1508] UDHR Article 11
[1509] Magna Carta 1215
[1510] Ferguson (2016) 131–158
[1511] *Ibid*
[1512] *Ibid* 140-143
[1513] *Ibid* 137
[1514] Ibid 137
[1515] *Ibid* 150
[1516] Zander (2018)
[1517] PACE 67 (7B) CODE E

Nonetheless, as the principle of the presumption of innocence is not present within KSA law, it is possible to say that, during investigation, detectives often harbour a preconception that suspects are not innocent,[1518] especially in the absence of practical support for innocence. This approach allows detectives to assume guilt rather than innocence, and this contagious idea seems to spread to criminal lawyers who, in turn, might refuse to represent criminals because the presumption becomes "guilty before even sentencing them"[1519] rather than innocent until proven otherwise. This assumption of the guilt of suspects is therefore a barrier to the right to an attorney. Additionally, this unintentional and subconscious assumption of guilt is present at all other investigative stages, not just at the stage of interrogation by detectives.

6.2.2.2 Powers of investigation (operations) in the KSA; the powers of search and seizure

It was mentioned in the previous chapter that the CPL 2013 allows PCIOs to search people and premises and seize criminal evidence.[1520] Those details will not be repeated here. It was also noted that one function of detectives is to operate as PCIOs.[1521] Therefore, as both detectives and PCIOs, members of the PP are allowed by CPL 2013 to conduct searches and seize criminal evidence.[1522] However, it is argued that detectives have too much power vested in them, as they are more powerful than other PCIOs[1523] because the PP issues search and seizure warrants,[1524] and also supervises search and seizure operations.[1525]

[1518] Interviews with Detectives of the PP D1 and D2
[1519] Interview with Criminal Defence Lawyer CL2
[1520] See Subsections 5.2.2 and 5.3.2
[1521] See previous subsection
[1522] The same rules addressed in Subsection 5.2.2.2 that apply to PCIOs also apply to detectives in later stages of the case.
[1523] Shareef (2016) 189-192
[1524] CPL 2013 Chapter 4
[1525] *Ibid*

6.2.2.3 Powers of investigation (operations) in the KSA; the powers of surveillance

Aside from the powers of search and seizure, detectives also have the power of surveillance.[1526] The KSA BLG prohibits the interception of communication data "except in cases specified by the law."[1527] Exceptions to this constitutional right are indicated within Chapter 5 of the CPL.[1528] Accordingly, the CPL 2013 specifies the Articles on surveillance in Chapter 5,[1529] stating:

> "Mail, cables, telephone conversations and other means of communication shall be inviolable and, as such, may not be accessed or monitored except pursuant to a reasoned order and for a limited period as provided for in this Law."[1530]

Therefore, detectives can carry out surveillance when they have obtained "a reasoned order" specified "for a limited period" of time.[1531] The chairman of the PP issues such orders:

> "The Chairman of the Bureau of Investigation and Public Prosecution may order seizure of letters, correspondences, publications, and packages and authorize monitoring and recording of telephone conversations, if such action is useful in solving a crime. Such order or authorization shall be reasoned and for a period not exceeding ten days, renewable according to the requirements of the investigation."[1532]

This Article comes late in the potential investigative process because it only allows surveillance after a crime has been committed and "if such action is useful in solving a

[1526] CPL 2013 Chapter 5
[1527] BLG Article 40
[1528] CPL 2013 Chapter 5
[1529] *Ibid* Chapter 5
[1530] *Ibid* Article 56
[1531] *Ibid*
[1532] *Ibid* Article 57

crime."[1533] In practice, the Chairman of the PP orders surveillance in many cases before a crime is committed,[1534] which is unlawful because the Article is clear about when to conduct surveillance. Moreover, as was addressed in Chapter 5, PCIOs conduct surveillance without any legal basis and before the crime is committed,[1535] which is also unlawful because such an operation is not addressed by the CPL 2013 nor by any other law. Instead, there may be oral ministerial (administrative) orders,[1536] but they do not enjoy any legislative authority.[1537] Orders are mainly issued by the King or the Crown Prince.[1538] This constitutional tool is called a *Royal Guidance*, and the operative rules are mostly unwritten.[1539] It is usually used by the King or the Crown Prince to fill in legislative gaps.[1540] It is to be assumed that it is meant for members of the Council of Ministers (Ministers) to act on it in the absence of written rules, but it is usually classified as secret[1541] and not published. Therefore, it is possible to speculate that the PP might have been guided by this non-legislative tool to fill in the gaps in the CPL 2013. Those gaps which might be filled by such an order are related to particular legal powers, empowerment of officers, and the timing of the threshold of suspicion.

Other Articles in Chapter 5 of the CPL 2013 restrict detectives from violating the confidentiality of seized intercepted communication means.[1542] Also, other Articles of Chapter 5 of the CPL 2013 emphasise that detectives must not keep the content such as records of seized intercepted communications secret from the accused,[1543] and they must give devices (such as mobile phones) back to the accused if it is urgently necessary after obtaining

[1533] *Ibid*
[1534] Interview with Detective of Public Prosecution D1
[1535] See Subsection 5.2.2.2
[1536] Interview with Police Officer PO3
[1537] See Naseeb et al (2011) 213-256
[1538] Shalhoob (1999) 97
[1539] *Ibid*
[1540] *Ibid*
[1541] Interview with Detective of the PP D1
[1542] CPL 2013 Articles 58, 61
[1543] *Ibid* Article 59

a copy of them in their records.[1544] In general, Chapter 5 of the 2 CPL 2013 covers the main aspects of the power of surveillance, but does not secure fairness or effectiveness because it does not go into detail about such a dangerous instrument in the hands of a public authority which involves the human right of privacy.

Nowadays, the power of surveillance has become an even more dangerous spying tool[1545] because KSA public authorities are accused of violating the human right to privacy by spying on people in virtual spaces.[1546] In the next section, surveillance of cybercrime in cyberspace will be addressed along with other investigative powers and investigatory institutions related to cybercrimes in the KSA.

6.3 The investigation of cybercrime in the KSA by detectives in the PP

This section will analyse the KSA's response to investigating cybercrime institutionally and operationally. Even though the KSA deals with cybercrime as being indistinct from NCCs in regard to the criminal procedure,[1547] including investigation, there is a fine line where the practice of detectives distinctively differentiates between the criminal process of cybercrime and NCCs, and it appears in the operation (powers of investigation).[1548] This agenda will be addressed under the following subheadings: Investigating Cybercrime: Institutional aspects; and Investigating Cybercrime: operational aspects.

6.3.1 Investigating cybercrime: Institutional aspects

[1544] *Ibid* Articles 60, 62
[1545] Zuboff (2019)
[1546] HRW (2014). https://www.hrw.org/news/2014/06/27/saudi-arabia-malicious-spyware-app-identified
[1547] See Section 2.2
[1548] Interviews with members of PP indicates that they notice such differences as will be discussed in this section

In general, the institutions that investigate cybercrime are the PP, and the detectives within that office who investigate cybercrime are the same detectives who investigate other types of crime.[1549]

In the PP, most cybercrime investigations are undertaken in practice by detectives whose speciality is crimes against honour and work in the Anti-honour Crimes Circuit[1550] in the PP.[1551] It might seem odd that investigating cybercrime is the responsibility of anti-honour crimes detectives who have no specialist knowledge in cyber issues.[1552] Even though 18 interviewees out of 21, including all 6 members of the PP,[1553] strongly agreed that detectives are properly trained to deal with cybercrime, it is no surprise that they think that the training that they went through in the Academy related to NCCs is sufficient, along with having training courses to obtain basic computer skills and knowledge.[1554] Unlike the KSA's approach to investigating cybercrime, the UK's approach is arguably more fair and effective.

Firstly, the UK takes the principle of separation of power within its institutions very seriously, separating investigation from prosecution because each is a powerful tool with special powers which should not be vested in one institution alone.[1555] However, the principle is not strictly absolute, and, in some cases, powers are shared among investigative and prosecutorial institutions. Here, the UK identifies such shared powers and justifies why such powers need to be exceptionally shared.[1556] For instance, the UK Serious Fraud Office shares such powers,[1557] but it handles only a few specialised cases. [1558] Secondly, the UK stipulates

[1549] Interviews with Detectives of the PP D1, D2 and D3
[1550] In 7.3.1 the word "circuit" will be found to be similar to division and department.
[1551] Interviews with Detectives of the PP D1, D2 and D3
[1552] Interview with Criminal Defence Lawyer CL2
[1553] 18 interviewees out of 21 including all 6 members of the PP
[1554] Ibid
[1555] Iyer (2018) 507-528
[1556] The Crown Prosecution Service (2018) <https://www.cps.gov.uk/legal-guidance/police-and-cps-relations>
[1557] Powers are allowed by Criminal Justice Act 1987
[1558] HM Crown Prosecution Service Inspectorate. (2012) 17 and 27

that police detectives must have proper training on how to deal with cybercrime,[1559] and such training has proven to be effective in tacking cybercrime.[1560] Thirdly, the UK has designated detectives for dealing with cybercrime, and specialism is more evident at the institutional level. Prime examples are the UK NCA specialised unit,[1561] the NCSC[1562] and the City of London Police unit that combats online fraud and cybercrime,[1563] and implements Secured By Design, an official initiative by the police to secure places using cyber technology.[1564] Therefore, it can be said that the KSA's approach toward investigating cybercrime institutionally indicates that the KSA does not prioritise cybercrime sufficiently in its current approach, and so institutions such as the PP might continually struggle with the criminal procedure of cybercrime. Moreover, there are no forensic institutions that specialise in cybercrime[1565] in the KSA which contributes to the overall ineffectiveness of the KSA's approach toward investigating cybercrime. However, availability of cyber experts for the PP is ameliorated as the ACL specifies that CITC should provide needed aid to the PP.[1566] Nowadays, this kind of aid is shared between CITC and similar governmental entities,[1567] and they collectively form what can be viewed as forensic expertise over cybercrime.

As well as lacking institutional specialism, there have been some cases in the KSA where the PP has not investigated cybercrimes but has been bypassed.[1568] Those cybercrimes are linked to two highly dangerous types of crimes; terrorism and corruption.[1569] Even though both types of crime are within the PP's jurisdiction by law, the jurisdiction can be transferred

[1559] College of Policing <https://www.college.police.uk/What-we-do/Learning/Professional-Training/digital-and-cyber-crime/Pages/Digital-and-cyber_crime.aspx>
[1560] Cockcroft et al (2018) 10-26
[1561] UK NCA <https://www.nationalcrimeagency.gov.uk/what-we-do/crime-threats/cyber-crime>
[1562] UK NCSC <http://www.ncsc.gov.uk/>
[1563] City of London Police <https://www.cityoflondon.police.uk/advice/advice-and-information/fa2/fraud/online-fraud/>
[1564] Police Crime Prevention Initiatives Limited <https://www.securedbydesign.com/>
[1565] Interviews with Police officers PO1, 2 and 3, Detectives of the PP D1, 2, and 3 and CCJs CJ 1, 2 and 3
[1566] ACL Article 14
[1567] See Section 2.2
[1568] Interview with detective of the PP D2
[1569] *Ibid*

to a specially formed committee which, as a creature of a form of royal prerogative, is not mentioned within the CPL 2013, and which self-dissolves after achieving its purpose.[1570]

It might be argued that those committees are unlawful because they overstep existing regular criminal process laws. In the KSA, for the law to be legitimised it must be passed by a competent authority.[1571] According to the KSA BLG, legislation is passed by Royal Decree, and the only authority to issue a Royal Decree is either the King or the Crown Prince.[1572] For instance, the CPL 2013 was passed based on a Royal Decree, and so the argument is that those committees have also been established by the most powerful tool of legislation - Royal Decree. Thus, the self-dissolving investigative committees that have been formed over the past years in the KSA are viewed as authorised by a Royal Decree, such as the most recent in 2017.[1573] Therefore, this gives them legitimacy within the principles of the KSA's legal system, and their legitimacy is almost never challenged legally. The 2017 Royal Decree does not include cybercrime by name, mentioning only fighting "public corruption" as the objective which it seeks.[1574] Nevertheless, it can be implied that public corruption includes cybercrime and cyber evidence. Additionally, the Royal Decree outlines the investigative powers given to the committee which can be viewed as unlimited powers:

> "First: The formation of a supreme committee headed by His Royal Highness, the Crown Prince, and the membership of: the head of the Oversight and Investigation Authority, the head of the National Anti-Corruption Authority, the head of the General Auditing Bureau, the head of the Public Prosecution, and the head of Presidency of State Security.

[1570] BBC News (2019)
[1571] BLG Articles 67 and 70
[1572] *Ibid* Articles 65, 66 and 70
[1573] KSA Royal Decree No (A/38) 2017
[1574] *Ibid*

Second: As an exception from the statues, regulations, instructions, orders and decisions, the committee performs the following tasks:

1- Confining the violations, crimes, persons and related entities in cases of public corruption.

2- Investigating, issuing arrest warrants, banning from travel, checking accounts and portfolios and freezing them, and tracking the current funds and assets which are transferred or transferred by persons and entities whatever their status are, and they have the right to take any precautionary measures that they see until they are referred to the investigation authorities or judicial authorities according to conditions.

3- Taking what is necessary with those involved in public corruption cases, and taking what they see necessary against persons, entities, funds and fixed and movable assets inside and outside and returning the funds to the state's public treasury and registering property and assets in the name of the state's real estate, and the committee shall decide for the greater good what measures to take with those who cooperate.

Third: The committee may seek assistance from whomever they see suitable, and it may form teams to investigate and so on, and it may delegate some or all of its powers to these teams.

Fourth: Upon completion of its duties, the committee will submit a detailed report to us on its findings and what it has determined in this regard."[1575]

While a legal basis might be located, it might be argued that these committees lack sufficient legal understanding of the criminal processes and technical intricacies applicable to cybercrimes, especially in regard to the investigation stage. The committees usually contain

[1575] *Ibid*

one senior member of the PP as a detective and a prosecutor and a CC.[1576] Although their involvement helps maintain an image of the legality of such committees, the reality is that others who are not lawyers often play a more leading role.

Before addressing how detectives operate in response to cybercrime, it might be better to address why those committees influence other investigative institutions, such as the PP. The idea addressed in the previous Chapter[1577] about "high policing" and "low policing"[1578] might be applicable in regard to investigations held by the KSA's PP and the formation of self-dissolving committees. It might be possible to consider the KSA PP as a "low" investigative institution and the formed self-dissolving committees as "high" investigative policing institutions. Even though the focus of this Chapter is the PP as it practices the narrow concept of investigation, the formed self-dissolving committees also play a similar role. Moreover, formed self-dissolving committees that practice narrower types of investigation and that are considered as high investigative institutions sets the rules of investigation for the PP to follow. One reason for characterising those committees as high investigative institutions is that membership of those committees are given only to high profile seniors of investigative and judicial institutions, such as the PP and the CC.[1579] Another reason for such characterisation is that those committees only target serious crimes which low investigative institutions are not yet sufficiently equipped to deal with,[1580] such as terrorism, corruption, and cybercrime involving espionage and incitement against the government. Finally, the nature of the authoritarian governance in the KSA makes it possible that such an investigative institution falls under the characterisation of high policing.

[1576] *Ibid*
[1577] See Subsection 5.3.1
[1578] Brodeur (1983) 508-520
[1579] *Ibid*
[1580] The equipment here refers to legal tools not materials. Since the KSA law is not developed enough to deal with complicated crimes that the law says less about their criminal process, the committee has one of the most effective legal tool which is the Royal Decree vested in the head of the committee whose verbal orders considered to be a binding law in the absence of written law. See Shalhoob (1999) 87-102

Therefore, it is possible to say that those formed self-dissolving high investigative committees might be considered as the role model for the low investigative institution which might follow their practice, even though such practice may violate basic human rights. Thus, addressing the function of those committees would be in order to provide a broader picture when it comes to testing the fairness and effectiveness of the criminal investigation of cybercrime later in Section 6.4.

Generally, investigating cybercrime at an institutional level is undertaken by detectives of the PP as a low investigative institution. In exceptional circumstances, serious cybercrimes might be dealt with by the high investigative institutions that are formed by a Royal Decree and self-dissolve when they accomplish their purposes. Between the two institutions, the PP investigates the majority of cybercrimes[1581] and it follows the practice of high investigative institutions whenever the main law of criminal procedure (CPL 2103) has less to say about the criminal procedure of cybercrime.[1582] The practice of investigative institutions is also related to a number of operational facets, as will be addressed in the coming sub-section.

6.3.2 Investigating Cybercrime: Operational aspects

One of the aims of this chapter is to address how cyber evidence and cyber suspects are dealt with during investigations the KSA. Therefore, the processing of both cyber evidence and cybercrime suspects during the course of cybercrime investigation will be addressed in regard to the operational investigatory powers that are used by detectives. Moreover, addressing the investigatory operational powers will help to move toward testing

[1581] Interviews with detectives of the PP D1 and D3
[1582] Next section

the fairness and effectiveness of investigating cybercrime in the KSA, which will be analysed in the next section of this Chapter.

It has been mentioned earlier that the CPL 2013 grants the powers of interrogation, search, seizure, and surveillance to detectives, and since the KSA has no special law that deals specifically with the criminal procedure of cybercrime,[1583] it is expected that the same provisions that apply to NCC are applicable to cybercrime. This kind of dual application might be acceptable when it comes to investigative institutions, but when it comes to investigatory operational powers, it will be not possible to apply the rules of physical space to cyberspace, especially in regard to the powers interrogation of search, seizure and surveillance as human rights are involved in the process.[1584]

6.3.2.1 Investigating Cybercrime: Operational aspects – power of interrogation

Interrogation of cybercrime suspects is not treated differently to interrogating NCC suspects.[1585] Both powers are held by detectives of the PP. Moreover, it should be known that committing cybercrimes within cyberspace does not mean that interrogation of this type of crime should be held in cyberspace, although some interrogation has been held by detectives in cyberspace. However, this practice has nothing to do with the nature of cybercrime. It is instead related to the circumstances in general, such as interrogating suspects in cyberspace during the curfew caused by the spread of Coronavirus in April 2020.[1586]

As addressed earlier, similar to NCC suspects, most cybercrime suspects have limited access to a criminal defence attorney for the same reasons concluded in that subsection.[1587] However, even though there are no official statistics in the KSA, it is generally supposed that

[1583] See Subsection 6.2.2
[1584] Murray & Klang (2005) 10
[1585] Interviews with Detectives of Public Prosecution D1, D2 and D3
[1586] *Ibid.* According to Detectives, this has happened just for a few days, and it has been discarded.
[1587] See Subsection 6.2.2.1

cybercrime suspects are underrepresented. According to the data collected during the fieldwork,[1588] cybercrime suspects do not hire criminal defence lawyers for various reasons, some of which have been mentioned in the previous section.[1589] Nevertheless, for the coming argument, two of the given reasons are highlighted. The first reason is that the evidence against them is solid and cannot easily be challenged in most cybercrime cases.[1590] It is to be argued that there are two possible answers to why evidence can be difficult to challenge. The first is because of technicalities. It seems impossible to find forensic scientists who can act for the suspect,[1591] though there are high quality forensic experts who act for the Public Prosecutor,[1592] as noted by Detective D2, some of whom work for government institutions such as CITC, MoI, and KACST.[1593] Similarly, the UK NCSC provides cybercrime investigative institutions with cyber forensic experts.[1594] By comparison, cybercrime suspects in the UK have more access than in the KSA to private and independent cyber forensic experts who operate for private profit such as CYFOR.[1595] The second answer is because of non-disclosure of the evidence. The rules of disclosure in KSA are limited and ambiguous, which allows the PP the option of refusal to disclose the evidence.[1596] However, in England and Wales, the disclosure rules are specified more clearly and more peremptorily applied under the Criminal Procedure and Investigation Act 1996.

The second reason, as addressed in the previous subsection, is that the investigation of cybercrime is carried out within the Anti-honour Crimes Circuit in the PP, indicating that cybercrime is categorised as crimes against honour in the KSA. This categorisation makes it

[1588] The data in this case is analysed based on interviews with those who have direct interaction with cybercrime suspects; police officers, detectives, prosecutors, CCJs and criminal defence lawyers.
[1589] See Subsection 6.2.2.1
[1590] Interviews with Criminal Defence Lawyers CL2 and CL3
[1591] Albalawi (2009)
[1592] Al Beshri (2008)
[1593] Interview with Detective of the PP D2
[1594] UK NCSC <https://www.ncsc.gov.uk/>
[1595] CYFOR, About Us <https://cyfor.co.uk/about-us/>
[1596] Interview with Criminal defence Lawyer CL 3

difficult for cybercrime suspects to hire an attorney, because the matter of honour within KSA society is very sensitive, and that is, as addressed earlier, one reason why most criminal defence lawyers tend to avoid representing cybercrime suspects.[1597]

Since the evidence against cybercrime suspects cannot be easily challenged, and the suspects are often unrepresented, they tend to depend on the integrity of detectives to handle the criminal case against them or their personal connections properly to pressure detectives into terminating the criminal case against them.[1598] Therefore, even if they found a criminal defence lawyer to defend them, they tend to look for one who has a strong personal connection with detectives, rather than one with a specialist legal background.[1599]

Criminal lawyer CL1 notes that in the KSA:

> "All highly successful criminal lawyers are former detectives [he means detectives of the PP] or former judges [including CCJs]. They had an early retirement, and they now use their connections with judges and detectives to dismiss criminal cases. They should be banned from being lawyers."[1600]

Even if this is not always true, criminal defence lawyer CL3, who used to be a former detective, agrees that former detectives and judges make better lawyers because they know how the judicial system functions in practice.[1601] He himself says:

> "It is no shame that we [it seems that by 'we' he means 'I'[1602]] take advantage of our connections in the service of the greater good [by which he means justice], only when we know that the individual in the crimes

[1597] See Subsection 6.2.2.1
[1598] Interview with Detective of the PP D2
[1599] *Ibid*
[1600] Interview with Criminal Lawyer CL1
[1601] Interview with Criminal Lawyer CL3
[1602] It has been noticed by the Saudi linguist, Bandar Alghmaiz, that in the KSA and UAE, people say 'we' in cases of … when they do something wrong and they want to make light of it. Dr Alghmaiz is an expert on applied linguistic, and considered to be influential. See Alghmaiz (2018)

> [whether it is a cybercrime or NCC] does not press charges against our clients or connections."[1603]

If that is really the case, not only would cybercrime suspects would be at risk of violating their right to an attorney, but they also might be involved indirectly through experienced former detectives and CCJs' in other crimes such as corruption or bribery.[1604] Whether cybercrime suspects are represented by a lawyer or not, during interrogation detectives can present substantial evidence against them based on their powers of search, seizure and surveillance.

6.3.2.2 Investigating Cybercrime: operational aspects – powers of search, seizure, and surveillance

Powers of search, seizure and surveillance are granted to detectives by the CPL 2013.[1605] This Law does not distinguish these powers when it comes to virtual space surveillance. However, when it comes to using those powers to investigate in cyberspace and for cybercrime, detectives have to improvise new actions which later become unwritten rules which self-regulate those powers:

> "Sometimes you have to use your common sense to know what is right and what is wrong … spying is *Haram* [prohibited in Islam], so all types of spying are *Haram*, unless to prevent greater damage … the general *Sharia* rule says *Al-dharorat Tobeeh Al-mahdhorat* [necessity may authorise prohibited acts]."[1606]

[1603] Interview with Criminal Lawyer CL3
[1604] KSA Anti Bribery Law 1992 classifies the misuse of personal connection through abuse of power as a crime of bribery
[1605] See Subsections 6.2.2.2 and 6.2.2.3
[1606] Interview with Detective of the PP D1

In practice, detectives of the PP are a mixture of Law diploma holders and *Sharia* diploma holders.[1607] Together, they know the difference between cybercrime and NCC, so they use their own collective experiences to overcome some of the legal difficulties which might face them in their investigation of cybercrime, especially in regard to powers relating to search, seizure and surveillance.[1608] For instance, *Sharia* diploma holders would interpret the texts of *Sharia* to prohibit spying or hacking in order to obtain cyber evidence.[1609] Similarly, Law diploma holders would interpret legal texts to restrict spying or hacking when searching or seizing cyber evidence[1610] because the CPL 2013 does not cover all possible restrictions. This could be considered as self-regulation in the absence of clear legislation or *Sharia* doctrine. Even though these self-regulatory rules are unwritten, they could be viewed as guidance for detectives to follow.[1611] Earlier, in Chapter 2, a regulatory pyramid was introduced.[1612] It suggests that cyber self-regulation is at the bottom of the pyramid in the absence of the rules within the criminal law, civil law and formal regulatory law.[1613] Nevertheless, in order to consider this practice as self-regulation, it should first be identified and second be evaluated in order to consider its legality.

This self-regulation can be identified when looking at the pattern of the practices of detectives. For example, in multiple cybercrime cases, detectives search the smartphones of the accused without their permission and without a warrant because such a practice is common and no officer has been questioned about alleged misconduct in relation to it.[1614] As a result, the cyber evidence obtained is technically unlawful because it is based on an

[1607] Interview with Public Prosecutor PP1
[1608] *Ibid*
[1609] Interview with Sharia Epxert SE1
[1610] Interview with Law Professor LP3
[1611] Interview with Public Prosecutor PP1
[1612] See Subsection 2.2.1
[1613] Ayres and Braithwaite (1992) 35
[1614] Interviewees except for criminal defence lawyers CLs and law professors LPs agree that rules should not be followed if it is for the greater good of the people, and they agree that detectives violate only what they know it is necessary. The measurement for what constitutes necessary violation was the "common sense, and the good intention."

unlawful search, yet the officers still seize the cyber evidence and present it to the court, and it would then be admitted regardless of how it was obtained. [1615] One reason addressed earlier about why cyber evidence can be admissible even if obtained unlawfully is that the KSA's CPL does not allow for the termination of the criminal case based on procedural error.[1616]

Moreover, the PP may arrange for the surveillance of the cyber communication means, such as smartphones and laptops, with the help of internet service providers and may also ask for assistance regarding surveillance and obtaining cyber evidence from governmental entities, such as the NCA, the MCIT CITC, and the KACST.[1617] Detectives within the PP believe that they can perform this kind of surveillance based on powers in Chapter 5 of the CPL 2013.[1618] However, surveillance within cyberspace and physical space is different because cyber communication means are more complex and involve the data collections of the accused beyond the suspected crimes and data of other parties who are not part of the investigation.[1619] This situation has mainly resulted from the absence of law or other governance regarding the investigatory powers for cybercrimes in the KSA.

Those practices and other similar practices, such as asking the accused to "give them the password and numbers" for social media accounts so they can swiftly go through what might incriminate him,[1620] constitute a regular pattern within the practices of detectives which proves that self-regulatory rules have been established in the absence of clear law provisions that lawfully guide detectives or allow them to create guides for themselves. These informal practices by detectives are not self-regulation in any formal sense which could be construed as complying with fairness. However, it might amount to self-regulation in a broader sense, which includes the influence of internal police cultures, as discussed earlier in this section.

[1615] Interview with CCJ CJ1
[1616] See Subsection 5.3.2.1.1
[1617] See Subsection 2.2.1
[1618] See Subsection 6.2.2.3
[1619] Staden (2015) 3-4
[1620] Interview with Criminal Lawyer CL1

When evaluating such practices, it is possible to say that self-regulation applied by detectives toward their practice regarding investigative powers is questionable in terms of fairness and effectiveness of such unwritten rules, and appears to contradict with the soul of the highest law of land in the KSA, namely *Sharia*.

Even though, as discussed about the KSA PF, members of investigative entities employ ethical principles which prevent them from invading the privacy of others,[1621] they do not always follow this restraint. Therefore, questions necessarily arise about whether the current approach of the KSA regarding investigating cybercrime is fair and effective.

In comparison with the UK, legislation already described (such as the IPA 2016) as well as the issuance of codes of practice have been important responses.[1622] The UK has so far responded more fairly and effectively in this aspect of privacy than the KSA.[1623] In the next section, testing both the fairness and effectiveness of the KSA's response to investigating cybercrime will be conducted.

6.4 Effectiveness and fairness of the KSA's response to investigating cybercrime

As a major objective of this research, the KSA's response to investigating cybercrime will be tested for fairness and effectiveness in order to identify what improvements could be made in the KSA when tackling cybercrime.[1624] Elements of these tests are identified in Chapter 2.[1625]

[1621] See Subsection 5.3.2.1
[1622] College of Policing (2020)
[1623] Information Commissioners Office (2020)
[1624] See Section 1.3
[1625] See Section 2.4

6.4.1 Effectiveness of investigating cybercrime in the KSA

Investigating cybercrime is arguably hampered in the KSA because, as with NCCs, it is vested in the hands of the PP and not the PF.[1626] Additionally, at the investigation level, detectives apply the CPL 2013 in order to process cybercrime cases, but this Law has nothing to say specifically about cybercrime. [1627] Therefore, what is going to be tested in the coming subsections is whether the KSA's response to investigating cybercrime is effective. The tools for the test are conceptual effectiveness, comparative effectiveness, and national effectiveness.

6.4.1.1 Conceptual effectiveness of investigating cybercrime in the KSA

The question of whether the KSA's method of investigating cybercrime is successful and meets the objectives specified by the KSA authority is the subject matter of determining effectiveness from a conceptual point of view.[1628] Therefore, it is crucial to assume that the KSA has officially outlined the objectives of investigating cybercrime. However, what is found in official documentation are political promises of tackling cybercrime rather than official objectives stated by the legislative branch in the KSA (the Council of Ministers and Shura Council) or even the executive branch (the ministries and public commissions).[1629] Therefore, without objectives in the first place, the response is doomed to failure. However, this does not mean the KSA does not assess the investigation of cybercrime at all. The KSA's approach to the "success" of investigating cybercrime, according to Detectives and prosecutors[1630] of the PP, seems to point, as the main measurement for effectiveness (successfulness), to the rate of completion of the number of cases under investigation and not

[1626] See Subsections 6.2.1 and 6.2.2
[1627] Interview with Law professor LP1
[1628] See Subsection 2.4.1.1
[1629] Latest promise is the proposal of Crown Prince Mohammed Bin Salman to reform the KSA legislation. Naar (2021)
[1630] Prosecutors shifts between investigation and prosecution. See Section 7.2

to let them accumulate, so as to allow newer cases to be dealt with.[1631] Unfortunately, the way in which cases are completed or even their ultimate outcome seem less important.

6.4.1.2 Comparative effectiveness of investigating cybercrime in the KSA

The UK specifies objectives which it seeks to achieve through practical agendas. These objectives are found in various acts and the agendas are found in UK NCSS.[1632] Whether the UK achieves its objectives and agendas or not it is reflected in official documentation of its objectives and agendas, unlike the KSA. The UK NCSS 2022 implies that the previous five years strategy was a success.[1633] Moreover, UK law allocates investigatory powers in regard to cybercrime and cyber evidence in a way which is distinct from NNCs. Therefore, the KSA's approach is not as successful as that of the UK's, because it lacks the important basic methods (objectives and agendas), and it does not distinctively apportion investigatory powers in a targeted way to NCC. Nevertheless, many KSA nationalists[1634] may disagree out of passion and love for their country and not based on the fulfilment of necessary measures, such as having clear written objectives and agendas, proper training, and forensic facilities.

6.4.1.3 National effectiveness of investigating cybercrime

On the national level, all detectives are subject to general intensive training,[1635] and only a few are subject to any level of specialised training to deal with cybercrime.[1636] General

[1631] Interviews with members of the PP D1, D2, D3, D4, PP1, PP2, and PP3
[1632] UK NCSS 2016 to 2021
[1633] UK NCSS 2022 <https://www.gov.uk/government/publications/national-cyber-strategy-2022/national-cyber-security-strategy-2022#part-1-strategy>
[1634] The *Almadkhaliah* movement is a large religious movement that always support the kingdom's approach toward any subject out of the notion that *Guardians of Muslims* (Leaders) know better and must be obeyed under all circumstances. See Lacroix (2011). Nowadays, they are one of the most popular movements among the KSA
[1635] MEPPB Article 2
[1636] Interviews with detectives of the PP D1, D2 and D3

training can be divided into two parts. The first takes place in the Academy and begins after accepting trainees and before assigning them to their posts.[1637] This stage lasts one year maximum and six months minimum[1638] and is mostly theoretical, where all trainees study intensive courses about *Sharia* (only criminal aspects), criminal law and criminal procedure.[1639] The second part is also one year long, and takes place after finishing the theoretical training. In this part, the trainees receive instruction in the PP as they observe senior members and become partially involved within either investigation or prosecution under the supervision of each head of department to which they were assigned.[1640] Usually, almost all trainees pass those two parts.[1641] Specialised training in developed countries such as the US[1642] is also given to those chosen by the Head of PP; usually only three to five members are chosen annually.[1643] Training outside the KSA has been viewed by members of the PP as more effective than that given within the KSA, especially in relation to investigation techniques.[1644] This indicates that only a few detectives are well trained to deal with the criminal investigation of cybercrime. The absence of specialism negatively affects the overall effectiveness of the KSA approach.

Another feature is that, as already discussed, the KSA enjoys flexibility in being able to establish investigatory institutions with unlimited investigative powers based on highly fluid sources of law such as *Sharia* and royal authority (by Royal Decrees) in order to tackle serious crimes including cybercrime, yet it has never established an institution which is only dedicated to tackle cybercrime alone. In most other countries, including the UK, those

[1637] *Ibid*
[1638] MEPPB Article 2
[1639] Interviews with detectives of the PP D1, D2 and D3
[1640] MEPPB Article 2
[1641] Interviews with detectives of the PP D1, D2 and D3
[1642] *Ibid*
[1643] *Ibid*
[1644] *Ibid*

effective responses cannot be so legally implemented. [1645] However, countries as the UK do not follow the fluid approach of the KSA because of its lack of legality and respect for human rights. In *Malone v UK*,[1646] when the UK tried to use broad governmental non-legal powers to regulate surveillance, the powers were condemned on human rights grounds. This case shows the human rights problems related to the investigatory power of surveillance.[1647] Despite the lesson, the fault has been repeated in the UK laws of surveillance.[1648] Although the KSA might see its approach as effective, it is not acceptable because it fails to consider the rule of law and fairness, especially in terms of respect for privacy, due process and legal certainty.[1649]

6.4.2 Fairness of investigating cybercrime in the KSA

Similar concerns to the PF approach towards human rights have arisen in regard to the fairness of investigating cybercrime in the KSA. In order to test whether investigating cybercrime in the KSA is just, this test should be applied in three aspects: conceptual, international, and national.

6.4.2.1 Conceptual meaning of fairness in regard to investigating cybercrime in the KSA

The conceptual meaning of the KSA's approach to investigating cybercrime tests that the approach is fair. The international community is concerned that the KSA is in breach of human rights from multiple aspects, including the rights to privacy and due process.[1650] Whereas representatives of the KSA have stated in multiple international events that KSA

[1645] *Almadkhaliah* views the KSA policies as special measures that only KSA is blessed with. See Lacroix (2011)
[1646] *Malone v the United Kingdom*. (1985) 7 EHRR 14, [1984] ECHR 10, 7 EHRR 14
[1647] Another case was Halford v UK (20605/92) [1997] ECHR 32 (25 June 1997)
[1648] Hirst (2019) 403-421
[1649] UPR, Saudi Arabia 3rd cycle. <https://www.ohchr.org/EN/HRBodies/UPR/Pages/SAindex.aspx>
[1650] Amnesty International, Saudi Arabia 2017-2018 <https://www.amnesty.org/en/countries/middle-east-and-north-africa/saudi-arabia/report-saudi-arabia/>

law is not in such violation because it applies *Sharia,*[1651] these complaints about privacy, due process and so on remain unresolved. In the coming sections, both arguments will be addressed.

6.4.2.2 International meaning for fairness in regard to investigating cybercrime in the KSA

International human rights stipulate that people should be guaranteed the right to privacy, private property, and proper due process in order for the state response to be fair. [1652] Those rights are the most frequently violated when it comes to state intervention in the criminal process of cybercrime, including the investigatory process.[1653] During the investigation stage, detectives may obtain cyber evidence using investigatory powers.[1654] Among the most controversial of these is the power of surveillance.[1655] Countries such as the UK have held protracted debates about the use of investigatory powers that could violate the human right to privacy.[1656] Anderson reports that, even though some might consider privacy as a "luxury of civilisation", it relates to major human rights such as freedom of homes from being intruded which is an ancient right that is recognised in many ancient traditions and religions.[1657] It might be possible to say that those debates have resulted with the issuance of multiple Acts in the UK, most of which have been replaced by the comprehensive IPA 2016.[1658] Even though the UK might be considered as one of the fairer countries in their approach to tackling cybercrime with fairness,[1659] it has still struggled with powers such as

[1651] Chehaye (2018)
[1652] Franck (1995) 6–9
[1653] Murray & Fussey (2019) 32-33
[1654] McKay (2017) 30
[1655] Murray & Fussey (2019). 31-60
[1656] Cobbe (2018) 14
[1657] Anderson (2015) 25
[1658] Hirst (2019) 403-421
[1659] Murray and Fussey (2019) 31-60

bulk surveillance.[1660] However, the UK's response to the matter can be considered as being exemplary in terms of thorough consideration and comprehensive legal statements as well as oversight, especially via the Investigatory Powers Commissioners Office (IPCO),[1661] and the KSA could learn from this approach.[1662]

In the KSA, operational powers are barely addressed in the legislation, leaving a huge gap between unfair practices on the part of the detectives and the legal restrictions of the state.[1663] Consequently, the human rights to privacy and proper due process are always in danger of being violated.

International standards of human rights entitle everyone subjected to the criminal procedure, including for cybercrimes, to an attorney (including during the investigation of crimes), accurate records, access to medical treatment, and notifying their family of their detention.[1664] International human rights standards prohibit any form of torture or inhuman treatment during the process.[1665] The KSA complies with those standards from a legislative point of view.[1666] The CPL 2103 prohibits torture during the process, and entitles everybody to an attorney.[1667] However, as noted by Human Rights Watch[1668] and Amnesty International,[1669] some detectives use torture and coercion with cybercrime suspects, especially if the crime is political in nature.[1670] Moreover, in most of those cases, suspects

[1660] *Ibid* 33
[1661] See IPCO <https://www.ipco.org.uk/>
[1662] IPCO, Annual Report (the extent of scrutiny) 2019 <https://www.ipco.org.uk/docs/IPC%20Annual%20Report%202019_Web%20Accessible%20version_final.pdf>
[1663] See Subsections 6.2.2. and 6.3.2
[1664] Henkin (1990)
[1665] ICCPR Article 6
[1666] Naseeb et al (2011) 321
[1667] CPL 2013 Article 2
[1668] HRW (2013) <https://www.hrw.org/report/2013/12/17/challenging-red-lines/stories-rights-activists-saudi-arabia>
[1669] Amnesty International, Saudi Arabia 2017-2018 <https://www.amnesty.org/en/countries/middle-east-and-north-africa/saudi-arabia/report-saudi-arabia/>
[1670] Gulf Centre for Human Rights. (2018) 12

have no access to an attorney.[1671] Thus, those concerns raised by the international community are justified, and it can be said that, from this perspective, the KSA's approach to the investigation of cybercrime is not fair because it fails to curtail breaches of human rights.

In conclusion, it is evident that the KSA does not meet the expectations set out in international human rights laws, and so it is continuously criticised for its shortcomings. However, some argue that the Western criticisms are unduly dogmatic[1672] and fail to appreciate other cultural perspectives and political differences. [1673] It is thought that this is the argument most Saudis would voice whenever the KSA is accused of violating human rights.[1674] However, it does not remove the unnecessary unfairness of investigative practices and laws. Therefore, the KSA still should apply international human rights more effectively within its criminal legal system. To do so, it needs first to be part of international human rights treaties, such as ICCPR.[1675]

6.4.2.3 National meaning for fairness in regard to investigating cybercrime in the KSA

The KSA passed the CPL 2013 after the international community pressured them to do so.[1676] However, some might argue that it was passed because the KSA protects human rights in compliance with *Sharia* only, as the BLG suggests.[1677] Also, some might argue that violations of human rights arise only as cases of individual misconduct, and that there is no proof of official orders to violate human rights.[1678] Moreover, others may say that the

[1671] *Ibid*
[1672] Supiot (2017)
[1673] *Ibid*
[1674] During interviews, Sharia experts SE1, SE2 and SE3 showed a strong opposition to human rights as adopted by the "Western countries" or the "Western world" as they call it.
[1675] UPR, Saudi Arabia 3rd cycle. <https://www.ohchr.org/EN/HRBodies/UPR/Pages/SAindex.aspx>
[1676] Both versions of the CPLs were passed as a consequence of continuous pressure by independent international human rights observers. See Subsection 4.2.4
[1677] Naseeb et al (2011) 321
[1678] Interviews with PO1, D1 and D2.

inhumane treatment of suspects is prohibited by both *Sharia* and legislation and that transgressors should be brought to justice.[1679]

These arguments might carry some weight if the PP were to be transparent. No official statements have ever been announced by PP or any investigative committees in regard to officers accused of violating human rights during the investigation of cybercrime.[1680] Moreover, these arguments might be true if it were not for the fact that the KSA uses the term "human rights", which is a term that has not originated in the *Sharia*.[1681] Many Muslim countries take it upon themselves to bend the term human rights to their advantage and use *Sharia* as a sacred justification to fall short of its full implementation.[1682] For the KSA, the term "human rights" was first introduced in the BLG in 1992 not only after international pressure, but also after internal national pressure, as it was used as tool to placate human rights movements within the country,[1683] and it was also a signal to the *Sahwah* faction that the state could determine ideology and values and cultures.[1684] Thus, it can be argued that its implementation was a clever political tactic, and was not the result of a moral belief in rights. Therefore, it is possible to assert that the KSA has not succeeded in protecting human rights during the criminal process of cybercrime, especially at an investigative level, due to its general approach towards issues of human rights when investigating cybercrime.

The human rights of privacy and due process are dealt with in the KSA as a religious issue rather than a legal one.[1685] The KSA issues legislation concerning the processing of crimes, such as cybercrime;[1686] otherwise, it would not have passed the CPLs of 2001 and

[1679] Interview with Criminal defence lawyer CL3
[1680] *Ibid*
[1681] Udah (2009) 43
[1682] Many observed human rights violations by Muslim countries were committed in the name of Sharia. See Amnesty International report 2020/2021 <https://reliefweb.int/sites/reliefweb.int/files/resources/POL1032022021ENGLISH.PDF>
[1683] Lacroix (2011)
[1684] See Subsection 4.4.1.3
[1685] Alanazi et al (2018) 6
[1686] Shareef (2016) 9

2013. However, it leaves issues of human rights to *Sharia*, which is the dominant doctrinal source of morality in the country,[1687] even though it says little about modern human rights, which eventually leads to the state officials violating contemporary human rights norms.

Issues of surveillance, due process, and human rights are not dealt with in detail within the CPL 2013 during the preliminary investigation of cybercrime, and that is why the investigative institutions in the KSA can spy on people with few legal restrictions. As discussed earlier in this Chapter, the CPL 2013 recognises the power of surveillance, and the rights to due process and privacy, but it is not enough to simply recognise these issues, barely saying anything about them, because such an approach allows institutions can get away with the violation of human rights.[1688] The assertion that the KSA deliberately violates human rights under the umbrella of *Sharia* might have some truth to it, because even though the international community pressures the KSA to be more sensitive towards human rights, the KSA is not always cooperative. *Sharia* experts insist that international community does not understand the true fairness of *Sharia*.[1689] Therefore, it is possible to say that the KSA considers those international pressures as interferences in its internal affairs, which, from its own perspective, can be dealt with only by the "perfect *Sharia"* not the "imperfect" international human rights.[1690] However, this perspective is theoretically weak, because *Sharia* prohibits spying, yet the investigative institutions in the KSA still spy on people.[1691] Furthermore, *Sharia* prohibits coercion, yet detectives coerce cybercrime suspects to elicit a confession.[1692] As for procedures, *Sharia* encourages Muslims to present arguments coherently and comprehensively[1693] and, if they cannot, they can ask others to present their

[1687] BLG Article 26
[1688] Interview with Criminal defence lawyer CL3
[1689] Interviews with experts on Sharia SE1, SE2, SE3
[1690] *Ibid*
[1691] See Subsections 6.2.2 and 6.3.2
[1692] *Ibid*
[1693] Udah (2009) 49

argument in order to avoid injustice.[1694] However, the human right to due process (especially related to legal representation) is not secured during the investigation of cybercrimes, as discussed earlier in this chapter.[1695] Therefore, it is possible to say that not only does the KSA fail to comply with international standards of fairness when it comes to the investigation of cybercrime, it also fails to comply with the standards of fairness found in *Sharia*, which officials claim is the basis of all of their legal provisions and observances.

6.5 Investigating cybercrime in the UK: policy transfer lessons

Another objective of this research is to learn from other countries' approaches regarding the criminal procedure of cybercrime.[1696] Therefore, an examination of the UK's response to investigating cybercrime will be addressed in this section.

Due to its early recognition of the differentiation between cybercrime and NCC, the UK has passed successive legislation which specifies the role of the Police in investigating cybercrime,[1697] some of which have been addressed in Chapter 4.[1698] It appears that the UK has drawn increasingly clear lines for the Police to function in cyberspace and detect cybercrime using lawful powers.[1699] Unlike in the KSA, the UK Police (rather than prosecutors) investigate cybercrime.[1700] The UK's response considers the investigative institutions and operations in detail. Furthermore, the UK Police have proven to be more effective in policing cybercrime and arguably fairer than the KSA in doing so, as discussed in Chapter 5.[1701]

[1694] *Ibid* 49
[1695] See Subsection 6.2.2.1
[1696] See Section 1.3
[1697] Fafinski (2009)
[1698] See Section 4.5
[1699] Walden (2007)
[1700] *Ibid*
[1701] See Section 5.5

Besides the two proposed lessons discussed in Chapter 5, which are redefining the role of the KSA PF and reconsidering the KSA's approach toward human rights,[1702] there are four additional lessons that the KSA can learn from the UK in regard to the investigation of cybercrime. The first is to create a clear separation between the investigation of cybercrime and prosecution. The second lesson is to enhance the role of criminal defence lawyers during the initial stages of the criminal process, along with access to medical treatment, accurate records, and notifying the accused's family. The third lesson is the UK's multidisciplinary approach. The fourth lesson is the UK legalistic approach.[1703] Each lesson will now be considered in detail.

6.5.1 Separation of cybercrime investigatory powers and the Public Prosecution

The UK separates investigation from prosecution, mainly for the purposes of implementing the principle of the separation of powers within its legal system which is seen as having important value in ensuring checks and balances amongst powerful state institutions for the purposes of the rule of law, accountability, and respect for the individual.[1704] Not only does the UK separate investigation from prosecution, it also separates investigating cybercrime from investigating NCCs within its policing agencies.[1705] It is believed that the separation of powers by the UK is a reason that the UK has been tackling cybercrime more effectively and fairly than the KSA. Also, the UK's approach in regard to investigation cybercrime has been more effective and fairer because it allows the development of specialisms as well as checks and balances.[1706]

[1702] *Ibid*
[1703] Gillespie (2019) 287-366
[1704] Iyer (2018) 507-528
[1705] McKay (2017)
[1706] McGuire & Dowling. (2013) 10, 14 and 15.

The KSA, on the other hand, does not vest the power of investigation in the hands of the PF as it did before the implementation of the CPL 2001.[1707] Since then, the KSA has moved all the investigative and prosecution powers from the PF to the BIPP, which was renamed in 2017 to the PP.[1708] This change was in name only and does not relate to its powers, as it continues to carry on both investigation and prosecution, and its members go back and forth between practicing prosecution and conducting investigations.[1709] The distinctive line that separates investigation from prosecution is found within the practices of the PP, where its members "do not practice investigation and prosecution at the same time for the same case." [1710] Not combining investigation with prosecution by a member of the PP for a specific case is not a separation of power in real terms and may violate the principle of the separation of power, even though the new given name to the institution indicates that it only practices prosecution. Yet, the KSA still vests investigative powers in detectives of the PP because the lawmakers think that "it is more effective"[1711] to vest the two powers in a single authority.

Moreover, even if the KSA were to be successful in its approach of vesting prosecution and investigation in one authority, which is practiced by its detectives and/or prosecutors, the PP combines investigating cybercrime with investigating honour related crimes which demonstrates that there is a lack of priority given to cybercrime. This is concrete proof that the KSA looks at cyberspace as being no different from physical space in terms of the criminal procedure of cybercrime. Moreover, as discussed in the previous Chapter, it has been found that the KSA PF lacks expertise, in terms of institutions and

[1707] Interview with Police Officer PO1
[1708] KSA Royal Decree No. A/240 of 2017
[1709] Interviews with members of Public Prosecution
[1710] *Ibid*
[1711] Interview with Law Professor LP2

operations,[1712] which is especially the case for the investigation of cybercrime. The UK has addressed these issues, and the institutional separation of functions is one reason why it promotes the multidisciplinary approach among its investigative institutions.[1713]

6.5.2 Multidisciplinary approach

The multidisciplinary approach in the UK is recognised by the NCA.

> "Part of the key to good cyber security is a multidisciplinary approach. You need to bring diverse skills and expertise together to try and better understand the threats being faced. What I've seen work really well is when you have Threat Intelligence (TI) professionals and an organisation's Security Operations Centre (SOC) completely joined-up and working in tandem. This is key."[1714]

The multidisciplinary approach differs from the separation of powers principle, because the latter focuses on separating the three main branches of government (legislative, executive, and judicial) from each other.[1715] However, a multidisciplinary approach tends to combine policing (investigation), intelligence, encryption and computing skills in one institution,[1716] such as the UK NCA. Also, it includes multi-agency linkages[1717] in specialist units, including the NCSA, and it is also true of the UK NCA. Yet, it is possible to say that it is not a violation of the principle of the separation of powers because the executive and judicial functions remain distinct and can be made accountable accordingly.[1718] The KSA should take

[1712] See Section 5.6
[1713] Roycroft (2016) 3-19
[1714] CSEurope (2020)
[1715] Roycroft (2016) 3-19
[1716] Ibid 3-19
[1717] *Ibid* 22
[1718] NCA cases still are handled by the CPS and not the NCA itself. The nearest to a breach of the separation of powers is actually the SFO under the Criminal Justice Act 1987, the SFO does investigate and prosecute. See < https://www.sfo.gov.uk/publications/>

into account the UK's experience regarding the multidisciplinary approach in tackling cybercrime procedurally, along with the UK legalistic approach.

6.5.4 Legalistic approach

The UK's legalistic approach towards investigating cybercrime can be considered fairer and more effective than the KSA's because it accomplishes its stipulated objectives, especially in its consideration of human rights issues. The UK's full, fair and effective catalogue of legal powers of investigation can be found especially within the IPA 2016.[1719] Furthermore, further related laws also address the important issue of cybercrime evidence gathering. Evidence gathering involves three main aspects: gathering evidence form people,[1720] places,[1721] and machines.[1722]

The lesson to be learned by the KSA is from the UK laws on gathering evidence from people, places and machines, whether individually or in bulk. Even though the KSA has hardly covered gathering evidence from places and people, it does not cover gathering evidence from machines because it does not legally differentiate between investigating NCC and cybercrime, and because it lacks necessary expertise to gather evidence (cyber evidence) from a machine. Expertise is also an issue when it comes to the accused's right for proper due process, namely, in this case, the right for an attorney.

6.5.4 Enhance the mechanisms to achieve fairness

In the UK, the Legal Aid Sentencing and Punishment of Offenders Act 2012[1723] grants the right for people to access justice. Even though the cost of hiring an attorney is not

[1719] McKay (2017)
[1720] PACE interrogation code of practice code C, E
[1721] PACE powers and Code A
[1722] The most important are RIPA 2000, IPA 2016
[1723] UK Legal Aid Sentencing and Punishment of Offenders Act 2012

affordable to many in the UK,[1724] Legal Aid provides help to those who cannot afford a solicitor by hiring one for them.[1725] Additionally, in the UK, there are a number of regulations about lawyers being specially trained to go to police stations so that they can receive public funding from legal aid.[1726] Also, Code C of PACE specifies that legal aid can be offered where there is detention, treatment and questioning of suspects (not related to terrorism) in police custody.[1727] Moreover, the disclosure regime under the Criminal Procedure and Investigations Act 1996[1728] safeguards mechanisms of fairness within UK law as the defence prepare for challenging detention and evidence, as will be addressed further Chapter 7.

By contrast, as already discussed, although the KSA's law allows for legal aid, hiring a criminal defence lawyer is not a preferred choice.[1729] Nonetheless, in the UK, hiring a lawyer in the initial stages of the criminal process of cybercrime is usually the first choice for all parties involved in the investigation because it helps to guarantee human rights are protected, especially the rights of the accused.[1730] Thus, it is seen as almost mandatory to hire a criminal defence attorney during the first stages of the criminal procedure, including in this case the investigation of cybercrime. Therefore, the KSA should benefit from these ideas. At first it should make hiring a criminal defence attorney mandatory by law for the initial stages of the criminal procedure of all crimes, including cybercrime, and the state should provide more access to assistance by hiring ones for those who cannot afford to pay for a lawyer. Then, society (especially individuals with a prejudice against criminal lawyers or suspects

[1724] Secret Barrister (2020) 164
[1725] *Ibid*
[1726] Police station representatives accreditation scheme <https://www.sra.org.uk/solicitors/accreditation/police-station-representatives-accreditation>
[1727] GOV.UK (2014) <https://www.gov.uk/guidance/duty-solicitors-rotas-information-and-guidance >
[1728] UK Criminal Procedure and Investigations Act 1996
[1729] See Subsection 6.2.2.1 and Subsection 6.3.2.1
[1730] Secret Barrister (2020)

and play the "shame card" against them)[1731] would become more accustomed to it and, consequently, they would stop preventing suspects from being deprived of their right to legal counsel during the initial stages of the criminal procedure of cybercrime.

6.6 Conclusion

It has been repeatedly asserted during this thesis that the KSA does not differentiate between the criminal procedure of cybercrime and NCCs, which is a major reason why it struggles to tackle cybercrime effectively and fairly. Investigation of cybercrime in the KSA is not properly carried out, mainly because of the legal obstacles which then arise within the KSA criminal justice system,[1732] and this is why this chapter suggests learning lessons from a better approach, such as that carried of the UK, which continually produces new laws and updates its existing ones to keep pace with the modern phenomena of cyberspace and its impact.[1733] However, although it still faces certain difficulties as mentioned in this chapter, when comparing them with those of the KSA, the UK's approach has sought positively to achieve effectiveness in all aspects of investigation (especially surveillance) and in respect for basic human rights.[1734]

The KSA is not the only state that struggles with its approach toward investigating cybercrime, as its neighbouring countries also face similar issues.[1735] One common issue between those countries is *Sharia,* which may be seen as ineffective in dealing with modern phenomena.[1736] Therefore, the KSA and its neighbours have a duty to adjust their laws to procedurally tackle cybercrime, especially during the backbone of the criminal procedure of

[1731] See Section 4.5
[1732] Interview with Law Professor LP1
[1733] Saunders (2017) 4-15
[1734] Secret Barrister (2020) 144
[1735] Hakmeh (2018)
[1736] *Ibid*

cybercrime: the investigation. What makes investigation of cybercrime so crucial is that the previous and subsequent stages depend on its success,[1737] and because it involves human rights aspects[1738] which the KSA has broadly failed to protect.[1739]

One finding of this Chapter is that understanding cyberspace helps the investigation of cybercrime to be effective and fair. It is believed that developed countries, including the UK, understand cyberspace and its impact on the criminal justice system better than developing countries, including the KSA, which is one reason why countries such as the UK are able to act effectively and fairly in investigating cybercrime.[1740] This enhanced understanding of cyberspace has led the UK to understand the nature of cybercrime and cyber evidence and distinguish them from NCC and non-cyber evidence.[1741] Consequently, this understanding of the different nature of cybercrime and cyber evidence has led the UK to pass the IPA 2016 and continue to reform it. On the other hand, the KSA does not completely understand this modern phenomena and its impact on investigating cybercrime.[1742] When looking to the KSA CPL 2013, it is no surprise that there is no mention of the investigation of cybercrime or the collection of cyber evidence. The reason why the CPL 2013 does not mention such modern phenomena is that this Law just recognises investigative needs and basic human rights in physical space. Therefore, it is possible to say that the necessary reforms in the KSA have been much slower than those in developed countries including the UK.

Another finding of this chapter is that there is a strong correlation between securing basic human rights and the effectiveness and fairness of the investigation of cybercrime. Investigating cybercrime is no different from investigating NCC when it comes to basic

[1737] Gehl and Plecas (2016) 46
[1738] *Ibid* 11-13
[1739] Gulf Centre for Human Rights (2018)
[1740] McKay (2017) 30
[1741] Walden (2007)
[1742] Interview with Law Professor LP1

human rights because, in both types, human rights must be protected under all circumstances.[1743] Securing basic human rights during the investigation of cybercrime is the first factor that indicates the effectiveness and fairness of the investigation process. This is why it is thought that the UK has a better approach toward investigating cybercrime than the KSA. Issues of due process, especially the right for legal counsel, are expressly considered in the UK,[1744] whereas, in the KSA, this is one main issue which is of great concern in relation to human rights.[1745] Moreover, issues of human rights related to the collection of cyber evidence and surveillance, such as privacy, are given great weight in UK law,[1746] and the government is strictly restricted from plainly violating the human right to privacy.[1747] However, in the KSA, privacy is governed by an old interpretation of *Sharia*[1748] which makes it possible to violate human rights because the gap between *Sharia* (which is 14 centuries old) and the innovations of cyberspace and the related criminal process issues (that are less than half century old) are not properly studied, addressed and implemented within the KSA criminal justice system.

Finally, in accordance with other findings, this Chapter finds that there is a gap between law and practice and the KSA approach regarding the investigation of cybercrime both institutionally and operationally which is mainly due to NCC and cybercrime being treating as if they are the same. This gap is identified when applying the Model Code[1749] as heuristic device to measure what the KSA has done and what is yet to be done to tackle cybercrime both effectively and fairly. Therefore, it is possible to say that the KSA needs more detailed and specialised powers to deal with the investigation of cybercrime on the

[1743] Murray & Klang (2005) 10
[1744] Secret Barrister (2020) 152
[1745] UPR, Saudi Arabia 3rd cycle <https://www.ohchr.org/EN/HRBodies/UPR/Pages/SAindex.aspx>
[1746] McKay (2017) 40
[1747] *Ibid* 41
[1748] Alanazi et al (2018) 10
[1749] See section 4.6

functional level, and it needs specialised trained detectives to deal with investigating cybercrime as well as oversight mechanisms at the institutional level.

Chapter 7

Prosecution and trial of cybercrime in the KSA

7.1 Introduction

This Chapter addresses the prosecution and trial of cybercrime in the KSA. It will analyse the role of the KSA's PP and the CC as parts of the final stages of the criminal procedure of cybercrime. In this exercise, it will explain how to prosecute cybercrime and how to bring a case before the CC. Neither appeal nor punishment will be fully addressed but will be briefly covered when relevant to issues that fit with the aims and objective of this thesis. The legal framework is mainly found under the CPL,[1750] even though this legislation has been enacted by depending on unfamiliar premodern traditions[1751] that are explored when addressing the classes of punishments in Section 7.4 of this chapter. Similar to the approach in the previous Chapters related to policing and investigating cybercrime, this chapter will analyse the prosecution of cybercrime after first outlining the KSA's approach towards prosecuting NCCs. This study is necessary as the KSA, for the most part, does not differentiate between the criminal procedure of cybercrime and NCCs.[1752] Similarly, the role of CCs in the criminal process of crime in general will be outlined in order to ascertain what the KSA's approach toward NCCs is, as the KSA applies it to the criminal process of cybercrime. Moreover, an assessment of the KSA's approach toward prosecution and trial, which constitute the final stages of the criminal procedure, will be conducted as the two aspects are crucial to understanding what is holding the KSA back from tackling cybercrime procedurally.

[1750] CPL 2013. Articles 13 and 15
[1751] Mallat (2020) 3-4
[1752] See Sections 5.1 and 6.1

As in previous two chapters, this Chapter will first analyse prosecution of NCCs and cybercrime from two main standpoints. The first is institutional, and mainly answers the question of who the prosecutors are and in what structures they operate. The second aspect is operational, answering the question of what powers they have and how they function, such as how to present and disclose cyber evidence in CCs. Moreover, this chapter will analyse the role of CCJs in light of the criminal procedure of cybercrime. Similarly, the aspects to be covered in regard to CCs are institutional (who are they and in what structures do they operate?) and operational (what powers do they have?). One main objective of this thesis is to evaluate and analyse the KSA's approach to the criminal procure of cybercrime. To help achieve this aim, this chapter will outline the KSA's approach to the prosecution and trial stages of the criminal process, and will also address what features, or lack of them, are holding back the KSA from tackling cybercrime from a procedural perspective, and whether the KSA's current approach is fair and effective. Thus, this chapter will firstly investigate the KSA's approach and subsequently test its fairness and effectiveness. Moreover, it will discuss whether distinct processes and laws should be adopted for cybercrimes.

The standards of fairness and effectiveness are addressed in Chapter 2 as main instruments of analysis[1753] upon which to base the tests for conceptual, comparative, international and national standards of both fairness and effectiveness. As discussed in Chapter 2, the KSA's legal system is a mixture of inquisitorial and adversarial systems but is dominated by a unique system inspired by *Sharia.*[1754] Thus, the CCs in the KSA have similar powers to the PP, such as investigation, which in itself is a power vested in the PP rather than the PF.[1755] This feature may negatively impact on the fairness and effectiveness of both the

[1753] See Section 2.4
[1754] See Section 2.3
[1755] Investigation has been transferred from the PF to the PP after the CPL 2001 was passed. See Section.5.2.3

PP and CCs, as will be addressed throughout the Chapter as an objective of this thesis to test fairness and effectiveness of the KSA's approach to the criminal procedure of cybercrime.

It is crucial to this Chapter to explain at the outset the meaning of the key terms "prosecution" and "trial". First, prosecution includes the idea that the defence of the public interest must be done with integrity.[1756] In the UK, prosecutors are required to act with integrity on behalf of the public based on the idea that they are "minsters of justice."[1757] The word "minister" here refers not the executive function of a public servant but rather to the authority which the prosecutors have over public interest to prove someone's guilt before the court.[1758] Lord Devlin was able, in 1958, to declare that, unlike earlier in the century, it was "now well established" that the prosecution lawyer should "act as a minister of justice rather than as an advocate, he is not to press for a conviction but is to lay all the facts, those that tell for the prisoner as well as those that tell against him, before the jury."[1759] The discussion here is related to the UK and not the KSA, but it might be relevant to the KSA on the ground that prosecutors in the KSA seek to pursue the public interests even though, in the KSA, they have a lesser role in the criminal procedure, as will be discussed in Section 7.2. Therefore, the meaning of prosecution which the UK adapts might be as follows:

> "Prosecution is about filtering out cases that should not go to court. That requires rules and guidelines to decide how cases should be processed once they have reached the stage of prosecution. Arrangements will often involve a certain level of discretion on behalf of the prosecuting authority."[1760]

Therefore, it is possible to say that prosecution is the process where prosecutors can build a criminal case against a suspect and present it to a level that meets the required burden

[1756] Plater (2011) 9
[1757] *Ibid* 9
[1758] *Ibid* 21-24
[1759] Devlin (1958) 27
[1760] Pakes (2019) 98

of proof in a way that complies with evidential and procedural requirements before the courts.[1761] In the UK, this gives rise to issues of admissibility, disclosure, the ways in which the public interest might be articulated, accountability and oversight,[1762] which will be covered when addressing prosecution in the KSA during this chapter[1763] with respect to the purpose of policy transfer.

When it comes to the prosecution of cybercrime, the task becomes more complicated because prosecutors should be equipped with knowledge, equipment and expert assistance to deal with the technological changes[1764] that might affect certain types of complex cybercrimes, such as financial scams.[1765] However, it is possible to say that prosecution in the KSA means the public authority which is represented by public officers who function as public officers to represent the public interest before the criminal courts, by presenting the criminal case before the Court and trying to persuade the Court of the guilt of the accused.[1766] This meaning of prosecution adopted by the UK, and the Crown Prosecution Service (CPS)[1767] refers to the independent public authority that carries out this meaning of prosecution in England and Wales.[1768] Moreover, the UK law declares the standard of proof that prosecution should prove as guilt beyond reasonable doubt.[1769] However, this meaning of prosecution is not fully adopted by the KSA criminal justice system because there are no clear standards of proof within the KSA law which will be addressed in Section 7.5.

Second, "trial" broadly means the processes of examining the evidence which has been found to be admissible within the justice system and passing judicial judgments

[1761] Campbell (2019) 196
[1762] In the UK Her Majesty's Crown Prosecution Service Inspectorate inspects and assesses the CPS work. See <https://www.justiceinspectorates.gov.uk/hmcpsi/>
[1763] See Subsection 7.2.2.3
[1764] Grabosky (2007b) 201-223
[1765] Sundaresh and Siew (2012) 243-256
[1766] Alqahtani (2017b) 14
[1767] UK CPS
[1768] The Code for Crown Prosecutors 2.1 <https://www.cps.gov.uk/publication/code-crown-prosecutors>
[1769] *Woolmington v DPP* [1935] UKHL 1

accordingly.[1770] In the KSA, the admissibility of evidence is mainly determined by the CCJs, and they can decide what is admissible,[1771] as the BLG makes it clear that judges are only bound by the broad concepts of *Sharia*[1772] (and not the highly detailed and technical evidential law as in England and Wales) as will be addressed in Section 7.5. However, a promising proposal was announced by the KSA Crown Prince at the beginning of 2021 which suggests that the legal system would be reformed in accordance to the KSA *Vision 2030*, including aspects of the criminal legal system, such as the criminal procedure and the codification of *Sharia*.[1773] Although the proposal lacks certainty, it might be considered promising as it suggests moving toward fairness.[1774] Nevertheless, the proposal did not provide details and only introduces the big picture. This proposal would imply that the KSA's current approach on the criminal process of crimes, including cybercrime, is in need for reform.[1775]

This Chapter will discuss the addressed issues at the final stage of the criminal procedure of crime which is carried out by CCJs to determine whether the accused is guilty and sentencing, if they are proven guilty after examining the evidence brought against them by prosecutors.[1776] The reliability, admissibility and disclosure of cyber evidence seem to be imperfect in late modern countries such as the UK,[1777] and problems are tackled even less assuredly in pre-modern countries such as the KSA.[1778] For example, in English law, there was the technical rule in PACE s.69[1779] which stated that evidence from computer records shall be inadmissible unless conditions relating to the proper use and operation of the

[1770] Campbell (2019) 345
[1771] CPL Articles 189, 190, and 191
[1772] BLG Article 46
[1773] Naar (2021)
[1774] *Ibid*
[1775] Rashad (2021)
[1776] CPL 2013 Articles 189, 190, and 191
[1777] Casey (2002)
[1778] Alfaize (2015) 148-149
[1779] PACE s.69

computer are shown to be satisfied.[1780] This was repealed by the Youth Justice and Criminal Evidence Act 1999, s.60.[1781] The change in 1999 followed the report of the Law Commission, *Evidence In Criminal Proceedings: Hearsay And Related Topics*.[1782] It was viewed as an impossibly tough standard.[1783] There remains a common law presumption of the proper functioning of mechanical devices.[1784] Thus, distrust of technological evidence was reflected in English law for a time, but this has been reconsidered. The problem in the KSA is not only that distrust remains but that the position is often left unclear.[1785]

Furthermore, as well as meeting their own burden and standards of proof, the prosecutor (and the judge) has to be fair to the defence by allowing disclosure of evidence.[1786] As the prosecution in the KSA sometimes fails to present the suspect with the cyber evidence against them,[1787] it is suggested that the court should enable suspects to access digital materials by way of discovery, so that the fairness of the criminal procedure would not be undermined.[1788] This will allow opportunities at trial to put forward rebuttals and new evidence, such as problems with computing devices or other defences.[1789] This is the case in the UK, but not in the KSA as will be addressed in Sections 7.2 and 7.3.

The Chapter will study the CPL 2013 along with other related doctrinal legal data. Then, an examination of both effectiveness and fairness of the KSA response to prosecution and trial of crimes and cybercrime, will be conducted in order to meet the research objectives

[1780] Consultation Paper (1995) 200-207 <https://www.lawcom.gov.uk/project/evidence-in-criminal-procedings-hearsay/#evidence-in-criminal-procedings-hearsay-report>.
[1781] Youth Justice and Criminal Evidence Act 1999, s.60
[1782] Report of the Law Commission (1997) Chapter 13 <https://s3-eu-west-2.amazonaws.com/lawcom-prod-storage-11jsxou24uy7q/uploads/2015/03/lc245_Legislating_the_Criminal_Code_Evidence_in_Criminal_Proceedings.pdf >
[1783] Ladkin et al (2020) 1-14
[1784] Mason (2017)
[1785] Alobaidi F (2020)
[1786] Yaroshevsky (2011) 1322
[1787] Interview with Criminal Defence Lawyer CL3
[1788] Turner (2019) 310-311
[1789] Yaroshevsky (2011) 1322

regrading identifying what is holding the KSA back from combating cybercrime in a procedural sense. Also, to meet the research objectives, this chapter will reference the UK jurisdiction and how it responds to prosecuting and trying cybercrime in order to learn lessons from the country's approach to cybercrime in a procedural sense where the procedure is shown to be better than that of the KSA, especially when it comes to the handling of cyber evidence and the disclosure of such evidence. In cases involving multiple jurisdictions, international cooperation is needed to tackle cybercrime procedurally, especially in terms of the prosecution and trial of cybercrime. Higher standards of fairness in national laws are likely to make international cooperation more feasible. However, this will not be addressed in this chapter, nor will it be addressed in this thesis due to its primarily domestic law focus and restrictions as to words and time allotted for conducting this thesis. Additionally, when collecting data from interviews, most interviewees had little to say about international cooperation which suggests that primary data related to it is not readily available at present.

7.2 Prosecution of NCCs in the KSA

In this section, the role of the PP will be analysed in light of the prosecution of NCCs in accordance with the CPL 2013.[1790] It is necessary to look at NCCs first rather than cybercrimes because the KSA does not differentiate between the NCCs and cybercrime procedurally.[1791] Relevant institutions and powers are the main focus of this section in regard to prosecuting crime in general. In terms of institutions, this section will introduce the public entities which prosecute NCCs. Also, it will cover how well trained and competent the prosecutors are. Moreover, in terms of operations, this section will address the prosecutorial powers which are allowed to them by the CPL 2013. As addressed in Chapter 2, the KSA

[1790] Shareef (2016) 61
[1791] See Section 2.2

tends towards inquisitorial features which involve the judicial branch in the investigation process.[1792] Therefore, the gathering of evidence of NCCs at both institutional and operational levels will be addressed in order to apply the findings to cybercrimes in the next section.

7.2.1 Prosecuting NCCs in the KSA: Institutional aspects

Before the issuance of the first CPL 2001, prosecution in the KSA was recognised in the PPL (previously the BIPPL),[1793] and, ever since, prosecutors have been referred to as "members" of the PP (previously the BIPP).[1794] After the issuance of the 1989 Law, prosecutors were assigned to PF stations[1795] until 1995[1796] because they are linked to investigation,[1797] and investigation was one function of the PF in the KSA before 2001.[1798] Older PF officers who used to investigate crimes before 2001 see prosecutors as "employees who deliver papers to the court."[1799] Although a great deal of time has since passed and prosecutors moved to the new established BIPP in 1995 and have been practicing prosecutorial functions from 2001,[1800] it seems that prosecutors have not been important members of the PP.

According to the CPL 2013, the PP is the core institution that prosecutes crimes. Article 13 states:

[1792] *Ibid* section 2.3
[1793] The name PPL has replaced the previous name BIPPL in 2017 mainly because the whole institution has been recognized as a judicial institution rather than executive institution which the name PP suits more; however, the change was only in the name not in the powers or the legislation related. See Subsections 4.2.4
[1794] KSA Royal Decree No (A/240) 2017
[1795] Interview Police Officer PO2
[1796] Aldosari (2019) 10
[1797] Shareef (2016) 61-62
[1798] Aldosari (2019) 66
[1799] Interview with PO1
[1800] Aldosari (2019) 10.

> "The Bureau of Investigation and Public Prosecution [Public Prosecution now] shall conduct its investigation and public prosecution in accordance with its Law and Implementing Regulations."[1801]

Similarly, Article 15 says:

> "Pursuant to its Law, the Bureau of Investigation and Public Prosecution [now the Public Prosecution] shall have jurisdiction to initiate and pursue criminal actions before competent courts." [1802]

The two Articles indicate that, along with its main function as an investigatory institution, the PP also functions as a prosecutorial institution.[1803]

It might be argued that the PP's main function is prosecutorial as the name of the institution implies.[1804] However, "prosecution" should more accurately be considered as a function that is secondary to investigation, which is the main function of the institution due to the investigatory and prosecutorial powers that detectives possess,[1805] as will be discussed in the next subsection about operations. Even though the name of the institution has been changed from the BIPP to the PP in 2017,[1806] numerous related laws (meaning the CPL 2013 and its CPLER 2015 and criminal legislation passed before 2017)[1807] have not been updated to refer to the BIPP as the PP. It can be said that the KSA has no intention to completely separate investigation from prosecution in the near future,[1808] even though it seeks a fairer approach.[1809]

[1801] CPL 2013 Article 13
[1802] *Ibid* Article 15
[1803] PPL Article 3 Para C
[1804] Interview with CL1
[1805] Interview with D1
[1806] Based on Royal Decree No (240/ A) 2017
[1807] See Subsection 4.2.3
[1808] The proposal made by the Crown Prince of the KSA MBS does not include separating investigation from prosecution. See Rashad (2021)
[1809] Aldosari (2019) 246-247.

As discussed in Chapter 6 (Section 6.6), separating PP from the investigation function in general is likely to result in fairer outcomes when it comes to the right of the accused not to be abused by the extensive powers that the PP possesses.[1810] It might be argued that the dangers of combining investigation and prosecution can be explained as follows. First, it is one less independent check at a crucial point where the suspect faces court (or not).[1811] Second, it is less rigid in terms of allowing official narratives to be sustained at a time when not all facts are known.[1812] In comparison, the UK police idea of investigative interviewing[1813] seeks to move away from the more rigid idea of always obtaining a confession and conviction,[1814] thereby reflecting a fairer approach. The investigative interviewing approach was adopted by the police in England and Wales in the 1980s after a series of miscarriages of justice causes by the investigators methods to get confessions at all costs.[1815] After adopting this model, more ethical and professional interviews have been conducted, stronger defensible investigation conclusions have been reached,[1816] and stakeholder confidence in the ability of the investigative authority has increased.[1817]

Aldosari notes that "whenever there is a separation of investigation and prosecution procedures, there will be increased likelihood of fairness to an accused."[1818] It is been declared by the KSA that the reason for considering the PP as a judicial authority is to increase the likelihood of fair legal procedures.[1819] Although the PP is considered in the KSA as a judicial authority,[1820] it might not function as one because members of the PP practice

[1810] See Section 6.6
[1811] Aldosari (2019) 217-222
[1812] *Ibid*
[1813] College of Policing, 'Investigative Interviewing' <https://www.app.college.police.uk/app-content/investigations/investigative-interviewing/>
[1814] Williamson (2006)
[1815] *Ibid*
[1816] Clarke and Milne (2011)
[1817] Poyser and Milne (2015) 265-280
[1818] Aldosari (2019) 10 and 222
[1819] Royal Decree No (240/ A) 2017
[1820] PPL Article 1

executive powers rather than judicial powers, as will be explained in the next subsection. Moreover, it may be crucial to consider that, within the KSA, PP officers – whether they are prosecutors or detectives – are referred to in the PPL as "members of the PP."[1821]

This indicates that "members" of the PP have dual functions: as detectives and as prosecutors.[1822] Referring to them as "members" means that one PP officer can be either a detective or a prosecutor.[1823] Therefore, detectives might function as prosecutors and vice versa,[1824] and all it takes for this dual functions to be actualised is an order, written or verbal, from the Public Prosecutor (the head of the PP), or his subordinates (heads of investigation circuits).[1825] Moreover, despite the PP's name, "members" receive the same training outlined in the previous chapter[1826] and have no specialised training related to prosecution.[1827] As a result, it is possible to say that the dominant function of the KSA's PP is investigation and not prosecution,[1828] even though the name of the institution suggests otherwise. This dual function can be seen throughout the CPL 2013, for example, by Article 65:

> "During investigation, the accused may seek the assistance of an agent or a lawyer. The investigator shall investigate major crimes as provided for in this Law. He may also investigate other crimes if the circumstances or gravity of the case so require or may file a lawsuit to summon the accused to appear in person before the competent court."[1829]

This Article clearly indicates the dual functions of detectives by allowing them to "file a lawsuit" or, in other words, to prosecute.[1830] This indicates that "members" of the PP are two

[1821] *Ibid* Article 2 and beyond
[1822] Interviews with Criminal Defence Lawyers CL1, CL2
[1823] *Ibid*
[1824] Interview with Detective of the PP D1
[1825] Interview with Public Prosecutor PP1
[1826] See Chapter 6 section 6.4
[1827] Interviews with Detectives of the PP D1 and D2 and Public Prosecutor PP1
[1828] Interview with Criminal Defence Lawyers CL1 and CL2
[1829] CPL Article 65
[1830] *Ibid*

sides of the same coin. Moreover, the number of PP "members" who function as Prosecutors appears to be significantly less than the PP "members" who function as detectives.[1831] This might suggest that the KSA pays more attention to investigation than prosecution despite the name of the institution emphasising prosecution.[1832] Moreover, the function of prosecutor is mentioned throughout the CPL 2013 in multiple Articles, which means that there is recognition of the prosecutor's function within the KSA's law. Yet, it is posited that it is a "pseudo-function",[1833] which indicates that it is not highly respected as a function in the KSA, as will be proposed in the discussion of their powers. However, neither of the main laws related to PP, the CPL 2013 and the PPL, explicates who those prosecutors are in precise terms. For instance, the PPL recognises the hierarchical job names within the PP, but only refers to detective ranks, especially in the first stages, and the prosecutor of appeal not the prosecutors in the first stages.

In its latest update in 2017, Article 9 of the PPL says:

"1 - The names of the positions of the members of the Commission shall be as follows:

Attendant Investigator

Investigator [detective] (C).

Investigator [detective] (B).

Investigator [detective] (A).

Deputy Head of an Investigation and Prosecution Circuit (B).

Deputy Head of an Investigation and Prosecution Circuit (A).

Head of Investigation and Prosecution Circuit (B).

Head of Investigation and Prosecution Circuit (A).

[1831] There are no official statistics, but form data analysed from the interviews with all PP members, the institution is dominated by investigation function.
[1832] CPL Article 65
[1833] Interview with CL1

Prosecutor of appeal.

Head of investigation and prosecution departments." [1834]

This Article proves again that dual functions are held by detectives, and more importantly, it proves that investigation is the dominant function of the PP. "Appeal" here refers to the second stage of trial (appeal), and it might be understood that the "prosecutor of appeal" is the PP "member" whose job is only to prosecute at the appeal stage.[1835] However, members of the PP say that this name is only a rank not a real function, and its purpose is to be an equivalent to the function of Judges of Appeal (JA) in relation to salaries and status, but not functions, and most of those who named prosecutors of appeal are detectives not prosecutors.[1836] Therefore, it might be asked how the prosecution of appeal comes to function without recognition for prosecutors in the first stage of trial. In other words, who are the prosecutors during the initial stages of trials? The answer to this question, the PP interviewed members say, it is "detectives."[1837]

In Chapter 5, it is noted that the KSA transitioned toward a fairer approach when separating investigation and prosecution from the PF when the older CPL was passed in 2001.[1838] However, it is possible to say that the KSA stopped making such substantial leaps toward making the criminal procedure fairer after that year, because it seems to care more about the effectiveness of investigation with a view to prosecution.[1839] In the next subsection, the impact of the dominance of investigation in a prosecutorial institution will be discussed in regard to operations and the powers that prosecutors can exercise.

[1834] PPL Article 9
[1835] Interview with CL1.
[1836] Interviews with members of the PP D1, D2, D3, PP1, PP2 and PP3
[1837] Interviews with members of the PP D1, D2, D3, PP1, PP2 and PP3
[1838] See Section 5.2.3
[1839] The latest proposal made by the Crown Prince of the KSA MBS does not include prosecution in any sense. See Rashad (2021)

7.2.2 Prosecuting NCCs in the KSA: Operational aspects

As well as addressing the institution involved in prosecuting crimes within the KSA in the previous subsection, it is also crucial to address how its officers operate. According to the CPL 2013:

> "If the Bureau of Investigation and Public Prosecution [now the Public Prosecution], upon completion of the investigation, finds that there is sufficient evidence against the accused, the case shall be referred to the competent court, and summons shall be served to the accused to appear before it. The case shall be filed by means of an indictment including the following details…"[1840]

This Article suggests that the indictment should be written by detectives not prosecutors.[1841] However, it does not make explicit that suggestion, so one might still argue that writing an indictment should be recognised as a prosecutorial rather than investigatory power.[1842] Nonetheless, Article 24 of the CPL 2013 says that:

> "Preliminary criminal investigation officers shall be in charge of pursuing offenders and collecting information and evidence necessary for investigation and indictment."[1843]

PCIOs includes PF officers and members of the PP as well, as stated in Article 26 of the CPL 2013,[1844] which is confusing because PF officers can only conduct the initial investigation and not the preliminary investigation,[1845] and they do not write indictments because it is the job of the PP, as will be discussed later in the following subsections. Therefore, it is possible to say that what is meant in Article 24 is that the officers who should

[1840] CPL 2013 Article 126
[1841] *Ibid*
[1842] Interview with Law Professors L1 and L3
[1843] CPL 2013, Article 24
[1844] *Ibid.* Article 26
[1845] See Section 5.2

write indictments are the "members" of the PP, and not all are categorised as PCIOs.[1846] Thus, the question arises here of the identity of the PP "members" mentioned in Article 26 who can write indictments in accordance with Article 24. As discussed in the previous section, the use of the label "members" of the PP mainly refers to detectives rather than prosecutors, which is the implied meaning here as well. Indeed, when interviewing PP members, all of them asserted that detectives and not the prosecutor write indictments in practice, and prosecutors edit the indictments to imply that they write it.[1847] Therefore, the other question that arises here is what major powers other "members" of PP have regarding their functions as prosecutors. According to CLP 2013:

> "In crimes specified in the regulations of this Law, the prosecutor must attend court sessions related to public right, and the court shall hear his statements and decide thereon."[1848]

The Article does not specify any prosecutorial power and simply obligates prosecutors to attend the CC. Therefore, it is mandatory by law for the prosecutor to attend the CC, and the latter should hear them. As the CPL 2013 puts such a limited obligation on prosecutors, it would seem reasonable to at least mention their major obligations in detail. Since the CPL 2013 fails to do so, this omission would seem to indicate that detectives do most of the PP's jobs, except for attending court sessions.[1849] In interviews, D1 stated that "prosecutors are the secretaries of the Public Prosecution."[1850] This assertion is perhaps no surprise because detectives do all the work before the trial. Moreover, PP1 seems to agree with D1 on this point, saying that his job as a prosecutor "is not much of a headache".[1851] It might be said that a main reason why prosecution in KSA "is not much of a headache" is that the

[1846] Interview with Detective of the PP D1
[1847] Interviews with all 6 members of the PP
[1848] CPL 2013, Article 156
[1849] Interview with Criminal Defence Lawyer CL1
[1850] Interview with Detective of the PP D1
[1851] Interview with Public Prosecutor PP1

prosecutorial powers are not very substantial in the KSA. The CPL 2013 cautiously identifies some prosecutorial operational powers along with their obligation to "attend the court sessions." Moreover, the data collected from the fieldwork of this thesis identifies some other prosecutorial operational powers which might be considered as powers in some sense, and whether they are being collected from the data of the fieldwork or found within the CLP 2013. They can be vested with the following functions: presenting criminal cases before the CC, defending criminal cases before the CC, appealing or petitioning judgment on a criminal case before higher courts and disclosing evidence. These functions will now be considered in greater depth in relation to their operational consequences.

7.2.2.1 Presenting the criminal case before the CC

It seems logical to assume that the main reason why the CPL 2013 says in Article 156 that PPs must attend the court session[1852] is to present the case file, or dossier,[1853] before the CC. This dossier begins with the PF's report and ends with the detective's indictment.[1854] Moreover, it is possible to say that the CPL 2013 allows prosecutors to amend the indictment before such presentation. Article 159 of the CPL 2013 says:

> "Unless deliberations are closed, the court may, at any time, permit the prosecutor to amend the indictment, and shall notify the accused of such amendment and afford him ample opportunity to prepare his defence regarding such amendment, in accordance with the law."[1855]

The CPL 2013 gives the prosecutors the opportunity to present their cases and amend them when suitable under the following conditions: that the deliberation period is not finally closed

[1852] CPL 2013 Article 156
[1853] See Subsection 5.2.2.1
[1854] Interviews with Police Officer PO1 and Detective of the PP D1
[1855] CPL 2013 Article 159

"before trial begins"[1856] and that the accused is notified of such amendments.[1857] Moreover, as explained in the previous subsection, indictments are written by detectives not prosecutors as the collected fieldwork data indicates. However, Article 159 says that amendments on indictment should be made by prosecutors, who know less about the case than the detectives. Hence, giving the prosecutors the opportunity to amend the indictment might be an indication within the CPL 2013 that indictments should in fact be written by the prosecutor in the first place as a main part of their function as public defenders. However, in practice, detectives write such indictments, which, in light of the above, might be considered as overstepping into prosecutorial powers. However, prosecutors do contact detectives when such amendments are required by the CC,[1858] and sometimes detectives contact the prosecutor to ask the CC for permission to make amendments.[1859] Moreover, prosecutors say that when trial begins, they should read the indictment before the CCJs.[1860] This reading of the indictment by prosecutors before the CC hearing is not mentioned in the CPL 2013, which further indicates that prosecutors reading the indictment is, at most, good practice and not a prosecutorial power or duty.

7.2.2.2 Defending the criminal case before the CC

It would appear that prosecutors know enough about criminal cases to practice advocacy before the CC. Indeed, part of their training in the Academy[1861] includes the study of criminal law and criminal procedure,[1862] which gives them a general legal understanding. However, most of the information related to the criminal cases which they defend before the

[1856] Interview with Public Prosecutor PP1
[1857] CPL 2013, Article 159
[1858] Interviews with Public Prosecutors PP1 and PP2
[1859] Interview with Detective of the PP D1
[1860] Interviews with Public Prosecutors PP1, PP2, PP3 and D1
[1861] See Subsection 5.3.1.3
[1862] Interviews with all 6 members of the PP

CC is given to them by their colleagues (detectives).[1863] Therefore, it seems that they represent detectives rather than the public, which should be their main concern, and they are no different in this profile than private criminal defence lawyers,[1864] any other representative or the accused themselves which contradicts the ideal discussed in Section 7.1 about the public prosecutors being "ministers of justice". This may seem to be a hollow accusation because, as already discussed, the PP is intended to represent the public and, as members of the PP, the prosecutors' main role is to represent the public[1865] and not act as detectives. However, the prosecutors do almost nothing prior to the criminal case being filed by detectives before the CC, again similar to private criminal defence lawyers who mostly are hired by the accused after the criminal case is filed against them by detectives.

Therefore, it is possible to say that they should at least defend the interest of the public by pursuing their brief.[1866] However, their presence is not always beneficial to the case because they "have nothing to lose",[1867] especially compared to criminal defence lawyers who pursue their client's best interest and can be expected to do so due to various factors such as the receipt of fees from the accused and the need to maintain their professional reputation.[1868] Neither of these two factors applies to the prosecution, unless, exceptionally, they are related to the individual's ambitions.[1869] On the one hand, in England and Wales, professional reputation is surely still at stake, but seems to relate more to issues of standards of casework quality [1870] and national advocacy [1871] and accountability through the CPS Inspectorate.[1872] There is also accountability for solicitors and barristers through

[1863] *Ibid*
[1864] Interview with Criminal Defence Lawyer CL3
[1865] Alqahtani (2017b) 13-14
[1866] Interview with Criminal Defence Lawyer CL3
[1867] *Ibid*
[1868] *Ibid*
[1869] Interview with Criminal Defence Lawyer CL1
[1870] UK CPS <https://www.cps.gov.uk/publication/casework-quality-standards>
[1871] UK CPS (2008a) <https://www.cps.gov.uk/legal-guidance/advocacy-national-standards>
[1872] Glidewell (1998) Para 61-63

professional bodies such as Solicitors Regulatory Authority,[1873] Solicitors Disciplinary Tribunal[1874] and Bar Standards Board.[1875] On the other hand, the KSA lacks such guidelines or oversight, which indicates that almost nothing would happen if the prosecutor's work was of a low standard. Moreover, there are no equivalent institutions in the KSA to those of the UK for disciplining private lawyers in public prosecutions.

Therefore it is possible to say that, if the PP hired private criminal defence lawyers to do the job of prosecutors they might do a better job because they are more motivated than the prosecutor, and all they need is a brief from detectives about the criminal case.[1876] This criticism is supported by the findings from the interviews with PP members, who seem confused about their role in prosecution.[1877] Detectives all agree that they do the entire job,[1878] and so make comments such as: "their Excellencies [referring here to prosecutors] do nothing."[1879]

CL1, who was a former detective of the PP, said: "I always rejected the head of department's request to be a prosecutor."[1880] His reason for rejecting such a "comfy job"[1881] is because he wanted to "get more experience"[1882] before reaching the early retirement period allowed for public servants[1883] and then, after applying for early retirement, obtaining an attorney licence to work in the private sector.[1884] It is possible to say that there are two implied assumptions in this context. The first is that working as a prosecutor would not

[1873] Solicitors Regulatory Authority <https://www.sra.org.uk/>
[1874] Solicitors Disciplinary Tribunal <https://www.solicitorstribunal.org.uk>
[1875] Bar Standards Board <https://www.barstandardsboard.org.uk/>
[1876] Interview with Criminal Defence Lawyer CL1
[1877] Interviews with Public Prosecutors PP1, PP2 and PP3
[1878] Interviews with Detectives of the PP D1, D2 and D3
[1879] Interview with Detective of the PP D3
[1880] Interview with Criminal Defence Lawyer CL1
[1881] *Ibid*
[1882] *Ibid*
[1883] 10 years of serving officially in public domains in the KSA qualifies for early retirement according to Public Service Law 1976.
[1884] According to Advocacy Law 2001 in the KSA, three years of serving officially in public domains related to legal expertise [the PP included] allows for lawyering licence under the condition that public servant would be released consensually and officially from their legal duties [not fired or sentenced of a crime]. See AL Articles 3 and 4

provide much experience to PP members, so they prefer to work as detectives because they have the ambition of being private criminal defence attorneys, mainly for "the money."[1885] The second possible assumption is that prosecutor powers in the courtroom are not vastly different from private criminal defence lawyers, but that the latter pays more.[1886] This leads to a further factor which is having independence and being self-employed. Unlike, prosecutors, private defence lawyers are independent from the PP and mostly self-employed which gives them more motivation to do well in their advocacy.[1887] This motivation might be based on their independent status as well as economic interests.[1888] Therefore, it is possible to say that when private criminal defence lawyers represent the accused, they would be more motivated to win cases than prosecutors who have less motivation and are also less knowledgeable about the case. However, many prosecutors would use their power of appealing or petitioning before the Courts of Appeal (CA)[1889] when opposing the initial judgment made by first instance CC judges, especially when their opponent is a former colleague of theirs,[1890] which motivates them to prove their worth.

7.2.2.3 Appealing or petitioning a judgment in a criminal case before higher CCs

Besides the obligation of attending court sessions, appealing or petitioning the judgment in a criminal case before higher CCs are the second most apparent operations that could constitute a prosecutorial power, as mentioned within the CPL 2013. Article 192 of the CPL 2013 states:

> "The convicted person, prosecutor or claimant of private right shall be entitled to appeal or petition review of judgments rendered by the courts of

[1885] Interview with Criminal Defence Lawyer CL1
[1886] *Ibid*
[1887] *Ibid*
[1888] Bessis (2019) 188-211
[1889] See Section 7.4
[1890] Interview with Criminal Defence Lawyer CL1

first instance during the statutory period. The court rendering the judgment shall notify said parties of such right upon pronouncing the judgment."[1891]

This Article entitles the prosecutors to appeal or petition the CCJ's judgments before the CA under the condition that such a power should be invoked no later than the statutory period, which is 30 days after the day the judgment was passed. Article 194 says:

> "Petition for appeal or review shall be made within thirty days. If the appellant fails to submit his petition within said period, his right for appeal or review shall be deemed forfeited..."[1892]

The appeal or petition is not a power as such, but is a right because it could be invoked by either the prosecutor (a claimant for a public right) or other parties involved in the criminal case, such as the accused and an effected third party who claims a private right.[1893] In practice, it has been observed by CCJs that the accused use this right of petitioning or appealing more often than prosecutors, who most of the time agree with the CC judgments.[1894] Therefore, it might be asked why prosecutors do not invoke this right of appeal.

One possible answer is that prosecutors are well trained and very knowledgeable about the law, so they know whether justice is served.[1895] Therefore, one reason that prosecutors do not invoke the right of petitioning or appealing CC judgments may be because they believe that judges have correctly served justice.[1896] However, as prosecutors have received less training and are less knowledgeable than other PP members about the law,[1897] the assertion that they agree so often with the CC judgments because they are legally

[1891] CPL 2013 Article 192
[1892] CPL 2013, Article 194
[1893] *Ibid*
[1894] Interviews with CCJs CJ1 and CJ2
[1895] Interviews with Public Prosecutors PP2
[1896] *Ibid*
[1897] Interview with detective of the PP D3

knowledgeable and well trained might be doubted. Therefore, it is possible that prosecutors might also take preference to a negative action (i.e. not appealing) because the CCJs are more powerful, and they can reinvestigate the criminal case with similar but final investigatory powers of those of the PP and discard their claims[1898] as well be discussed in Subsection 7.4.2. Perhaps a prosecutor's appeal or petition would not be as welcomed as the CPL 2013 suggests. Moreover, unlike the accused or claimants of private rights, prosecutors have almost nothing to lose if they do not appeal or petition the CC judgments, and for that they might not be trusted with such public duty. One exception is that, in serious crimes which involve serious punishments, the CC judgments should be appealed before the CA, as required by Article 194 of the CPL 2013:

> "…judgments of death, stoning, amputation, or qisas in cases requiring capital punishment or less shall be submitted to the court of appeals for review, even if none of the parties so requests."[1899]

It might be inferred that prosecutors are not to be trusted with the public duty of defending the public interests by petitioning or appealing the CC judgments, and that might be why this Article insists on action to test the delivery of justice in the direst circumstances.[1900]

In an interview with CL1, he implies that if the prosecutors were to be trusted with such a heavy burden, such a provision would not be needed, but this legislation originated from the people (legislative branch) who know the people (prosecutors).[1901] Nonetheless, neither this Article nor any other Articles within the KSA law say who should appeal the CC judgments that involve serious crimes and serious punishments, so the question that arises here is who should appeal the CC judgments. The logical answer would be the prosecutors

[1898] Interviews with CCJs CJ1, CJ2 and Detective of the PP D1
[1899] CPL 2013 Article 194
[1900] There are no official statistics about appeals or how many fall in this Article 194 category. According to the Law in the KSA, every case that allows the death penalty must be heard before Court of Appeal. See CPL 2013 Art.195
[1901] Interview with Criminal Defence Lawyer CL1

because it lies within their functions as public defenders, but they do not do it. It is the electronic justice services platform (*Najiz*)[1902] that automatically transfers serious criminal cases to the CA[1903] or, in legal terms, appeals them before the CA in service of the public interests. Therefore, a machine that is not trained as a prosecutor does the prosecutor's job in this matter, which implies that the KSA trusts a machine more than it trusts prosecutors to ensure the proper operation of criminal justice. It might be argued that Article 194 is mandatory, so the prosecutor has no discretion in this case anyway. Article 194 talks directly to prosecutors as their job is to appeal, despite what falls under Article 194, and that would be apparent from the word "submit" in the Article. Moreover, before *Najiz* was released in 2019, prosecutors used to appeal in accordance with Article 194,[1904] which indicates that an electronic platform could partially replace prosecutors, and that would again gain weight to the notion that, given the prosecutor's function in the KSA, it is inappropriate to name the institution after them.

7.2.2.4 Disclosure of evidence.

Lord Bingham observed in *R v H* that:

> "Fairness ordinarily requires that any material held by the prosecution which weakens its case or strengthens that of the defendant, if not relied on as part of its formal case against the defendant, should be disclosed to the defence. Bitter experience has shown that miscarriages of justice may occur

[1902] Najiz is an electronic justice services platform, that was released in April 2019, through which all the Ministry of Justice's electronic services are provided through a unified portal in an effort to increase the satisfaction of the Ministry of Justice's beneficiaries, including citizens, residents and business sectors, and to facilitate users to access and deal with electronic justice services in an easy and fast manner. It includes many electronic justice services, such as court services, agencies, real estate, implementation, and others. See .<https://najiz.moj.gov.sa/Account/Login?ReturnUrl=%2FHome%2FDashboard>

[1903] Interview with Public Prosecutor PP1

[1904] Interview with Criminal Defence Lawyer CL 1

where such material is withheld from disclosure. The golden rule is that full disclosure of such material should be made."[1905]

This "golden rule" of disclosing criminal evidence is followed in the UK and in other common law systems such as that of the US.[1906] In the UK, the rules of disclosure are set out in the Criminal Procedure and Investigations Act 1996.[1907] As Lord Bingham notes, the issue of proof was not to be "resolved by any rule of thumb, but on examination of all the facts and circumstances of the particular provision as applied in a particular case."[1908] Yet, there is no clear equivalent to this fundamental rule of fairness in the KSA approach even though all interviewed detectives say that they discuss "all" evidence with suspects during investigation.[1909]

In the KSA, it is not mandatory that evidence be disclosed at any pre-trial criminal procedure stage, including prosecution. However, it might be argued that an equivalent to this "golden rule" in the KSA might be found in the CPLER 2015 where it states in Article 22 that the accused must know the reason for detention and arrest.[1910] However, Article 22 seems equivalent to the rule in the UK PACE s.28, which is not the same as disclosure of the evidence after charging and during prosecution.[1911]

It should be emphasised that the right of the accused to know the reason for detention (which might be enforced in common law by a writ of *Habeas Corpus*)[1912] is different from disclosing evidence because the first is related to the individual's right to freedom[1913] while the second is related to the individual's right of defending the criminal case built against

[1905] Regina v H *[2004] UKHL 3 at [14]*.
[1906] Brady v Maryland 373 U.S. 83 (1963)
[1907] UK CPS (2008b) <https://www.cps.gov.uk/legal-guidance/disclosure-guide-reasonable-lines-enquiry-and-communications-evidence>
[1908] Regina v H *[2004] UKHL 3 at* [21].
[1909] Interviews with Detectives of the PP D1, D2, D3 and Criminal Defence Lawyer CL1
[1910] CPLER Article 22 Paragraph A
[1911] PACE s.28
[1912] UK GOV (2017) Part 87 <https://www.justice.gov.uk/courts/procedure-rules/civil/rules/part-87-applications-for-writ-of-habeas-corpus>
[1913] Carlson (1969) 1171-1189

them.[1914] However, it is possible to say that in both situations the accused must not be prevented by the authority from knowing why they are being detained so they can challenge detention, and they should be allowed to know the evidence against them in case they would like to challenge that too. Therefore, Article 22 of the CPLER 2015 does not encompass disclosure of evidence as a general procedural right. Even though detectives (not prosecutors)[1915] might disclose evidence during detention or during investigation in some cases, they do not do so because they might be required by law,[1916] but because they think "it is the right thing to do."[1917] Hence, going back to the discussion on morality,[1918] the PP members disclose evidence in some cases because they feel it is fairer than hiding evidence.[1919] However, dependence on the mercy and morality of the PP members is neither effective nor fair. Therefore, the KSA law should draw a line by adopting the golden rule in English law. At present, during trial, the indictment that the detectives draw up should implicitly indicate to the prosecutors details of the evidence that should be disclosed to the accused during the trial as will be discussed in Section 7.4. In England and Wales, the indictment also does not indicate the details of the evidence,[1920] but there are detailed rules for disclosure under the Criminal Procedure and Investigations Act 1996, plus codes and guidance.[1921]

Even though detectives should disclose evidence with the accused before trial at the time of the indictment,[1922] there is no clear legal consequence if they do not as no clear legal provisions in the KSA obligate detectives to disclose evidence. Even though the PPL makes

[1914] *Ibid*
[1915] Interviews with Detectives of the PP D1, D2, D3 and Criminal Defence Lawyer CL1.
[1916] Interview with Detective of the PP D2.
[1917] *Ibid*
[1918] See Subsection 5.2.3
[1919] Interview with Detective of the PP D1
[1920] UK CPS Guidance <https://www.cps.gov.uk/legal-guidance/drafting-indictment>
[1921] See https://www.gov.uk/government/publications/criminal-procedure-and-investigations-act-code-of-practice.
[1922] CPL 2013 Article 101

it possible to discipline members of the PP, it does not clearly specify in which cases they should be disciplined.[1923] Article 16 mentions two general vague cases which call for discipline; committing wrongdoings that are contrary to job duties or the job's requirements.[1924] Moreover, there are two ways to discipline a PP member – either "retirement or blame."[1925] Retirement might be considered as a form of discipline, but blame alone is not a way to discipline public employees. Therefore, due to the lack of adverse consequences, prosecutors may not operate properly, and they lack accountability which might lead to poor standards of prosecution of either NCCs or cybercrimes.

7.3 Prosecuting cybercrime in the KSA

This section will focus specifically on prosecuting cybercrime in the KSA. It will evaluate the KSA's response to prosecuting cybercrime, both operationally and institutionally, using the heuristic device created in Chapter 4 as a main instrument of analysis in order to identify the gaps between what the KSA has put in place and what has yet to be done.[1926] Also, this section will identify the insufficiencies within the KSA's current approach to prosecuting cybercrime. Again, it will focus on the dual powers of investigation and prosecution that the PP has. As mentioned in the introduction of this chapter, the analysis for the prosecution's role in cybercrime cases will follow the same structure as the analysis undertaken in relation to NCCs, covering institutions and operations.

[1923] PPL Articles 15-26
[1924] *Ibid* Article 16
[1925] *Ibid* Article 25
[1926] See Section 4.6

7.3.1 Prosecuting cybercrime in the KSA: Institutional aspects

This subsection has less to add to than Subsection 7.2.1 about the institutional aspects regarding NCCs because no prosecutorial powers are expressed in regard to the main and only response of the KSA regarding prosecution of NCCs. Consequently, it is no wonder that there is no mention of powers in KSA law regarding the prosecution of cybercrime. Therefore, it is only possible to say that prosecutors within the Anti-Honour Crimes Circuit, where the investigation of cybercrime is mainly held,[1927] practice their limited functions of prosecuting cybercrime and NCCs in accordance with what the indictment suggests. "Circuits" here refers to a judicial division, not to the historic meaning found in England and Wales,[1928] which implies geographical regions,[1929] where circuits indicates the six distinct geographical regions which England and Wales are split into for the practice of the courts.[1930] They are the areas around which the High Court judges travel (go out on circuit) that were introduced in 1166 (by legislation known as the Assize of Clarendon). However, the circuits in the KSA mean the specialist departments or divisions within the judicial institutions.

According to the PPL, the PP consists of multiple investigation and prosecution circuits.[1931] Therefore, it is possible to say that prosecutors within the circuits that investigate cybercrimes are the prosecutors of cybercrime, and they operate and practice cybercrime related prosecutorial powers in the same way they would prosecute NCCs.[1932] However, based on interviews held with members of the PP, they agree that prosecution of cybercrime is not limited to one circuit, and that prosecutors within National Security Circuits would prosecute cybercrimes investigated in Anti-Honour Crime Circuits.[1933] This indicates that

[1927] See Subsections 6.3.1 and 4.5.2
[1928] Hurnard (1941) 374-410
[1929] Ibid 374-410
[1930] *Ibid*
[1931] PPL Article 9
[1932] Interviews with all 6 PP members
[1933] *Ibid*

prosecution might be considered as a non-essential procedural process in cybercrime cases for a number of reasons. First, prosecutors are only trained to investigate crimes (including cybercrime) and do not receive training on prosecution during their first year in the Academy.[1934] Second, prosecutors' main expertise and experience are obtained from investigations when they function as detectives not from the PP as discussed in the previous section, and most of the experience obtained is unrelated to cybercrime.[1935] Third, as discussed in the previous section and Chapter 6,[1936] members of the PP who function as detectives and prosecutors must be either *Sharia* diploma holders or law graduates, which would indicate this is the most important qualification to be a member of the PP, with no extra qualification needed, whether that be in regard to cybercrime in particular or NCCs in general. Fourth, as addressed in earlier in Section 7.3, prosecutors are not subject to disciplinary action when they commit a procedural error related to both cybercrime and NCCs, which allows space for committing more errors as a result of a lack of effective supervision. Therefore, it might be possible to say that this organisation seems to lack the required experienced officers to deal with cybercrime from both institutional and operational points of view, as will be discussed in the next subsection.

7.3.2 Prosecuting cybercrime in the KSA: Operational aspects

As discussed before, the prosecutors have no clear powers in KSA law, but they have some assigned operations which can be considered as powers.[1937] However, as discussed in the same sub-section, those operations imply that the prosecutors in the KSA are not trusted even with those operations as suggested by the automatic appeal triggered by the court

[1934] See Subsection 6.4.3.1
[1935] Interviews with all 6 PP members
[1936] See Subsection 6.2.1.1
[1937] See Subsection 7.2.2

computer system for the most serious crimes. Therefore, it can be said that the prosecution of cybercrime is no different from the prosecution of NCCs. The approach of the KSA regarding prosecuting cybercrime will be tested for fairness and effectiveness in Section 7.6, which will include detail about what the KSA lacks in its current approach.

7.4 Trial processes for NCCs in the KSA

In this section, the role of the CCJ (institution) within the KSA will be introduced in light of the judicial powers (operations) that the CPL 2013 gives to them to try NCCs. It will also identify the role of the CC in trying NCCs within the KSA's jurisdiction. In terms of institutions, this section will introduce the public entities which try NCC. Also, it will cover how well-trained and competent the CCJs are. Moreover, in terms of operations, this section will address the judicial powers which are allowed to them by the KSA law, *Sharia*, the BLG, and the CPL 2013.

The KSA contains elements of an inquisitorial system[1938] which involves the judiciary branch becoming active in the investigation process.[1939] Therefore, both instigative and judicial powers vested in the CCJs will be addressed in order to apply them on cybercrime in the section after. Moreover, in the next subsection, institutional aspects of the CC should be identified before addressing its powers.

7.4.1 Trials of NCCs in the KSA: Institutional aspects

Judges, including CCJs, in the KSA are generally appointed by Royal Decree,[1940] and the CC Chief, who is given authority by an administrative order of the SJC, distributes

[1938] See Section 2.3
[1939] See Section 6.1
[1940] BLG Article 52

appointed CCJs to circuits.[1941] The Royal Decree, as a tool of appointment, may be considered by some as a biased political tool because it seems to contradict Article 46 of the BLG that says:

> "The judicial authority is an independent power. In discharging their duties, the judges bow to no authority other than that of Islamic Shari'ah."[1942]

However, the Article emphasises that the judicial branch is an independent authority when fulfilling their functions, which has been adopted by provisions of Judiciary System Law 2007 (JSL).[1943] Thus, it can be argued that there is no conflict of interest when judges are appointed by an administrative tool such as a Royal Decree or are distributed to circuits by the administrative order of the chief of the CC. The recognition of such administrative tools can be found in the BLG that states:

> "Judges are appointed and their service is terminated by a Royal Order upon a proposal by the supreme judicial council as specified by the law."[1944]

One reason why such an administrative tool is used in appointing judges is that the King is the head of the three branches of government, including the judicial branch.[1945] Article 44 of the BLG states:

> "The powers of the State shall comprise:
>
> - The Judicial Power
> - The Executive Power
> - The Organizational Power

[1941] JSL. Article 6
[1942] BLG Article 46
[1943] JSL, promulgated by Royal Decree No (A/40) 2007. Article 1
[1944] BLG, Article 52
[1945] Altaee (2009) 120-123. 121.

> All these powers shall cooperate in performing their duties according to this Law and other regulations. The King is the ultimate source of all these authorities."[1946]

Furthermore, not only can the King of the KSA appoint judges, but he can also function as a judge in cases where the judicial branch fails to deliver justice,[1947] regardless of the principle of separation of powers under Article 43 of the BLG:

> "The "Majlis" [Royal Court] of the King and the "Majlis" [Royal Court] of the Crown Prince shall be open to all citizens and to anyone who may have a complaint or a grievance. Every individual shall have the right to communicate with public authorities regarding any topic he may wish to discuss."[1948]

However, even though judicial power is given to the King and his deputy, they rarely function as Criminal or Civil Judges.[1949] Moreover, the secretaries of the *Majlis* (Royal Court) always encourage the public to seek a remedy for their right to trial within official Courts, whether civil or criminal,[1950] and it seems possible to say that this premodern protocol whereby Kings resolve disputes is fading as the country progresses. However, it remains a legally valid power. Nevertheless, the KSA's legal justice system has been evolving since the establishment of the KSA in 1932,[1951] and such evolution has led to the creation of the CC as an independent Court.[1952]

[1946] BLG, Article 44.
[1947] Altaee (2009) 120-123. 128.
[1948] BLG Article 43
[1949] See the Royal Court Platform 'Tawasol'. https://tawasol.royalcourt.gov.sa/
[1950] *Ibid*
[1951] Alsuhami S (2010)
[1952] *Ibid*

Before the establishment of the KSA's CC under the provisions JSL,[1953] all criminal cases were presented before general courts where judges could pass judgments on both civil and criminal cases.[1954] However, after the JSL was passed in 2007**,** criminal cases have been brought only before CCJs.[1955] This transition towards specialism serves the public's greater good and helps to deliver justice[1956] more effectively and fairly.

However, *Sharia* experts and judges in the KSA, including the CCJs, might disagree with legal experts in regard to the legal purpose of specialised courts as some of them see the whole concept of modern law including the JSL 2007 as contrary to *Sharia*.[1957]

On the one hand, *Sharia* experts and judges in the KSA see specialism as good for preventing the accumulation of unjust legal cases (whether civil or public) before judges.[1958] Nevertheless, they see specialism as an imposition of modernity that does not understand the approach of *Sharia* in regard to criminal or civil judgments.[1959] According to the mainstream view of the *Ulema*, judges (whether civil or criminal) should be experts in *Sharia* only[1960] and further legal specialism should not be needed if judges were the best of well-educated *Sharia* diploma holders[1961] because they can function as both criminal and civil judges concurrently due to their "comprehensive knowledge of *Sharia*."[1962] However, this argument is actually based on specialism and meritocracy, even if they believe they are opposing these "Western ideologies"[1963] because they themselves are applying them as they require judges to be specialized in *Sharia* (specialism) and choose the best of those who are well educated in *Sharia* (meritocracy).

[1953] JSL Article 7
[1954] Altaee (2009) 120-123
[1955] *Ibid* 133
[1956] *Ibid* 119
[1957] Almibrad et al (2015) 15-18
[1958] Interviews with CCJs CJ1 and CJ2
[1959]Almibrad et al (2015)
[1960] *Ibid*
[1961] Interviews with CCJs CJ1, CJ2 and Sharia Expert SE1
[1962] Interview with Sharia Expert SE1
[1963] Almibrad et al (2015)

On the other hand, legal scholars in the KSA see specialism as a way to achieve a more professional approach,[1964] which will deliver higher standards of justice. Moreover, this might be one reason why legal experts in the KSA were generally happier than *Sharia* experts and judges especially after the establishment of the permanent CC building in 2010 as a result of the King Abdulla Project to develop the judicial facilities,[1965] as they see specialism undermines those who claim to be protectors of Islam. However, "if *Sharia* was codified, law graduates will be judges, and they will be better than current judges"[1966] because after the codification of *Sharia*, the rest will be legal procedures not interpretation and application of *Sharia*. It might be possible to say that judges in the KSA, including CCJs, oppose the codification of *Sharia* because they "fear that law graduates will take over their places in courts"[1967] including in the CCs. Thus, it might be argued that opposing codification is one indication of opposing specialism in the KSA.

At the moment, the CC still employs only *Sharia* diploma holders as CCJs.[1968] After being appointed as Judges, they undergo intensive theoretical training for one year in the Higher Institute of Judiciary (HIJ) where they study law and special provisions of *Sharia* related to judicial aspects.[1969] Following this theoretical training, they are trained by senior judges for three years where they observe senior judges and participate in judicial rulings, being subjected to being corrected if they to make mistakes.[1970] After both stages of training, they are mostly appointed to serve as judges in rural areas where disputes are less complex than those in main cities.[1971] Therefore, *Sharia* experts are the only judges appointed in the CC, even though the main function of the CC is to try suspects of crimes according to the

[1964] Interviews with Law Professors LP1 and LP2
[1965] Aldosari (2009) 10
[1966] Interview with Law Professor LP1
[1967] *Ibid*
[1968] Interviews with all CCJs CJs 1, 2 and 3
[1969] *Ibid*
[1970] *Ibid*
[1971] Interview with CCJ CJ1

legal based indictments sent to them by the PP. However, they can in practice disregard those indictments, as will be discussed in the next subsection which addresses the CCJs' powers.

The CC consists of three main circuits; the circuits of *hudud* and *qiyas* cases, the circuits of *ta'zir* cases, and the circuits of juvenile cases.[1972] *Hudud, Qiyas* and *Ta'zir* are classes of punishments found within the *Sharia* [1973] and each will be defined in the following subheadings in order to explain how the CC functions.

7.4.1.1 Hudud

The first class of punishment is *Hudud* (lit. limits), which are "fixed punishments in the Quran or Sunnah for specific crimes."[1974] This class of punishment is considered as the right of *Allah,*[1975]and the *Ulama* compare this punishment to the modern idea of public interest or public rights which the state protects through punishing those who commit crimes.[1976] There are four conditions that must exist for *Hudud* to be applied.[1977] The violator must be an adult, sane, committed to *Islam* or live permanently in an Islamic territory[1978] and must know about the prohibition of the crime, if not the punishment, of *Hudud*.[1979] These crimes are *sariqah* (theft), *zina* (illegal sexual intercourse or adultery), *shorb al-khamr* (drinking alcohol), highway robbery, *qathf* (false accusation of adultery), and *ridah* (apostasy).[1980] Due to its relation to cybercrime, only *qathf* and *ridah* will be addressed next.

As for false accusation of fornication,[1981] the punishment is mentioned in *Quran*:

[1972] Shareef (2016) 213
[1973] Udah (2009) 78-80
[1974] *Ibid* 83
[1975] Saifi (2013) 122
[1976] Udah (2009) 80
[1977]. *Ibid.* 600
[1978] *Ibid*
[1979] Alshubily (2005) 5
[1980] *Ibid* 2
[1981] Abu Zahrah (1998)

> "And those who accuse chaste women and then do not produce four witnesses - lash them with eighty lashes and do not accept from them testimony ever after. And those are the defiantly disobedient."[1982]

Hence, the punishment for falsely accusing people of *Zina* is 80 lashes if they do not provide four trustworthy witnesses.[1983] Muslims are very careful when it comes to their reputation, especially when it is related to their family,[1984] and that may be apparent in the structure of PP as the circuit for crimes against honour.[1985] *Zina* in Muslim communities is considered to be a destructive wrong action because it conflicts with the main principles of Islam, and also ruins family relationships.[1986] Therefore, accusing others of committing *Zina* ruins the reputation of the family and the person him/herself,[1987] and that is why some *Sharia* experts in the KSA were not happy with the KSA's decision to abolish this punishment in 2020 because, as they believe, the purpose of punishment mentioned in the *Quran* is to make people aware of the seriousness of such false accusations and to discourage them from making them.[1988] As will be discussed later in this chapter, this class of punishment is reflected in the CC judgements as a cybercrime.

Another crime that carries a *Hudud* punishment is *ridah* (apostasy). The Prophet Mohammed stated that whoever changes his religion – from Islam to another – is to be executed.[1989] At that time, apostasy was a major issue because it was the beginning of Islam, and trustworthy people were needed to deliver God's message as it is.[1990] Therefore, if someone becomes Muslim, then converts to another faith, he/she might give the wrong

---

1982 Holly Quran, 24:3, Tr. Muhammad Asad (1980)
1983 Iz Alden (2018) 10
1984 *Ibid* 10
1985 Ironically, most cybercrime are delt with in this circuit. See Subsection 6.3.1
1986 Alshubily (2005) 33
1987 *Ibid*
1988 Interview with Sharia Expert SE2
1989 Alshubily (2005) 64
1990 Udah (2009) 661-663

impression of Islam,[1991] which is what the Prophet Mohammed was afraid of.[1992] Furthermore, he told people that once they become Muslim, they cannot leave Islam.[1993] On the other hand, in the KSA, application of *Hudud* in cases of apostasy is very rare even though there are people who have become atheists; the government of the KSA does not arrest them or force them to retract their apostasy, unless they go public.[1994] However, the KSA has not abolished this type of *Hudud* because there remain some cases where the KSA authorities have severely punished people who published ideas against Islam,[1995] which might be considered as a type of terrorism[1996] or a cybercrime.[1997]

7.4.1.2 Qisas and Diyya

The second class of punishment in Islam is *qisas* and *diyya*.[1998] The *Qisas* is considered the standard punishment, while *Diyya* is an alternative punishment in cases where *Qisas* is not executed, for whatever reason.[1999]

Qisas (legal retribution) is, in simple terms, the Islamic concept of an eye for an eye.[2000] This kind of punishment is executed in cases of murder or other intentional physical harm to others.[2001] In its demonstration to this class of punishment, the Quran says:

> "O you who have believed, prescribed for you is legal retribution for those murdered - the free for the free, the slave for the slave, and the female for the female. But whoever overlooks from his brother anything, there should be a suitable follow-up and payment to him with good conduct. This is an

[1991] *Ibid*
[1992] *Ibid*
[1993] Alshubily (2005) 64-66
[1994] *Ibid*.
[1995] HRW (2015) <https://www.hrw.org/news/2015/11/23/saudi-arabia-poet-sentenced-death-apostasy>
[1996] Wehery (2015) 75
[1997] Alfaize (2015) 227
[1998] Abu Zahrah (1998)
[1999] *Ibid*
[2000] Udah (2009) 663
[2001] *Ibid*

alleviation from your Lord and a mercy. But whoever transgresses after that will have a painful punishment."[2002]

It is possible to say that *Islam* prevents any kind of assault whatsoever, especially physical assault.[2003] Therefore, if anyone suffered any physical damage caused by other people, the punishment is *qisas*.[2004] However, *qisas* can be waived by the victim or the victim's heirs if they choose *diyya* over *qisas*.[2005]

Diyya (compensation; sometimes called blood money) is a punishment that comprises compensating the injured person or heirs for damages caused by others.[2006] *Islam* encourages this way of punishment instead of *qisas,* especially when it comes to the death penalty.[2007] In 2000, the KSA established the Commission of Reconciliation[2008] in order to convince people to choose *diyya* over *qisas*.[2009] Moreover, in Islam, it is considered better for the victim to choose forgiveness over both *qisas* and *diyya*, which Islam actively encourages.[2010]

7.4.1.3 *Ta'zir*

The third class of punishment is *ta'zir* (censure), which means discipline of the wrongdoing of Muslims for sins or crimes that are not included in *hudud* or *qisas*.[2011] *Ta'zir* is very flexible, and judges can decide on a suitable punishment.[2012] The punishments meted out by judges based on *ta'zir* differ from judge to judge and from case to case.[2013] Importantly, the punishment that the judge gives must not violate or conflict with the

[2002] Holly Quran, 2:178, Tr. Muhammad Asad (1980)
[2003] Saifi (2013) 214
[2004] Idrees (1986) 15
[2005] *Iibid* 22
[2006] *Ibid*.
[2007] *Ibid*.
[2008] Commission of Reconciliation in Mekah.<https://islah.gov.sa/pages_show.php?show=1>
[2009] *Ibid*
[2010] Idrees (1986) 2
[2011] Alshatheli (2015) 8
[2012] *Ibid*
[2013] Interview with CCJ CJ1

fundamental principles of *Sharia*.[2014] Therefore, the judge should be scholar in *Sharia* and be able to interpret *Quran* and *Sunnah* in order to determine what punishment should be applied to the particular case.[2015]

In the KSA, based on the principles of *ta'zir*, many punishments have been codified due to the danger that an act poses to society, such as long-term imprisonment for drugs offenses, gun trafficking and cybercrime.[2016] Additionally, punishments for white-collar crimes, such as bribery and forgery, have also been codified based on *ta'zir*.[2017]

The death penalty can be given based on *ta'zir* for serious crimes such as rape.[2018] However, many judges in the CAs must review such punishments before they are carried out, so this process can take many years.[2019] Moreover, the purpose of some punishments that are based on *ta'zir* is to correct violators' behaviour.[2020] Hence, judges could sentence offenders to menial work, such as street cleaning or other community services under the observation of the police.[2021]

In relation to cybercrime and its procedures, the ACL was passed based on *ta'zir,*[2022] which indicates that this class of punishment is also used as a legislative and judicial instrument, as will be addressed in Sections 7.5 and 7.6.

7.4.1.4 The organisation of KSA CC in accordance with the classes of punishment

Since its creation, almost all criminal cases are tried before the CC,[2023] and criminal cases are distributed to circuits within the CC based on the class of punishments[2024]

[2014] *Ibid*
[2015] Interview with Sharia Expert SE2
[2016] Alshatheli (2015) 11
[2017] *Ibid*.11-13
[2018] Interview with CCJ CJ1
[2019] *Ibid*
[2020] Alshatheli (2015) 11-13
[2021] Udah (2009) 632
[2022] Azzam (2018) 101-104
[2023] Interviewees agree on this point as it is suggested by the JSL.

discussed in the previous subheadings. However, the juvenile circuit is categorised based on the age of the accused and not the class of punishment,[2025] no matter what crimes the accused has committed.[2026] This indicates that CCJs are trained to deal with all crimes and there is no specialism required in the law as long as they are specialized in *Sharia,* because juveniles commit crimes, the punishment for which can fall into any of the above classes. This arrangement, therefore, can add a level of confusion and complexity regarding the criminal justice system in the KSA because, when juveniles commit cybercrime, their cases will be seen before the juvenile circuit that has less expertise in dealing with cybercrime.[2027] Moreover, since juveniles are seen as vulnerable in most countries, including the UK,[2028] there should be official authorities that monitor justice for young adults to prevent the authorities, including the judiciary, from abusing their power against them.[2029] This safeguard does not exist in the complex criminal justice system of the KSA.

Due to the complexity of the classes of punishments and the absence of any comprehensive codification of *Sharia,* the main four circuits branch out into sub-circuits to deal with complex crimes (such as cybercrimes), serious punishments (which include inflicting damage to a part of the body),[2030] or less complex crimes and punishments. For serious punishments or complex crimes, the sub-circuits are formed of three CCJs[2031] to limit the chances of committing judicial errors.[2032] For crimes that are not complex or where the potential punishments do not include causing damage to the body, other circuits are

---

[2024] Almusallam (2018) 12
[2025] *Ibid* 12
[2026] *Ibid* 13
[2027] Interview with Criminal Defence Lawyer CL3
[2028] Youth Justice Board <https://www.gov.uk/government/organisations/youth-justice-board-for-england-and-wales/about>
[2029] Office on Drugs and Crime <https://www.unodc.org/unodc/en/justice-and-prison-reform/cpcj-justice-for-children.html>
[2030] Almusallam (2018) 16
[2031] *Ibid* 12-16
[2032] *Ibid* 16

formed with only a single judge.[2033] Therefore, it is possible to say that the CC is a *Sharia* driven institution, whether in regard to its institutional or operational aspects, as will be addressed in the next sub-section.

7.4.2 Trials of NCCs in the KSA: Operational aspects

The *Sharia* not only contributes to the organisation of the institution of the CCs, it also contributes, perhaps to an even greater extent, to the implementation of judiciary powers as exercised by CCJs. As addressed in the previous section, classes of punishments within *Sharia* are the most apparent factors that directly contribute to the institution of the KSA criminal justice system. Additionally, the same factor allows CCJs to exercise judiciary powers, some of which are *Sharia* powers, such as *Ijtihad,* and others are *Sharia* based powers, such as investigation, examination of evidence and sentencing.

7.4.2.1 *Ijtihad*

Ijtihad is not, in itself, a judiciary power[2034] but is rather a tool used by *Ulema* to interpret *Sharia* and formulate opinions based on their knowledge of *Sharia,* especially in cases where an issue is not specifically mentioned by religious texts, such as the *Quran* or the *Hadith* literature.[2035] This tool has been adopted by the KSA legal system to cover contemporary legal civil and criminal issues not covered by legislation.[2036] Given the scope of this work, the focus here will be on criminal issues. Even though the KSA has passed numerous pieces of legislation on multiple crimes since 1932,[2037] many crimes have not been

[2033] *Ibid* 12-16
[2034] Khan and Ramadan (2011)
[2035] See Section 2.3
[2036] Alshatheli (2015) 12
[2037] Saifi (2013) 19

covered fully, and some crimes mentioned in *Sharia* have not been codified.[2038] Therefore, there is a need for judges who obtain a reasonable amount of knowledge of *Sharia* to apply the provisions and principles found in it to contemporary issues using *Ijtihad* to formulate judicial decisions.[2039] Therefore, *Ijtihad* is a supreme power which is applied to other judiciary powers, including investigation, examination of evidence and sentencing. Moreover, it is possible to say that this power is not only used by CCJs in the absence of legal or religious texts but also in cases where texts are present.[2040] This will be addressed in Section 7.5.2 when addressing the trial of cybercrimes.

7.4.2.2 Investigation

In late-modern states with an adversarial system such as that of the UK, investigation is usually done in the pre-trial stage.[2041] However, in the KSA, investigation is both a part of the pre-trial stage and also a power given to the CCJs by the CPL 2013, where they can discard the whole criminal case dossier and start over.[2042] Article 161 of the CPL 2013 states:

> "If the accused at any time confesses to the charge, the court shall hear and examine his statement in detail. If the court is satisfied that the confession is valid and sees no need for additional evidence, it shall decide the case. Otherwise, it shall further investigate the case."[2043]

Also, Article 162 says:

> "If the accused denies the charges or refuses to respond, the court shall proceed to hear the evidence and take necessary action. It shall interrogate the accused in detail regarding the evidence and charges.

[2038] *Ibid*
[2039] Udah (2009) 62
[2040] Interview with all CCJs CJ 1,2 and 3
[2041] UK Criminal Procedure and Investigations Act 1996. Part IV
[2042] Shareef (2013) 192
[2043] CPL Article 161

> Each of the parties may, with the permission of the court, cross-examine witnesses and evidence."[2044]

According to those two Articles, CCJs can take the "necessary action" to reinvestigate the criminal case brought to them by the PP.[2045] CCJs reinvestigation mainly includes interrogating the accused, and they can discard the whole investigation conducted during earlier stages of the criminal procedure under the condition that such an early investigation lacks credibility.[2046] Therefore, this may more properly be considered to be a type of judicial review,[2047] especially as there is no separate entity whose main function is to supervise the law and practice in the KSA, as there is in the UK.[2048] CCJs' extensive powers will be assessed in terms of its fairness and effectiveness in Section 7.6.

7.4.2.3 Examination of evidence

CCJs in the KSA have the power to examine the evidence provided against, or by, the accused.[2049] After the examination of evidence, CCJs can dismiss certain pieces of evidence which might lead to the dismissal of the whole criminal case if the case was built on such evidence.[2050] Moreover, the power to examine criminal evidence is not limited to particular pieces of evidence, but it can extend to cover all the evidence presented before the court.[2051] Furthermore, CCJs might use external unbiased experts to examine technical evidence[2052] such as cyber evidence.[2053]

[2044] CPL Article 162
[2045] *Ibid*
[2046] Interviews all with CCJs CJ 1,2 and 3
[2047] It might be considered as a second look rather than the more technical meaning of judicial review within administrative law. For technical administrative law, see Bin Ammar (2015)
[2048] The UK Administrative Court Judicial Review Guide 2018 <https://www.judiciary.uk/wp-content/uploads/2018/11/Admin_Court_JRG_2018_content_v3_web.pdf>
[2049] CPL Article 162 and 169
[2050] CPL Articles 189, 190, and 191
[2051] Interviews with CCJs CJ 1,2 and 3
[2052] CPL Article 173
[2053] Interviews with CCJs CJ 1,2 and 3

Not only do CCJs have the power to examine the evidence, but also they have the power to examine the facts.[2054] On the one hand, in the UK, judges examine evidence and facts only in the Magistrates' Courts where criminal charges are not so serious,[2055] while in Crown Courts, judges deal only with criminal law and process and not the evidence in the criminal case,[2056] which is examined by juries to determine guilt.[2057] On the other hand, the CCJs' powers are extensive because they have the final say in the criminal case. One apparent reason why the CCJs can examine the facts of the criminal case is that they can pass judicial judgements on the case to determine whether the accused is guilty or not.[2058] In common law countries such as the UK, judges can examine the evidence in criminal cases but not the facts,[2059] and it is the role of the jury to determine whether the accused is guilty or not.[2060] Although systems where juries can decide whether the accused is guilty have been criticised, especially when it comes to the lack of legal specialism of the jurors, it is also considered by some to be fairer to the accused.[2061] One reason for this is that it could be unfair to leave the fate of the accused in the hand of the judges[2062] who have an excessive amount of power over the accused, such as in the case of the KSA. CCJs in the KSA can employ the power of *Ijtihad* to determine the guilt after examining the fact.[2063]

[2054] Shareef (2016) 152
[2055] Hoffman and Rowe (2013) 42-44
[2056] *Ibid*
[2057] Reichel (2018) 191-197
[2058] *Ibid*
[2059] Pakes (2019) 191
[2060] Ibid 191-193
[2061] *Ibid*
[2062] *Ibid*
[2063] Interviews with CCJs CJ 1,2 and 3 and Criminal Defence Lawyers CL1, 2 and 3

7.4.2.4 Sentencing

The CCJs can employ the power of *Ijtihad* to determine a suitable punishment based on *Ta'zir* if the person is found to be guilty.[2064] Until recently, even though the CPL 2013 prohibits any sort of punishment without legitimate texts in either *Sharia* or legislation,[2065] CCJs used to sentence the accused based on *Ta'zir be Alshubhah*,[2066] even without any clear proof of guilt, a practice which violates the BLG [2067] and the CPL 2013.[2068] However, in 2019, the SJC prohibited such practice, viewing it as a violation of both *Sharia* and legislation.[2069] It might be said that the absence of legal codification of criminal law in the KSA leads to this unfair practice.[2070] Even though the data collected from interviewing CCJs, criminal defence lawyers and *Sharia* experts shows that all of them apply the criminal law principle equivalent to the following rule, "Doubt is interpreted in favour of the accused [*In dubio pro reo*]",[2071] and the *Sharia* principle, "No Hudud is given on suspicious proof,"[2072] those or any similar principles are not specified in any legislation.[2073] It was a surprising that some *Sharia* experts and criminal defence lawyers thought that those principles are codified in the KSA law.[2074]

CCJs in the KSA apply the discussed principles, which are based in legislation or *Sharia*.[2075] However, it is often unclear what the law means, so in 2017, the KSA MoJ published the *Majmuat alahkam Alqadha'iah* (Judicial Rulings Collection) for 2014, which is

[2064] Pakes (2019) 110
[2065] CPL Article 3
[2066] The practice takes place until the year 2019 where it was abolished by Supreme Judicial Council Order No 1205/T Dated 27/04/1440 Ah (03/01/2019)
[2067] BLG Article 38
[2068] CPL Article 3
[2069] Supreme Judicial Council Order No 1205/T Dated 27/04/1440 Ah (03/01/2019)
[2070] Mallat (2020) 1-3
[2071] Udah (2009) 302
[2072] Udah (2009) 209
[2073] Interviews with Law Professor LP1
[2074] Some of the interviewees insisted that the CPL includes the presumption of innocence principle, and took a while to process the fact that it does not exist in it such as Criminal Defence Lawyers CL1 and 2, Detective of the PP1 D1 and Sharia Experts SE1 and SE2
[2075] Interviews with CCJs CJ1, 2 and 3

comprised of 13 volumes of judicial rulings on criminal cases.[2076] Almost all rulings on criminal cases include legal or *Sharia* principles in relation to crimes[2077] which proves that CCJs follow certain principles in their rulings. However, those principles are not codified and do not enjoy the status of legal enforcement. Moreover, some rulings contradict others because *Ijtihad* varies between judges.[2078] Furthermore, one judge's ruling does not oblige another to make the same judgment because the KSA does not approve of the concept of legal precedent.[2079] However, when training judges in the HIJ, they (as all KSA law schools) study the Egyptian Penal Code[2080] where criminal law principles are codified with a strong French influence.[2081] Therefore, they apply those principle in their judicial judgments based on *Ijtihad*, even though such principles do not exist in the KSA criminal justice system.

Therefore, it is possible to say that the power of *Ijtihad* allows for multiple approaches to making judicial rulings within the KSA, and, for some, this might be a fairer approach because it makes it possible to cope flexibly with the variables surrounding a case using the principles of fairness that exist within *Sharia*.[2082] Moreover, it allows new innovative sentences to be produced for crimes not mentioned in legislation.[2083] As previously mentioned in Subsection 7.4.1.3, there are two types of *Ta'zir*; one is officially codified, and the other is based on the ability of the judge to produce a new crime or punishment as a result of *Ijtihad* under the condition that it does not violate *Sharia*.[2084] However, in a single coded *Ta'zir* crime, judges might establish a new punishment based on their own *Ijtihad* even though the *Sharia* rule clearly states that "there is no *Ijtihad* if the text

[2076] MoJ, Judicial Rulings Collection <https://www.moj.gov.sa/ar/SystemsAndRegulations/Pages/System1435.aspx>
[2077] *Ibid* Vol 13
[2078] *Ibid*
[2079] Pakes (2019) 110
[2080] Interviews with CCJs CJ1, 2 and 3
[2081] Mallat (2020) 4
[2082] Udah (2009) 162
[2083] *Ibid*
[2084] Alshatheli (2015) 17

is present".[2085] For instance, the coded *Ta'zir* crimes in the KSA mostly mention imprisonment and/or fines as the main two punishments, and none of the codified *Ta'zir* crimes legislation impose punishments unique to the *Sharia* such as flogging,[2086] yet CCJs impose such punishments based on their own knowledge of *Sharia* which is obtained during their university studies or during their training in the HIJ and based on *Ijtihad*. As will be addressed in the next section, this power – along with others – impacts on cybercrime cases presented before the CC.

There may be two aspects of unfairness arising from the previous discussion. The first aspect is lack of certainty, which is more or less inherent in the reliance on pre-modern *Sharia*. The second aspect is inequality. There is no certainty that like cases will be treated alike, since the judges vary greatly in their appreciation and application of *Sharia*.[2087]

7.5 Trials involving Cybercrime in the KSA

This section analyses the KSA's responses to trials involving cybercrime. As a part of the analysis, it will identify who should try cybercrime, what judicial powers they have, and what standards they follow especially in regard to cyber evidence. The main aspects that will be addressed in this section are again depicted as institutional (CC) and operational (CCJs powers). The very competence of the CCJs with their current qualifications to try cybercrime should be addressed. This leads to a key question in this research, which is whether or not the KSA's current approach regarding the criminal procedure of cybercrime is fair and effective. This question is answered later in Section 7.6.

[2085] Ibn Baz's Fatwa
[2086] Saifi (2013) 21
[2087] Marmor (2005) 27–38

7.5.1 Trials of cybercrime in the KSA: Institutional aspects

Similar to NCCs, cybercrimes are mainly processed in the CC,[2088] and CCJs are the competent judicial authority assigned by the relevant legislation. Moreover, cybercrime cases are handled before a Joint Triumvirate Circuit.[2089] This is a sub-circuit of the overall *Ta'zir* circuit where three judges look into cybercrime cases along with other NNCs that could receive serious punishments or other complex crimes.[2090] The CCJs who adjudicate on cybercrime cases in this sub-circuit are specially trained in the HIJ to deal with cybercrime.[2091] The training mainly includes studying literature related to cyberspace, cybercrime, and cyber evidence,[2092] most of which is translated into Arabic from English[2093] and is somewhat Islamised[2094] to reflect the provisions of *Sharia.*[2095] It could be argued that this is ineffective training for two reasons. The first is that it focuses on doctrinal literature and lacks the technical aspects of training. The second is that it seeks to apply *Sharia* to the late-modern phenomena of cybercrime, which might exacerbate the difficulties surrounding the criminal procedure of cybercrime in the KSA rather than alleviating them. As has been addressed in Chapter 5, some Muslim jurists may act out of dogmatism without fully considering the possibility that they may be mishandling novel issues.[2096]

Therefore, giving judicial authority only to *Sharia* diploma holders in order for them to rule on cybercrime cases may be a fragile and shallow response that may deepen the inefficacy of the KSA's approach to the criminal process of cybercrime. It might be

[2088] Interviews with CCJs CJ1, 2 and 3
[2089] Almusallam (2018) 16
[2090] *Ibid*
[2091] Interview with CCJs CJ1 and CJ2
[2092] *Ibid*
[2093] *Ibid*
[2094] See discussion in 2.2.2 about liberal democracy values on cyberspace and how they would affect other culture in the long run although they try to resist them
[2095] Interview with CCJ CJ2
[2096] See Subsection 5.4.2.3

understood that, as the KSA is an Islamic country (as specified in the BLG),[2097] it wants its criminal justice system to be in line with *Sharia*. However, the late modern phenomenon of cybercrime is not effectively dealt with judicially by officials who lack expertise on technical law and evidence relating to cybercrime. Yet, as found in the BLG, the judicial branch must rely on *Sharia*.[2098] It is assumed that only *Sharia* experts possess the key to all the KSA judiciary issues. This assumption might have been true in earlier times, when the KSA was a closed and insular society,[2099] but becomes inappropriate when the State expresses its wishes to modernise. Moreover, this approach might not be fair, at least if viewed beyond the norms of *Sharia*, such as in international law, as will be addressed in Section 7.6 after addressing the CCJs' powers in regard to trial of cybercrime in the next sub-sections.

7.5.2 Trials of cybercrime in the KSA: Operational aspects

The powers of CCJs related to the trial of cybercrime are not very different from NCCs. However, in the trial of cybercrime, CCJs are more bound by the authority of legislation than the authority of *Sharia* compared to the NCC,[2100] because cybercrime related legislation is compatible with *Sharia.*[2101] Furthermore, it is possible to assert that the reason why they surrender to the authority of legislation is because the judiciary know less about the nature of cybercrime[2102] and *Sharia* appears to be silent on that topic in any direct, meaningful way. Therefore, there is almost a unanimous practice within the CC to adhere to the legislation to avoid further judicial errors in cybercrime cases.[2103] Nonetheless, this does not mean that CCJs would not use their *Sharia* based power of *Ijtihad* when dealing with

[2097] BLG Article 1
[2098] *Ibid* Article 46
[2099] Alrasheed (2002)
[2100] Interviews with CCJs CJ1, CJ2 and CJ3
[2101] *Ibid*
[2102] Interview with CCJ CL1 and Law Professor LP1
[2103] Interview with CCJ CJ2

cybercrime. As addressed in Chapter 4, ACL fails to comprehensively cover cybercrime both substantively and procedurally,[2104] which might be why CCJs enforce *Ijtihad* even though there is specific legislation covering cybercrime.[2105] Nonetheless, this argument is more a justification for extending judicial discretionary power rather than a solution to an existing gap. In the Judicial Rulings collection, which is the recent KSA official published judicial judgments,[2106] in 5 out of 6 published judicial judgments for cybercrime, CCJs sentenced the convicted person to lashing, even though no such punishment exists in the extant legislation.[2107] One judgment was based on *Hudud* as the convicted falsely accused (*Qathf*) a complainant with *Zina.* The other three judgments were based *Ta'zir*. However, the fifth case was dismissed, yet if the accused was to be proven guilty, the power of *Ijtihad* would have been applied.

7.5.3 Six examples of cybercrime trials

It is crucial for the analysis of cybercrime trials to examine more fully the six official published judicial judgments for cybercrime and see how the CCJs operated in these instances. All six summaries were obtained from the MoJ's Judicial Rulings Collection[2108] and have not been analysed previously. Those six summaries are the only published summaries related to cybercrime, even though the CC has ruled over hundreds of criminal cases related to cybercrime[2109] which were not published and, therefore, not accessible. In Appendix F, the official summaries of judgments are translated from Arabic to the English by

[2104] See Section 4.2.1
[2105] Interviews with Law Professors LP 1& 3 and CCJs CL 2 and 3
[2106] MoJ, Judicial Rulings collection <https://www.moj.gov.sa/ar/SystemsAndRegulations/Pages/System1435.aspx>
[2107] As been said in the previous sections, this unique punishment is not addressed in any piece of legislation in the KSA which might indicates that the legislative branch in the KSA is less strict in applying *Sharia*.
[2108] MoJ, Judicial Rulings collection <https://www.moj.gov.sa/ar/SystemsAndRegulations/Pages/System1435.aspx>
[2109] Interviews with Criminal Defence lawyer CL3 and CCJs CJ1, CJ2 and CJ3

the researcher to help in further analysis in the thesis; however, a brief summary of all six cases is found in the next table.

Table 7.1 Brief summary of the six reported cybercrime cases

Case No	Charges	Law applied	Verdict	Sentence	Extras
Case 1	Cybercrime; Qathf using email	Sharia & ACL Article 3/5	Guilty of Qathf	80 lashes; 2 months imprisonment; 5000 riyals fine.	Main evidence: emails, police initial investigation & confession. Appeal approved.
Case 2	Cybercrime; ruining reputation using social media	CPL 2013 Article 192 & ACL Article 15	Dismissal of case for fundamental procedural error	NA	Appeal approved.
Case 3	Cybercrime; selling and possessing pornographic materials	Sharia & ACL Article 6	Guilty of charges	300 lashes; 1 year imprisonment; 5000 riyals fine; destruction of confiscated materials; recommendation of deportation.	Evidence: flash memories, police initial investigation & confession. Appeal approved.
Case 4	Cybercrime; possession of naked pictures of women and voice recording of blackmailing a woman.	Sharia	Guilty of Charges	10 lashes; 1 month imprisonment; confiscation of 2 mobile phones.	Evidence: 2 personal mobile phones in possession of the accused search by police. Appeal approved.
Case 5	Cybercrime; possession of pornographic materials	Sharia overrules ACL Article 6	Not guilty but suspicious.	70 lashes; 20 days imprisonment.	Evidence does not prove guilt. Appeal approved.
Case 6	Cybercrime; Possession of sexual materials, taking photos of a minor female	Sharia & ACL Articles 6 & 13.	Guilty of Charges.	50 lashes; 3 months imprisonment; 200 riyals fine; confiscation of mobile phone.	Confession was the main evidence. Appeal approved.

When looking at these cybercrime judgments and case summaries, there are multiple similarities and correlations between them, especially in regard to what has been addressed during the last four sections of this Chapter. First, the prosecution plays more of a presentation role rather than actually defending the criminal case. The prosecution simply presented the cybercrime case files and, in some cases, relied on the investigation of the arresting authorities, not the PP's investigation which might suggest that the PP does not investigate cybercrime properly. Moreover, the prosecution's role within the CC can be considered negative rather than positive because the prosecution remained silent during the trial until the end when they may object.[2110] This would indicate that the prosecution role is neither properly addressed in the legislation nor does the office effectively engage in the criminal process, as discussed in Sections 7.2 and 7.3.

Second, the impact of *Sharia* on cybercrime is very noticeable, both procedurally and substantively, although cybercrime has been codified at least substantively based on *Ta'zir*[2111] as a classification of *Sharia* punishment. When looking at the judgment summaries, CCJs have imposed *Sharia* related punishments that are not mentioned in the legislation, such as the punishment of lashing based on *Ta'zir* or *Hudud* by using the power of *Ijtihad*. This would show the extensive discretionary power that the CCJs have in regard to imposing punishments that they see to be fit, even though there is no clear written guidance to measure this power,[2112] except for the legal provisions that enhance this power, such as Article 46 of the BLG, where the judiciary branch is only governed by the authority of *Sharia*.[2113] However, it is possible to say that legislation is part of *Sharia* because, as the BLG states, legislation must

[2110] According to the collected data from the interviews Detective of the PP D1 and Public Prosecutor PP2 and the six cases found in the Judicial Rulings Collection, prosecutors can object after the verdict is passed by the CCJs, not during the trial where they can answer questions asked by Judges. This might sound odd when compared to the objections by prosecutors in the UK, but it might be possible to say that prosecution in the KSA is not well understood as KSA law and practice might suggest, as discussed in this section.
[2111] Alathli (2015) 13
[2112] Mallat (2020) 4
[2113] BLG Article 46

be in line with *Sharia*[2114] and it is to be assumed that most if not all legislation in the KSA is compatible with *Sharia*.[2115] Nonetheless, CCJs circumvent legislation and impose punishments that are not included within the legislation, despite the legal texts that prohibit imposing punishments without valid texts in either *Sharia* or legislation.[2116] Moreover, the CA confirmed those judgments and they allow for uncodified punishments to be imposed.[2117] However, unlike the UK or other common law jurisdictions, judges (including CCJs) in the KSA are not bound by legal precedents even though they try to be consistent.[2118] Therefore, disparities between punishments and judgments for similar cybercrime cases might happen, mainly because the power of *Ijtihad* ultimately differs from one judge to another.[2119] For instance, in the summary of Judgment 2, the judge dismissed the cybercrime case due to a procedural error where the alleged crime has not been investigated by the PP, and the CA confirmed the dismissal. However, in the summaries of Judgments 3, 4, 5 and 6, similar procedural errors were committed by the PP where the PP did not investigate the cybercrimes and just relied on the arresting authority investigation; yet neither the CCJ nor the CA dismissed the cybercrime case on the grounds of procedural error. This disparity between judgments would suggest that the KSA is less concerned about the rule of law than the UK.[2120] What seems to matter most to the KSA is the rule of *Sharia*[2121] which would be more acceptable if *Sharia* is applied consistently, rather than having unjustified disparities and incorporating vague interpretations. Even the KSA government has noticed the wrongful interpretation of *Sharia* based on *Ijtihad* when dealing with contemporary issues such as the criminal procedure of cybercrime; otherwise, it would not seek to abolish *Ta'zir be Alshubhah*

[2114] *Ibid* Article 7
[2115] Alathli (2015) 5
[2116] CPL Article 3 and BLG Article 38
[2117] MoJ, Judicial Rulings collection 2017 Vol 13. Most cases are confirmed by the CA.
[2118] Mallat (2020) 3
[2119] Interview with Sharia Expert SE2
[2120] Pakes (2019) 135
[2121] BLG Article 7

despite much opposition from *Sharia* experts.[2122] However, the rule of *Sharia* is decreasing on the whole in the KSA as a more formalised rule of the law is slowly taking over[2123] as a result of the KSA's *Vision 2030* that seeks a fairer approach.[2124]

As discussed in Chapter 2, the KSA is currently seeking to modernise many parts of society through its reform programme, *Vision 2030*, and, as a feature of modernity, society should free itself from out-dated traditions and beliefs,[2125] especially if they conflict with science due to their superstitious metaphysical grounds. This, therefore, may be one reason why the KSA is slowly letting go of old traditions and beliefs, including those which comprise its criminal justice system, such as by abolishing *Ta'zir be Alshubhah* in 2019 and flogging punishments in 2020.[2126] In the near future, this line of reform may help to change the KSA's approach toward the criminal procedure of cybercrime. *Vision* 2030 might be an important explanation in this regard, but there may be other factors. One that has been identified is the difficulty of deriving legal judgments based on *Sharia* which are consistent and clear. Another is the failure to fit with the technology or even to understand it in order to deliver appropriate outcomes in cases. Moreover, another factor might be growing professionalism; people are better educated and can see the difference between premodern and modern approaches.

Third, it has been said in the previous section that the CCJs exercise the power of investigation where they can reinvestigate the criminal case and reinterrogate the accused in the courtroom. In all the six summaries of judgments, judges seem to have partially interrogated the accused. It is becoming a routine in the courtroom in the KSA to interrogate

[2122] Sharia Expert SE2 and Detective of the PP D1 were not happy for such a change when the issue came up during the interview.
[2123] Interviews with Law Professors LP 1and 3
[2124] The Ministry of Justice contribution to reform the legal system in the KSA with accordance to *Vison* 2030 <https://www.moj.gov.sa/English/Ministry/vision2030/Pages/default.aspx>
[2125] See Section 2.5
[2126] Supreme Judicial Council Order No 1492/T Dated 25/09/1441 Ah (18/05/2020)

the accused in order to examine whether they have been treated with fairness in previous criminal procedure stages,[2127] and this is apparent in the summary of Judgment 2, where the judge dismisses the case based on his own interrogation. However, this power of reinvestigation is extensive and dangerous because judges can easily abuse it,[2128] especially in the absence of any comprehensive legal code of practice or legal safeguards such as disclosure and legal advice. However, it might be argued that this power helps to keep track of fairness and in this role the judges may be better considered a judicial review authority because they can supervise both practice and legislation and overrule it with their own views that are mainly driven from their understating of *Sharia.*[2129] Nonetheless, it can be argued that vesting this power in the CCJs might undermine the wish of officers acting in the previous criminal procedure stages to execute their duties properly, because they would know that there is a superior power over them that corrects their errors with no punishment, warning or any other forms of unpleasant consequences that could deter them from committing intentional harm[2130] or negligent errors within the process.

Fourth, one similarity between the six judgment summaries is the disclosure in court of the cybercrime evidence. All the accused were presented with the evidence against them. However, the CCJ did not examine whether the evidence was gathered and presented properly, even though they have the power to examine such evidence, as addressed in the NCCs section in relation to the CCJs' powers.[2131] The CPL 2013 allows CCJs to appoint an expert in their field to give their professional opinion on the matter referred to them.[2132]

[2127] Interviews with CCJs CJ 1, 2 and 3 seem to be in line with the published judicial rulings in Vol 13, and both indicate that judges mostly interrogated the accused
[2128] Interviews with Criminal Defence Lawyers CL 2 and 3 and Law Professor LP1
[2129] Pakes (2019) 140
[2130] It is socially common among KSA population to use their connections with public officials to convince them to drop criminal cases, which can happen at any stage from policing to trial.
[2131] See Subsection 7.4.2.3
[2132] CPL 2013 Article 171

Therefore, due to the complexity of, and difficulties surrounding, cyber evidence,[2133] CCJs should have appointed an expert to examine the evidence in most cases. However, according to the six judgment summaries, their approach to the modern phenomenon of cybercrime was to rely on the traditional modes of proof (especially confessions) rather than an appropriate proof such as a cyber expert opinion, which they do have access to according to the law. This dependence on confession as a proof would suggest that the KSA prefers to hold onto traditional approaches to deal with modern issues rather than face modern issues with modern approaches. Even in late modern states such as the UK, confession is referred to as the "queen of evidence,"[2134] yet the UK does not just depend on confession as it is not easily obtained under the procedures of investigative interviewing described earlier,[2135] which is distinct from the KSA where officials are able to coerce a suspect to confess to a crime.[2136] Therefore, the UK recognises the right of silence as being important in order that justice be fairly administered, giving the suspect the right to not incriminate themselves.[2137] Moreover, the standard of proof in the UK is that guilt must be proven beyond reasonable doubt,[2138] while, in the KSA, there is no such a clear standard, and it might be possible to say that the PP's standard of proof might be psychological as CL1 says "if you know the Judge's psyche, you will win your case."[2139] It might be odd to assume that the PP should know how the CCJs think and based their proof on it, but this assumption might be false when taking about judges who have lesser powers than the KSA CCJs. Therefore, out of respect to their extensive power, the PP should know how the CCJs think and reach decisions based on such knowledge, which may be due to the absence of legal guidance in this regard.

[2133] Casey (2011) 179
[2134] This phrase was first used by the Russian prosecutor Andrei Yanuarevich Vyshinsky: "confession is a queen over all sorts of evidence" (Vaksberg (1990) 79)
[2135] Greer (1990) 709-730
[2136] Gulf Centre for Human Rights (2018) 12
[2137] Greer (1990) 709-730
[2138] Johnston (2019) 233
[2139] Interview with Criminal Defence Lawyer CL1

Furthermore, most of these crimes are not considered to be crimes at all in western jurisdictions whether relevant to cyberspace or otherwise. For instance, criminal libel did exist but was abolished in England and Wales after disuse for a century[2140] in accordance with Section 73 of the Coroners and Justice Act 2009.[2141] Moreover, due to its involvement in causing physical harm, punishment by strokes of the birch, or lashing, has been abolished in modern societies. One of its last applications was in Isle of Man (a territory dependant on the UK Crown even though it is not part of the UK) in the 1970s,[2142] in line with the notion that "the more the punishment is less severe the more the society is civilised".[2143]

In light of what has been addressed, the question of whether such an approach is fair and effective arises. Thus, after testing the fairness and effectiveness of the KSA's approach toward the prosecution of cybercrime in the next section, a test of fairness and effectiveness of the KSA's approach toward the trial of cybercrime will follow.

7.6 Fairness and effectiveness of the KSA's responses to prosecution and trial of cybercrime

As one principal objective of this research, the KSA's response to prosecution and trial of cybercrime will be tested for fairness and effectiveness in order to identify shortcomings in how the KSA criminal processes tackle cybercrime.[2144] In regard to the fairness and effectiveness of the role of CCJ, *Sharia* plays the leading role within the judicial branch; therefore, a test for both fairness and effectiveness of the KSA's adherence to *Sharia* will be conducted in order to analyse why the KSA insists on applying *Sharia* within its judicial system even though *Sharia* does not explicitly cover cybercrime.

[2140] Walker (2006)169-203
[2141] Coroners and Justice Act 2009 Section 73
[2142] *Tyrer v UK* application No. 5856/72, 1978
[2143] Habeeb (1999) 15
[2144] See Section 1.3

7.6.1 Fairness and effectiveness of the KSA's response to the prosecution of cybercrime

Part of the aims and objectives of this chapter is to test whether the KSA's response toward the criminal processing of cybercrime is fair and effective, which will be conducted in this section. In the next subsections, the fairness and effectiveness of the prosecution of cybercrime in the KSA will be tested using conceptual, international, and national tests for fairness and effectiveness as set out in Chapter 2.[2145]

7.6.1.1 The fairness and effectiveness of the prosecution of cybercrime from a conceptual perspective

According to the conceptual meanings of both fairness and effectiveness discussed in Chapter 2,[2146] fairness means that the procedure is just[2147] and effectiveness means that it secures successful outcomes.[2148] Thus, the question which should be asked here is whether the current approach of the KSA's prosecution of cybercrime is fair and effective in accordance with the conceptual standards of both. In order to answer this question, it is crucial to go back to the analysis made in Sections 7.2 and 7.3 to come up with appropriate evidence for such an answer.

It has been stated that, in regard to all crimes (including cybercrimes), the prosecution as an institution in the KSA has not been properly addressed in the literature or in the law.[2149] Similarly, prosecutorial powers in the KSA are not covered in either the law or the literature.[2150] Moreover, there are no written official objectives for prosecutors to follow, which indicates that the KSA's current approach is unsuccessful and, as a result, is

[2145] See Section 2.4
[2146] *Ibid*
[2147] *Ibid* Subsection 2.4.2.1
[2148] *Ibid* Subsection 2.4.1.1
[2149] See Subsections 7.2.1 and 7.3.1
[2150] See Subsections 7.2.2 and 7.3.2

ineffective. Therefore, if the KSA's current approach was found to be ineffective, it is inevitable that unfairness would naturally follow because, for fairness to be established, effectiveness should be present as an aspect of legitimacy.[2151]

Next, prosecutions might be unfair for several reasons. First, the rights of the accused might not be secured at this stage in both law and practice. Second, the supervision that exists over prosecutors might be inadequate, which gives the PP the opportunity to abuse their powers. Third, because detectives are prosecutors behind the scenes, their power should be defined in order to control it, rather than simply trusting them with far reaching powers that are easily abused.

7.6.1.2 Fairness and effectiveness of the prosecution of cybercrime from an international perspective

As previously mentioned, the international standards of fairness and effectiveness are found within international human rights norms, which are ratified by the majority of countries including the UK.[2152] International standards of effectiveness are not promulgated, though John Stuart Mill's happiness principle is widely cited.

The UK is a signatory member of all major human rights treaties, which has positively affected its approach toward the prosecution of crimes in general, and cybercrime in particular. Unlike in the KSA, the role of prosecution and prosecutorial powers of cybercrime in the UK is clear and is separate from investigation. This clarity of approach is linked to Mill's principle as it ensure happiness to the majority of people, and this would lead to effectiveness, especially after encouraging public support to be involved within the process[2153] in order to avoid issues such as delays and biases. Public support would result in

[2151] Beetham (1991)
[2152] UN OHCHR <https://www.ohchr.org/documents/publications/coretreatiesen.pdf>
[2153] Tyler and Huo (2002) 3

the population generally trusting the authority which would further legitimise its power.[2154] Furthermore, the UK ensures fairness by implementing international human rights standards within its prosecution related laws, such as due process.[2155] Therefore, it can be said that the UK's approach in this matter is fairer and more effective than the KSA's approach. Consequentially, this comparison reveals that the KSA is in a critical situation because it does not pay enough attention to the prosecution of cybercrime and puts most of its effort into its investigation instead, which has its own issues as discussed in Chapter 6.[2156] Therefore, it is possible to say that, from an international perspective, the prosecution of cybercrime in the KSA is not as fair and effective as the international community demands.[2157]

7.6.1.3 Fairness and effectiveness of the prosecution of cybercrime from a national perspective

In the KSA, the ultimate standard of fairness and effectiveness with regard to its legal measures is known through its compatibility, or lack thereof, with *Sharia.*[2158] As long as the approach toward prosecuting cybercrime does not conflict with *Sharia*, it can be viewed as fair and effective. This measurement is not simple due to the complexity of *Sharia* and its variety of interpretations over the course of 14 centuries, and there is no clear measurement for the KSA to follow in regard to legal issues that are subject to *Sharia*, such as the issue of prosecution. However, it is possible to say that *Sharia* does not conflict with international human rights in regard to due process.[2159] Thus, similar conclusions for the international test would appear. However, in practice, the core function of the prosecution of cybercrime is vested in the detectives of the PP. Therefore, if the investigation of cybercrime is found to be

[2154] *Ibid* 102
[2155] Hoffman and Rowe (2013) 63-92
[2156] See Section 6.6
[2157] UPR, Saudi Arabia 3rd cycle <https://www.ohchr.org/EN/HRBodies/UPR/Pages/SAindex.aspx>
[2158] See Section 2.4
[2159] Reza (2013) 1-27

fair and effective, the prosecution of such crimes would follow in a similar vein, but since the investigation of cybercrime in the KSA has been viewed as ineffective and unjust,[2160] prosecution does not meet such a test.

7.6.2 Fairness and effectiveness of the KSA's response to the trial of cybercrime

As well as the prosecution of cybercrime, a test of the fairness and effectiveness for the KSA's response toward the trial of cybercrime will be conducted as a main aim and objective of this thesis. Therefore, in the next subsections, the fairness and effectiveness of the trial of cybercrime in the KSA will be tested using the standards of conceptual, international, and national fairness and effectiveness discussed in Chapter 2.[2161]

7.6.2.1 Fairness and effectiveness of the trial of cybercrime within a conceptual perspective

The criminal procedure of cybercrime in the KSA is a tricky subject, especially when it comes to the final stage of trial because the criminal justice system as a whole is complex because it is founded on *Sharia*. This complexity is perhaps more apparent in the trial stage because, as it is clearly stated in the KSA's BLG, there is no authority over judges except for the authority of *Sharia*[2162] including CCJs who hear cybercrime cases. Therefore, the question which arises here is whether the KSA's current approach toward the trial of cybercrime is fair and effective from a conceptual perspective.

In accordance with the standards of conceptual fairness and effectiveness, the KSA's current approach towards the trial of cybercrime might not be just and effective, because it does not have official and explicit written objectives to follow. Furthermore, despite this lack

[2160] See Subsection 6.4.2
[2161] See Section 2.4
[2162] BLG Article 46

of written objectives, there are some general objectives of the judiciary that are found in the MofJ's contribution to the KSA's *Vision 2030*,[2163] yet there are none that relate directly to the trial of cybercrime, which enhances the chances of the relevant measures being ineffective, contrary to *Vision 2030*'s aims which states it is actively seeking to improve the effectiveness of the KSA's legal system.[2164] Furthermore, not only might the trial of cybercrime in KSA be found to be ineffective, it may also be found to be unjust. The most important measurement of procedural fairness is to be just in the eyes of the community.[2165] The community here should be divided into two: the international community and the national community, and both perspectives of what is fair and just will be discussed in the next subsections, respectively.

7.6.2.2 Fairness and effectiveness of the trial of cybercrime from an international perspective

The international standards of effectiveness of the trial of cybercrime will be governed by the same standards discussed in Chapter 2, which is ensuring the greatest amount of happiness to the greatest number of people.[2166] Although this is not an international standard for effectiveness, it is the one that the UK follows. Therefore, this comparative standard may be representative of the late modern world. It might not be possible to measure whether the KSA population are happy with the country's current approach regarding the trial of cybercrime, because there are no statistics, either no official or unofficial, which investigate this issue, or even similar ones. Hence, one can only assume that

[2163] MoJ. National Transformation Plan Program. https://www.moj.gov.sa/English/Ministry/vision2030/Pages/NationalTransformationProgram.aspx
[2164] KSA Vision 2030 'Strategic Objectives and Vision Realization Programs' <https://vision2030.gov.sa/sites/default/files/vision/Vision%20Realization%20Programs%20Overview.pdf>
[2165] Franck (1995) 6–9
[2166] Mill (2003 copy)183

because the greatest number of the KSA population are Muslims,[2167] they would be happy about the KSA's current approach toward the trial of cybercrime, because it would be assumed that they are satisfied about their country applying *Sharia.*[2168] Therefore, their assumed happiness might indicate that the KSA's current approach toward the trial of cybercrime might be effective. However, as discussed in Chapter 2, being effective does not suffice because fairness trumps effectiveness.[2169]

Fairness of the criminal procedure of crime in the eyes of the international community is best described as respecting international human rights treaties,[2170] and this is the standard which the KSA's approach toward the trial of cybercrime should be tested upon. One of the most well-known standards of international fairness of trials is the right to a fair trial.[2171] Due to its complexity and the limited scope of this thesis, this section will discuss only basic elements of what constitutes a fair trial in the context of cybercrime in the KSA. The most crucial elements of a fair trial are "public hearing, within a reasonable time, by an independent and impartial court,"[2172] and perhaps the most important of these is the stipulation of an independent and impartial court. As discussed earlier in this Chapter, the CC is a newly established independent court that hears criminal cases, and it does not properly differentiate between cybercrime and NNCs within its circuits.[2173] This would suggest that cybercrime is not heard before judges with the relevant expertise. The CC is dependent only on *Sharia*[2174] which brings a high level of uncertainty. In addition, judges can intervene in the criminal process by reinvestigating cybercrime cases[2175] which gives them an vast amount of

[2167] Alhussein (2019)
[2168] This has been reflected in mainstream nationalism of the KSA. see Alhussein (2019)
[2169] See Subsection 2.4.3
[2170] Franck (1995) 47
[2171] UDHR Article 10.
[2172] Council of Europe, Right for Fair Trial <https://www.coe.int/en/web/impact-convention-human-rights/right-to-a-fair-trial >
[2173] See Section 7.3
[2174] JSL Article 1
[2175] CPL 2013 Articles 161 and 162

power which they could easily abuse. Moreover, the problem is not just the nature of the court itself but also the process, especially in relation to non-disclosure, the exclusion of lawyers and holding secret hearings,[2176] which goes beyond what the KSA is trying to resolve.[2177] Therefore, from an international perspective, it might be said that the KSA's current approach towards the trial of cybercrime fails to meet expected standards.

7.6.2.3 Fairness and effectiveness of the trial of cybercrime from the national perspective

Both national fairness and effectiveness standards derive from compatibility with *Sharia*.[2178] Therefore, if the trial stage of processing cybercrime is to be tested by such standards, this stage would be viewed as fair and effective because it is the most disciplined stage in applying *Sharia* in the process. In addition, the disciplined application of *Sharia* would be apparent in the appointment of judges; they are typically the most proficient graduates from *Sharia* schools around the KSA.[2179] Also, KSA law makes it clear that they are only bound by *Sharia.*[2180] However, the question which arises here is what measurement can be applied to *Sharia* for the trial of cybercrime. There is no clear measurement of such an issue because, since the very beginning of the Islamic era, *Ulema* have disagreed on many legal matters based on their own jurisprudential methodologies and their interpretation of the sources of *Sharia*.[2181] Disagreements of this type continue to the present, and judges in the KSA, including those within the CCJs who look cybercrime cases, utilise *Ijtihad*[2182] which increases the likelihood that legal disagreements will occur. Consequentially, this is one

[2176] CPL 2013 allows for secret trials in Article 155.
[2177] UPR, Saudi Arabia 3rd cycle.
[2178] See Subsections 2.4.1.3 and 2.4.2.3
[2179] Interviews with CCJs CJ 2 and 3
[2180] BLG Article 46 and JSL 2007 Article 1
[2181] Interview with Sharia Expert SE 2
[2182] Interviews with Sharia Experts SE 2 and 3

reason why conflicts arise between judicial judgments, as discussed in Section 7.5. However, neither CCJs nor *Sharia* experts see it as a conflict because they are driven in their perspective by the principle that [disagreement between Ummah is a mercy].[2183] Yet, mercy itself is a broad concept that has caused disagreement about what constitutes mercy. Moreover, in this modern or even late modern era, in places such as the UK, the written law is the ultimate source by which both the official authority and people are restricted,[2184] and knowledge of it is not exclusive to a single class of the population, where the rest of the population cannot easily obtain such knowledge, such as in the case of the KSA. Therefore, it might be possible to say that even from a national perspective, the trial of cybercrime in the KSA might not be as fair and effective as it should be because it does not set out clearly, and in public, its own standards of fairness and effectiveness.

7.7 Conclusion

After putting the final stages of the criminal process under analysis and evaluation, it is concluded that the prosecution and the trial stages of cybercrime in the KSA are both ineffective and unfair in several of their aspects.

In the prosecution stage of cybercrime in the KSA, prosecutorial powers are rarely vested clearly in prosecutors, whether in law or in practice.[2185] This does not mean that no prosecutorial powers are exercised in relation to cybercrime within KSA law and practice, but that prosecution of crimes, including cybercrime, within the KSA's jurisdiction is not respected because in both the KSA law and practice the institution of the PP and the function of prosecutor are taken over by detectives of the PP.[2186] These issues have been fully addressed in Sections 7.2 and 7.3, but what has not been discussed is how the KSA should

[2183] Interview with Sharia Expert SE1
[2184] Klosko (2019) 16
[2185] See Subsections 7.2.2 and 7.3.2
[2186] *Ibid*

reform to overcome such issues. First, the KSA should not have changed the name of the institution from the BIPP to the PP because the former name identifies the existence of the detectives within the institution, while the changed name masks their existence, despite being the PP's dominant function. Second, the KSA should have at least regulated the function of the prosecutors and transferred the prosecutorial powers from the detectives to the prosecutors, who are more deserving of it. Third, if the KSA did not intend to change its current approach toward the prosecution of crime, including cybercrime, it should hire private criminal defence lawyers who possess more knowledge over criminal cases and are driven by accomplishing higher economic status and motivated by achieving solid professional reputation. In England and Wales, prosecution used to be conducted by private barristers hired by the police, but, after the UK established the CPS, prosecution became vested in a public entity[2187] as a result of the Royal Commission on Criminal Procedure (RCCP) recommendations in 1981.[2188] The RCCP recommendation to separate prosecution from investigation was based on grounds of fairness, openness, and accountability.[2189] However, due its previous experience of hiring private barristers, the prosecution in England and Wales still hires private barristers to represent it in court in serious cases.[2190] Thus, it might be suggested that the KSA should consider the value of an independent prosecution system and also should seek to draw upon expertise, whether in the public or private legal sectors.[2191] However, there is no guarantee of achieving fairness, and constant change can undermine the official internalisation of new ideas.[2192]

[2187] MacDonald (2008) 10
[2188] Munday (1981) 195 and 196
[2189] *Ibid* 193
[2190] MacDonald (2008) 15
[2191] Here are the rules by which the CPS decides whether to have an in house lawyer or an external lawyer. <https://www.cps.gov.uk/legal-guidance/advocates-selec>
[2192] Interview with Law Professor LP2

In the trial stage of cybercrime in the KSA, the right for a fair trial is recognised within KSA law,[2193] but just because it exists in theory within the legislature, it does not mean it is ensured in practice or by other legal provisions within the KSA. Generally, the trial of cybercrime in the KSA is governed by the authority of *Sharia* even though *Sharia* itself has nothing direct to say about cyberspace where such crimes are committed. This does not suggest that the KSA should relinquish *Sharia* as a basis for its legal system, but it should not use *Sharia* as the ultimate governing tool over matters that are based on modern technologies. Having *Sharia* to be the only standard of fairness and effectiveness for the trial of cybercrime has resulted in continuous undesired results – even from a *Sharia* perspective, as the current approach of the KSA toward the trial of cybercrime may contradict *Sharia.* For example, one contradiction between *Sharia* and the KSA's approach toward the trial of cybercrime is that *Sharia* insists on individuals' right to privacy, yet CCJS in the KSA continue to approve cyber evidence that has been obtained by brazenly violating the privacy of suspects. It could be assumed that CCJs will continue to violate international human rights in the KSA due to their lack of knowledge about criminal law, especially when it comes to cybercrime. One reason for such an assumption is the lack of commitment to international human rights – shown above all, by the failure to ratify the ICCPR.[2194] It even refused to sign the UDHR, but it is arguably binding anyway.[2195] Another reason is that CCJs lack the appropriate training on cybercrime. This lack of training seems to be apparent in their judgment reasoning which has less to do with cybercrime, cyberspace and cyber evidence and has more to do with *Sharia,* in which they are experts. Applying *Sharia* over cybercrime in terms of classes of punishment has resulted in more confusion and maintains the lack of differentiation between NCCs from cybercrime. This lack of differentiation might be the fault of CCJs who keep

[2193] BLG articles 26 and 47
[2194] Meral (2009) 876-886
[2195] Alwasil (2010) 1072-1091

ignoring the specific issues of cybercrime and insist on applying general *Sharia* principles which reflect their training. Moreover, the CCJs practice extensive power over criminal cases, including those related to cybercrime, as they can play the role of supervisors over PP members by reinvestigating their cases and dismissing what is found by the PP. This might cause the PP members to put less effort into criminal cases, as they may feel their work is not respected by the CCJs, and this would negatively affect the overall effectiveness and fairness of the KSA's approach toward the criminal process of cybercrime. Therefore, if the KSA wants to be fairer and more effective in its approach toward the criminal process of cybercrime, it should make more relevant its sources of law and governance; otherwise, it cannot move toward a more effective and fairer approach.

According to the Model Code created in Chapter 4, the KSA must do more to develop an effective and fair approach towards prosecution and trials of cybercrime. Prosecutorial powers to deal with cybercrime are not detailed and specialised at a functional level. Similarly, special evidential rules for cybercrime and process rules for cybercrime in court are not mentioned in the law. Moreover, at the institutional level, there are no specialised trained prosecutors to deal with prosecuting cybercrime, and no special courts or judges exist to deal with the trial of cybercrime. Once again, treating cybercrime as indistinct from NCCs and insisting on relying only on *Sharia* in terms of procedure in the KSA are key factors which have led to such inefficacy and unfairness.

Chapter 8

Conclusion

8.1 Thesis summary

The criminal process relating to cybercrime can be considered as related to a late modern phenomenon (cyberspace) which falls mainly under the control of private and non-profit organisations.[2196] This private ownership of the internet has been addressed in Chapter 2 and has resulted in diminished national and international state-based control over the internet. Thus, sovereign states struggle to regulate the use of the internet, especially when it comes to crimes committed in this space (cybercrimes).[2197] Moreover, the struggle relates to both the substantive and the procedural aspects of criminality, the latter being the main focus of this thesis. Additionally, the difficulties relating to the private control of cyberspace give rise to the need for various new types of expertise and collaborative arrangements, some of which the KSA does not possess.

The KSA is neither an industrialised country, nor can it be called a developed country. On the whole, it is better to categorise the Kingdom as a pre-modern state, which means that it struggles to deal fairly and effectively with issues that arise from late modernity. Thus, it is no surprise that the KSA must import experts from developed countries such as the US[2198] to deal with technological issues related to cyberspace, such as cybersecurity and cyberattacks against the country. However, when it comes to issues which are more closely related to aspects of national sovereignty and security, such as the criminal

[2196] See Subsection 2.2.1
[2197] *Ibid*
[2198] Interview with LP1

procedure of cybercrime, the KSA prefers to retain more control and so deals with the issue as it would NCCs. This approach tends to be ineffective, because there is a lack of expertise and suitable mechanisms being utilised for dealing with cybercrime and cyber evidence.[2199] Although universities in the KSA teach cybersecurity, they do not teach cybercrime or cyber law, which hampers reform of the overall outdated approach of the KSA toward cybercrime.[2200]

Furthermore, major institutions that are directly involved within the criminal procedure of cybercrime, such as the PF, the PP and the CC, also lack expertise and training on cybercrime and cyber evidence.[2201] This lack of expertise indicates that cybercrime and related criminal procedures are tackled using inadequate legal tools, such as those that are found in *Sharia*,[2202] which has also been misinterpreted and waywardly implemented within the KSA legal system.[2203] Therefore, the false interpretation and application of the pre-modern instrument, *Sharia,* is being pitted against the late modern phenomena of cyberspace. Not surprisingly, such pre-modern tools have proven to be not very effective (or fair) in the face of late-modern criminal activity such as cybercrime.

The KSA's response to the late modern phenomenon is perhaps predictable for a country whose main law of the land is primarily a pre-modern doctrine inspired by *Sharia*. As tested in Chapter 4,[2204] even though *Sharia* does not address issues of late modernity, it carries within its principles that could, to some extent, enable the KSA to deal efficiently and fairly with late modern issues, such as the criminal procedure of cybercrime, if applied correctly, such as through the principle of *Al Shura* (not the KSA version of the

[2199] See Subsection 2.2.1
[2200] See 2.2.3
[2201] See 5.3.2, 6.3.2, 7.3.2, and 7.5.2
[2202] BLG Articles 1 and 7.
[2203] See 4.5
[2204] See 4.4.1 and 4.4.2

institution).[2205] However, Chapter 4 found that the KSA does not sufficiently adopt those principles in practice,[2206] leading to an ineffective and unfair approach toward the criminal procedure as it relates to cybercrime.

The criminal procedure of cybercrime in the KSA consists of four major stages: policing, investigation, prosecution and trial, all of which have been found to be ineffective and unfair according to both conceptual and international (comparative) standards, except for the trial stage that, while it has been found to be effective on the surface, is also deeply unjust.[2207] When compared to national standards, all stages were initially found to be fair and effective on the surface, but when delving deeper, the four stages were found to be less fair and effective than desired by the KSA, which is especially evident at the trial stage.[2208]

While the KSA is in the process of moving toward modernity and even late modernity through the country's reform project *Vision 2030,* many false applications of *Sharia* were identified, some of which were abolished as a result of the Ministry of Justice's contribution to Crown Prince Mohammed Bin Salman's *Vision 2030,* such as: the abolition of *Ta'zir be Alshubhah* in 2019,[2209] the promising approval of dismissing some cybercrime cases based on procedural errors,[2210] and the abolition of lashing as a form of punishment.[2211] Crown Prince Mohammed Bin Salman has proposed to reform many laws including the CPL[2212] which could result in the establishment of a more effective and fair approach toward the criminal process of cybercrime. One cannot ignore the enormous positive legal and social changes implemented under his leadership which contributes to the optimism that the KSA will eventually change its approach toward the criminal procedure of cybercrime.

[2205] See 4.3.2
[2206] See 4.4
[2207] See 5.4.2, 6.4.2, 7.6.1, and 7.6.2
[2208] See 7.6.2
[2209] SPA (2019)
[2210] See analysis of the six cybercrime cases in 7.5.3
[2211] Supreme Judicial Council Order No 1492/T Dated 25/09/1441 Ah (18/05/2020)
[2212] See discussion in 7.1

8.2 Findings and recommendations

This section addresses how the thesis has met the aims and objectives that were drawn in Chapter 1.[2213] In other words, this section reprises the main findings of this thesis, especially those presented in the key Chapters 4, 5, 6 and 7. In addition, it discusses possible recommendations as they relate directly to findings. Moreover, although Chapter 2 illustrated the background and context of the research topic, it carries within it some crucial elements that help in achieving the aims and objectives of this thesis. Similarly, Chapter 3 discusses methodologies employed in this thesis, so an assessment of whether those methods were successful, especially the fieldwork, will be made in this section. Then, in the Table 8.2.1, a schedule of findings will briefly summarise what has been addressed in this section.

It is the overall aim of the thesis to evaluate cyberspace as a phenomenon in the KSA, and to assess how the KSA deals with issues surrounding cyberspace. Then the focus is narrowed down to the criminal procedure of cybercrime. Before delving into the findings of key chapters, it should be said that all key chapters are dependent on the methodologies discussed in Chapter 3 which were initially introduced in Chapter 1. Therefore, it is possible to say that without those methods, the key chapters would not have been able to effectively glean results from the data, especially in regard to the fieldwork method which involved conducting interviews with elite Saudi experts who possess knowledge regarding the criminal procedure of cybercrime. Due to the lack of written publications in regard to the discussed subject, the interviews can be considered a success, especially when it comes to the question of how the criminal procedure of cybercrime works in practice. Moreover, other methods were helpful to the thesis, especially doctrinal analysis and policy transfer which provided better approaches and practices adopted by the UK which pointed to what the KSA should do

[2213] See 1.2.1 and 1.2.2

in the future to be more effective and fairer. Despite their help to the thesis, there have been some limitations, which will be covered in Section 8.4.

As addressed throughout this thesis, especially in Chapters 4, 5, 6 and 7, where a considerable amount of data has been derived from interviews in order to enrich the very limited literature on the KSA's approach to the criminal procedure of cybercrime, the KSA has a less effective and fair approach when comparing it the UK for the purpose of policy transfer. Yet, most interviewees initially disagreed with this verdict because they viewed the KSA's approach to be fair and effective in general.[2214] It is important to mention that the researcher had to explain to them what is meant by "effectiveness" and "fairness" during each interview, leading some to change of their initial opinions,[2215] as they did not have any measurement of fairness and effectiveness except for the mainstream political measurement which is in essence not to oppose the government.[2216] Nonetheless, some stuck to their opinions, arguing that the distinction here is about what is *Haram* (prohibited) and what is *Halal* (permitted).[2217]

Those two measurements, which are *Sharia*-based, are mainly aimed at correcting one's own behaviour and eradicating immorality to ensure compliance with the teachings of *Quran* and *Sunnah.*[2218] Those measurements might be valid in the early era of the establishment of the KSA, when there was almost no modern legislation,[2219] and so people followed religious authorities because the *Ulema* were in control of the minds of the populace and would spread the idea that modern law is Satanic and based on infidelity to religious

[2214] 20 interviewees found the KSA approach to be fair and effective
[2215] 7 interviewees out of the 20 who found the KSA approach to be fair and effective have changed their initial opinion
[2216] It was common with all interviews conducted that interviewees would say some respectful words to the government of the KSA and repeatedly express that they do not oppose it.
[2217] See discussion in 4.4.1.2
[2218] See discussion about national measurements of effectiveness in 2.4.2.3
[2219] Alrasheed (2002)

authority[2220] and, therefore, not to be obeyed.[2221] However, since that time, the KSA has passed hundreds of pieces of legislation,[2222] including the BLG which states that all legislation must be in line with *Sharia*,[2223] so it is no wonder why those measurements of *Halal* and *Haram* are the first to come to mind in this context. Yet, such measurements are broadly interpreted and easily misused, because there is a great variation in how they are applied by the religious authorities.

Although the measurements of fairness and effectiveness varied within the fieldwork interviews, the fieldwork was fruitful in regard to the assessment of the KSA's approach to the criminal procedure of cybercrime, as it revealed the practical aspects of the KSA's approach. In other words, the interviews were crucial in ascertaining how the KSA's criminal procedure regarding cybercrime works in practice, which is not discussed in the literature or in official government reports in any depth. Moreover, some interviews suggested interesting solutions to reform the KSA's criminal justice system with a direct link to the criminal procedure of crimes (including cybercrime).

One suggestion regarding the PF was to apply moral codes inspired by *Sharia* against spying on people, especially in the absence of written rules.[2224] Thus, it seems that some police officers do not want to abuse their power even though the law is silent about restraints. Another idea was to not allow the dismissal of cybercrime cases based on procedural error so as to stop suspects escaping justice.[2225] Additionally, it has been proposed that the PF should be more transparent in regard to their work.[2226] Another thought was to update the CPL to

[2220] *Ibid*
[2221] Almibrad et al (2015) 13
[2222] Shalhoob (1999) 62
[2223] BLG Articles 1 and 7
[2224] See 5.2.3 and 5.3.2
[2225] 5.3.2.1.1
[2226] 5.5.1

include policing aspects[2227] and it was also suggested to draw lines for the PF's intervention.[2228]

In regard to the PP, it was suggested that lawyers should be available or even present during investigation and that people should know the importance of accessing legal counsel. It was further suggested that prosecution officers should be private not public, because the current PP is ineffective. Moreover, one participant posited that the PP investigation should not be subject to investigation by the CC. Finally, one suggestion was to create an investigation department specifically for cybercrime and to not vest it in the AHC.

One important suggestion regarding the CC was to codify *Sharia* to limit the CCJs' scope for *Ijtihad.* Another suggestion was to train CCJs to deal with cybercrime, and it was suggested that CCJs should also be law graduates not just *Sharia* experts. Also, it has been suggested that CCJs powers should be limited, and it was repeatedly suggested that CCJs should not reinvestigate cybercrime cases and that the law should prevent them from doing so.

Alongside some of interviewees' foregoing suggestions, the UK has dealt more effectively and fairly with the criminal procedure of cybercrime, especially regarding the investigation of cybercrime at the legal, institutional, and operational levels, as Chapters 4, 5, 6 and 7 indicate, especially after comparing it to the KSA in terms of the standards of fairness and effectiveness set out in Chapter 2. Therefore, the KSA should consider and learn from the more explicit and comprehensive approach of the UK when making reforms related to the criminal procedure of cybercrime.[2229] The suggestions for policy transfer have been discussed in Chapters 4, 5, 6 and 7, and the most worthwhile ideas are indicated in the next paragraph.

[2227] 5.5.1
[2228] 5.5.1
[2229] See 3.3

One crucial lesson is that the UK policy and law has accounted for the differences between physical space and cyberspace, resulting in the differentiation between the criminal investigation of NNC (which is mainly the province of PACE) and that of cybercrime. Thus, it passed the Regulation of Investigatory Powers Act 2000 and then the IPA 2016 as extensive and sophisticated legal responses to the criminal investigation of cybercrime.[2230] Another lesson that can be learned is that the human right of privacy is better protected within the UK's jurisdiction than it is in the KSA, especially in regard to surveillance within cyberspace as an operational power, and the UK State is restricted by the IPA from disproportionate spying on citizens. This is accompanied by respect for, and protection of, all international human rights, especially those related to the criminal procedure, such as due process.[2231] The KSA could learn this lesson from the UK by restricting itself and fully joining international human rights treaties such as the UDHR and ICCPR unreservedly as a first reformative step toward establishing fairness within its legal system, because the other reformative steps are dependent on this one.

8.2.1 Key findings of each chapter

Chapter 2 finds that the KSA has struggled to regulate the use of cyberspace (including the Internet) since it allowed the public access to it in late 1990s.[2232] One apparent reason for this is that cyberspace is a product of late modernity, and the KSA desires to regulate its use by depending on a legal system that is gives ultimate supremacy entirely to pre-modern traditions over modern laws. This supremacy of *Sharia* has resulted in limiting the use of the Internet within its jurisdiction based on what *Sharia* allows or as discussed in Chapter 4, on how the *Ulema* of the KSA interpret the *Sharia.* For instance, the KSA blocks

[2230] See discussion in 4.5
[2231] See 5.5.2
[2232] See 2.2.1

pornographic websites and considers accessing them to be a cybercrime that is punishable by imprisonment and/or fines.[2233] The employment of *Sharia* within the KSA's legal system and its troubling consequences for the overall response of the KSA to cyberspace in general, and cybercrime in particular – especially in terms of criminal procedure of such crimes – is problematic simply because the sources of *Sharia* have nothing to say directly about cyberspace. Therefore, the enforced projection of pre-modern *Sharia* has resulted in the KSA's response to the late-modern phenomena of cybercrime in terms of procedure being neither effective nor fair.

Therefore, in regard to the same main aim of this thesis (in other words, to evaluate the KSA's general response to the criminal procedure of cybercrime by setting out measurements of fairness and effectiveness along with the possibility of policy transfer as objectives of this thesis), this thesis has revealed that the KSA has struggled to cope with late-modern, or even modern, issues related to the criminal procedure of cybercrime. In Chapter 4, a Model Code of the KSA's response to the criminal procedure of cybercrime was proposed to discuss what the KSA has done and what remains to be done about it.[2234] Although the KSA has recognised such struggles, its approach to the criminal process of cybercrime might be considered to be both ineffective and unfair, especially in relation to international standards of human rights and in comparison to the UK's response, as discussed in Chapters 5, 6 and 7 in much greater detail. The KSA claims to protect human rights in its BLG in accordance with *Sharia*, yet it has not specified what human rights it protects, especially in regard to individual interests to privacy and free speech.

Besides revealing that the KSA's approach to criminal procedure is often ineffective and unfair due to the incompatibility with international and comparative standards of fairness

[2233] In chapter 7, various cybercrime cases were addressed as CCJs convicted the accessed. See 7.5.3
[2234] See 4.6

and effectiveness, this thesis has found that the KSA treats cybercrime as being indistinct from NCCs or traditional crimes in terms of its criminal procedure. This lack of differentiation is another reason for the state's ineffective and unfair approach to the criminal procedure of cybercrime, as discussed in Chapters 5, 6 and 7. On the other hand, the UK seems to better protect human rights in relation to cybercrime, both in terms of substance or procedure.[2235] Also, as a late-modern state, the UK has actively differentiated between both types of crime and acted according to the distinctions, resulting in a more effective and fairer approach to the criminal process of cybercrime.

As an objective to the discussed aim, policy transfer from the more effective and fairer response of the UK could be one solution to this problem. One common ground to base policy transfer on is respecting international human rights as a whole and not picking and choosing those rights that satisfy the sociocultural background of the KSA. Another common ground is that the KSA should pay more respect to the rule of law, including the demands of certainty in law, and not just the rule of *Sharia*. Indeed, the KSA, as represented by government officials who are involved in the criminal procedure of cybercrime, too often use the *Sharia* as an excuse to violate international human rights and claim that the international community must respect all personal or common beliefs. However, even if the international community has endorsed such an excuse in reservations issued by the KSA when signing international instruments, or even refusals to ratify such as CEDAW and the ICCPR, with time it has become even more sceptical of the ability of *Sharia* as practiced by the KSA to protect human rights.[2236] Therefore, the KSA should learn from the UK and give more respect to the international community's values, such as international human rights in order to enhance the fairness of its criminal procedure. Moreover, one common ground to base the

[2235] See 4.5
[2236] Amnesty International report 2020/2021, 310-312
<https://reliefweb.int/sites/reliefweb.int/files/resources/POL1032022021ENGLISH.PDF >

transfer on is to differentiate between the criminal procedure of cybercrime and NCCs, especially in terms of evidence, jurisdiction, and human rights, which the UK has done and is therefore dealing with cybercrime in a better way than the KSA. Another common ground to base the transfer on is increasing expertise by professionally training officials involved with the criminal procedure of cybercrime. It is not a difficult task for a rich county that has the required financial resources for such professional training. Another common ground to base the transfer on is allowing for some space for constructive criticism that might help improving the current response, which will probably be best done by respecting the international human right for free speech. Finally, the UK continually updates its strategic plans to combat cybercrime and related issues, so the KSA should learn that it is important to have an updated detailed plan that directs the country's legal system towards effective processes and, ultimately, outcomes.

Another main aim of this thesis is to evaluate the role of *Sharia* in regard to the criminal procedure of cybercrime and whether it is fair and effective to rely on pre-modern traditions when tackling cybercrime procedurally. The objectives here are to test whether *Sharia*, as applied in the KSA, is fair and effective by applying the standards of fairness and effectiveness which have been set out in Chapter 2. For this aim and objective, Chapters 4, 5, 6 and 7 find that the faulty application of *Sharia* has resulted in the fragmentation of the law in practice, leading to complexity and obscurity of the KSA's legal system as a whole. Consequently, it has complicated the criminal procedure of cybercrime, especially in regard to the investigation and trial stages, where both of their personnel exercise extensive judicial and investigatory powers. This outcome threatens the international human rights of due process, privacy and fair trial. However, Chapter 4 finds that *Sharia* does encompass some pertinent effective and fair principles, such as *Shura* and *Azel Alhakim* which are either

ignored or misrepresented in the KSA, resulting in an overall ineffective and unjust response to the criminal procedure of cybercrime.

Next, Chapter 5 finds that the role of the KSA police force is less effective and fair than the UK's police force, since it is not compatible with the measurements of fairness and effectiveness set out in Chapter 2. The KSA's police force's involvement in the criminal procedure of cybercrime is only briefly mentioned in the CPL 2013, resulting in the policing of cybercrime being undertaken based on individual officer's personal ethical codes and haphazard direct orders from higher officers. This failing has led to arbitrary arrests, violations of human rights of due process and privacy in particular. Even though some police officers might not breach such rights due to their self-discipline, which is inspired from the teachings of *Sharia,* that is not the general position, because they might act out of good conscience and not out of obedience to the law, which has less to say about due process, privacy, and human rights in general.[2237]

Moving on to the next stage of the criminal process, Chapter 6 finds that the investigation of cybercrime is performed by detectives from the PP who have multiple functions and extensive investigatory powers. The functions of detectives have been examined, and it is revealed that they have multiple functions as PCIOs, detectives and prosecutors, resulting in them having extensive powers which they have been found to abuse. Although detectives were often well trained for NCCs, they have not been trained to deal with cybercrime which leads to mistakes, some of which are not corrected. However, some of those mistakes were corrected by personal effort by applying moral codes inspired by *Sharia,* such as not spying on people. However, this uncertainty in delivery has led to the abuse of

[2237] see 5.5.2

such functions and powers resulting in an ineffective and unfair approach to the criminal procedure of cybercrime in the KSA.[2238]

Finally, Chapter 7 reveals that the role of prosecutors in the KSA is confusing as they are tentatively involved within the process and their function has been taken over by detectives. However, when comparing the situation to the UK, the prosecutors have a crucial role in the process. The prosecutor's role is crucial because they are the main protectors of the public interests and may be called "ministers of justice". However, it might be observed that the prosecutor functions well in democratic systems because they represent the public in the courtrooms and in the criminal process as a whole. However, in non-democratic systems such as the KSA, the prosecutor tends to defend the government's interests, rather than that of the public because there is no democratic accountability in the KSA in almost all matters, including those related to crime.[2239]

Chapter 7 also finds that CCJs have been well-trained in regard to *Sharia*, yet they are less trained and less aware of matters concerning the criminal procedure of cybercrime. Thus, they find themselves applying provisions of *Sharia* on a late-modern issue that lies beyond their comprehension, which has resulted in significant violations of human rights and a breach of the concept of fairness as they continually abuse the extensive judicial powers afforded to them by legislation which they in any event consider themselves to be above.[2240]

Therefore, it can be said that in accordance with the proposed Model Code in Chapter 4,[2241] gaps that are found between practice and the proposals are located at both institutional and operational levels in all four stages of the criminal procedure of cybercrime in the KSA, especially regarding training and expertise.

[2238] See 6.4.2
[2239] See 7.2.1 and 7.3.1
[2240] See 7.6.2.2
[2241] See 4.7

For the future, using the KSA policy statement *Vision 2030* as a tool to judge reforms of the criminal justice system regarding cybercrimes, the thesis finds that there has been considerable and constant fair changes and reforms implemented by the KSA authorities throughout the past few decades in regard to criminal process, such as the establishment of the PP in 1986,[2242] separating prosecution from the police in 1989,[2243] issuing the first CPL in 2001, and modifying the law in 2013.[2244] Moreover, in compliance with *Vision 2030*, there have been some further changes implemented by the MoJ and the SJC, such as abolishing punishment by lashing in 2020[2245] and abolishing *Ta'zir be Alshubhah* in 2019.[2246]

8.2.2 Recommendations

As the thesis finds that the KSA's responses to the criminal procedure of cybercrime are neither effective nor fair when comparing them to the standards of fairness and effectiveness set out in Chapter 2, various reforms and solutions to the current approach are recommended. Thus, as the KSA seeks to progress toward becoming a modern or even late modern state, it should consider that one aspect of modernity must be to let go of pre-modern traditions and replace them with modern norms, including being informed by technology.

Cyberspace is a product of the development of science technology and is certainly not addressed in pre-modern traditions. The KSA keeps claiming that it puts *Sharia* over legislation and considers it to be a supreme law of the land which has affected all aspects of life, including in the way the state deals with late-modern science and technology. Moreover, *Sharia* experts in the KSA often oppose certain aspects of science for the reason that they

[2242] See 7.2.1
[2243] *Ibid*
[2244] See 4.4.1
[2245] Supreme Judicial Council Order No 1492/T Dated 25/09/1441 Ah (18/05/2020)
[2246] SPA (2019)

lead to atheism.[2247] Experts with such attitudes were in control of the mainstream ideology of the KSA population until 2016 when the KSA *Vision 2030* was announced.[2248] Thus, now is a golden opportunity for the KSA to try to modify the provisions of Article 1 of the BLG to depend less on *Sharia,* considering it as a main source of legislation but not the constitution of the KSA itself. Such a modification would put the KSA firmly on the path of modernising the country as it would be less obligated to the restrictions of ambiguous conceptions and interpretations of the *Sharia.* This kind of reform would then contribute to solving issues related to the criminal procedure of cybercrime, such as the codification of *Sharia,* protection of human rights (as modern law suggests) and on the promotion of legislation that is more precise, unambiguous and clear.

Moreover, academic legal institutions should consider teaching cybercrime and cyberlaw to spread awareness of the issues related to cyberspace and the law. Not only should academic legal institutions begin to tackle the issue of cyberspace and cybercrime, but so too should governmental institutions, especially those involved in the criminal procedure of cybercrime, such as the police, the PP and the CC. In particular, they should consider the differentiation between NCCs and cybercrime in terms of procedure. Moreover, since most of the issues related the KSA's approach to the criminal procedure of cybercrime are related to the absence of legislation that covers those issues, KSA lawmakers should consider passing legislation akin to the UK's RIPA and ISA 2016 that covers the relevant aspects of the criminal procedure of cybercrime within the KSA; or at least they should consider making reforms to the current CPL to cover issues of cybercrime criminal procedure.

Furthermore, as suggested in the findings section of this chapter, police officers, members of the PP, and CCJs should go through intensive training that makes them more fit

[2247] Alawaji (2016)
[2248] KSA Vison 2030 <https://www.vision2030.gov.sa/v2030/overview/>

to deal with the criminal process of cybercrime, because this thesis finds most of them lack the appropriate training to deal with it. Moreover, the policy transfer method of this thesis suggests, after thorough analysis, that the main issue related to the unfairness of the KSA's approach to the criminal procedure of cybercrime is a lack of protection for human rights. Hence, the KSA should consider joining major human rights treaties such as UDHR and ICCPR, which should be reflected in their domestic legislation by passing provisions that specifies what the human rights are that the KSA should protect.

As addressed earlier in this subsection, *Vision 2030* is a crucial reform instrument which has led to extensive and positive changes within the KSA, and it has already reformed some aspects of criminal procedure by urging governmental institutions to contribute to making reforms. Thus, governmental institutions such as the Ministry of Justice and the SJC should consider a joint committee to reform the current approach to the criminal procedure of cybercrime

However, even though some reforms have been implemented, there remains room for improvement, as observed by the international community.[2249] A lack of transparency is one reason why such reforms have not been very effective to date. For instance, only 6 cybercrime cases out of hundreds have been officially published by the KSA's Ministry of Justice.[2250] Moreover, publication of those cases is limited to information about the trial stages only, and there is no official publication of previous stages, either by the police or the PP, which makes it difficult for researchers and for oversight in the public interest in general. Although this thesis employs the qualitative method of conducting interviews with elite Saudi experts, there was also a lack of transparency noticed during the fieldwork, which could be due to the interviewees' own political and cultural views and criticisms of the KSA approach.

[2249] UPR, Saudi Arabia 3rd cycle, Summary of stakeholders' information. 2018. <https://www.ohchr.org/EN/HRBodies/UPR/Pages/SAindex.aspx>
[2250] See 7.5

Thus, their lack of transparency is not an alien to the political and cultural norms of the KSA society in whole. Therefore, it can be possible to say that transparency is an important element that must be addressed in the process of making reforms.

8.2.3 Schedule of findings and recommendations

Chapter	Problems	Suggested solutions	Proposal based on Model Code
Chapter 2	(1) Non-differentiation between cybercrime and NCCs in terms of process. (2) Dependence on the premodern *Sharia* to face late modern phenomena.	(1) Be aware of differentiations and apply them to law and practice. (2) Letting go of dependence only on pre-modern traditions.	Not included in Model Code.
Chapter 4	Whether *Sharia* has the ability to regulate and produce fair and effective laws.	(1) Appling principles within *Sharia* correctly. (2) Codify *Sharia*.	Not included in Model Code.
Chapter 5	(1) Policing cybercrime is indistinct from Policing NCCs. (2) Policing Powers are not clear. (3) Lack of legal safeguards for policing powers. (4) Not clear what the policing institutions are. (5) Cybercrime units are fragmented and ambiguous. (6) PF are not trained to deal with cybercrime. (7) PF personnel function as PCIOs.	(1) Include detailed policing powers. (2) Specify institutions and policing powers to deal with cybercrime. (3) Train PF officers to dear with cybercrime. (4) Change the policing investigation to initial rather than preliminary because it is under the supervision of the PP.	(1) Functional level: detailed and specialised powers to deal with the Policing of cybercrime. (2) Institutional level: specialised trained PF officers to deal with policing cybercrime.
Chapter 6	(1) Investigation of cybercrime is indistinct from investigation NCCs. (2) Investigation powers lack safeguards. (3) Detectives have multiple functions, and extensive reach. (4) Detectives are not trained well to	(1) Train detectives to deal with cybercrime. (2) Separate investigation from prosecution. (3) Limit detectives' powers. (4) Vest investigation of cybercrime in a specialised department rather than	(1) Functional level: detailed and specialised powers to deal with the investigation of cybercrime. (2) Institutional level: specialised trained detectives to deal with investigating cybercrime.

	deal with cybercrime. (5) Cybercrimes are investigated in the PP as honour crimes.	the Anti-Honour Crime department.	
Chapter 7	(1) Prosecution is not properly practiced in the KSA. (2) Prosecutors function as detectives. (3) Production function is overstepped on by detectives. (4) Prosecution does not differentiate between cybercrime or NCCs. (5) Prosecutors are not trained to deal with cybercrime.	(1) Train prosecutors to deal with prosecution of cybercrime. (2) Separate prosecution from investigation. (3) Detail prosecution function in law. (4) Activate private prosecutors.	(1) Functional level: detailed and specialised prosecutorial powers to deal with cybercrime. (2) Institutional level: specialised trained prosecutors to deal with prosecuting cybercrime.
	(1) CCJs do not differentiate between cybercrime and NCCs. (2) CC is exclusively governed by *Sharia.* (3) CCJs main preference is *Sharia* not law and *Sharia* driven powers such as *Ijtihad.* (4) CCJs are only Sharia graduate not law graduate. (5) CCJs are not trained to deal with cybercrime. (6) CCJs have both judicial and investigatory powers.	(1) Train CCJs to deal with cybercrime. (2) Limit judicial powers and abolish current investigatory powers and the power of *Ijtihad.* (3) Appoint law graduates as CCJs. (4) Codify *Sharia* and enhance the rule of law.	(1) Functional level: special evidential rules for cybercrime. and process rules for cybercrime in court. (2) Institutional level: special court and judges.

8.3 Originality

As asserted in Chapter 1 of this thesis, the KSA's approach to the criminal procedure of cybercrime has not previously been investigated in detail, especially in terms of fairness and effectiveness, or empirically, or through policy transfer. Thus, the originality of this work is claimed on these bases.[2251] In general, there is previous research that covers particular aspects of the KSA criminal procedure of crime.[2252] However, none of those works have addressed cybercrime in depth. Moreover, they do not investigate aspects of fairness and effectiveness of the KSA criminal procedure in general, and cybercrime in particular. Therefore, it is possible to say that the claim of originality has been met in this thesis in terms of substantive coverage, and especially in terms of the methodology utilised, which is comprised of fieldwork and policy transfer.

In regard to substantive coverage, the thesis has avoided areas of research that have been covered in other research studies, unless crucial to the presented arguments. For instance, the thesis avoided extensive explanation of the Articles about cybercrimes contained in the main legislation addressed in the thesis, particularly BLG and CPL, because they have been extensively covered in other studies.[2253] Yet, some Articles that are related to the criminal procedure of cybercrime were cited as they are to be considered to be crucial to the KSA's approach to the criminal procedure of cybercrime in general. Explanations of those Articles were made exclusively in light of the main aims and objectives of this thesis which are not addressed by other studies.

Also, in regard to methodology, even though some studies compared KSA practice and legislation with other jurisdictions or with international law,[2254] none have compared it

[2251] See 1.4
[2252] *Ibid*
[2253] See 1.4 and 1.5
[2254] *Ibid*

with the UK's jurisdiction in light of the criminal process of cybercrime for the purposes of policy transfer. Thus, this thesis has met its claim of originality because it has referred to the UK jurisdiction for the purpose of the objectives regarding how the UK performs better than the KSA, what lessons can be learned from the UK, and what common grounds there are to base such transfer on.

Moreover, conducting fieldwork interviews is a very uncommon method in legal research related to the KSA, as most legal research related to the KSA aims to explain doctrinally, while some make analysis based on *Sharia* and other familiar jurisdictions, such as Egypt. Yet, none have used interviews to investigate the criminal procedure of cybercrime or crimes in general. Most legal studies related the KSA are not socio-legal in nature, so this socio-legal thesis can claim originality.

8.4 Limitations

There are several limitations to this thesis affecting both methodology and substance. The next two subheadings will address both limitations. Before addressing these limitations, it should be understood that most limitations share one common reason which is the time limit imposed for PhD study.

8.4.1 Methodology limitations

One methodology limitation of this thesis is that it lacks quantitative data. Statistics are a crucial instrument of analysis but, as there are no published official statistics published by the KSA authority, so the researcher was unable to inform his research with such data sources. As pointed out in the findings section (Section 8.2), the KSA does not much practice official transparency, which is perhaps a product of the social norms in the country, where society is generally characterised as being authoritarian.

Next, even though the researcher manged to obtain a considerable amount of literature related to the subject matter, there is a noticeable lack of literature related to the criminal process of cybercrime or even crimes in the KSA. This deficiency was addressed to some extent by comparing Saudi sources with the sources on the same issues in the UK where the literature about the KSA tends to be more critical.

Another methodology limitation of this thesis, affecting the fieldwork, has been the result of the spread of Covid-19, especially during 2020 and the first half of 2021, and the subsequent difficulties it has presented, such as closing borders and educational institutions which the researcher planned to visit, especially those located in the KSA and Egypt. Moreover, there were some restrictions put on educational institutions in the UK where the researcher spent his time during most of those years. The temporary lockdown in the UK led the researcher to rely more on the available online resources, rather than depending on documentary materials that are located physically in the temporarily closed educational institutions.

Despite the Covid-19 pandemic, the researcher managed to conduct 34 interviews with Saudi elite experts on the subject matter, though only 21 interviews were beneficial to the thesis. Due to the spread of Covid-19, 32 interviews were conducted online, and only 2 interviews were conducted face-to-face during the researcher's brief visit to the KSA in 2021. At the beginning of the fieldwork process in cyberspace, most interviewees seem to be enthused, but with online communication, they became less enthusiastic and answered questions very briefly, often changing the meeting dates which made the process challenging.

Even though the interviewees possessed expertise on the subject matter due to their direct involvement in the field of cybercrime and criminal procedure, most of them were very brief in their answers, especially when it came to questions on fairness and effectiveness. Since the researcher has come from a similar environment to them, he perceived that they

were being careful to try show respect to the government and be uncritical. However, as the researcher was also concerned to show the government the same respect as them, the questions were sensitive and asked in a way that it is not inherently critical to the KSA's authorities but involved plenty of open questions. Nevertheless, some interviewees were very careful about the way they answered the questions, even though their knowledge could contribute to reforming the KSA's criminal justice system, especially the criminal process of cybercrime, in accordance with the KSA reform project. Moreover, some of them did not sign the informed consent form, possibly for similar reasons. Therefore, it was not possible to convince them otherwise, so those whose interviews were not fruitful or did not sign the informed consent form were excluded from the data analysis.

8.4.2 Substantive limitations

The main focus of this thesis is related to aspects of criminal law, so in order for the thesis to meet the time deadline civil law aspects such as restraint orders and confiscation of assets were excluded. However, they will be recommended for future research in Section 8.5.

It was also planned at the outset for this thesis to discuss the UAE jurisdiction as it contains similarities to the KSA's approach on the criminal procedure of cybercrime along with the jurisdiction of the UK for the purpose of policy transfer. It was also planned for this thesis to discuss international cooperation between the KSA and other jurisdictions in regard to the criminal process of cybercrime. Nonetheless, in view of the amount of data gathered on the core topics, and given these extra subjects are broad and are comprised of multiple aspects, they were excluded from the thesis due to the breadth of the subject matter and the limited time offset for the completion of this thesis. They will be recommended for further research in Section 8.5.

8.5 Future research

The researcher recommends further research in this field. First, international cooperation between the KSA and other jurisdictions regarding the criminal process of cybercrime could be divided into multiple areas of further research. One recommended area of research is international cooperation between the KSA and neighbouring countries (including through the GCC). The second recommended area of research is international cooperation between the KSA and other countries, especially the US, since most internet companies are located in it. The third recommended area of research is a comparative study between the KSA's current international cooperation on the criminal process of cybercrime and international cooperation based on the Budapest Convention 2001.

Additionally, further research into the area of the criminal procedure in the KSA is also recommended, especially after finding in this thesis that the KSA applies the same law provisions of process as NCCs on cybercrime. Although various literature covers the criminal process of crime in the KSA, the works are few and have not been updated to cover cybercrime. Therefore, to effectively combat cybercrime in a procedural sense, the KSA needs to effectively combat NCCs in the first place in order to be comprehensive in its procedural approach to combat all types of crime, including cybercrime. It is recommended for such research to reference to neighbouring countries such as the UAE in order to learn from their experience whether to follow their steps or to avoid their mistakes.

Moreover, since the KSA keeps reforming its approach towards legal issues in order to modernise the country, which has been furthered by its *Vision 2030* programme, some of the points covered in this research might already be subject to change, especially in regard to human rights issues and fairness. Therefore, whether this thesis was able to contribute to directing the KSA towards more effective and fairer approach, further research on the matter of fairness is needed in order to contribute to securing human rights within the boundaries of

the KSA, whether on substantive or procedural levels. Moreover, research into this matter should be addressed in the form of a comparative study, or at least with reference to the UK jurisdiction that helped in drafting the UDHR and the UCHR and, most importantly, has adopted them successfully and fairly within its national legislation.

In addition, other aspects of the KSA's approaches to cybercrimes are not criminal and go beyond the focus of this research, such as restraint orders and confiscation, which are civil law aspects. It is recommended that future research should cover these issues and contribute to the overall reform of the KSA approach.

Finally, it is recommended that more socio-legal based studies should be undertaken in order to gain a deeper understand of the religious nature of the social construct of the KSA's criminal legal system and to contribute by offering solutions to the traditional dimensions of the supreme law of the land (*Sharia*) and the overall approach of the KSA to criminal law, both substantively and procedurally. This will subsequently help researchers and reformers to contribute to resolving issues that the KSA faces related to the criminal procedure of cybercrime.

Bibliography

Aba-Namay R, 'The Recent Constitutional Reforms in Saudi Arabia' (1993) 42 *International and Comparative Law Quarterly* 295

Abdula'al U, *شرح القواعد العامة للقانون الجنائي العام: دراسة تحليلية تأصيلية مقارنة بين القوانين الوضعية وأحكام الشريعة الإسلامية Explaining the General Principles of Criminal Law; Analytical Study Compares Between Provisions of Sharia and Legislation* (مكتبة الرشد Alroshed Library 1st Edition 2015)

Abdulaati M, *تقنين الأحكام الشرعية ضرورة عصرية Codification Provisions of Sharia a Modern Necessity* (الشاملةComprehensive 2019)

Abdulaziz D, ' المسؤولية الجنائية عن جريمة الإبتزاز الإلكتروني في القانون السعودي: دراسة مقارنة Criminal Accountability for Electronic Extortion in the KSA Law: Comparison Study' (2018) 27 *Jil Journal of depth Legal Research* 1

Abo Zaid H, *الفقهي المعاصر في السياسة الشرعية* الاجتهاد *Contemporary Ijtihad in Sharia* (دار الكتب العلميةScientific Books House 2010)

Abu Zahrah M, *الجريمة والعقوبة في الفقه الإسلامي Crime and Punishment in Sharia* (دار الفكر العربي Arab Thought House 1998)

Akdeniz Y, Walker C, and Wall D S, *The Internet, Law and Society*, (Pearson 2000)

Ahmed N and Elmulthum M, 'Potentials of Achieving Saudi Vision 2030 Goal to Empower Saudi Women' (2016) 8 *International Journal of Current Research* 42716

Ala'ali M, 'Cybercrime and the Law: An Islamic View' (2007) 4 *Webology* 1

Alali I, شرح مبسط للجرائم الإلكترونية في السعودية *Simple Explanation to the Electronic Crimes in the KSA* (Personal request 2016)

Alabdulatif A, 'Cybercrime and Analysis of Laws in the KSA' (Masters dissertation University of Houston 2018)

Alajloni A, *تقنين الأحكام وأثره على مكانة النص الشرعي Codification of Sharia and its Impact on the Status of the Sharia Texts*' (جامع الكتب العربيةArab Books Collector 2004)

Alamro S, 'Cybercrime in Saudi Arabia: Fact or Fiction, 14 *International Journal of Computer Science* (2017)

Alanazi F, Joens A and Menon C, 'Sharia Law and Digital Forensics in Saudi Arabia' (2018) 13 *Journal of Digital Forensics, Security and Law* 5

Alatawneh M, 'Is Saudi Arabia a Theocracy? Religion and Governance in Contemporary Saudi Arabia' (2009) 45 *Middle Eastern Studies* 721

Alatawneh M, *Wahhābī Islam Facing the Challenges of Modernity, (*Brill 2008)

Alathli O, *الأحكام العامة للقانون الجنائي السعودي General principles of the KSA criminal law* (مكتبة الرشدAlrushed Library 2015)

Alawaji M, *انك على الحق المبين: رؤى تأصيلية في لتفكيك ظاهرة الإلحاد You Are on the Defiant Right: Fundamental Visions for Deconstructing Atheism Phenomena* (Alobekan Library 2016)

Albalawi S, ' فاعلية استخدام التقنيات الحديثة في الكشف عن جرائم القتل New Technologies and their Role in Detecting Crimes' (MA Dissertation, Naif Arab University for Security Science 2009)

Albukhari M 810-870 AD, *صحيح البخاري Sahih al-Bukhari*. https://sunnah.com/bukhari/93 (Accessed October 2, 2019)

Alexander, A and Aouragh M, 'Egypt's Unfinished Revolution: The Role of the Media Revisited' (2014) 8 *International Journal of Communication* 890

Alderson J, *Principled Policing: Protecting the Public with Integrity, Protecting the Public with Integrity,* (Waterside Press 1998 reprinted 2013)

Aldosari N, ‘The Functionalist Division of Powers in Criminal Procedure: The Principle of Separation of Preliminary Investigation and Public Prosecution Authorities’ (JSD thesis Kansas University 2019)

Alfahad A H, ‘From Exclusivism to Accommodation: Doctrinal and Legal Evolution of Wahhabism’ (2004) 79 *New York University Law Review* 485

Alfaize N, ‘The Impact of Culture and Religion on Digital Forensics: The Study of the Role of Digital Evidence in the Legal Process in Saudi Arabia’ (PhD thesis De Montfort University 2015)

Algaddafi, M, *The Green Book, The Solution of the Economic Problem: Socialism* 1976 (الكتاب الأخضر: *الحل لمشكلة الإقتصاد* العالمية للكتب والنشر International for Books and Publishing 2011)

Algarni A, ‘Policing Internet fraud in Saudi Arabia: Expressive Gestures or Adaptive Strategies?’ (2013) 23 *Policing and Society* 498

Algarni A, ‘Policing the Internet Fraud in Saudi Arabia: the Mediation of Risk in a Theoretic Society’ (PhD thesis University of Hull 2012)

Algarni A F, ‘Is a Sharia-based Law Compatible with Cybercrime? An Inquiry into the Saudi Regulations on Internet Fraud’ (2010) 2 *Journal of Law, Politics, and Societies* 1

Alghamdi A, *A* جرائم الانترنت وعقوباتها وفق نظام مكافحة الجرائم المعلوماتية 1428 هـ دراسة مقارنة *Comparative study of the Internet Crimes and their punishments with accordance to Anti Cybercrime Law 2007* (مركز الدراسات العربية Arabic Studites Centre 2017)

Alghamdi R and Drew S, ‘Seven Key Drivers to Online Retailing Growth in KSA’ [2011] IADIS *International Conference e-Society*

AlGharib M, *The legal Centre of the Public Prosecution, a comparative study* (*المركز القانوني للنيابة العامة دراسة مقارنة* دار الفكر العربي Arab Thought House 2001)

Alghazali M 1058-1111 AD. *The Alchemy of Happiness* (Claud Field (Tr), 1910) خيمياء السعادة

Alghmaiz B, ‘The Development of Refusals to Invitations by L2 Learners of Emirati Arabic: Language Proficiency and Length of Residence in the Target Community’ (PhD thesis, Indiana University 2018)

Alhargan A, ‘Saudi Arabia: Civil Rights and Local Actors. 19 *Middle East Policy* (2012) 126

Alhargan A, ‘Saudi Arabia and the International Covenant on Civil and Political Rights 1966: A Stalemate Situation’ (2005) 9 *International Journal of Human Rights*

Alhifnawi M, *الشبهات وأثرها في العقوبة الجنائية في الفقه الاسلامي مقارنا بالقانون Suspicions and their Impact on Criminal Punishment in Islamic Jurisprudence Compared to the Law* (مطبعة الأمانةAlamanah Print House 1986)

AlHamoudi A, 'Criminal Defense in Saudi Arabia: An Empirical Study of the Practice of Criminal Defense in Saudi Arabia' (PhD thesis, University of Washington 2014)

Alhussein E, ‘Saudi First: How Hyper-Nationalism is Transforming Saudi Arabia’ [2019] *European Council on Foreign Relations*

Aljare’e A, تقنين أحكام الشريعة بين المانعين والمجيزين *Codifying Sharia Provisions Between the Opposition and Support* (الشاملةComprehensive Library 2010)

AlKhateeb M, ‘Using Skype as a Qualitative Interview Medium within the Context of Saudi Arabia’ (2018) 23 *Qualitative Report* 2253

Alkharashi S, ‘Human Rights in the Stage of Criminal Investigation: A Comparison between Law and Practice in Saudi Arabia and England and Wales’ (PhD thesis, Sussex 2015)

Almerdas S, ‘Legal Responses to Cybercrime in Saudi Arabia with Special Reference to the Council of Europe Convention on Cybercrime and the Law of the United Kingdom’ (PhD thesis, University of Leeds 2016)

Almibrad M ,Alfuzan S (ed), Abarak A (ed), *كليات القانون والحكم بغير ماأنزل الله The Colleges of Law and The Ruling Without What Allah Has Revealed* (Writers’ own expense 2015)

Almuhaini M, ‘Saudi Arabia, before 1979 and after 2017’ (Alarabiya News 2017) <http://english.alarabiya.net/en/views/news/2017/10/29/Saudi-Arabia-before-1979-and-after-2017.html> (Accessed September 17, 2019)

Almusallam O. فقه القضاء الجنائي *Jurisdiction of the Criminal Judiciary* (معرفة Knowledge 2018)

Almutairi S, ‘Forensic Science Services In The Kingdom Of Saudi Arabia: Achievements And Challenges’ (2013) IV *Law & Justice Review* 103

Alobeid A, ‘Police Functions and Organization in Saudi Arabia’ (1987) 10 *Police Studies, International Review Police Division* 80

Alobaidi F, ‘ دور الدليل الرقمي في الإثبات الجنائي في النظام السعودي: دراسة مقارنة بالقانون الإماراتيThe Role of the Digital Evidence in Forensic Proof in the Saudi Law : A Comparative Study With Emirati Law’ (Master dissertation, Naif Arab University for Security Science, 2020)

Alomran A, ‘Saudi women embrace new freedoms as gradual reforms take hold’ (Financial Times, January 21 2020) <https://www.ft.com/content/81a8267e-1cc9-11ea-97df-cc63de1d73f4> (Accessed June 30, 2020)

Alqahtani H, ‘دور الإدعاء العام في الاعتراض على الأحكام الجزائية من منظور استراتيجي The Role of The Public Prosecution in Challenging Criminal Judgments from Strategic Perspective’ (Master dissertation, Naif Arab University for Security Sciences 2017)

Alqahtani F, ‘The Saudi Anti Cybercrime law of 2007. (A comparative Study Looking at the UAE Combatting Cybercrime Law Amended in 2012)’ (2017) 28 *Qarah Walid* 328

Alqahtani S, ‘Cyber Crimes Committed by Social Media Users in the KSA, (Altamimi Law Firm Magazine 2016) <http://www.tamimi.com/en/magazine/law-update/section-14/november-7/cyber-crimes-committed-by-social-media-users-in-saudi-arabia.html> (accessed March 9, 2018).

Alqarri A, *مجلة الأحكام الشرعية Sharia Provisions Journal* (تهامة للنشر Tohammah Publications, Abu Sulaiman A and Ali M (Eds) 1981)

Alqarri A. *مجلة الأحكام الشرعية Sharia Provisions Journal* (مكتبة القانون والإقتصاد Law and Economy Library, Alfuzan M (Ed) 2015)

Alqaysi A, إجراءات التحقيق الجنائي في الشريعة الإسلامية *Criminal Investigation Procedures in Islamic law* (دار الكتب العربية Arab Books House 2019)

Alrasheed M, *A History of Saudi Arabia* (Cambridge University Press 2002)

Alrasheed M, *Contesting the Saudi State: Islamic Voices from a New Generation* (Cambridge University Press, 2006)

Alsalabi A *فصل الخطاب في سيرة أمير المؤمنين عمر بن الخطاب The biography of Prince of Bleivers Omar Bin Alkhatab* (دار ابن كثيرIbn Katheer's House 2003)

Alsmadi I & Zarour M, 'Cybersecurity Programs in Saudi Arabia: Issues and Recommendations' [2018] *International Conference on Computer Applications & Information Security*

Alshathri M. المحاكم الجنائية في السعودية بين الماضي والحاضر *The Criminal Court in Saudi Arabia Between Past and Present* (Personal request 2015)

Alshatheli F, جرائم التعزير المنظمة في المملكة العربية السعودية *The Coded Ta'zir Crimes in the KSA.* (مكتبة الرشدAlroshed Library 3RD Edition 2015)

Alshathri A, ' حكم تقنين الشريعة الإسلامية من السياسة الشرعية *Judgment on Codification of Sharia from Islamic Politics*' (دار الصميعي للنشر والتوزيع Alsuma'ee Publishing 2007)

Alshubily Y, ' مذكرة مختصرة في فقه الحدود *A Brief Memorandum on Jurisprudence of Hudud,* (Writer's own expense 2005)

Alshura Council, ' مجلس الشورى يوافق على إضافة عقوبة التشهير في نص نظام مكافحة الجرائم المعلوماتية Alshura Council Agrees on including the penality of Naming and Shaming to Anti Cybercrime Law' (Al Shura Council 2015)

<https://www.shura.gov.sa/wps/wcm/connect/shuraarabic/internet/news/s+26.5.1436> (accessed Jun 9, 2018).

Alsowailm F, Hathaway M and Spidalier F, *Kingdom of Saudi Arabia Cyber Readiness at Glance* (Potomac Institute for Policy Studies 2017)

Alsubaie M, 'The right to a fair trial under Saudi Law of Criminal Procedure : a human rights critique' (PhD Thesis, Brunel University 2013)

Alsuhami S, ' عملية تطور القضاء في المملكة مستمرة منذ عهد موحدها الملك عبد العزيز The continuance process of developing the judiciary in the Kingdom since the era its unification by King Abdulaziz' (الاقتصاديةThe *Economist* 2010)

Alsulami D, ' *التجديد في التفسير في العصر الحديث مفهومه وضوابطه واتجاهاته* The Revival of Interpretation of Quran in Modern Age: Its concept, its measurement and its directions, (PhD thesis, Umm Alqura University 2014)

Alsuuti J 849-911 AD, صحيح الجامع *Sahih al-Jami.*

Altaee A, ' النظام القضائي في المملكة العربية السعودية: تأسيسه وتطوره Judicial System in the Kingdom of Saudi Arabia: its establishment and its evolution, 11 *Alrafidyn Journal for Legal rights* (2009) 119

Altermithi 824-892 AD, السنن *Alsunan*.

Alwasil A, 'Saudi Arabia's Engagement in, and Interaction with, the UN Human Rights System: an Analytical Review' (2010) 14 *The International Journal of Human Rights* 1072

Alzuhaili M, *القواعد الفقهية وتطبيقاتها في المذاهب الأربعة Jurisprudence and its applications in the four schools of thought (* دار الفكرThought House 2006)

Amnesty International, 'Saudi Arabia 2017-2018' <https://www.amnesty.org/en/countries/middle-east-and-north-africa/saudi-arabia/report-saudi-arabia/> (accessed April 9, 2019).

Amnesty International, 'Amnesty International Report 2017/18 the State of the World's Human Rights' <https://www.amnesty.org.uk/files/2018-02/annualreport2017.pdf> (Accessed April 9, 2020).

Amnesty International, Amnesty International Report 2020/2021. https://reliefweb.int/sites/reliefweb.int/files/resources/POL1032022021ENGLISH.PDF (Accessed September 29, 2021)

Anderson D, A Question of Trust Report of the Investigatory Powers Review, (2015) <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/434399/IPR-Report-Web-Accessible1.pdf> (Accessed October 20, 2021)

Awwad M, ' دور وحدة مكافحة الجرائم المعلوماتية في الحد من جريمة الابتزاز: من وجهة نظر العاملين في الرئاسة العامة لهيئة الأمر بالمعروف والنهي The Role of the Anti-Cybercrime Unit in Reduction of Extortion Offences from the Viewpoint of Workers in the General Presidency for the Promotion of Virtue and Prevention of Vice' (Master dissertation, Naif Arab University 2020)

Ayres I and Braithwaite J, *Responsive Regulation Transcending the Deregulation Debate* (Oxford University Press 1992)

Azzam E, ' العقوبة في نظام مكافحة الجرائم المعلوماتية في المملكة العربية السعودية: دراسة تأصيلية مقارنة Punishment in the Anti Cybercrime Law in the Kingdom of Saudi Arabia: a Comparative Study*'* (2018) 82 Aladel 84

Baderin M, 'A comparative Analysis of the Right to a Fair Trial and Due process Under International Human Rights Law and Saudi Arabian Domestic Law' (2006) 10 *International Journal of Human Rights* 241

Bakhsh M, Mahmood A and Awan I, ‘A comparative Analysis of Cybercrime and Cyber Laws in the Islamic Republic of Pakistan, Kingdom of the KSA, and the United Arab Emirates’ 1 *Imam Journal of Applied Sciences* (2016) 1

Bandler J and Merzon A, *Cybercrime Investigations a Comprehensive Resource for Everyone* (CRC Press 2020)

Bassiouni M, *The social system and morality of Islam* (Middle East Institute 2012)

Beetham D, *The Legitimation of Power* (Macmillan 1991)

Beck U, Giddens A and Scott L, *Reflexive Modernization, Politics, Tradition and Aesthetics in the Modern Social Order* (Polity Press1994)

Benson D and Jordan A, ‘What Have We Learned from Policy Transfer Research’ (2011) 9 *Political Studies Association, Political Studies Review*

Berg P, ‘Risk Management: Procedures, Methods and Experiences’ (2010) 2 RT&A 79

Bessis F and Chaserant C, ‘A New Analysis of the Market for Legal Services. The Lawyer, homo economicus or homo conventionalis?’ (2019) 44 *Historical Social Research* 188

Bin Ammar D, ‘Evolution of the Foundations of Legal Liability’ (PhD thesis, University of Zian 2015)

BinAbdulaziz S, *Political Development in the Kingdom of Saudi Arabia and Evaluation to Alshura Council* (التطور السياسي في المملكة العربية السعودية و تقييم لمجلس الشورى مكتبة الملك فهد الوطنيةKing Fahad National Library 2002)

Bjola C, ‘Propaganda in the Digital Age’ (2017) 3 *Global Affairs* 189

Blanc F, ‘Tools for Effective Regulation: Is “More” Always “Better”?’ (2018) 9 *European Journal of Risk Regulation* 465

Blandy S, ‘Socio-legal Approaches to Property Law Research’ (2014) 3 *Property Law Review*

BMG Research, ‘Public Perceptions of Policing in England and Wales 2018: Prepared for: Her Majesty’s Inspectorate of Constabulary and Fire & Rescue Services’ (BMG Research Jan 2019) <https://www.justiceinspectorates.gov.uk/hmicfrs/publications/public-perceptions-of-policing-in-england-and-wales-2018/> (Accessed October 10, 2020)

Boukalas C, ‘Overcoming Liberal Democracy: "Threat Governmentality" and the Empowoerment of the Intelligence in the UK Investigatory Powers Act, in Sarat A (Ed), *Studies in Law, Politices, and Society* (Emerald Publishing Limited 2020)

Brady v Maryland 373 U.S. 83 (1963)

Brintion J, *The Mixed Courts of Egypt* (Yale University Press 1930)

British Embassy in Riyadh, ‘List of lawyers in Saudi Arabia’ <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/943729%2FLocal_Lawyers_List_2020_Saudi_Arabia.pdf> (accessed October 21, 2021)

Broadbent M, ‘The Digital Services Act, the Digital Markets Act, and the New Competition Tool European Initiatives to Hobble U.S. Tech Companies’ [2020] *Centre for Strategic and International Studies*

Brodeur J P, ‘High policing and low policing’ (1983) 30 *Social Problems*

Brodeur P, *The Policing Web* (Oxford University Press. 2011)

Bronson R, *Thicker than Oil America’s Uneasy Partnership with Saudi Arabia* (Oxford University Press 2006)

Brown, J, *The Future of Policing* (Routledge 2014)

Brown W, McLean L and McMillan A, *The Concise Oxford Dictionary of Politics and International Relations* (Oxford University Press 4th edition 2018)

Brownsword R, ‘Code, Control, and Choice: Why East is East and West is West’ (2005) 25 *Legal Studies* 1

Bryman A, ‘Integrating Quantitative and Qualitative Research: How Is It Done’ (2006) 6 *Qualitative Research Journal* 97

Buil-Gil D, Miró-Llinares F, Moneva A, Kemp S and Díaz-Castaño N, ‘Cybercrime and Shifts in Opportunities During COVID-19: A Preliminary Analysis in the UK’ (2020) 23 *European Societies* S47

Campbell L, Ashworth A and Redmayne M, *The Criminal Process* (Oxford University Press 5th Edition 2019)

Carlson R, ‘False or Suppressed Evidence: Why a Need for the Prosecutorial Tie?’ [1969] *Duke Law Journal* 1171

Casey E, ‘Error, uncertainty, and loss in digital evidence’ [2002] *International Journal of Digital Evidence*

Casey E, *Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet* (Elsevier Inc 3rd Edition 2011)

Cesario J, Johnson D and Terrill W, ‘Is There Evidence of Racial Disparity in Police Use of Deadly Force? Analyses of Officer-Involved Fatal Shootings in 2015–2016.’ (2018) 10 *Social Psychological & Personality Science* 586

Chayes A and Chayes A H, ‘Our Compliance 1993’ in Simmons B and Steinberg R (Eds), *International Law and International Relations* (Cambridge University Press 2007)

Chehaye K, ‘Saudi Arabia’s Biggest Obstacle to Progress Lies in its Systematic Human Rights Violations’ (Amnesty International. 2018) <https://www.amnesty.org/en/latest/news/2018/01/saudi-arabias-biggest-obstacle-to-progress-lies-in-its-systematic-human-rights-violations/> (Accessed November 13, 2021)

City of London Police, 'Online Fraud and Cybercrime' <https://www.cityoflondon.police.uk/advice/advice-and-information/fa2/fraud/online-fraud/> (Accessed November 9, 2020)

Clarke C, and Milne R, 'National Evaluation of Investigative Interviewing, (Home Office Report No: PRAS/149 2011)

Clyde & Co LLP, 'UAE Anti-Commercial Fraud Law Passes Through the Federal National Council' (2014) <http://www.lexology.com/library/detail.aspx?g=723a2a47-569f-4d45-b5d6-40df9f1ad614> (accessed Jun 10, 2018)

Cobbe J, 'Casting the dragnet: communications data retention under the Investigatory Powers Act' [2018] *Public Law Journal* 10

Cockcroft T, Shan-A-Khuda M, Schreuders Z and Trevorrow P, 'Police Cybercrime Training: Perceptions, Pedagogy, and Policy' (2018) 15 *Policing A Journal of Policy and Practice* 15

Colarik A, *Cyber Terrorism: Political and Economic Implications* (Idea Group Publishing. 2006)

Collins M, 'Desert Storm: A Look Back' (US Department of Defence 2019) <https://www.defense.gov/Explore/Features/story/Article/1728715/desert-storm-a-look-back/> (Accessed June 19, 2020).

Convention against Torture and Other Cruel, Inhuman or Degrading Treatment or Punishment 1984 (UNTS Vol.1465) p. 85

Convention on Cybercrime 2001 (ETS No. 185)

Cordner G, 'Community policing' In Reisig M and Kane R (Eds), *The Oxford Handbooks of Police and Policing* (Oxford University Press 2014)

Cornish P, Hughes R and Livingston D, 'Cyberspace and the National Security of the United Kingdom: Threats and Responses' (Chatham House Report 2009)

Council of Europe, 'Full list of members' <https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185/signatures?p_auth=YmNLTrEX> (Accessed February 4, 2020)

Crawford A, 'The partnership approach to community crime prevention' (1994) 3 *Social & Legal Studies* 497

CSEurope. 'Face-to-Face with… Ben Russell, NCA' (Cyber Security Europe 2020) <https://www.cseurope.info/face-to-face-with-ben-russell-nca/> (Accessed November 15, 2020)

Dalacoura K, *Islam Liberalism and Human Rights* (I.B. Tauris Publishers 1998)

Devlin P, *The Criminal Prosecution in England* (Yale University Press 1958)

Dolowitz P D, Hulme R, Nellis M and O'Neill F, *Policy Transfer and British Social Policy; Learning from the USA?* (Open University Press 2000)

Edwards L, *Law, Policy and the Internet* (Hart Publishing 2019)

Egyptian Criminal Procedure Law No. 150 of 1950.

Elnaim B, 'Cyber Crime in Kingdom of Saudi Arabia. The Threat Today and the Expected Future' (2013) 3 *Journal of Information & Knowledge Management* 14

Emon M, Ellis M and Glahn B, *Islamic Law and International Human Rights Law* (Oxford University Press 2012)

Emsley C, *The Great British Bobby: A History of British Policing from the 18th Century to the Present* (Quercus 2009)

Esmaeli H, 'On a Slow Boat towards the Rule of Law: The Nature of Law in the Saudi Arabia Legal System' [2009] *Arizona Journal of International and Comparative Law* 1

Esposito J (ed), 'Oxford Dictionary of Islam' (Oxford Islamic Studies Online) <http://www.oxfordislamicstudies.com/article/opr/t125/e1107> (accessed Sep 21, 2019).

European Commission, 'E-evidence - Cross-Border Access to Electronic Evidence' <https://ec.europa.eu/info/policies/justice-and-fundamental-rights/criminal-justice/e-evidence-cross-border-access-electronic-evidence_en> (accessed February 4, 2020)

European Commission, 'Proposal for a Regulation of the European Parliament and of the Council on preventing the dissemination of terrorist content online' (European Commission 12 September 2018) <https://ec.europa.eu/commission/sites/beta-political/files/soteu2018-preventing-terrorist-content-online-swd-408_en.pdf> (accessed February 15, 2019)

European Commission, 'The Digital Services Act package' (2021) <https://digital-strategy.ec.europa.eu/en/policies/digital-services-act-package> (Accessed September 14, 2021)

European Convention on Human Rights 1950

European Parliament study, 'Cybersecurity in the EU Common Security and Defence Policy (CSDP) Challenges and risks for the EU' (Scientific Foresight Unit (STOA) EPRS, European Parliamentary Research Service, European Parliament 2016) <http://publications.europa.eu/resource/cellar/2e35913c-1d03-11e8-ac73-01aa75ed71a1.0001.01/DOC_1> (Accessed September 23, 2021)

European Union Agency for Cybersecurity, 'National Cyber Security Strategy of Saudi Arabia' <https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map/strategies/national-cyber-security-strategy-of-saudi-arabia/view> (Accessed January 16, 2020)

Europol, ‘Cybercrime Presents a Major Challenge for Law Enforcement: The Hague, the Netherlands’ <https://www.europol.europa.eu/newsroom/news/cybercrime-presents-major-challenge-for-law-enforcement> (accessed February 19, 2019)

De Botton A, *Status anxiety* (Hamish Hamilton 2004)

Dworkin R, *Taking Rights Seriously* (Cambridge: Harvard University Press 1977)

Fafinski S, *Computer Misuse; Response, Regulation and the Law* (Willan Publishing 2009)

Feldman N, *The Fall and Rise of the Islamic State* (2008)

Ferguson P R, ‘The Presumption of Innocence and its Role in the Criminal Process’ (2016) 27 *Criminal Law Forum* 131

Financier Worldwide, ‘Cyber security and data privacy law in the KSA*’* (Financier Worldwide 2015) <https://www.financierworldwide.com/cyber-security-and-data-privacy-law-in-saudi-arabia> (accessed March 18, 2018)

Finlay A, ‘Global Information Society Watch 2009 Focus on Access to Online Information and Knowledge – Advancing Human Rights and Democracy’ (Global Information Society Watch 2009)

Fleishman G, ‘Cartoon Captures Spirit of the Internet’ (New York Times 14 Dec 2000) <https://web.archive.org/web/20171229172420/http://www.nytimes.com/2000/12/14/technology/cartoon-captures-spirit-of-the-internet.html> (Accessed February 20, 2020)

Fleming J and Rhodes R, ‘Bureaucracy, Contracts and Networks: The Unholy Trinity and the Police’ (2005) 38 *Australian and New Zealand Journal of Criminology* 192

Foreign & Commonwealth Office, ‘United Kingdom-Saudi Arabia Joint Communiqué’ (Gov.uk. 2018) <https://www.gov.uk/government/news/united-kingdom-saudi-arabia-joint-communique> (accessed September 20, 2021)

Fox, Campbell and Hartley v United Kingdom, App. no. 13590/88 judgment of 30 August 1990

Francis P, Davies P and Jupp V, *Policing Futures, the Police, Law Enforcement and the Twenty-First Century* (Palgrave 1997)

Franck T, *Fairness in International Law and Institutions* (Oxford University Press 1995)

Freedom House, Freedom on the Net 2020: Saudi Arabia. <https://freedomhouse.org/country/saudi-arabia/freedom-net/2020> (Accessed September 15, 2021)

Fukuyama F, *The End of History and the Last Man* (Penguin 1992)

Fukuyama F, *Trust: The Social Virtues and the Creation of Prosperity* (Hamish Hamilton 1995)

Gehl R and Plecas D, *Introduction to Criminal Investigation: Processes, Practices and Thinking* (Justice Institute of British Columbia 2016)

Giddens A, *The consequences of modernity* (Polity Press 1990)

Gillespie A, *Cybercrime: Key Issues and Debates* (2nd edition Part V, Routledge 2019)

Ghafar A, 'A Stable Egypt for a Stable Region: Socio-economic Challenges and Prospects' (European Parliament 2018)

Glidewell I, *The Review of the Crown Prosecution Service Summary of The Main Report with the Conclusions and Recommendations* (Stationary Office 1998)

Gooch G and Williams M, *A Dictionary of Law Enforcement* (Oxford University Press 2nd Edition 2015)

GOV.UK, 'Duty solicitors: rotas, information and guidance' (2014) <https://www.gov.uk/guidance/duty-solicitors-rotas-information-and-guidance> (Accessed November 16, 2020)

Government Publishing Office, ‘Public Law 108 - 187 - Controlling The Assault Of Non-Solicited Pornography And Marketing Act Of 2003", Or The ``Can-Spam Act Of 2003’ (2017) <https://www.gpo.gov/fdsys/pkg/PLAW-108publ187/content-detail.html> (accessed June 18 , 2018)

Grabosky P, *Electronic Crime* (Person Education Inc 2007)

Grabosky P, ‘Requirements of Prosecution Services to Deal with Cybercrime’ (2007) 47 *Crime, Law and Social Change* 201

Graves R, *The Greek Myths: The Complete and Definitive Edition* (Penguin 2017)

Greenwald G, *No Place to Hide: Edward Snowden, the NSA and the Surveillance State* (Hamish Hamilton 2014)

Greer S, ‘The Right to Silence, Defence Disclosure and Confession Evidence’ (1990) 53 *Modern Law Review* 709

Gulf Centre for Human Rights, ‘Mapping Cybercrime Laws and Violations of Digital Rights in the Gulf and Neighbouring Countries’ (June 2018)

Gulf Cooperation Council <https://www.gcc-sg.org/en-us/AboutGCC/MemberStates/pages/Home.aspx> (Accessed November 24, 2021)

Habeeb M, *أصول على الإجرام The fundamentals of criminology* (العاتك Pure Redness 1999)

Haddad Y and Stowasser B, *Islamic Law and the Challenges of Modernity* (Altamira Press 2004)

Hakmeh J, ‘Cybercrime and the Digital Economy in the GCC Countries’ (Chatham House 2017) <https://www.chathamhouse.org/sites/files/chathamhouse/publications/research/2017-06-30-cybercrime-digital-economy-gcc-hakmeh.pdf> (accessed March 17, 2018).

Hakmeh J, ‘Cybercrime Legislation in the GCC Countries: Fit for Purpose?’ (Chatham House 2018)

Hakmeh J, 'Tackling Cybercrime: Time for the GCC to Join Global Efforts' (Chatham House 2016)

Halford v UK (20605/92) [1997] ECHR 32

Hallaq W, *Shari'a: Theory, Practice, Transformations* (Cambridge University Press 2009)

Hanson M, 'The Influence of French Law on the Legal Development of Saudi Arabia' (1987) 2 *Arab Law Quarterly* 272

Harper R, *Saudi Arabia 2nd Edition* (Chelsea House 2007)

Hart HLA, *The Concept of Law* (2nd Edition Clarendon Press 1994)

Harvey W, 'Strategies for conducting elite interviews' (2011) 11 *Qualitative research* 431

Hawkins G, *Beyond Reasonable Doubt* (Australian Broadcasting Commission 1977)

Haykel B, Hegghammer T & Lacroix S (Eds), *Saudi Arabia in Transition* (Cambridge University Press 2015)

Hegel G, *The Phenomenology of Spirit 1807* (Terry Pinkard (tr), Cambridge University Press 2018)

Hellman A, 'The Convergence of International Human Rights and Sharia Law Can International Ideals and Muslim Religious Law Coexist?' [2016] *New York Bar Association*

Henkin L, *The Age of Rights* (Columbia University Press 1990)

Henry L, *Information Technology for Management* (Jacobs Foundation 2009)

Hoffman D and Rowe J, *Human Rights in the UK: An Introduction to the Human Rights Act 1998* (4th edition, Pearson 2013)

Hirst P, 'Mass surveillance in the age of terror: bulk powers in the Investigatory Powers Act 2016' (2019) 4 *European Human Rights Law Review* 403

Hodgson J *French Criminal Justice: A Comparative Account of the Investigation and Prosecution of Crime in France* (Hart 2005)

Hoffer E, *The True Believer: Thoughts on the Nature of Mass Movements 1951* (Perennial. 2002)

Howard P and Hussain M *Democracy's Fourth Wave? Digital Media and the Arab Spring* (Oxford University press 2013)

Human Rights Watch, 'Egypt: Intensifying Crackdown Under Counterterrorism Guise: Emergency Courts Used to Prosecute Activists, Journalists, Bloggers' (July 2018) <https://www.hrw.org/news/2018/07/15/egypt-intensifying-crackdown-under-counterterrorism-guise> (Accessed January 6, 2020)

Human Rights Watch, 'Challenging the Red Lines Stories of Rights Activists in Saudi Arabia' (2013) https://www.hrw.org/report/2013/12/17/challenging-red-lines/stories-rights-activists-saudi-arabia (Accessed November 21, 2021)

Human Rights Watch, '"Kettling" Protesters in the Bronx Systemic Police Brutality and Its Costs in the United States' (2020). https://www.hrw.org/report/2020/09/30/kettling-protesters-bronx/systemic-police-brutality-and-its-costs-united-states (Accessed October 22, 2021)

Human Rights Watch, 'Precarious Justice' (2008) <https://www.hrw.org/reports/2008/saudijustice0308/saudijustice0308webwcover.pdf , 2008> (Accessed June 6, 2020).

Human Rights Watch, 'Saudi Arabia Events of 2019' (2020) <https://www.hrw.org/world-report/2020/country-chapters/saudi-arabia> (Accessed October 1, 2020)

Human Rights Watch, 'Saudi Arabia: Malicious Spyware App Identified' (2014) <https://www.hrw.org/news/2014/06/27/saudi-arabia-malicious-spyware-app-identified> (Accessed November 20, 2021)

Human Rights Watch ‘Saudi Arabia: Poet Sentenced to Death for Apostasy’ (2015) <https://www.hrw.org/news/2015/11/23/saudi-arabia-poet-sentenced-death-apostasy> (Accessed May 20, 2021)

Human Rights Watch, ‘The Internet in the Middle East and North Africa: A Cautious Start’ (1999) <https://www.hrw.org/legacy/advocacy/internet/mena/int-mena.htm> (Accessed September 17, 2021)

Human Rights Watch, ‘The Internet in the Mideast and North Africa: Free Expression and Censorship: Saudi Arabia’ (1999) <https://www.hrw.org/legacy/advocacy/internet/mena/saudi.htm#TopOfPage> (Accessed September 17, 2021)

Hurnard N D, ‘The Jury of Presentment and the Assize of Clarendon’ (1941) 56 *English Historical Review* 374

Hughes C, ‘An Introduction to Qualitative Research’ (University of Warwick) https://warwick.ac.uk/fac/soc/sociology/staff/hughes/researchprocess/an_introduction_to_qualitative_research.docx (accessed March 18, 2018)

Hyde J, ‘First Female Law Firm Opens in Saudi Arabia’ (The Law Society Gazette 3, January 2014) https://www.lawgazette.co.uk/practice/first-female-law-firm-opens-in-saudi-arabia/5039261.article (Accessed September 15, 2021)

Ibekwe C, ‘The Legal Aspects of Cybercrime in Nigeria: An Analysis with the UK Provisions, (PhD thesis, University of Stirling 2015)

Ibn Baz’s Fatwa فتوى ابن باز <https://binbaz.org.sa/fatwas/1335/%D8%AD%D9%83%D9%85-%D8%A7%D9%84%D8%A7%D8%AC%D8%AA%D9%87%D8%A7%D8%AF-%D9%85%D9%82%D8%A7%D8%A8%D9%84-%D8%A7%D9%84%D9%86%D8%B5> (Accessed 14 May, 2021)

Ibn Kather 1301-1372 AD, تفسير ابن كثير *Ibn Kather's Interpretation of Quran* (دار الكتب العلمية Scientific Books House 2016 Vol 4)

Idrees A, الدية بين العقوبة والتعويض في الفقه الإسلامي المقارن *Diyya Between Punishment And Compensation In Comparative Islamic Jurisprudence* (دار مكتبة الهلال Crescent Moon House 1986)

Imam Mohammed Bin Saud Islamic University, College of Sharia, Curriculum <https://units.imamu.edu.sa/colleges/sharia/Pages/tosifatnew.aspx> (Accessed September 13, 2021)

Information Commissioner's Office (ICO), 'About ICO' <https://ico.org.uk/about-the-ico/> (Accessed July 2, 2020)

International Covenant on Civil and Political Rights, G.A. res. 2200A (XXI), 21 U.N. GAOR Supp. (No. 16) at 52, U.N. Doc. A/6316 (1966), 999 U.N.T.S. 171, entered into force Mar. 23, 1976.

Internet Architecture Board (IAB) <https://www.iab.org/about/iab-overview> (Accessed September 15, 2021)

Internet Corporation for Assigned Names and Numbers (ICANN) <https://www.icann.org>

Internet Engineering Task Force (IETF) < https://www.ietf.org/about/> (Accessed September 13, 2021)

Internet Society (ISOC) <https://www.internetsociety.org/about-internet-society/> (Accessed September 13, 2021)

Iyer V, 'Separation of Powers: The UK Experience' (2018) 5 *Journal of International and Comparative Law* 507

Iz Alden K. 'العقوبة بالجلد في الفقه الإسلامي وإمكان تطبيقها في الأنظمة الجزائية الحديثة Punishment by Flogging in Islamic Jurisprudence and the Possibility of Applying it in Modern Penal Codes' (2018) 5 *Legal Forum Journal*

Jackson J, Hough M, Bradford B, Hohl K and Kuha J, 'European Social Survey: Policing by Consent: Understanding the Dynamics of Police Power and Legitimacy' [2012] ESS *Country Specific Topline Results Series*

Jaghman Y, *الطرق السلمية في تغيير الحاكم الفاسد Peaceful Islamic Ways of Changing the Corrupt Ruler* (المكتبة الشاملة الحديثة Modern Comprehensive Library 2008)

Jerichow A, *Saudi Arabia: Outside Global Law and Order: a Discussion Paper* (Curzon 1997)

Johnston E, 'The Defence Lawyer in the Modern Era' (PhD Thesis, University of the West England 2019)

Jones S, *Virtual Culture. Identity & Communication in Cyberspace* (Sage Publication 1997)

Jorn T, 'Ḥisba (modern times)"' in Fleet K, Kramer G, Matringe D, Nawas J and Rowson E (eds) *Encyclopaedia of Islam* (3rd edition, Brill 2017)

Juanena C J and Smith L T, *Decolonizing Methodologies Research and Indigenous Peoples* (Zed Books Ltd 2009)

Kahn R, Leiner B, Cerf V, Clark D, Kleinrock L, Lynch D, Postel J, Roberts L and Wolff S, 'The Evolution of the Internet as a Global Information System' (1997) 29 *International Information & Library Review* 129

Kaminski J, 'Bureaucracy and Modernity: A Comparative Qualitative Analysis of Public Administration in the West and OIC States' (2013) 3 *Politics, Bureaucracy and Justice* 1

Kenyon D and Stansfield C, 'Research on the comparability of the oral proficiency interview and the simulated oral proficiency interview' (1992) 20 *System* 347

Karagiannopoulos V, 'China and the Internet: Expanding on Lessig's Regulation Nightmares' (2012) 9 SCRIPT 150

Katyal N, ‘Criminal law in cyberspace’ (2001) 149 *University of Pennsylvania Law Review* 1003

Khan A and Ramadan H, *Contemporary Ijtihad. Limits and Controversies* (Edinburgh University Press 2011)

Khalifa H, *إجراءات التحقيق والمحاكمة في نظام الإجراءات الجزائية السعودي Trial and Investigation Proceedings in Saudi Criminal Procedure Law* (معهد الإدارة العامة General Management Institute 2019)

Khidher A, السمات الموضوعية والإجرائية للنظام الجنائي في المملكة العربية السعودية *The objective and procedural features of the criminal system in the Kingdom of Saudi Arabia* (كتب عربية Arabic Books 2007)

King Abdul-Aziz City for Science and Technology <https://www.kacst.edu.sa/eng/about/Pages/WhoWeAre.aspx> (accessed May 15, 2018)

King Saud University <https://ksu.edu.sa/en/about-ksu> (Accessed September 20, 2021)

Kleinwachter W, ‘From Self-Governance to Public-Private Partnership: The Changing Role of Governments in the Management of the Internet's Core Resources’ (2003) 36 *Loyola of Los Angeles Law Review* 1103

Klosko G, *Why Should We Obey the Law?* (Polity Press 2019)

Knight A and Ruddock L, *Advanced Research Methods in the Built Environment* (Willy-Blackwell 2008)

KSA Al Shura Council, ‘Shura in the Kingdom of Saudi Arabia’ <https://shura.gov.sa/wps/wcm/connect/ShuraEn/internet/Historical+BG/> (Accessed September 10, 2019)

KSA Al Shura Council Law 1992 Royal Decree No. A/91

KSA Anti Commercial Fraud Law 2008 Royal Decree No. M/19

KSA Anti Cybercrime Law 2007 Royal Decree No. M/17

KSA Basic Law of Governance 1992 Royal Decree No. A/90

KSA Bureau of Investigation and Public Prosecution (Public Prosecution) Law 1989 Royal Decree No. M/56

KSA Centre for International Communication <https://cic.org.sa/about-cic/> (accessed March 11, 2018).

KSA Centre for International Communication, 'Saudi Arabia Sets Up Cyber Security Authority To Boost National Security' (November 2017) <https://cic.org.sa/2017/11/saudi-arabia-sets-up-cyber-security-authority-to-boost-national-security/> (accessed July 12, 2018)

KSA Communication and Information Technology Commission, 'ICT Report E-Commerce in Saudi Arabia' (2017) <https://www.citc.gov.sa/en/reportsandstudies/Reports/Documents/CITC_ECOMMERCE_2017_ENGLISH.PDF> (accessed July 31, 2019)

KSA Council of Ministers Law 1993 Royal Decree No. 13/A

KSA Council of Ministers order no (289) 2016

KSA Criminal Procedure Law 2001 Royal Decree No. M/39

KSA Criminal Procedure Law 2013 Royal Decree No. M/2

KSA Criminal Procedure Law Executive Regulation 2015 Council of Ministers Order No. 142

KSA Electronic Transactions Protection Law 2007 Royal Decree No. M/8

KSA Embassy in the US, 'Saudi Arabia's Reforms and Programs to Empower Women' (2019) <https://www.saudiembassy.net/sites/default/files/Factsheet%20on%20Progress%20for%20Women%20in%20Saudi%20Arabia.pdf> (Accessed September 13, 2021)

KSA Laws Collection on the Expert Authority website. <https://laws.boe.gov.sa/BoeLaws/Laws/> (Accessed 22 October 2021)

KSA Members and Employees of the Public Prosecution Bylaw 2016 Royal Decree No. 406

KSA Ministry of Communications and Information Technology, 'Developing National Information Security Strategy for the Kingdom of Saudi Arabia – NISS, Draft 7' (2013)

KSA Ministry of Justice, مجوعة الأحكام القضائية Judicial Rulings collection <https://www.moj.gov.sa/ar/SystemsAndRegulations/Pages/System1435.aspx> (Accessed 17 May, 2021)

KSA Ministry of Justice, ' وزير العدل: ٨٥ مشروعًا تطويريًا تحت التنفيذ... وتقنين الأحكام القضائية مسألة محسومة Minister of Justice: 85 development projects under implementation, and Codifying Sharia is in Last Stages' (KSA Ministry of Justice 10 April 2019) <https://www.moj.gov.sa/ar/MediaCenter/News/Pages/NewsDetails.aspx?itemId=788> (Accessed September 17, 2019)

KSA Ministry of Justice, 'MoJ's Initiatives' <https://www.moj.gov.sa/English/Ministry/vision2030/Pages/MoJInitiatives.aspx> (Accessed April 15, 2020)

KSA Ministry of Justice, 'National Transformation Plan Program' <https://www.moj.gov.sa/English/Ministry/vision2030/Pages/NationalTransformationProgram.aspx> (Accessed May 10, 2020)

KSA Ministry of Justice, ' قرار من المجلس الأعلى للقضاء: لا عقوبة للشبهة .. إما إدانة أو براءة Order from the High Judiciary Council: No Punishment for Suspicion, Either Convection or Innocence, (2019) <https://www.moj.gov.sa/ar/MediaCenter/News/Pages/NewsDetails.aspx?itemId=70> (Accessed September 13, 2021)

KSA Royal Decree No (A/240) 2017

KSA Royal Decree No (A/38) 2017

KSA Supreme Judicial Council Order No 1492/T Dated 25/09/1441 Ah (18/05/2020)

KSA Vision 2030 <https://vision2030.gov.sa/en> (accessed March 23, 2018)

KSA Vision 2030, 'National Transformation Programme; Delivery Plan 2018-2020, (2017) <https://vision2030.gov.sa/sites/default/files/attachments/NTP%20English%20Public%20Document_2810.pdf> (Accessed April 16, 2020)

KSA Vision 2030, 'Strategic Objectives and Vision Realization Programs' <https://vision2030.gov.sa/sites/default/files/vision/Vision%20Realization%20Programs%20Overview.pdf> (Accessed January 7, 2020)

Kshetri N, *The Global Cybercrime Industry: Economic, Institutional, and Strategic Perspectives* (Greensboro Springer Science & Business Media 2010)

Lacroix S, *Awakening Islam; Religious Dissent in contemporary Saudi Arabia*. (Gorge Holoch (tr), Harvard University Press 2011)

Ladkin P, Littlewood B, Thimbleby H and Thomas M, 'The Law Commission Presumption Concerning the Dependability of Computer Evidence' (2020) 17 *Digital Evidence and Electronic Signature Law Review* 1

Lash S, Szerszynski B, and Wynne B, *Risk, Environment & Modernity Towards a New Ecology* (Sage Publication 1996)

Latham and Watkins LLP, 'Pro Bono Practices and Opportunities in Saudi Arabia' (ProBono Institute 2019)

<https://www.lw.com//admin/Upload/Documents/Global Pro Bono Survey/pro-bono-in-saudi-arabia-3.pdf> (Accessed October 19, 2021)

Legal Information Institute at Cornell Law School, 'Surveillance' <https://www.law.cornell.edu/wex/surveillance> (Accessed April 7, 2020)

Lentz S and Chaires R, ‘The Invention of Peel's Principles: A Study of Policing ‘Textbook’ History’ (2007) 35 *Journal of Criminal Justice*

Lessig L, *Code and Other Laws of Cyberspace* (2nd Version, Basic Books 2006)

Lessig L, *The Future of Ideas; The Fate of The Commons in Connected World* (Random House 1999)

Leung L, 'Validity, Reliability, and Generalizability in Qualitative Research' (2015) 4 *Journal of Family Medicine and Primary Care* 324

Liberty v Home Office [2018] EWHC 957 (Admin)

Limongelli V, ‘Digital Evidence: Findings of Reliability, Not Presumptions’ (2008) 2 *Journal of Digital Forensic Practice* 13

Lloyd D, *The Idea of the Law* 1964 (Alsuways S (tr) علم المعرفةFlag of Knowledge 1981)

Lo Iacono V, ‘Symonds P, and Brown D. Skype as a Tool for Qualitative Research Interviews’ (2016) 21 *Sociological Research Online* 103

Loader B D, *The Governance of Cyberspace* (Routledge 1997)

Luna E and Wade M, *The Prosecutor in Transnational Perspective* (Oxford University Press. 2012)

Lyman M, *Criminal Investigation the Art and Science* (6th edition, Prentice Hall 2011)

Mack N, Woodsong C, MacQueen K, Guest G and Namey E, *Research Methods: A Data Collector’s Field Guide* (USAID 2005)

Madiega T, ‘Regulating online TV and radio broadcasting. European Union’ [2019] *EPRS*

Maghaireh A, ‘Sharia Law and Cyber-Sectarian Conflict: How can Islamic Criminal Law Respond to Cybercrime?’ (2011) 2 *International Journal of Cyber Criminology* 337

Magna Carta 1215

Mahdi O, *نظرية البطلان في نظام الاجراءات الجزائية السعودي The Theory of Nullity in the Saudi Procedures Law* (مكتبة القانون والإقتصاد Economy and Law Library 2013)

Mainwaring S, 'Always in control? Sovereign states in cyberspace' (2020) 5 *European Journal of International Security* 215

Mallat C, 'Mapping Saudi Criminal Law' (2020) 86 *American Journal of Comparative Law*

Malone v the United Kingdom (1985) 7 EHRR 14, [1984] ECHR 10, 7 EHRR 14

Mansell R, 'Human Rights and Equity' in Cyberspace' in Murray A and Klang M (eds), *Human Rights in the Digital Age* (Glass House Press 2005)

Marmor A, 'Should Like Cases be Treated Alike?' (2005) 11 *Legal Theory* 27

Sutherland v HM Advocate [2020] UKSC 22

Mason S and Seng D (Eds), *Electronic Evidence* (University of London Press 2017)

Mawby R I, 'Models of Policing' in Newburn T (ed), *Handbook of Policing* (2nd edition, Routledge 2008)

Mazawi A, 'The Academic Workplace in Public Arab Gulf Universities' in Altbach P (ed), *The Decline of the Guru the Academic Profession in the Third World* (Palgrave Macmillan 2003)

McCullagh D, 'What Larry Didn't Get' (Cato Institute 4 May 2009) <https://www.cato-unbound.org/2009/05/04/declan-mccullagh/what-larry-didnt-get> (accessed January 15, 2019).

MacDonald K, 'Building a Modern Prosecuting Authority' (2008) 22 *International Review of Law, Computers & Technology* 7

McGuire M and Dowling S, 'Cybercrime: A Review of the Evidence Chapter 1: Cyber-Dependent Crimes' (2013) 75 *Home Office Research Report*

McKay S, *Blackstone's Guide to the Investigatory Powers Act 2016* (Oxford University Press 2017)

McKay S, *Covert Policing Law and Practice* (Oxford University Press 2010)

McNair B, 'The Internet and the Changing Global Media Environment' in Chadwick A and Howard P, *Routledge Handbook of Internet Politics* (Routledge 2009)

Menthe D, 'Jurisdiction in Cyberspace; a Theory of International Space. *Cyber Harvard* [1998]

Meral Z, 'Muslim-Majority States and Human Rights: From the UDHR to Durban Conference' (2009) 5 *Religious Compass* 876

Mill J, *On Liberty* (1859, reprint Amazon Classics 2017)

Mill J, *Utilitarianism* (1879 reprint The Floating Press 2009)

Mill J, *Utilitarianism and On Liberty Including Mill's 'Essay on Bentham' and Selections from the Writings of Jeremy Bentham and John Austin* (Warnock M (ed) 2nd Edition, Blackwell 2003)

Moafa F, 'Classifications of Cybercrimes-Based Legislation: A Comparative Research between the UK and the KSA' (2014) 4 *International Journal of Advanced Computer Research*

Mohammed K, في داخل اروقة قسم السويدي في الرياض *Inside the Alswaidi Department in Riyadh* (Private memo 2017)

Montagu C, *Civil Society in Saudi Arabia: The Power and Challenges of Association* (Chatham House 2015)

Morgan C, 'About the Internet Architecture Board' (Internet Architecture Board May 2016) <https://www.iab.org/2016/05/23/about-the-internet-architecture-board/> (accessed September 18, 2018).

Mousmouti M, 'Making Legislative Effectiveness an Operational Concept: Unfolding the Effectiveness Test as a Conceptual Tool for Law-making' (2018) 9 *European Journal of Risk Regulation* 445

Munday R, 'The Royal Commission on Criminal Procedure' (1981) 40 *Cambridge Law Journal* 193

Murray A, *Information Technology Law; The Law of Society.* (4th Edition, Oxford University Press 2019)

Murray A, *The Regulation of Cyberspace: Control in the Online Environment* (Routledge-Cavendish 2007)

Murray A & Klang M (eds), *Human Rights in the Digital Age* (Glass House Press 2005)

Murray D and Fussey P, 'Bulk Surveillance in the Digital Age: Rethinking the Human Rights Law Approach to Bulk Monitoring of Communications Data' (2019) 52 *Israel Law Review* 31

Naar I, 'Saudi Crown Prince Announces 4 New Laws to Reform Kingdom's Judicial Institutions' *Alarabiya News* (Riyadh, 2021) <https://english.alarabiya.net/News/gulf/2021/02/08/Saudi-Vision-2030-Saudi-Crown-Prince-announces-reforms-to-improve-legislative-environment->

Nasasra M, 'The Frontiers of Empire: Colonial Policing in Southern Palestine, Sinai, Transjordan and Saudi Arabia' (2021) 59 *Journal of Imperial and Commonwealth History* 899

Naseeb M, Algarba M and BinSaeed E, *القانون الدستوري السعودي: دراسة قانونية تطبيقية Saudi Constitutional Law: legal Empirical Study* (القانون والإقتصاد Economy and Law 2011)

Newburn T, *Handbook of Policing* (2nd edition, Routledge 2012)

Newburn T and Jones T. *Private Security and the Public Policing* (Clarendon Press 1998)

Newburn T and Peay J. *Policing Politics, Culture and Control* (Hart Publishing 2012)

Newburn T and Reiner R, 'From PC Dixon to Dixon PLC: policing and policing powers since 1954' [2004] *Criminal Law Review* 601

Newburn T, Williamson T and Wright A, *Handbook of Criminal Investigation* (Willan Publishing 2009)

Nurunnabi M, 'The preventive strategies of COVID-19 pandemic in Saudi Arabia' (2021) 54 *J Microbiol Immunol Infect* 127

O'Malley P. *Risk, uncertainty, and government* (Glass House Press 2004)

Obaid R, 'Saudi Arabia had 7mln cyberattacks in 2021' [2021] Zawya. <https://www.zawya.com/mena/en/legal/story/Saudi_Arabia_had_7mln_cyberattacks_in_2021-SNG_205663554/> (Accessed September 13, 2021)

Obeidat O and Zaza A, 'The New Anti-Commercial Fraud Law in the UAE: AN IP Perspective' [2017] <http://www.tamimi.com/en/magazine/law-update/section-15/february-9/the-new-anti-commercial-fraud-law-in-the-uae-an-ip-perspective.html> (accessed March 12, 2018).

Oparnica G, 'Digital evidence and digital forensic education' (2016) 13 *Digital Evidence and Electronic Signature Law Review* 143

Opdenakker R, 'Advantages and Disadvantages of Four Interview Techniques in Qualitative Research' (2006) 7 *In Forum Qualitative Sozialforschung* 1

Otto J M, *Sharia and National Law in Muslim Countries* (Leiden University Press 2008)

Oxford Dictionaries. <https://en.oxforddictionaries.com> (accessed March 12, 2019).

Pakes F, *Comparative Criminal Justice* (4th Edition, Taylor and Francis Group 2019)

Peters R, *Punishment in Islamic Law. Theory and Practice from the Sixteenth to the Twenty First Century (*Cambridge University Press 2005)

Plater D, 'The Changing Role of the Modern Prosecutor: has the notion of the "Minister of Justice" Outlived its Usefulness?' (PhD thesis, University of Tasmania 2011)

Police Crime Prevention Initiatives Limited. About Security by Design. Police CPI Ltd. <https://www.securedbydesign.com/> (Accessed November 12, 2020)

Police Foundation and Policy Studies Institute, *The Role and Responsibilities of the Police* (Policy Studies Institute 1996)

Police Station Representatives Accreditation Scheme. <https://www.sra.org.uk/solicitors/accreditation/police-station-representatives-accreditation> (Accessed November 16, 2020)

Poyser S and Milne R, 'No Grounds for Complacency and Plenty for Continued Vigilance: Miscarriages of Justice as Drivers for Research on Reforming the Investigative Interviewing Process' (2015) 88 *Police Journal* 265

Qaisi N, ' الجرائم الإلكترونية الموجهة ضد مستخدمي الانترنت دراسة مسحية لبعض مستخدمي الانترنت بالمملكة العربية السعودية Cybercrime Directed Against Internet Users in the KSA' (MA dissertation, Imam Muhammed Bin Saud Islamic University 2010)

R v Gold and Shifreen [1988] 1 AC 1063

Regina v Exall and Others [1866] Kingston Crown Court, Surrey Spring Assizes, (929)

Regina v H [2004] UKHL 3

Reichel P, *Comparative Criminal Justice Systems; A Topical Approach* (7th edition, Pearson 2018)

Reza, S, 'Due Process in Islamic Criminal Law' (2013) 46 *Washington International Law Review* 1

Richards T and Richards L, 'The Way Ahead in Qualitative Computing' (2003) 2 *Journal of Modern Applied Statistical Methods*

Romaniuk S and Manjikian M (ed), *Companion to Global Cyber-Security Strategy* (1st edition, Routledge 2021)

Rose R, *learning from Comparative Policy* (Routledge 2005)

Roycroft M, *Police Chiefs in the UK Politicians, HR Managers or Cops?* (Palgrave 2016)

Saifi A, *الأحكام العامة للنظام الجنائي في الشريعة الإسلامية والقانون General Principles of Criminal law in Sharia and Legislation* (دار المطبوعات الجامعية University Prints House 2013)

Salameh M, 'The Development of Legal Education in Kingdom of Saudi Arabia' (2017) 11 *Fiat Justisia Journal of Law* 290

Salomon E, *Guidelines for broadcasting regulation* (2nd edition, Commonwealth Broadcasting Association 2008)

Sanchez R, 'Saudi Arabia's crown prince promises to lead his country 'back to moderate Islam' *The Telegraph* (24 October 2017) <https://www.telegraph.co.uk/news/2017/10/24/saudi-prince-promises-lead-country-back-moderate-islam/> (Accessed January 7, 2020)

Sandywell B, 'On the globalisation of Crime: The Internet and New Criminality', in Jewkes Y and Yar M (Ed), *Handbook of Internet Crime* (Routledge 2011)

Saudi Digital Library <https://sdl.edu.sa/SDLPortal/Publishers.aspx> (Accessed 20 October 2021)

Saudi Gazette. King orders setting up of National Cyber Security Authority. Saudi gazette <http://saudigazette.com.sa/article/520782/SAUDI-ARABIA/King-orders-setting-up-of-National-Cyber-Security-Authority> (accessed 24 March 2018)

Saudi Press Agency. General / Supreme Council of the Judiciary: No penalty for suspicion . either conviction or innocence. Saudi Press Agency 03/01/2019. <https://www.spa.gov.sa/search.php?lang=en&search=Supreme%20Council%20of%20the%20Judiciary> (accessed 14 February 2019).

Saudi Press agency, 'سمو ولي العهد يعلن عن تطوير منظومة التشريعات المتخصصة His Royal Highness Crown Prince Announces the Development of Specialised Legislation System' (28 February 2021) <https://www.spa.gov.sa/2187777>

Saudi Press Agency, 'Saudi Federation for Cyber Security and Programming Board Formed' (7 January 2018). <https://www.spa.gov.sa/1706467> (accessed 24 May 2018)

Saunders J, 'Tackling cybercrime - the UK response' (2017) 2 *Journal of Cyber Policy* 4

Schiffrin A, 'Disinformation and democracy' (2017) 71 *Journal of International Affairs* 117

Schmitt M (Ed), *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (Cambridge University Press 2017) 107

Schonberger V M, 'Demystifying Lessig' (2008) 4 *Wisconsin Law Review* 713

Schrag P, 'Progressive California: The Long Road Back' (2016) 27 *American Prospect* 11

Schwartz P M, 'Beyond Lessig's Code for Internet Privacy: Cyberspace Filters, Privacy Control, and Fair Information Practices' (2000) 54 *Wisconsin Law Review* 751

Secret Barrister, *Fake Law the Truth about Justice in the Age of Lies* (Picador 2020)

Segal A, 'China's Alternative Cyber Governance Regime, submitted before U.S. China Economic Security Review Commission' (Council on Foreign Relation 2020) <https://www.uscc.gov/sites/default/files/testimonies/March%2013%20Hearing_Panel%203_Adam%20Segal%20CFR.pdf> (Accessed 20 August 2021)

Shalhoob A, *' النظام الدستوري في المملكة العربية السعودية بين الشريعة الاسلامية والقانون المقارن Constitutional Law in the KSA in Comparison with Comparative Law'* (Published on the expense of the author 1999)

Sharaf A, 'Community Policing: Prospects of Implementation in the Kingdom of Saudi Arabia' (PhD thesis, University of Aberdeen 2009)

Shareef A, *الوجيز في شرح قانون الإجراءات الجزائية السعودي The Brief on Explaining the KSA Criminal Procedural Law* (Arab World Library 2016)

Sheehy P, *Inquiry into Policing Responsibilities and Rewards* (Cm 2280, London 1993) <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/273130/2280_i.pdf> (accessed 1 July 2020).

Sherry V N, ‘Bad Dreams: Exploitation and Abuse of Migrant Workers in Saudi Arabia’ (2004) 16 *Human Rights Watch*

Shore M, Du Y and Zeadally S, ‘A Public-Private Partnership Model for National Cybersecurity’ (2011) l3 *Policy & Internet* 1

Siddique M, Khan A and Zia K, ‘The influence of Religion and Culture on HR practices: A Comparative study of Saudi Arabia and Iran’ (2016) 8 *Business & Economic Review* 35

Silverman D, *Doing Qualitative Research* (2nd Edition, Sage Publication 2005)

Smith B and Brook-Holland L, ‘UK arms exports to Saudi Arabia: Q&A’ (House of Common Library 2021) <https://researchbriefings.files.parliament.uk/documents/CBP-8425/CBP-8425.pdf> (Accessed September 01, 2021)

Smith G J H, *Internet Law and Regulation* (3rd Edition, Sweet & Maxwell 2002)

Smith L and Abouammoh A, *Higher Education in Saudi Arabia Achievements, Challenges and Opportunities* (Springer 2013)

Spencer J, ‘Adversarial vs Inquisitorial Systems: is There Still Such a Difference?’ (2016) 20 *International Journal of Human Rights* 601

Staden W, ‘An Investigation into Reducing Third Party Privacy Breaches During the Investigation of Cybercrime’ (2015) 106 *SAIEE Africa Research Journal*

Strobl S, ‘Policing in the Eastern Province of Saudi Arabia: understanding the role of sectarian history and politics’ **(**2015**)** 26 *Policing and Society* 544

Sundaresh M and Siew T G, ‘Key challenges in tackling economic and cybercrimes’ (2012) 15 *Journal of Money Laundering Control London* 243

Supiot A, *Homo Juridicus: On the Anthropological Function of the Law 2006 ‘Translated by Saskia Brown’* (Verso 2017)

Szabo and Vissy v Hungary 37138/14 (Court (Fourth Section)), [2016] ECHR 579

Taha J, *النظرية العامة لحقوق الإنسان بين الشريعة الإسلامية والقانون الوضعي General theory of human rights between law and Sharia* (الحلبي Alhalabi 2009)

Taylor S J, Bogdan R and DeVault M, *Introduction to Qualitative Research Methods: A Guidebook and Resource* (John Wiley and Sons 2015)

Thomas D and Hodges I, *Designing and Planning Your Research Project: Core Skills for Social and Health Researchers* (Sage Publications 2010)

Tomkins A, 'Justice and Security in the United Kingdom' (2014) 47 *Israel Law Review* 305

Trechsel S and Summers S (assistance), *Human Rights in Criminal Proceedings* (Oxford University Pres 2005)

Troeller G, *The Birth of Saudi Arabia Britain and the Rise of the House of Sa'ud* (Routledge 2013)

Turkle S, *Life on the Screen. Identity in the Age of the Internet* (Toutchstone 1997)

Turner, J, 'Managing Digital Discovery in Criminal Cases' [2019] *Journal of Criminal Law & Criminology* 237

Tyler T and Huo Y, *Trust in the Law: Encouraging Public Cooperation with the Police and Courts* (Sage 2002)

Tyler T, 'Legitimacy and criminal justice: The benefits of self-regulation' (2009) 7 O*hio State Journal of Criminal Law* 307

Tyrer v UK application No. 5856/72, 1978. <https://www.bailii.org/eu/cases/ECHR/1978/2.html> (Accessed June 14, 2021)

UAE Federal Law No 1 2006 on Electronic Transactions and Electronic Commerce

UAE Federal Law No 5 on Combating Cybercrime 2012

Udah A, *التشريع الجنائي الإسلامي مقارنا بالقانون الوضعي Islamic Criminal law with comparison to Legislation,* (دار الحديث Talk House 2009)

UK Administrative Court Judicial Review Guide 2018 <https://www.judiciary.uk/wp-content/uploads/2018/11/Admin_Court_JRG_2018_content_v3_web.pdf> (Accessed May 15, 2021)

UK Code for Crown Prosecutors <https://www.cps.gov.uk/publication/code-crown-prosecutors> (Accessed June 15, 2021)

UK College of Policing, 'Authorised Professional Practice: The Extraction of Digital Data from Personal Devices' (3 October 2020) https://beta.college.police.uk/article/consultation-extracting-data-electronic-devices-released (Accessed October 17, 2021)

UK College of Policing, 'Investigative Interviewing' <https://www.app.college.police.uk/app-content/investigations/investigative-interviewing/> (Accessed June 22, 2021)

UK College of Policing, 'Professional Training, Digital and Cybercrime, <https://www.college.police.uk/What-we-do/Learning/Professional-Training/digital-and-cyber-crime/Pages/Digital-and-cyber_crime.aspx> (Accessed November 10, 2020)

UK Coroners and Justice Act 2009

UK Courts and Tribunals Judiciary <https://www.judiciary.uk/about-the-judiciary/the-justice-system/jurisdictions/criminal-jurisdiction/> (accessed February 17, 2020)

UK Criminal Procedure and Investigations Act 1996.

UK Criminal Justice and Police Act 2001

UK Data Protection Act 2018

UK Data Retention and Investigatory Powers Act 2014

UK Government, 'Being arrested: your rights' <https://www.gov.uk/arrested-your-rights/legal-advice-at-the-police-station> (accessed February 17, 2020)

UK Government, 'Confidence in the Local Police' (March 2020) <https://www.ethnicity-facts-figures.service.gov.uk/crime-justice-and-the-law/policing/confidence-in-the-local-police/latest> (Accessed October 11, 2020)

UK Government Communication Headquarters <https://www.gchq.gov.uk/what-we-do> (accessed September 17, 2018)

UK Government, 'UK Defence and Security Export Statistics for 2019' (2020) https://www.gov.uk/government/statistics/uk-defence-and-security-export-statistics-for-2019/uk-defence-and-security-export-statistics-for-2019 (Accessed September 02, 2021)

UK Her Majesty's Crown Prosecution Service Inspectorate, 'Report to the Attorney General on the Inspection of the Serious Fraud Office' (HMCPSI. 2012) <https://www.justiceinspectorates.gov.uk/crown-prosecution-service/wp-content/uploads/sites/3/2014/04/SFO_Nov12_rpt.pdf> (Accessed October 17, 2021)

UK Her Majesty's Crown Prosecution Service Inspectorate <https://www.justiceinspectorates.gov.uk/hmcpsi/> (Accessed June 29, 2021)

UK Her Majesty's Inspectorate of Constabulary and Fire & Rescue Services, 'Cyber: Keep the Light on An Inspection of the Police Response to Cyber-Dependent Crime' (HMICFRS, October 2019) <https://www.justiceinspectorates.gov.uk/hmicfrs/wp-content/uploads/cyber-keep-the-light-on-an-inspection-of-the-police-response-to-cyber-dependent-crime.pdf> (Accessed October 1, 2020)

UK Home Office, 'Computer Misuse Act 1990: Call for Information' (2021) <https://www.gov.uk/government/consultations/computer-misuse-act-1990-call-for-information> (Accessed September 18, 2021)

UK House of Lords Select Committee on Communications, 'Regulating in a digital world' (2017-19 HL Paper 299).

UK Human Rights Act 1998

UK Information Commissioners Office, ‘Mobile phone data extraction by police forces in England and Wales, Investigation Report’ (2020) <https://ico.org.uk/media/about-the-ico/documents/2617838/ico-report-on-mpe-in-england-and-wales-v1_1.pdf> (Accessed November 14, 2021)

UK Intelligence Services Act 1994

UK Investigatory Powers Act 2016

UK Investigatory Powers Commissioners Office <https://www.ipco.org.uk/> (Accessed November 13, 2021)

UK IPAB, 'Five year strategic partnership with Kingdom of Saudi Arabia Ministry of the Interior – Continuation Training across multi-disciplinary activities' (RE No: 427, 2016) <https://www.statewatch.org/media/documents/news/2016/jun/uk-ipab-saudi-forensics-partnership-torture.pdf>

UK Justice and Security Act 2013.

UK Legal Aid Sentencing and Punishment of Offenders Act 2012.

UK Ministry of Defence, ‘1990/1991 Gulf Conflict’ <https://webarchive.nationalarchives.gov.uk/20120816163733/http://www.mod.uk/DefenceInternet/AboutDefence/WhatWeDo/HealthandSafety/GulfVeteransIllnesses/19901991GulfConflict.htm> (Accessed June 19, 2020).

UK Ministry of Justice, ‘Criminal Procedure and Investigations Act 1996 (section 23(1)) Code of Practice Revised in accordance with section 25(4) of the Criminal Procedure and Investigations Act 1996 and presented to Parliament pursuant to section 25(2) of the Act’ (2020) <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/931173/Criminal-procedure-and-investigations-act-1996.pdf>

UK Ministry of Justice, 'Post-legislative assessment of the Fraud Act 2006: Memorandum to the Justice Select Committee' (2012) <http://www.justice.gov.uk/downloads/publications/corporate-reports/MoJ/2012/post-legislative-assessment-fraud-act-2006.pdf> (accessed March 12, 2019).

UK National Crime Agency, 'What we do' <https://www.nationalcrimeagency.gov.uk/what-we-do/crime-threats/cyber-crime> (accessed April 17, 2020)

UK National Cyber Security Strategy 2016-2021 <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/567242/national_cyber_security_strategy_2016.pdf> (Accessed January 14, 2020)

UK National Cyber Security Strategy 2022 <https://www.gov.uk/government/publications/national-cyber-strategy-2022/national-cyber-security-strategy-2022#part-1-strategy> (Accessed January 02, 2022)

UK National Police Chief's Council, 'Dedicated Cybercrime Units Get Million Pound Cash Injection' (11 April 2019) <https://news.npcc.police.uk/releases/dedicated-cybercrime-units-get-million-pound-cash-injection> (accessed April 20, 2020)

UK National Police Chief's Council, 'Policing Vision 2025' <https://www.npcc.police.uk/NPCCBusinessAreas/ReformandTransformation/PolicingVision2025.aspx> (accessed April 20, 2020)

UK Police (Northern Ireland) Act 2000

UK Police Act 1997

UK Police and Criminal Evidence Act 1984

UK Police and Criminal Evidence Act interrogation code of practice code C, E.

UK Police and Criminal Evidence Act powers and Code A.

UK Procedure and Investigations Act 1996

UK Regulation of Investigatory Powers Act 2000

UK Security Service Act 1989

UK Serious Fraud office, 'About us' <https://www.sfo.gov.uk/about-us/> (Accessed January 30, 2020).

UK Solicitors Disciplinary Tribunal <https://www.solicitorstribunal.org.uk> (Accessed November 14, 2021)

UK Solicitors Regulatory Authority <https://www.sra.org.uk/> (Accessed November 14, 2021)

UK The Crown Prosecution Service (CPS), 'Police and CPS Relations' (CPS 2018) <https://www.cps.gov.uk/legal-guidance/police-and-cps-relations>

UK Youth Justice and Criminal Evidence Act 1999

UK Youth Justice Board, 'About US'< https://www.gov.uk/government/organisations/youth-justice-board-for-england-and-wales/about> (Accessed May 20, 2021)

UN High Commissioner for Human Rights, 'Compilation on Egypt A/HRC/WG.6/34/EGY' (February 21, 2019)

UN High Commissioner Office for Human Rights, 'The Core International Human Rights Treaties' (OHCHR) <https://www.ohchr.org/documents/publications/coretreatiesen.pdf> (Accessed September 22, 2021)

UN Office on Drugs and Crime. Justice For Children <https://www.unodc.org/unodc/en/justice-and-prison-reform/cpcj-justice-for-children.html> (Accessed May 14, 2021)

UN Human Rights Office of the High Commissioner, 'Status of Ratification Interactive Dashboard' (OHCHR) <https://indicators.ohchr.org/> (Accessed October 12, 2021)

UN Human Rights Office of the High Commissioner, 'Optional Protocol to the Convention Against Torture (Opcat) Subcommittee on Prevention of Torture' (OHCHR) <https://www.ohchr.org/en/hrbodies/opcat/pages/nationalpreventivemechanisms.aspx > (Accessed June 30, 2021)

Universal Declaration of Human Rights, G.A. res. 217A (III), U.N. Doc A/810 at 71 (1948)

Universal Periodic Reports from the UN and UNESCO reports <https://en.unesco.org/countries/saudi-arabia> (Accessed September 13, 2021)

Universal Periodic Review - Saudi Arabia. <https://www.ohchr.org/EN/HRBodies/UPR/Pages/SAindex.aspx> (Accessed November 13, 2021)

University of Leeds, Research ethics and integrity <https://ris.leeds.ac.uk/research-ethics-and-integrity/>(accessed September 21, 2021)

US Department of State, 'Saudi Arabia 2017 Human Rights Report' <https://www.state.gov/documents/organization/277507.pdf> (accessed April 11, 2019)

USA CLOUD Act 2018

Vanderstoep S and Johnston D, *Research Methods for Everyday Life Blending Qualitative and Quantitative Approaches* (Jossey-Bass 2009)

Vogel F B, *Islamic Law and Legal System. Studies of Saudi Arabia* (Brill Leiden 2000)

Wagner P, 'Information Wants to be Free: Intellectual Property and the Mythologies of Control' (2003) 103 *Columbia Law review*

Walden I, *Computer Crimes and Digital Investigations* (Oxford University Press 2007)

Wall D S, 'Cybercrimes: New Wine, No Bottles' in Wall D, *Cyberspace Crime.* Reissued in (2018 by Routledge)

Wall D S, *Crime and Deviance in Cyberspace* (2nd series, Ashgate 2009)

Wall D S, *Crime and the Internet* (Routledge 2001)

Wall D S, *Cybercrime; The Transformation of Crime in the Information Age* (Polity Press 2007)

Wall D S, 'Policing Cybercrimes: Situating the Public Police in Networks of Security within Cyberspace' (2007) 8 *Police Practice and Research: An International Journal* 183

Wall D S, Levi M, Doig A, Gundur R and Williams M, 'The Implications of Economic Cybercrime for Policing, Research Report with Cardiff University' (City of London Corporation, October 2015)

Wall D S and Williams M, 'Policing Cybercrime: Networked and Social Media Technologies and the Challenges for Policing' (2013) 23 *Policing and Society* 409

Walker C, *Crime, Criminal Justice, and the Internet* (Sweet and Maxwell 1998)

Walker C, 'Reforming the Crime of Libel' (2006) 50 *New York Law School Law Review* 169

Walker C and Staniforth A, 'The Amplification and Melding of Counter-Terrorism Agencies: From Security Services to Police and Back Again' in Walker C and Masferrer A (eds), *Counter-Terrorism, Human Rights and the Rule of Law: Crossing Legal Boundaries in Defence of the State* (Edward Elgar 2013)

Walsh A, 'What Has Changed in Policing since the Arab Uprisings of 2011? Surveying Policing Concepts and Modes of Contestation' (Arab Reform Initiative 2020) <https://www.arab-reform.net/publication/what-has-changed-in-policing-since-the-arab-uprisings-of-2011/> (Accessed September 13, 2021)

Weber I and Lu J, 'Internet and Self-Regulation in China: The Cultural Logic of Controlled Commodification' (2007) 29 *Media, Culture & Society* 772

Webley L, *Qualitative Approaches to Empirical Legal Research* (Oxford 2010)

Wegman J, ‘Computer Forensics: Admissibility of Evidence in Criminal Cases’ [2005] JLERI

Wehrey F, ‘The Authoritarian Resurgence: Saudi Arabia’s Anxious Autocrats’ (2015) *26 Journal of Democracy* 71

Wheeler D, ‘Islam, Community, and the Internet: New Possibilities in the Digital Age’ (2002) 2 *Journal of Education, Community and Values* 1

White M D and Marsh E, ‘Content Analysis: A Flexible Methodology’ (2006) 55 *LT*

Williamson T, *Investigative Interviewing, Rights, Research, Regulation* (Willan 2006)

Woolmington v Director of Public Prosecutions [1935] AC 462

Xanthaki H, ‘An Enlightened Approach to Legislative Scrutiny: Focusing on Effectiveness’ (2018) 9 *European Journal of Risk Regulation* 431

Yamin M and Mattar R, ‘E-Government in Saudi Arabia - An Empirical Study’ (2016) 8 *BIJIT - BVICAM’s International Journal of Information Technology* 944

Yar M and Jewkes Y (Ed), *Handbook of Internet Crime* (Routledge 2011)

Yar M and Jewkes Y, ‘Policing Cybercrime: Emerging Trends and Future Challenges’ in Newburn T (ed), *Handbook of Policing* (2nd edition, Routledge 2008)

Yar M and Steinmetz K, *Cybercrime and Society* (3rd Edition Sage 2019)

Yaroshevsky E, ‘Prosecutorial Disclosure Obligations’ (2011) 62 *Hastings Law Journal* 1321

Yazbeck Y, Barbara H and Stowasser F (Eds), *Islamic Law and the Challenges of Modernity.* (Altamira Press 2004)

York J and Hunasikatti M, ‘Egypt's Draconian New Cybercrime Bill Will Only Increase Censorship’ (Electronic Frontier Foundation July 12, 2018) <https://www.eff.org/deeplinks/2018/07/draconian-new-cybercrime-bills-vietnam-and-egypt-will-only-increase-censorship> (Accessed September 03, 2019)

Yousef R, ‘United Arab of Emirates Experience on Tackling Cybercrime Regarding E-commerce’ (2000) 50 *Jordanian Journals for Libraries and Information* 127

Zada S and Zada M, ‘Codification of Islamic Law in the Muslim World: Trends and Practices’ [2016] *Journal of Applied Environmental and Biological Sciences* 163

Zander M, *The Police and Criminal Evidence Act 1984* (8th Edition, Sweet and Maxwell 2018)

Zekos G, *State Cyberspace Jurisdiction and Personal Cyberspace Jurisdiction* (Oxford University Press 2007)

Zuboff S, *The Age of Surveillance Capitalism* (Profile Books 2019)

Appendices

Appendix A: Interview information sheets

Information about the research.

The research is entitled *Anti-Cybercrime legislation in the Kingdom of Saudi Arabia (KSA): An analysis and evaluation to the KSA criminal procedure approach to cybercrime with reference to the England and Wales (UK jurisdiction)* It aims to make an academic assessment of the ability of the KSA's law of criminal process to combat cybercrime fairly and effectively. To do this it evaluates the role of *Sharia* in regard to the criminal process law regarding cybercrime. Furthermore, the research analyses the KSA *Vision 2030* role in combating cybercrime in a procedural sense. Finally, the research suggests lessons from other countries, especially the UK which is one of the leading countries in terms of modern law, including the criminal process law regarding cybercrime. The project is being conducted for a PhD at the University of Leeds (UK) and has been approved by King Saud University (where I am a lecturer in law) and financed by a scholarship from the government of the KSA.

Information about participation

Your participation in this research is fully voluntary and optional. The main aim of participation is to collect data for the research based on your practical expertise and experiences as an elite professional by interviewing you for around one and a half hours. Your practical expertise and experiences are rarely found in reliable written sources due to their practical nature. Therefore, it is one of my objectives to collect this practical data and put them into an academic framework.

Interviews will consist of multiple questions related to the research. They will be audio recorded but, if you do not feel comfortable about being recorded, I ask your permission to write your answers down instead.

All questions are related to the research where we raise inquiries about the current approach in policy, law, and practice of the KSA regarding criminal process of cybercrime. The research takes a general approach, so personal cases where individuals are identified should not be mentioned, though hypothetical examples of case types can be given.

Confidentiality of participation

Confidentiality in this context means that all data and information regarding participation in this research must and will be kept secret, and no one will have access to them except for me. I am obligated by the law and by codes of ethics set by the university and by other academic bodies to not reveal any information whatsoever about participation in this research, and I am also obligated to encrypt all information and data collected from you. For example, based on the UK Data Protection Act 2018, the University of Leeds Code of Practice on Data Protection, and the General Data Protection Regulation, I am obligated to ensure the confidentiality of you and not to disclose any information whatsoever which identifies you or might lead to you being identifiable in the write-up of the research.

It is up to you to choose the platform where you want to be interviewed. My advice to ensure your confidentiality is to choose a secure platform such as Facetime, Google due and Microsoft Teams, and please keep in mind that your participation must stay confidential.

Consent form

In order to ensure your voluntary and informed involvement, I will provide you with a consent form to be signed by you and I (in your onle presence). The consent form explains the nature of participation and gives you the option of withdrawal two weeks after the interview has been completed.

Data storage

All data collected, whether voice records or handwritten notes, will be put onto my own laptop computer immediately after the interview along with the code name assigned to each participant to ensure confidentiality and anonymity. As well as ensuring confidentiality, I am obligated by the law and by codes of ethics to ensure your anonymity so no one will identify you. After putting all those data onto my own computer, they will be encrypted immediately using a sophisticated encryption programme approved by University of Leeds which is called Cryptainer. Then, after the encryption, all data will be uploaded onto the secure internet-based drive provided to me by the University of Leeds. Because the University of Leeds provides a very secure network drive, putting the data after encrypting them onto the University internet drive will ensure that no one will have access to them except for me. Also, in order to ensure confidentiality and anonymity, all non-encrypted data, whether they are original versions (such as written notes) or copies on the computer will be destroyed.

Contact details

Abdulmajeed Alsulami
Email: lwaka@leeds.ac.uk
Phone numbers: +447470810954
+966558181977

Appendix B: Interview guide

This guidance is not a detailed interview schedule. It is only an outline narrative the purpose of which is to show the headings that will be covered in the interview.

Section 1: Introduction

This section will cover the following:

1. Introduce the researcher to the participants.
2. Give an overview of the thesis, including the main objectives and the purposes of the study and its importance.
3. Explain how their involvement will assist me in understanding legal challenges in practice, not only in law and policy.
4. Explain how long the interview will last and what it should cover.
5. Give an outline narrative of the interview.
6. Explain how their data will be recorded, stored, protected, anonymised and reported.

7. Explain how confidentiality will be maintained.

Section 2: Personal profile

This section will include questions related to participant's expertise on the subject matter. All questions that will be asked in this section will be about their career and their experience of the criminal process of cybercrime.

Section 3: The KSA response to cybercrime; policy and environment

In this section, participants will answer several questions about what holds the KSA back from tackling cybercrime in a procedural sense. Participants will also answer several questions about how the KSA response to cybercrime is different since the KSA *Vision 2030* was launched in regard to both policy and security responses.

Section 4: Saudi legal response to the cybercrime and the criminal process of cybercrime. Assessment for the existing laws and the role of Sharia

In this section, participants will answer several questions about the KSA's legal response to cybercrime and criminal procedure. Participants will also answer several questions about the existent law and policy related to the criminal procedure of cybercrime. What are those laws? Are they fair and effective? In this section, participants will answer several questions about their opinion on the role of Sharia regarding the criminal process of cybercrime. Additionally, they will answer questions regarding policing, investigating, prosecuting, and trying cybercrime.

Section 5: General suggestion

The participant will have the chance to add any other relevant information regarding the subject matter.

Section 6: Conclusion

In conclusion,

1. The researcher will thank the participants for their time and for the data given during the interview.
2. Remind them that they still have a chance to withdraw within a week without reason and with no consequences.

3. Ask them if they have anything they want to ask.
4. Remind them that, if they have any queries about their involvement in this study or if they have any additional information to add to not hesitate to contact the researcher through the official channel: lwaka@leeds.ac.uk

Appendix C: Consent form

Participant consent form

Consent to take part in [Anti cybercrime legislation of the Kingdom of Saudi Arabia (KSA): An analysis and evaluation to the KSA Criminal Procedure Approach to Cybercrime with reference to the UK and the England and Wales Jurisdictions (UK jurisdiction)]	Add your initials next to the statement if you agree
I confirm that I have read and understand the information letter dated […] explaining the above research project and I have had the opportunity to ask questions about the project.	
I understand that my participation is voluntary and that I am free to withdraw within 2 weeks after the interview is completed without giving any reason and without there being any negative consequences. In addition, should I not wish to answer any particular question or questions, I am free to decline. In case you need to contact me, you can either send an email to lwaka@leeds.ac.uk or call on +966558181977 All the information provided will be completely eliminated after withdrawal.	
I understand that a part of collecting data is to voice recording interviews; therefore, I allow my interview to be voice recorded and consent to written notes being taken.	
I understand that my name will not be linked with the research materials, and I will not be identified or identifiable in the report or reports that result from the research. I understand that my responses will be kept strictly confidential.	
I agree for the data collected from me to be stored and used in relevant future research in an anonymised form.	
I understand that relevant sections of the data collected during the study, may be looked at by my supervisors and auditors from the University of Leeds where it is relevant to my taking part in this research. I give permission for these individuals to have access to my records.	
I agree to take part in the above research project and will inform the researcher should my contact details change during the project and, if necessary, afterwards.	

Name of participant	
Participant's signature	
Date	
Name of lead researcher	Abdulmajeed Kuwayran H Alsulami
Signature	
Date*	

*To be signed and dated in the presence of the participant.
Once this has been signed by all parties the participant should receive a copy of the signed and dated participant consent form, the letter/ pre-written script/ information sheet and any other written information provided to the participants. A copy of the signed and dated consent form should be kept with the project's main documents which must be kept in a secure location.

Appendix D: Data management plan

The Data Management Plan (DMP) ensures that the data collected for the research is generated and stored using an accessible shareable format. This will enhance the quality and rigour of the research, and will help in maximising its impact. The researcher is aware of and complies with the University of Leeds's Data Management Guidelines.

Existing Data

The research is entitled *Anti-Cybercrime legislation in the Kingdom of Saudi Arabia (KSA): An analysis and evaluation to the KSA criminal procedure approach to cybercrime with reference to the England and Wales (UK jurisdiction)*. It generally evaluates and analyses the existing laws of the KSA regarding the criminal process of cybercrime, whether they are based on legislation or *Sharia*. Additionally, the possibility of transferring policies from countries with better approaches of tackling cybercrime in a procedural sense will be covered in the research particularly the UK. In order to pursue those aims, it is an objective for the researcher to base the collection of data on primary sources, such as legislation and books. Also, secondary sources are considered and referred to throughout the research. As well as

the documentary data, interviews will be conducted as a major method of producing data for the research.

Data Collection

The interviews will produce qualitative data. Semi-structured, online interviews will be conducted with (elite interviewees). They have been selected based on their expertise on the subject matter and will include judges, prosecutors, defence lawyers, police officials and organisations that have dealt with relevant cases, in term of the criminal process of cybercrime. The interviews will be conducted in Arabic, the native language of both the interviewer and interviewees, and it will be audio recorded after a written permission is given by each participant individually and their contents will be transcribed. The sub-populations that the researcher will chose interviewees from are as follows: ((**list has been changed see Table 3.1**))

1. The public police - 3 members
2. The public prosecutor office - 3 members
3. The criminal court - 2 members
4. *Sharia* law experts (*Ulama*) - 2 members
5. Royal court "law-making authority" - 2 member
6. Saudi entities: Ministry of Finance - 2 members, Ministry of Interior - 2 members, Ministry of Communications and Information Technology - 2 members, and National Cybersecurity Authority - 2 members.
7. Private lawyers - 2 members
8. Cybersecurity experts - 2 members
9. Human right public organization in the KSA - 2 members
10. Human right private organization in the KSA – 2 members
11. Law professors – 2 members

Privacy

Consent forms will be provided which allow research participants to determine whether they will allow their data to be shared.

Data collected from individuals will be anonymised and encrypted using the software *Cryptainer*. All the data will be kept in encrypted documents that will be uploaded to the University of Leeds cloud drive. They will not be disclosed to anyone except for the researcher. Original recording and written statements will be digitalised and then be stored under code names.

The research will completely comply with the KSA laws on data protection. In addition to the KSA law on data protection, the researcher will comply with General Data Protection Regulation and UK Data Protection Act 2018.

Data Analysis

Qualitative interview transcripts and field notes will be analysed. Data analysis will be conducted in accordance to the research objectives and aims. All participants will be given code names in order to avoid violating terms of confidentiality and anonymity. Those code names will be essential in further analysis. There is no doubt about the processes to be followed, and the student has undertaken training courses, reading of literature, and supervision on the relevant processes.

Analysing the data will be according to issues raised in the research chapters. All linked concepts will be organised and categorised putting similar data into groups that have common characteristics. To start analysing and grouping the data into different categories, the data must be analysed deeply to ensure a full understanding of what has been said, making it easy to code and analyse the data considering the research chapters. After that, the researcher will identify themes, which emerge as an outcome of the previous stages.

Because there is no software that supports the Arabic language, including the last version of NVivo, data will be transcribed and translated into the English language in order to use NVivo as a main instrument of analysis. One use of NVivo is to use keywords or search terms, derived from key issues set out in the thesis chapters (especially as derived from the research objectives), to search the transcripts, and all linked concepts will be gathered into categories created by the research using NVivo. The coding will be by way of words or terms

such as phrases or concepts. This approach is suitable, given the conceptualisation of the thesis.

Data Sharing

Original data will not be shared with anyone; only processed and anonymised data published in the thesis or academic publication will be shared.

Quality assurance (security/ storage)

All the interviews will be conducted and transcribed in Arabic. During data collection, data will be recorded either by audio recording or by handwritten notes. All participants will be aware that their participation will be anonymous, even if quoted. Care will be taken at all stages to ensure that handwritten notes do not contain any information that can directly or indirectly identify the participants. All data will be stored in an encrypted file using *Cryptainer*. All codes will be uploaded to the University drive, which is password protected, as soon as possible and removed from the laptop using appropriate data elimination software.

Therefore, it can be said that after each interview, any handwritten notes will be digitalised. Then, both voice recordings and handwritten notes will be uploaded onto the researcher's laptop and encrypted using *Cryptainer*, and will then be uploaded onto the University cloud, and then original non-encrypted data will be destroyed, whether digital or otherwise. In case of academic challenges or for publication purposes, data will be completely eliminated after 3 years from the award of the thesis.

Ethical issues

This research will involve human participants for interviewing and collecting data proposes. The interview will be undertaken by selecting individuals who possess expertise on the subject matter. Individual selection will include judges, prosecutors, defence lawyers, police officials and anon-governmental agencies who have been involved with the field of the criminal process of cybercrime. In total, there will be 30 interviewees, all Saudis. **((Numbers have been changed see Table 3.1))**

In order to keep track of the data, all interviews will be recorded and then transcribed as soon as possible. The researcher aims to use audio recordings as a first option, after the consent is given by each participant. Audio recording preserves the original and complete format of the interview, and is also an effective way of saving time and providing the interviewer with

more time to concentrate on the participant's response. As for the second option, note- will be employed during the time the interview is conducted along with the audio recording and in case the participant did not give the permission to record the audio digitally. Every participant will be able to decide how they want to be recorded.

In order to ensure the anonymity of the audio recordings, the recorded interview will be uploaded onto the University drive and transcribed into a document, which will be encrypted and uploaded onto the university drive. The original will be deleted from the recorder. Other records in hard copy format will be scanned and transferred into digital formats, and they will be kept on the university drive, in accordance with the University of Leeds data protection policy. The original hard copies will be eliminated once they are on the digital cloud.

An invitation letter will be provided to participants, and they will be given an information sheet that explains the research and the terms of their participation, such as how their data will be used, how their anonymity will be ensured, that their participation is voluntary and how they are free to withdraw within 2 weeks after the interview is conducted. When participants agree to take part in the study, they will be given an informed consent form to read and sign in order to ensure that their rights are protected in accordance with the law and university policy.

All personal data that might identify participants such as their names, addresses, telephone numbers, and positions will not be published in order to ensure their anonymity. Additionally, other information which might indicate who the participants are will not be released and confidentiality will be maintained at all times.

Copyright/Intellectual Property Rights

Intellectual property data will remain with the University of Leeds. However, the University's policy for the management of research data requires that all data arising from research projects be made available where possible. The researcher is not going to make any data available for anyone but himself. It will be encrypted and uploaded to the cloud and it will not be made available to anyone. The research will not use any data covered by the Copyright, Designs and Patents Act of 1988, or any other similar data legislation.

Responsibilities

The researcher will undertake overall responsibility for implementing the data management plan. The Faculty IT manager will be responsible for ensuring that the permissions of the electronic files are properly assigned and provide advice on other aspects of data storage and security. The data management plan will be monitored in meetings with supervisors. Immediately after each interview, the physical data will be digitalised, and then physical data will be destroyed, and digitalised data will be encrypted using *Cryptainer* and uploaded to the University cloud.

Appendix E: Interview Schedule

The main propose of conducing this fieldwork is to collect data that is related to the criminal processes to deal with cybercrime in the KSA. Even though the main method of collecting data in my research is study of literature, the professional experts in the KSA possess much unpublished knowledge about the criminal process of cybercrime in the KSA and so can greatly enrich my research.

Please be assured that as a researcher, I must protect the confidentiality and anonymity of each participant under all circumstances as obligated by the law and by the rules of the University of Leeds (UK) in which I am registered for my PhD.

Questions will be about general experiences and ideas rather than specific cases. Therefore, interviews must not breach professional confidence, and the interview may be halted if such information is divulged.

Code for the interviewee ( )

A. General questions

A1. Can you please tell me your job title and area of expertise?

A2. How long and in what ways have you had experience of involvement with the criminal processes relating to cybercrime?

B. Questions about the KSA overall response to the criminal process of cybercrime

In this section I shall ask about the criminal process overall, by which I mean the procedure that a person accused of a cybercrime would go through. The procedures can include identifying the person accused of cybercrime, then possibly detaining them, interrogating them, collecting evidence, building a criminal case against them (including though victims, witnesses and experts), prosecuting them and trying them. The questions in this section will be generally about the KSA response to the criminal processing of cybercrime;

B1. What is your opinion on how, if at all, is the KSA way of dealing with the criminal processing of cybercrime different or special compared to other crimes offline?

B2. In your view, how well known and understood are the existing laws regarding the criminal processing of cybercrime in the KSA? What do you think about the levels of (a) clarity and (b) detail and (c) coverage?

B3. What in your opinion are the main obstacles or limitations that the criminal process faces regarding dealing with cybercrime?

B4. Do you think the KSA policies about cyberspace give enough attention to the criminal processing of cybercrime? Are there enough resources and sufficient priority compared to other crimes?

B5. Do think there are limitations which hold back (a) the government (Ministry of Justice or Ministry of the Interior) or (b) the legislators from tackling cybercrime in terms of the criminal process? If so what and how?

C. Questions about fairness and effectiveness of criminal process of cybercrime

C1. Do you think the KSA criminal process responses to cybercrime are (a) effective or (b) fair?

C2. How do you measure in your perspective what is (a) effective or (b) fair?

C3. What is required by (a) effectiveness and (b) fairness in KSA criminal process which might be improved upon in regard to cybercrimes in KSA?

C4. Do you think there are any factors which hold back the KSA from tackling cybercrime (a) effectively or (b) fairly?

C5. What is your opinion on how, if at all, is the KSA policy regarding the criminal process of cybercrime might be affected by the KSA Vision 2030?

C6. Do you think there are any other social and political changes in the KSA which might have an effect on the criminal processing of cybercrime?

C7. What is your view on how, if at all, does Sharia affect the KSA law of criminal process regarding cybercrime in terms of (a) efficiency and (b) fairness?

D. Questions about law and policy overall regarding the criminal process of cybercrime

This section contains questions about the KSA response to the criminal processing of cybercrime both in law and policy. The questions in this section will be about the different stages of the criminal process of cybercrime (Policing, Investigation, Prosecution, and Trial).

D.1 Questions about law and policy regarding the criminal process of cybercrime: policing

D1.1. How well in your view is the policing of cybercrime in the KSA designed and established? Are the KSA policing institutions fit for purpose for dealing with the policing of cybercrime? What institutional reform is required, if any?

D.1.2. In your perspective, are the police in the KSA sufficiently trained to deal with cybercrime?

D.1.3. In your perspective, are the policing powers (a) sufficient and (b) fairly and effectively used in regard to cybercrime? What are the most important policing powers which can be used to tackle cybercrimes? What are the most frequently used powers?

D.2 Questions about law and policy regarding the criminal process of cybercrime: Investigation and prosecution

D.2.1. What in your experience are the most relevant and important KSA investigation and prosecution powers regarding cybercrime? Are they used appropriately in accordance with their legal purposes?

D.2.2. Do you think it is fair and effective to vest the power of prosecuting and investigating cybercrime in one entity ie Public Prosecution.

D.2.3. Do you think that investigators and prosecutors are trained sufficiently well to deal with cybercrime? Do they have access to sufficient resources? Are computer experts sufficiently available to help the criminal process? Do defence lawyers or defence forensic experts have a role at this stage?

D.3 Questions about law and policy regarding the criminal process of cybercrime; Trial

D.3.1. How well developed and appropriate are the mechanisms in KSA law for presenting cyber evidence in courts and taking judicial decisions on cybercrime? Overall are trials about cybercrimes handled fairly and effectively in court or not?

D.3.2. Do you think the criminal judges are sufficiently well trained to deal with cybercrime?

D.3.3. Do you think criminal judges take appropriate account of (a) legislation about cybercrimes and (b) sharia. Is there any imbalance between these two sources?

D.3.4. In your view, do criminal judges apply effective and fair sentences to cybercriminals?

D.3.5. Do you think Prosecutors build criminal cases with appropriate consideration to cybercrime legislation and Sharia principles?

D.3.6. In your experience, to what extent are experts available in the criminal courts during the criminal processing of cybercrime?

D.3.7. In your perspective, do cyber experts play an appropriate role in the course of cybercrime cases?

D.3.8. Do you think an accused of cybercrime needs a defence lawyer during the trial? If present, what roles do defence lawyers play during the trial stage?

D.3.9. What is your view on the following issues that could affect the effective and fair criminal processing of cybercrime: disclosure; delay and costs; and legal aid?

D.4 Questions about law and policy regarding the criminal process of cybercrime: international aspects

D.4.1. How does the KSA law compare in your view with cybercrime law and policy in other countries (such as the UAE, or France, the US or UK) – is it better or worse?

D.4.2. Are international law standards on cybercrime process currently embodied in KSA laws? Are you aware of international law standards affecting cybercrimes which might improve the KSA law?

D.4.3. What mechanisms have you experienced or know about for the cooperation between the KSA and other countries regarding the criminal processing of cybercrime. Are they helpful or not? Are they often relevant or not? Which countries might be relevant to cybercrimes in the KSA?

F. Others

F.1. Is there any further information regarding the subject matter you want to share? Are there any other points you wish to make based on your knowledge and experience of dealing with cybercrimes?

G. Special questions for each sub-population

G.1 Special questions: police officers

G.1.1 What does a typical cybercrime investigation look like for the police? Which officer and department deals with it and is there anything special or difficult about such an investigation for the police?

G.1.2. Do you think the situation is different after passing the Criminal Procedure Law 2001? Did the 2001 Law make the situation fairer and more effective?

G.1.3. How often does it happen (if at all) and in what circumstances might a criminal investigation contain flaws in the procedure? What sort of faults might occur?

G.1.4. Do you think the 2013 Law is helpful to police officers? Do breaches of powers given by the 2013 Law occur in cybercrime cases, and if so how?

G.1.5. In your view, are the rights of a person accused of cybercrime sufficiently protected?

G.1.6. In your view how appropriately are issues such as (a) the disclosure of evidence, (b) availability of experts, (c) legal aid for the suspect, and (d) delays dealt with?

G.1.7. In your view are the Public Prosecution and the Criminal Court doing a good job in the criminal processing of cybercrime?

G.1.8. Do you think it is fair and effective for members of the Public Prosecution to both prosecute and investigate cybercrime at the same time?

G.1.9. What is your view on criminal judges being allowed to reinvestigate cybercrime cases during the trial?

G.1.10. Do you have any experience of enforcement processes based on a foreign inquiries or mutual legal assistance regarding cybercrime?

G.2 Special questions: members of the Public Prosecution: detectives and Prosecutors

G.2.1. What does a typical cybercrime investigation look like for the prosecution? Which officer and department deals with it? Is there anything special or difficult about such an investigation for the prosecution?

G.2.2. In your experience, which investigation powers are commonly selected, and how do they work in the context of cybercrime?

G.2.3. In regard to members of the Public Prosecution who prosecute and investigate cybercrime at the same time, what do you think is the balance of their duties and is one done better than the other?

G.2.4. Are the rights of accused with cybercrime protected appropriately at this stage?

G.2.5. In your view how appropriately are issues such as (a) the disclosure of evidence, (b) availability of experts, (c) legal aid for the suspect, and (d) delays dealt with?

G.2.6. Do you have any experience of enforcement processes based on a foreign inquiry or mutual legal assistance regarding cybercrime?

G.2.7. In your experience, how often you rely on cyber forensic experts and technology to present evidence in criminal court in connection with cybercrimes?

G.2.8. What is your view on criminal judges reinvestigating cybercrime cases during the trial?

G.2.9. In your view, are the Police and the Criminal Court doing a (a) fair and (b) effective job in the criminal processing of cybercrime?

G.3 Special questions: Criminal judges

G.3.1. In your view, what are suitable judicial qualifications to deal with cybercrimes. Should there be specialist computer expertise? Should criminal judges be trained in cyber technology?

G.3.2. Do you think knowledge of the specialist legislation more important than knowledge of Sharia?

G.3.4 Are there any special or common features in how criminal judges deal with the processing of cybercrime and cyber evidence? How is it different to non-cyber crimes?

G.3.5. Do you think it is fair and effective to deal with the criminal process of cybercrime as non-cyber crime by relying only on Sharia? IS Sharia clear enough on this topic? Should it be codified?

G.3.6. Do you have any experience of enforcement processes based on a foreign inquiry or mutual legal assistance regarding cybercrime?

G.3.7. Do you think the rights of those accused with cybercrime are appropriately protected?

G.3.8. In your view how appropriately are issues such as (a) the disclosure of evidence, (b) availability of experts, (c) legal aid for the suspect, and (d) delays dealt with?

G.3.9. Do you consider the different nature of cybercrime in your rulings, verdicts or sentences? If so, how?

G.3.10. What is your view on criminal judges reinvestigating cybercrime cases during the trial? Is it appropriate? How is it done, if at all?

G.3.11. In your view, are the Police and the Public prosecutors (a) fair and (b) effective in the criminal processing of cybercrime?

G.4 Special questions: lawyers

G.4.1. Do you think the rights of persons accused with cybercrime are protected appropriately in terms of having a lawyer available during the process?

G.4.2. Based in your experience, what are the main special issues that face lawyers when dealing with the criminal process of cybercrime?

G.4.3. Do you think codifying Sharia is a necessary step in order to achieve more fairness and effectiveness in regard to the criminal process of cybercrime? Why?

G.4.4. Based on your experience, what possible legal solutions might be suggested in order to overcome the flaws, if any, within the criminal procedure such as violating privacy and human rights?

G.4.5. In your view how appropriately are issues such as (a) the disclosure of evidence, (b) availability of experts, (c) legal aid for the suspect, and (d) delays dealt with?

G.4.6. Do you have any experience of enforcement processes based on a foreign inquiries or mutual legal assistance regarding cybercrime?

G.4.7. In your view, are the Police and the Public prosecutors and the Criminal Courts doing well in the criminal processing of cybercrime?

G.5 Special questions: Law Professors

G.5.1. Do you think codifying Sharia is a necessary step in order to achieve more fairness and effectiveness in regard to the criminal process of cybercrime? Why?

G.5.2. Based on your experience, what possible legal solutions might be suggested in order to overcome the flaws within the criminal procedure such as violating privacy and human rights?

G.5.3. Do you think the rights of accused with cybercrime are protected?

G.5.4. In your view how appropriately are issues such as (a) the disclosure of evidence, (b) availability of experts, (c) legal aid for the suspect, and (d) delays dealt with?

G.5.5. In your view, are the Police and the Public prosecutors and the Criminal Courts doing well in the criminal process of cybercrime?

G.5.6. In your opinion, do you think Sharia experts understand the nature of cybercrime especially in terms of the criminal process?

G.5.7. In your view, what is the appropriate role of Sharia in regard to the criminal process of cybercrime?

G.5.8. In your opinion, what part is played by prosecutor and what part is played by the criminal judges in regard to the criminal process of cybercrime?

G.6 Special questions: Sharia experts

G.6.1. Do you think there the specialist KSA legislation about the criminal processing of cybercrimes compliant with Sharia? If not, why not?

G.6.2. Based on your knowledge, do you agree that Sharia can protect human rights in relation to the criminal process of cybercrime? Why and how?

G.6.3. What in your opinion has Sharia to say about the criminal processing of cybercrime?

G.6..4 In your opinion, do you think law professionals understand Sharia especially in terms of its principles regarding the criminal process ?

G.6.6. Do you think codifying Sharia is a necessary step in order to achieve more fairness and effectiveness in regard to the criminal process of cybercrime? Why?

Appendix F: Six summaries of cybercrime cases (translated from the original Arabic) found in the Judicial Rulings Collection, released by KSA MoJ in 2017. Vol 13.

1. The Public Prosecutor instituted a case against a male defendant and sought to prove his guilt for sending emails via his own personal e-mail to the plaintiff (also a claimant of a private right) and other persons' e-mails that contained *Qathf*. In other words, he insulted the others. The prosecutor demanded the imposition of a sentence which was the *Hadd* [singular of *Hudud]* of *Oathf* and to the penalty mentioned in Paragraph 5 of Article 3 of the ACL 2007. When the accused was confronted in the CC with the facts, he acknowledged them but argued that he had already apologized to the plaintiff for that. Then, the plaintiff was summoned to the CC and claimed a private right, and claimed as the prosecutor claimed, that the punishment of *Qathf* be imposed on the accused. In view of his acknowledgment, the judge convicted him, and he was sentenced to eight lashes for slander, while the request of the person

claiming the private right to punish him with *Ta'zer* was dismissed because the *Hadd* of *Qathf* was sufficient. He was also sentenced to two months imprisonment and received a fine of five thousand Riyals. The parties objected, but the judgment was upheld by the Court of Appeal." [2255]

2. "The Public Prosecutor instituted his case against a female defendant and demanded that she prove her allegations to avoid a conviction for defaming others and harm them through social media by tarnishing the reputation of one of the halls designated for celebrations. She claimed that she had found insects in the food presented to her, publishing this in websites of communication in the information network. When presenting the case to the plaintiff's lawyer, he admitted that his client had published the aforementioned news, and he asserted that the Bureau of Investigation and Public Prosecution did not investigate the defendant nor did they investigate the news attributed to that hall, even though it is relevant to the judgment. By confronting the prosecutor with that point, he said that the investigation authority was satisfied with the questioning of the defendant by the arresting authority based on the Criminal Procedures Law, and given that the Anti-Cybercrime Law stipulated that investigation of crimes to under this law is within the jurisdiction of the Bureau of Investigation and Public Prosecution, and as this text is private and it shall precede the general text found in the Criminal Procedure Law. Because neither the defendant nor the news attributed to that hall was investigated the case was blemished with a fundamental error. Hence, the judge decided not to hear the prosecutor's case against

[2255] Ministry of Justice. Judicial Rulings collection 2017. Vol 13. 268-269

the defendant. Although the prosecutor objected, the judgment was upheld by the Court of Appeal."[2256]

3. The Public Prosecutor filed a claim against a male defendant, to justify his conviction of possessing, selling and storing pornographic films, and relating this to offending religious values and public morals by the means of the information network. The prosecutor asked for the accused to be sentenced to the penalty mentioned in Article 6 of the Anti Cybercrime Law. When the case was presented to the defendant, he acknowledged its validity, and given the applicability of the offense description contained in the Anti-Cybercrime Law against the defendant, the conviction for what was attributed to him was proven to the judge in the case, and a sentence was imposed of one year in prison, three hundred time-separated lashes, a fine of five thousand riyals, an oath not to return to such a crime and destruction of the seized confiscation with the recommendation that he be deported to his country after completing his sentence. Both parties objected, and the judgment was confirmed by the Court of Appeal."[2257]

4. The Public Prosecutor instituted a case against a male defendant and sought to prove his conviction for the possession of pornographic clips and images stored on his mobile phone, and for blackmailing a woman through an audio recording found on his mobile phone. The prosecutor asked for a Ta'zer punishment and confiscation of his mobile phone. When presenting the case to the defendant, he denied its authenticity. By requesting the evidence from the public prosecutor, he relied on the evi-

[2256] *Ibid* 273-274
[2257] *Ibid* 282

dence contained in his case file, including the arrest warrant and the reports for inspection by the arresting and investigating authorities that support the validity of the case as well as the presence of a witness who testified to the pornographic and immoral materials in the accused's mobile phone along with the audio recording for the extortion of the woman, as the witness saw him. So, the conviction of the defendant was proven to the judge, and the judge sentenced him to one month imprisonment, ten lashes in one session, and ordered that the two mobile phones used in the crime be confiscated. The public prosecutor objected, but the judgment was confirmed by the Court of Appeal."[2258]

5. The Public Prosecutor instituted a case against a male defendant and sought to prove his conviction for the possession of pornographic materials that violate religious values and public morals and storing them on his mobile phone. The prosecutor requested a prison sentence to be applied along with the fine mentioned in the first Paragraph of Article 6 of the Anti-Cybercrime Law. Also, the prosecutor requested the confiscation of the mobile phone. Upon presenting the case to the defendant, he denied its authenticity and argued that he had obtained a memory card from one of his friends and that he was not aware of its contents. On a request for his evidence from the public prosecutor, he relied on the evidence contained in the case file, including the briefing record and arrest warrant that supported what was stated in the case file, and given that the defendant is not a Muslim. Because the evidence presented by the public prosecutor was not sufficient to convict the defendant nor did it strengthen the accusation against him with the validity of what was attributed to him, it was not enough for the judge to prove the defendant's conviction of possession of

[2258] *Ibid* 286

pornographic material, and he decided to dismiss the prosecutor's request of imposing the penalty stipulated in the Anti-Cybercrime Law against the accused. But, for suspicion, a punishment of twenty days imprisonment and seventy lashes at a time was imposed. The public prosecutor objected, but the judgment was confirmed by the Court of Appeal."[2259]

6. "The public prosecutor instituted a case against a male defendant and sought to prove his conviction for photographing a young girl, releasing her pictures, and possessing pornographic video clips on his mobile phone. The prosecutor requested the penalty stipulated in the Anti-Cybercrime Law with a disciplinary penalty, and confiscating the accused's mobile phone. When confronting the accused with the case, he admitted that it was true, and therefore it was established to the judge that the defendant was guilty of photographing a girl and publishing her pictures, and possessing sex video clips and pictures of girls on his mobile phone. The defendant was sentenced to three months in prison, received repeated lashes in three instalments and a fine of two hundred riyals, and had his mobile phone confiscated. The Public Prosecutor objected, but the judgment was confirmed by the Court of Appeal."[2260]

[2259] *Ibid* 291-292
[2260] *Ibid* 295