Protection of human rights – the relationship between the individual and the stat...

ABSTRACT

This dissertation contains five chapters dedicated fully to examine and analyse the relationship between the State and the individual citizen of the State. Specifically analysing whether the state security infringement on citizen's communications, data retention and processing of the same data is in fact interfering with the right to privacy of the individual citizen under Article 8 of the European Convention of Human Rights. The introduction chapter is dedicated to introduce the background to this research study and the reasons for which the topic is a national concern. Research aim, objectives and the significance of the study is also compiled under the introductory chapter.

The Literature review will involve a discussion of the views of the academics, critiques, commentaries and political enthusiasts respect of this growing issue between strategies to protect state security as oppose to privacy rights. This dissertation is solely based on secondary resources. Hence the chapter on research methodology insights on the methods carried out in researching and collecting data for this dissertation. The Data analysis chapter will include an analysis of the discovered data and views on this topic extensively. It includes the position of the State and the individual citizens in this hassle. The concluding chapter will enumerate conclusion drawn from the analysis done in the previous chapter, the future prospects on the said area of research and the recommendations that can be adopted by the State to enhance the current situation with the citizens in respect of protecting their privacy rights and implementing feasible and proportionate strategies to assure state security and preventing crime.

List of Abbreviations

- DPA 1998 – Data Protection Act 1998
- ECHR – European Convention on Human Rights
- ECTHR – European Court of Human Rights
- EU – European Union
- ICA 1985 – Interception of Communications Act 1985
- ISA 1994 – Intelligence Services Act 1994
- RIPA 2000 – The Regulation of Investigatory Powers Act 2000
- UK – United Kingdom

CHAPTER ONE

INTRODUCTION

1. 1 Introduction

Chapter 1 of this dissertation introduces the research case study. This dissertation examines the relationship between an individual and the State. However, focuses more fully on the infringement of citizen’s communications by the State security services. The section ‘ Background of the study’ illustrates the reasons behind the selection of the research topic and the background information on it. ‘ Research aim’ and ‘ Research objectives’ itemise the intended final aim of the research evaluation and the purpose for carrying out this research, respectively. ‘ Research questions’ enumerates the questions that are intended to be discussed and evaluated in the following chapters. ‘ Rationale of the study’ will discuss the practicality,

rationality and lucidity of the of the selected area of research whilst ‘ Significance of the research study’ examines the importance of this selected area of research to the researcher as an individual and more generally, the ‘ Scope of the study’ enumerates the extent and the capacity of the topics covered.

1. 2 Background of the study

When the seriousness of the current terrorist threat to the United Kingdom is evaluated, it is imperative that the Government maintains a high calibre of readiness and promptness to respond to an imminent potential attacks. For the same reason the Government is keen on compiling legislation to both prevent attacks of terrorism and fairly sanction the suspects in order to protect the state.[1] It is a highly debated amongst many Human rights activists and academics whether the Government’s strategies to prevent terrorism and related attacks has attained its dual objective of protecting the state and upholding the individual’s including the human rights of a citizen up to a fair degree. However the same strategies has developed a high level of tension in this dual objective that is between protecting the state and upholding individual rights. This individual is therefore subjected to the anti-terrorism strategies of the Government and thereby exposed to the sanctions and interceptions imposed by the same. It is in this regard that a debate exists over the issue of interception and investigations in to individual communications by the security authorities in the name of national security. The debate led to the disclosure of the extent of the Government authorities accessing the individual records of the citizen’s communication patterns, the increased authority to intercept emails and telephone

conversations and to scrutinize and inspect homes and businesses of the citizens. The lessening of the evidentiary standards which require obtaining court approvals for the collection of the information by Government authorities has been strongly debated[2]. The Government has not given any lucid explanation justifying the legislations on the surveillance and interception powers and strategies used in monitoring the communication and collecting information as yet. Therefore the powers that are extensively given to the security authorities to carry out surveillance, communication interception and data retention measures by the State has in fact deprived the individual citizen’s right to privacy and right to fair trial[3]. Consequently upon such a background, it is vital to examine the extent to which these security strategies imposed by the State balances the status quo between the state security and protection of individual’s human rights regarding the privacy of communication.

1. 3 Research Aim

The aim of the dissertation study is to extensively discuss the relationship between the individual citizen and the state whilst focusing primarily on the infringement of citizen’s communication portals by the law enforcing authorities of the United Kingdom.

1. 4 Research Objectives

To analyse whether the current laws in the United Kingdom effectively confer a blanket cover for the security services to infringe on the privacy of innocent citizens without being accountable for their action.

To identify that the security laws does not confer absolute power on the

security services to pry into citizen’s privacy without adequate checks and balance which is laid out in both European Convention of Human Rights (ECHR) as incorporated to UK law by the Human Rights Act and in UK legislation.

To examine the nature and extent of the powers exercised by the law enforcing authorities in the name of state security.

To study and analyse the recent advancement of law with respect to the social security, state security and surveillance actions.

1. 5 Research Questions

How is the status quo between the competing needs of the State security and protection of individual rights is maintained?

What are the manners in which the government can be held accountable with respect to the powers exercised in the name of state security?

Can the Regulation of Investigatory Act 2000, Data Communication Bill or such subsequent legislations provide an adequate legal framework for any information sharing and disclosure arrangements by the state authorities of the UK to the detriment of the privacy of an individual?

How will the fast developing technological innovations and other social media platforms be relevant to the interception and disclosing strategies imposed by the State authorities?

1. 6 Significance of Study

It is of highest importance to determine whether the state security carries a greater weight than the individual rights when anti-terrorism strategies and security of the state is concerned. Therefore, considering this high level of

importance of the state security, if the individual citizen is to accept and consent to certain forms of surveillance in order to ensure state security, the state should be accountable for its actions. If the State and the law enforcing authorities are left with unfettered discretion to carry out these surveillance strategies, it is of greater disadvantage of the individual citizen and his rights. Therefore, it is vital to examine and analyse this debate and thereby find consequential options and recommendations to maintain the balance between the state security and the protection of individual's privacy rights.

1. 7 Rational of Study

Having said the significance of this research study it is noteworthy to discuss the rationality behind the same. This research tries to examine and critically analyse the UK Government's strategies to uphold state security has attained its dual objective of ensuring social and state security from terrorist and other potential attacks and the protection of citizen's rights. However, in the light of the analysis of recent legislations such as the Regulation of Investigatory Powers Act 2000 (RIPA), Civil Contingencies Act 2004 along with the data advanced Bill, the citizen is made aware of his footing in this dilemma. Further the effectiveness of the RIPA will be examined to determine its continue existence as a viable tool in maintain the balance of trust between disclosure of information to the state and the privacy rights. [4] More over with the fast growing social media platforms and the instant communication methods, it is important to note the extent of the power authorized by the law enforcing authorities to investigate, disclose and intercept the communications that happen via the said instant communication platforms. Therefore it is apparent that the balance between

the civil liberties and the state security is hard earned and often it is hard to trade-off between the two. However this has been a fueled debate for long and this research study aims to continue the said debate between the state security and the civil liberties and to lucidly inspect and criticize the same.

1. 8 Scope of the Research

This research topic examines laws on privacy, laws on surveillance and investigations, human rights, laws on state security and constitutional law. This analysis will be used to examine the rights to privacy, freedom of expression and right to fair trial primarily. In the UK massive growth of state surveillance aimed at crime prevention and detention are mostly unencumbered by law[5]. However the legislations that are passed following the practices and strategies adopted by the state are found to be violating the human rights of the citizens specially the right to privacy. Therefore it is of vital importance to determine the impact of the European Convention of Human Rights has on the legislation respect to the covert surveillance by the state law enforcing authorities. As a result of the intense debate on the above mentioned points there is a large number of literatures on this issue. Therefore the scope of this research study will be concentrating on whether the current laws of UK confer a balance between the state security and the protection of civil liberties of the individuals in addition to whether such laws provide blanket immunity for the state to infringe on the privacy laws of communication of the citizens without being accountable for their actions. The research will be solely based on secondary sources.

1. 9 Summary

Chapter 1 provides directions to the evaluation of the research study which is more fully analysed in the chapters following this chapter. The research study is aimed to explore the social concern relevant to the relationship between the state, state security and individual and protection of his rights. Further analysis will be done on the existing laws relevant to the same.

CHAPTER TWO

LITERATURE REVIEW

2. 1 Introduction

Chapter 2 of this dissertation is dedicated to the literature review. This chapter will consider and evaluate the existing literature on the relationship between an individual and the State, whilst focusing more fully on the infringement of citizen's communications by the State security services. The chapter will more fully review on the infringement of privacy of individuals of the state. Further literature on the analysis of the current legislation which regulates these notions will be examined.

2. 2 Interpretation of the key terms

Before evaluating a detailed discussion of the debate as to the relationship between the State and the citizen with regard to the extent to which the state security measures protects the citizen's right to privacy it is worth noting the specific meanings as to these key terms. A citizen is a legally recognised individual who owes loyalty to and entitled by birth neutralization to the protection of the state[6]. United Kingdom is a sovereign state forming a constitutional monarchy with a parliamentary system.

State security refers to the requirement to maintain the survival of the state through the use of economic power, diplomacy, power projection and political power. It is a matter of national security to ensure the safety of the state against criminal activity such as terrorism, theft or espionage. However the term ‘ national security’ is not defined under any UK law or European law. It is said that the subsequent governments did not define the term for the simple reason that the term should be flexible enough to encompass all changing circumstances[7].

Right to privacy is the most comprehensive and valued right amongst citizen’s to date. There is no definitive definition to the right of privacy of an individual. Article 8 of the ECHR gives an understanding as to what entails the word ‘ privacy’ but however does not define the same. But however in 1990 the Callut Committee on privacy and related matters agreed to a helpful definition. That is, “ the right of the individual to be protected against intrusion into his personal life or affairs, or those of his family, by direct physical means or by publication of information.”[8]

Whenever a threat of violence, terrorism, social disorder or violent crime is likely to occur the UK government spring into full action to safeguard the country, for which they acts extensively sometimes degrading the civil liberties of the citizens. When the government has a reasonable belief that there is a threat to the nation thereupon it will carry out an investigation to determine whether or not the threat is real. Throughout the history there is much technological advancement which has assisted the government in enhancing their power to carry out surveillance in citizens. This constant gaze over the citizens, or rather the anti-terrorism strategies adopted by the

state must have a dual objective at its core. Namely it must equally protect the state and to a fair degree, must uphold the human rights of an individual citizen.

2. 3 Security or Privacy? Is that a false choice?

Above mentioned balance between protections of the society whilst protecting the civil liberties of the citizens is a hard objective to achieve. It was argued by Emily Owen in her articles to the E-international relations students' website that, these two objectives are not mutually exclusive but interdependent[9]. For that simple reason it makes the balancing exercise extremely complex. Privacy advocates argues that a choice between security and privacy is a false one but on the other hand other experts argue that a choice has to be made. Don Solove, a privacy law expert at George Washington Law School, said that privacy vs. security framing has interfered with what could be a healthy national debate about using high-tech tools to fight terror. He further goes onto say that asking the general public whether you want security or privacy is a false choice and is similar to asking ' do you want the police to exist or not?' , however he further mentions that if people wants to make a choice with limitations and transparency, they can make a choice about how much surveillance they are willing to tolerate. He further argues that by creating a tension between security and privacy the governments have intended a heavy weapon to wield against those who raise civil liberty concerns. But however it is a question, he says, that the citizen's have to ask themselves and who would not trade a little personal data to protect another citizen's life?[10]

Although Solove is an American academic speaking of the status in his country after the Edward Snowdan a former technical assistant to the National Security Agency revealed the secret US government programme to establish technical infrastructure to monitor all online communications worldwide, the insights observed by him is valid to UK as well because the disclosure in US has paused arguments all over the world regarding the notion, privacy Vs security[11]. Bruce Schnier argues that the real dichotomy is liberty Vs control and not privacy Vs security[12].

Therefore it is apparent that there is nothing like absolute privacy or absolute security. The circumstances will be changed rapidly and therefore the desires of people and the state is tend to change. [13] With these extensive and hasty changes the society will have to make choices and will have to suffer and tolerate consequences or rather inconveniences[14]. Therefore, there is a balance to be found between citizen’s individual right to privacy and collective right to security. An informed and responsible debate is needed to inquire into the circumstances which justify this perception.

2. 4 Covert surveillance and processing of personal data

The prime problems of information security are privacy and data protection. This is crucial because the data about us can be used for purposes beyond our control. The current interest in privacy concerns is related with surveillance and processing of personal data. Surveillance generally means monitoring the behaviour of persons, objects or systems[15]. However, surveillance needs not to be only a visual process but it can be over a wide array of things using different technologies. Interception of communications

or colloquially known as ‘ wiretapping’ is one of the key type of surveillance methods. This surveillance of personal data to monitor the actions and communications of persons was given a further timely definition by Dr. David Murakami Wood. That is surveillance studies network information with the intent to influence and control aspects of behaviour or activities of individuals or groups. The Data Protection Act 1998 (DPA) and the 1995 European Data Protection Directive 95/46/EC states that processing of personal data shall mean any operation which is performed on personal data whether or not by personal means, such as collection, recording, organisation, storage, adoption, alteration, retrieval, consultation, use, disclosure by transmission dissemination, alignment or combination, blocking, erasure and destruction[16]. Data sharing, data matching and data mining and profiling are the primary types of data processing methods. Whereas the latter concerns analytical tools that to detect patterns in large set of data having the purpose of predicting certain kinds of behaviour of individuals such as the probability to engage in crime and other terrorist activities[17].

2. 5 Contemporary surveillance and data use

The information commissioner argues that individuals leave electronic footprints behind the click of a mouse, making phone call, using a payment card or just walking down a road under CCTV operation. All the information about the citizens lives are tracked, citizens’ intentions is identified and their profiles are maintained all with the objective of ensuring the public protection or rather the security. The Constitutional Committee report on Surveillance states further that National security, public safety, the

prevention and detection of crime, and the control of borders are among the most powerful forces behind the use of a wide range of surveillance techniques and the collection and analysis of large quantities of personal data. With the rapid development of the ICT sector, the technology for monitoring, tracking and identification purposes has also developed. That is with the fast growing amount of software and minute gadgets that can be used for surveillance purposes with maximum level of secrecy and efficiency.

2. 6 Covert surveillance

Covert surveillance includes undisclosed tracking of individuals, interception to communications and the analysis of traffic data[18]. Assistant Chief Constable Nick Gargan, the former Chair of the Covert Investigation (Legislation and Guidance) Peer Review Group within Association of Chief Police Officers told us that " the use of covert surveillance is indispensable to the Police Service and to our colleagues involved in the fight against all forms of criminality…"[19] there are instances in which this covert surveillance may be authorized by law and otherwise. Specifically, covert surveillance may be authorised under the Regulation of Investigatory Powers Act of 2000 (RIPA 2000), if it is either intrusive or directed. Intrusive surveillance is covert surveillance that is carried out in relation to anything taking place on residential premises or in any private vehicle (and that involves the presence of an individual on the premises or in the vehicle or is carried out by a means of a surveillance device) and Directed surveillance is covert surveillance that is not intrusive but is carried out in relation to a specific investigation or operation in such a manner as is likely to result in the obtaining of private information about any person[20]. Surveillance as to

the interception of communication in the course of its transmission is governed by the Part 1 of the RIPA 2000. Part 1 of the RIPA 2000 provides that the interception to communications of the public can only be authorized by the Secretary to the State. However exceptions to the said norm is also included the Part 1 of RIPA 2000 and provides that if one party to the conversation consents then it is deemed as authorization for the purposes of s 48(4) of the RIPA 2000[21].

The RIPA 2000 and the Intelligence Services Act 1994 (ISA 1994) stipulates that a person granting an authorization or warrant for directed or intrusive surveillance must do so in accordance with the belief of the knowledge of the statutory grounds that allows such authorization. Under s 28(3) of the RIPA 2000 an authorization for directed surveillance may be granted by an authorising officer who believes that the authorisation is necessary for an don the grounds that it is; in the interest of national security, for the prevention and detection of crime an disorder, in the interests of public safety, in the interests of the well-being of the economy of the UK, for any other purpose prescribed by an order made by the Secretary of the State in which case the purpose should satisfy the Art 8(2) of ECHR. An authorising officer is interpreted under the s 30(1) of RIPA 2000 to include individuals holding such offices, ranks or positions with relevant public authorities as are prescribed under the schedule 1 of the Act. Whereas, for intrusive surveillance, the authorisation can only be granted by the Secretary of the State for applications by the senior authorising officers, Ministry of Defence or HM forces[22]

RIPA 2000 iterates that the surveillance carried out should be propionate to what is sought to be achieved by carrying it out. Therefore obtaining a warrant under the Act will only ensure that the interception authorised is a justifiable interference with an individual’s rights under the Article 8 of the European Convention of the Human Rights (ECHR). Thereby Secretary of the State should be mindful about the balancing of the interference as oppose to the need for it in operational terms. More over if there are any reasonable means of achieving the objective than intrusion, such means should be sought. However, the practical encumbrance is whether this attentive are met today when surveillance is carried out and citizens’ communication is intercepted.

2. 7 Advantages and disadvantages of Surveillance and interception to communications of the citizens

Protecting the public is a duty of the government. Surveillance by means of CCTV and DNA collection has helped in has effectively helped in detecting, preventing and investigating crime. In this regard Constitution Committee Report refers to Councillor Hazel Harding, Leader of Lancashire County Council and Chair of the Local Government Association Safer Communities Board, suggested that “ the number one issue for people are to feel safe. I think it is more than something people aspire to; I think it is a basic human need”.[23] Collection and processing of public data are important to the development of the public policies. However the crucial disadvantage would be the infringement of privacy of the individuals.

2. 8 The threat to Privacy and trust in the state

However surveillance by its very definition involves a reduction of the privacy. It has been observed by a handful of academics that loss of privacy in some cases may be harmless because of the benefits of the surveillance and data collection.[24] It is argued by professor Ian Loader, Director of the Centre for Criminology, University of Oxford that " it is not only those that who have something to hide that have something to fear, but also something to protect"[25] This is because the individuals would tend to keep their personal affairs private and on a very low profile and would not like the state as a complete outsider interfering with the same. Consequently it is clear that from this violation of the civil liberties of citizens, there is a threat or a disturbance to the relationship between the State and the individual citizen. However it should also be noted that citizens expect security from the state is to protect their rights and liberties and to live and walk free without any hindrance. But this should not overturn that is the security strategies must not take away and impede those rights and liberties from the citizens.

The legal system of UK is based on direct relationships between the individual and the state and therefore the increase of state security strategies erode this fundamental relationship which will in fact result in change in the constitutional strategies of the country. Thereby this loss of trust in the state might result in serious consequences to the functioning of the government. [26]Therefore the Constitutional Committee observes in their report that trust in the state is an essential prerequisite for compliance with the law and as a result anything that undermines trust has the potential to generate resistance and lead to the creation of an antagonistic relationship between the individual and the State[27].

There is a lacuna in the domestic law as to the fact that there is no lucid definition to privacy but however as mentioned above to maintain the flexibility the status is maintained as such. Despite this lacuna, the right to privacy is enshrined in many international documents and national statutes. Remarkably, Article 8 of the ECHR provides the ‘ right to respect for private and family life’. It is noteworthy to mention the significant comment made in the Canadian case of R v Duarte (1990 65 DLR (4th) 240[28] that ‘ one can scarily imagine a state activity more dangerous to individual privacy than electronic surveillance’[29]. Nick Taylor observes that such surveillance strategies have been lawful within the UK even in the absence of legal regulation. [30] Article 8 of the ECHR whilst recognizing the right of privacy also provides for a mechanism to allow individuals to enforce it against the state where the state has infringed their rights under the Convention. There are several principles that have to be noted when interpreting exception to the said general right of privacy of an individual. Citizen’s established right under the convention cannot be interfered unless he is aware that such infringement is in accordance with the law. Such interference should be directed at a specific legitimate objective. More over such interference should be proportionate to mean that the interference to the social right is needed to fulfil a social need and is proportionate reaction to the same. In the light of above principles, the lack of regulations governing the electronic surveillance and interception to communication is challenging.[31]

In the celebrated case of Malone v Metropolitan Police Commissioner No. 2[32], the Defendant was prosecuted for allegedly handling stolen property and during the trial it was revealed that the Defendant had tapped the

telephone of the Plaintiff. The court of first instance found that tapping of telephone is not an infringement of English law. However when Malone took the case to the European Court of Human Rights held that his right to private life has been infringed[33]. It was observed in the said case that, " The requirement of forseeability cannot mean that an individual should be enabled to foresee when the authorities are likely to intercept his communications so that he can adapt his conduct accordingly. Nevertheless, the law must be sufficiently clear in its terms to give citizens an adequate indication as to the circumstances in which and the conditions on which the police are empowered to resort to this secret and potentially dangerous measure."[34] It was in this regard that the UK government compiled the Interception of Communications Act 1985 (ICA 1985). The Act was a failure and only regulated merely public telephone interceptions and the metering of telephone calls. This point is reiterated in case law such as Halford v UK[35]. The consequences of failure of the Act were seen up until the Act was repealed by the RIPA 2000. However it was observed by Taylor and Walker in 2001 that although the Act formulated a legal base as to the interception is questionable whether it created clear boundaries and remedies[36].

In the event of collection of evidence and information through interception of communications and surveillance strategies imposed by the law enforcement authorities, who would thereby infringe Article 8 right to privacy, could still be presented in court proceedings as evidence. This was envisaged in the case of Khan V UK[37]. The case went to appeal to the Court of Strasbourg after the House of Lords dismissed an appeal stating that Article 8 of the

convention did not necessitate the exclusion of the evidence gained as a result of a surveillance device admitted at a suspect’s property. The European Court of Human Rights (ECtHR) held that breach of privacy in this instance could have been generally justified as falling under the exception of ‘ prevention of disorder or crime’. Moreover the court held that if the evidence obtained by breaching article 8 would thereby infringe the individual’s right to fair trial under Article 6 of ECHR, then such evidence should be excluded for the trial. Nevertheless the ECtHR held that considering all the surrounding circumstances there is no harm in admitting the evidence obtained by infringing Article 8 of ECHR.

Police Act of 1997 was brought forward by the Government around this time to regulate the surveillance strategies that could otherwise involve unlawful conduct on the part of law enforcement authorities such as trespass or criminal damage.[38] However as observed and as a response to the case of Harman and Hewitt v UK[39], it was noted that Security Services Act 1989, the Intelligence Services Act 1994 and Security Services Act 1996 has expanded the role of MI5 to aid the Police in investigate into the social threats and detecting serious crimes.[40] This affects the individual in such a way that, larger the number of law enforcing authorities work towards implementing different strategies to intercept communication, more the social liberty and privacy of the individual will be deprived.

RIPA 2000 finally brought a strategic attempt to provide a comprehensive piece of legislation as to the surveillance and other strategies adopted by the government to protect and uplift state security. The means by which this was brought up by the Act was discussed earlier in this chapter. This Act was

widely assisted by the Human Rights Act of 1998 (HRA 1998) by providing a domestic interpretation to the ECHR and thereby upholding the right to privacy of the citizens. The HRA 1998 declares that all legislation of UK has to be read and all public authorities should act, in a way compatible with the rights recognized under the ECHR. Nick Taylor comments that ‘ this would have the effect of ensuring that the target of any unregulated surveillance practice by the state would have a right to a remedy in a domestic court’. [41] Having said that is striking to note that the input of the domestic courts’ interpretation of Article 8 could mean that the regulatory system will have to evolve to meet more exacting standards. Thereby the state should also be able to justify their reasons for infringing such a right under the name of state security and prevention of crime in a court of law.

2. 9 Developments of social media and interception of communication by the State

Social media refers to Internet based applications that enables people to communicate and share resources and information. Blogs, discussion forums, chat rooms, wikis, you tube channels; LinkedIn, Facebook, Twitter and Whatsapp are some examples of social media. Social media can generally be accessed by computer, smart and cellular phones. Social media has grown a social security threat with the high tide of development of it for the past decade.

However even though social media is a threat to national security, it can also be used for the benefit of the government. Government can use social media as a monitoring and warning thereby threat preventing tool. As a monitoring

tool the government is able to recognize the first signs of any hostile or potentially dangerous activity by collecting and analyzing messages in order to try to predict events that could be a danger to national security[42].

In the UK, the question of surveillance on the internet has been the most recent flashpoint. The draft communications bill, announced during the Queen’s Speech has, despite few details currently being known, attracted a long queue of critics and detractors. Privacy and civil liberty groups and politicians have condemned the bill as illiberal, intrusive and indiscriminate. Some oppose, in principle, the colonisation and taming of online spaces that such surveillance entails. The data communication bill is said to be suggesting collecting records of every individual who has communicated with another person or an entity continuously and keeping it stored for one year. These records will also include time and the place of origin[43]. The report further entails that, the Communications Data Bill raises a number of concerns with regards to the right to privacy under Article 8 of the Human Rights Act. There are also concerns about the right to free expression under Article 10 and the right to freedom of assembly and association under Article 11 due to the potential chilling effect of the menace of surveillance. Therefore it is clear that the draft communication data bill in fact re-evaluate the powers of the under the RIPA 2000[44].

2. 10 Summary

Academic reviews and commentaries on the relationship between the state and the individual regarding the surveillance and interception to communications are discussed under this chapter. The status of the

regulations governing this area of law is under high criticism today in UK. It is apparent from the discussion of this chapter that a clear cut answer cannot be given to the question whether the status quo between protection of privacy and the state security is balanced today in the UK. The literature review is written through perusal of secondary sources only. The research methodology will be discussed extensively in the next chapter.

CHAPTER 3

RESEARCH METHODOLOGY

3. 1 Introduction

This chapter sustains a comprehensive discussion on the research methodology that was used in completing this dissertation. This dissertation concerns data and information researched through secondary sources only. Therefore, it is worth noting the impact, effect, benefits and issues in using secondary sources as your research base. Topics that follow this chapter will emphasise on research philosophy, research strategy, data collection methods, techniques and the limitations in carrying out a research using secondary sources.

3. 2 Research philosophy

Research philosophy is the most vital part in writing a dissertation for the simple reason that the quality of the analysis of the dissertation solely depends on a high-quality research. Therefore selecting the accurate and correct research method is crucial. High quality research is a result of an excellent vision. It refers to the assumptions of a mind made related to the visions of theories, facts and figures that one confronts and the way in which

those encounters are interpreted and analysed. The main two types of research philosophies are ontology and epistemology. Ontology concerns the nature of reality and social entities. It particularly deals with how the researcher views the things that happens around him, around the world. Objectivism and subjectivism are the two main propositions under ontological considerations.[45] Objectivism means that the occurrences in the society exist as independent units and has no effect from the difference personnel of the society. On the other hand subjectivism proposes that social occurrences originate due to social interactions and thereby researcher will see the phenomena in his point of view and another would see it in a different angle.[46]

Epistemological considerations constitute the acceptable knowledge in a chosen field of study. It solely depends on the researcher ought judgment on the importance of the study that he is to do. Positivism, realism and interpretativism are the three positions under the philosophy epistemology. Positivism is application of the methods of natural sciences into the social reality. Realism refers to the proposition that what people see is the reality. Interpretativism refers to the understanding the difference between the people in the society and the natural sciences[47].

The relevant research philosophy for this dissertation is ontological method. This concerns the things that constitute reality and how the researcher understands its existence. The current research topic is the relationship between the state and individual with respect to interception of communication by the law enforcing authorities for the purposes of states security. Therefore the reality of the situation depends on how it affects each

and every individual citizen of the state; it depends on how much they care for their privacy rights. Therefore it is clear that the perspective of the reality would differ from person to person and the philosophy used in this dissertation is how the researcher understands the existence of the reality. Further the perception of the researcher solely based on the commitment of researcher in understanding the reality. The position of ontological consideration that is relevant in this dissertation would be the subjectivism approach. It means that the social phenomena are the results of social interactions and that it can also be varied from one viewer to the other. However this dissertation analyses the view of the researcher, how he sees the reality behind the interception of communication by the state authorities and the effect it has on the citizens. The researcher further believes that said perception is as a result of the relationship or rather the social interaction between the state and the individual.

3. 3 Research approach

Research approach refers to the method by which the researcher analyse the data and come into a final conclusion. There are two main types of research approaches. Namely; deductive and inductive research approaches. Deductive research approach involves the researcher deducing a hypothesis on the basis of the knowledge and theoretical considerations in a particular sphere. Whereas, with the inductive approach the researcher infers conclusions from his findings and observations to form a theory[48]. The approach relevant to this dissertation is inductive approach which is also known as ‘ bottom-up’ approach. The researcher will observe the ideas and perceptions of the citizens and then comments of the state with respect to

the strategies adopted by the state to protect the state mainly by surveillance and communication interception. And through these findings and observations, the researcher will conclude in inferring a theory as to whether there will be a balance between protection of the state security and privacy of an individual.

3. 4 Research strategy

Research strategy refers to the process by which the research is conducted. There are two types of research strategies namely qualitative and quantitative. Quantitative research includes quantification in the collection of data and research analysis. On the contrary qualitative research strategy involves gathering of information and data rather than measurements and numbers.[49] What is ideal for this particular dissertation is qualitative strategy for the reason that the research question specifies that the sources that have to be perused are only secondary sources. And there is no requirements as to collect numerical data or rather do a survey as to the same. It only depends on the basis of observations made by the researcher on the available articles, commentaries and views of the academics and the general public which are published in the databases, websites, newspapers, blogs and other related interfaces. This strategy emphasizes on the inductive approach which was discussed above. In analysing the balance between the protection of the state and the privacy of the individuals the researcher has examined and scrutinised secondary sources such as journals, articles, commentaries, blogs, newsletters and newspaper articles and other related academic abstracts. Further no field study or survey was involved. Therefore the research is done in a qualitative manner.

3. 5 Data collection methods

Data collection methods can be differentiated in to several ways. One of which is division between primary and secondary data. Secondary sources generally interpret and analyses primary data. Articles, journals, criticisms, commentaries, blogs and newsletters are a few examples[50]. This dissertation is specified to be done through secondary sources. This is because the research topic concerns analysis of social phenomena, social issues and social interactions. And it is important to examine different ideas of different people of different social stages. Because the effect of strategies imposed by the law enforcing authorities in terms of protection of the state is such that it invades the privacy of the citizens and those effects are different from citizen to citizen. Therefore it is important to review these secondary sources to get a good insight about those viewpoints to conclude the current research topic.

- I. Data collection techniques

Data collection techniques are usually of two different types. That is primary data collection and secondary data collection techniques. Since this research solely based on secondary sources, the relevant technique is secondary data collection[51]. In which previously existing data is collected as to the relevant topic at hand. Therefore the researcher has examined the existing literature and information on the research topic to get a good understanding about the views expressed by citizens on the issue of protection of the state vs. state security.

- II. Data analysis

Analysis of the data collected will be different as to strategies used to collect data and research. That is analysis would be different to both qualitative and quantitative strategies. The thematic approach is the one which is mostly used to analyse data found through qualitative strategy. Thematic approach let the researcher to identify a limited number of themes which adequately reflect the textual data.[52] Therefore the themes use by the researcher relevant to this dissertation are the relationship between the state and the individual in UK, the strategies executed by the authorities to preserve state security, the extent to which the interception of communication has affected the citizens' privacy.

- III. Limitations of research methodology

The key limitation relevant to the current research study is that the researcher is confined to secondary sources as discussed above. Which means only existing work can be examined. The primary data cannot be collected because the views of the citizens with respect to this research topic and those are vividly presented only in secondary sources. The reliability of data is critical in a topic like this which has a huge impact on the society. The relevance of the data used in today's context is also important. Therefore the researcher has to be very much sensitive about the selection of the data.

3. 6 Ethical Issues

Ethical issues are important and affect the quality of the research. Since secondary sources and data are used in this research study, the reliability and relevance of the data examined is vital. It is important to use sources that have publications in the recent history because the world and society

changes rapidly and so are the perceptions of the people. The accuracy of the data is critical for the data analysis. Therefore, the researcher has been cautious as to the selection of sources. Use of unpublished data is erroneous. The quality of the research study and the accuracy of the analysis depends on all of the above.

3. 7 Summary

Selection of the appropriate research methodology is vital for a high quality dissertation because, selection of correct method of data collection, the sources and the analysing method are all equally important in deducing an excellent dissertation. The current dissertation is to determine whether there is a balance between state security and the protection of individual privacy which in fact is a very sensitive topic. Therefore the ontological considerations are used as the research philosophy. Qualitative research strategy is been used for the above mentioned reasons. Thematic approach is used to analyse the data collected through the secondary sources. The research study is limited to secondary sources. The ethical issues are rectified by using relevant, reliable and accurate data and information.

CHAPTER 4

DATA ANALYSIS

4. 1 Introduction

Chapter 03 of this dissertation is dedicated to the data analysis. This chapter will extensively consider and evaluate the existing literature which was construed in the Chapter 02 on the relationship between an individual and the State, whilst focusing more fully on the infringement of citizen’s

communications by the State security services. This dissertation concerns data and information researched through secondary sources only. The chapter will more fully review on the infringement of privacy of individuals of the state. Further it will discuss the position of the EU policies and measures in respect of the same. The chapter will more fully discuss the position of the state and the citizen in this crucial situation.

4. 2 Interception of communication, data retention and the rule of law of the citizen

Rule of Law cannot exist without a transparent legal system. The set of rules that govern the country must be freely accessible to all the citizens. There must be strong enforcement structures, and an independent judiciary to protect citizens against the arbitrary use of power by the state, individuals or any other organization[53]. Therefore the intercept of communication of the citizens and retention of the said collected data potentially offends the rule of law. Because the citizen should be aware of the instances, circumstances in which the State will intercept their communications install surveillance appliances and conduct surveillance.

4. 3 Interception of communication, data retention and the EU

Since September 2001 the European Union has taken steps to, in particular by granting Member State authorities discretion to gather data for security and criminal investigation purposes. EU Justice and Home Affairs Ministers have drafted a Framework Decision on data retention which is under discussion as yet[54]. The proposed measure would oblige Member States to require communications providers to retain for up to two years traffic data

relating to every communication carried, in case of need in a subsequent criminal investigation or prosecution[55].

Directive 2002/58/EC was enacted in mid-2002 to regulate the processing of personal data, including traffic data, on electronic networks[56]. That Directive sensibly and prudently only permitted retention measures where “ necessary, appropriate and proportionate” within a democratic society. Hence the Privacy International argues in their report that the notion of unrestricted, blanket data retention was expressly rejected. The Framework Decision, on the contrary, would compel European businesses to retain communications data, thereby creating a regime far more intrusive. The report argues further that by requiring the accumulation of huge stores of data traffic, containing countless items of private and personal information, it would generate opportunities for abuse by public authorities or private actors, such as hackers. It will follow from this framework if adopted is effects to the competitiveness of telecommunications and network service providers in Europe.[57] Similar stances have been adopted by the member states of the EU by compiling national legislation.

European Convention of Human Rights establishes basic rights and liberties that will cover the citizens around the member states. The implementation of the same is monitored by the former European Commission and currently by the European Council and European Court of Human Rights. The European Court of Human Rights overseas whether the Article 8 of the ECHR is preserved and that is the individual’s right to respect for his private and family life. The Article specifies that public authorities may only interfere with this right in narrowly defined circumstances. Every interference must

be in accordance with law and necessary in a democratic society, in view of such public interests as national security and the prevention of crime. The European Court of Human Rights usually decides upon cases in which state surveillance and interception of communication has affected the citizens. In these cases, the Court adopts a three-part test for assessing the legality: firstly the Court inquires whether a right protected by Article 8 has been interfered with; secondly, it inquires whether the interference was in accordance with law. This enquiry requires not only that there be a basis in domestic law for the interference, but also that the legal basis accord with the principle of the rule of law, that it be accessible and that its operation be foreseeable by all citizens and finally, the Court inquires whether the interference was necessary in a democratic society[58].

European Court of Human Rights by deciding the cases mentioned below provides support for the following conclusion. That is the data retention regime mentioned above as a draft Framework decision and which has in turn adopted by many national legislations are in fact in breach of Article 8 of the ECHR, such is not accordance with rule of law and is not foreseeable to the citizen because of the difference and varying nature of the methods and strategies adopted by the State.

4. 4 A right protected by Article 8 has been interfered

The European Court of Human rights established in the case of Klass v Germany (Series A, NO 28) (1979-80) 2 EHRR 214 that the interception of mail in fact creates a ‘ menace of surveillance’ for all the people who uses mail services and it in fact interferes with the right to respect for private life

under Article 8. In a similar capacity retention of today's' traffic data will in turn be an interference with the right to privacy. Traffic data is defined to be any data which is processed to convey a communication on an electronic communications network and includes the data relating the route, duration and time of a communication[59]. Today the communication services will generate a record of a person's pattern of communication activities and it threatens the users that this record will be abused either by public or private authorities.

In Amann v Switzerland (2000) 30 EHRR 843 the European Court of Human Rights held that it is irrelevant whether the retained data is used against such individual by the public authority's thereafter and hence mere retention or interception of communication is an interference of the right to privacy of an individual. In this case when State security services kept a record indicating that the applicant was a contact of the Soviet Embassy, after intercepting a telephone call from the Embassy to the applicant. The Court specifically noted that storage of the information on an index card alone was sufficient to constitute interference in private life and that the subsequent use of the stored information had no bearing on that finding. There is no distinction between retention of traffic data as opposed to individual communications. This difference has been diminished with the recent advancement of the technology. For the reason that today, mobile phone companies are able to state the exact location from which the call has been made, internet service providers can track every move of its users and address books of emails and social media portals gives out almost all the details about the individual.[60] However ultimately as the European Court

of Human Rights have established interferences with the Article 8 right to privacy of the citizens whether or not the intercepted retained data is used against them.

4. 5 The interference was in accordance with law

Subsection 2 to the Article 8 of the ECHR states the exception to the notion of interference by the state invades right to privacy of an individual. Therefore if the state is acting under those exceptional circumstances then the interference by the State is justified. However the European Court of Justice has interpreted this sub section narrowly and has states that the requirement under the section is such that such interference must be ‘ in accordance with the law’. This is to say that the interference must be authorised by a certain law and it should meet the standards of accessibility and forseeability under the concept of rule of law. Therefore it is clear that as the Privacy International report states that the very idea of blanket data retention offends the standard of foreseeability as it has been developed by the Court.[61] The forseeability requirement means that the State should give adequate indication to the citizens regarding the general and usual instances and circumstances in which the State will intercept communication of the general public and retain the traffic data. By which the citizen is well aware of the unsolicited intrusions and interferences that can occur to their right to privacy.

The European Court of Justice in the case of Malone v United Kingdom (1984) 7 EHRR 14 in respect of secret surveillance held that “ contrary to the rule of law for the legal discretion granted to the executive to be expressed in terms

of an unfettered power, rather what makes a law foreseeable is the extent to which it distinguishes between different classes of people, thereby placing a limit on arbitrary enforcement by the authorities". There are certain instances as the Report by the Privacy International argues that where the State recognises as sufficiently special to warrant a degree of protection would similarly discriminate the principle of foreseaability. For example in the case of Kopp v Switzerland 27 Eur. H. R. Rep. 9 the European Court of Justice decided that a law authorising interception of telephone calls would in certain circumstances contradict other provisions of Swiss law according protection to confidential attorney-client communications. Attorney-Client communications is one good example which experiences a protected status throughout the EU[62]. The academics and critiques hence have criticised that the strategies adopted by the UK government in intercepting the communication for state security purposes does not take any effort to distinguish between such communications.

4. 6 The interference was necessary in a democratic society.

Article 8(2) of the ECHR states that the right to respect privacy of an individual requires that any interference should not be greater than is necessary in a democratic society. European Court of Justice retains the same narrow interpretation in relation to this condition under the Article 8 as well. Privacy International report states in this regard that the principle underlying this requirement must in terms of the need for any interference in Article 8 rights to correspond to a pressing social need and to be proportionate to the legitimate aim pursued. Therefore the blanket interception of communications and retention of data of the citizens fails at

achieving this equilibrium. In the case of Foxley v United Kingdom (2001) 31 EHRR 25 the European Court of Justice found that the interception of a bankrupt’s mail violated Article 8 because of the absence of adequate and effective safeguards ensuring minimum impairment of the right to respect for his correspondence. That is to say that when the State is adopting a strategy to intercept communications of the individual then simultaneously put in place safeguards ensuring that interference with the right to privacy of the individual is no greater than necessary.

In this regard it is apparent that the legislation of law related to blanket data retention and communication interception strategies is not the only feasible option for combating crime or protecting national security. Having the focus on this growing issue all 15 member states that is when the total number of member states were 15 and now there are 28 states, to EU signed a policy decision to the effect that data will be retained on a selective basis where the authorities have reason to believe that the information may be relevant to a criminal investigation. In that way the unnecessary blanket strategies of intercepting communications need not to be implemented. Hence the citizen’s privacy will be protected and unnecessary interferences will be minimal. Thereby the democracy of the country will be guarded.

4. 7 Draft Communications Data Bill

The Draft Communications Data Bill is a report submitted to the Joint Human Rights Committee by Theresa May, the Home Secretary which proposes authorising collection of records of every individual or entity with whom any

given individual has communicated electronically for one year inclusive of the time and location of the communication from which it originated.

It is no surprise that the Draft communication Bill would stand to create a system of blanket collection and retention of data that would definitely fails to distinguish between the classes of people and hence would increase the menace in the citizens regarding their privacy rights. The draft communications data bill has relatively expanded the current period of the retention of data as for the Directive 2006/24/EC from six months to two years. The nature of the bill is such that the state cannot foresee the instances it will apply because of the expansion of surveillance strategies that can be adopted by the State. The RIPA 2000 in fact authorises the Police to self-authorise access to the retained communications data and Privacy International argues that this remains the lowest standard internationally. Because, it is apparent that there is no comprehensive internationally recognised legislation as similar to this draft bill. The necessity of a new draft bill in this regard is minimal due to the fact that RIPA 2000 exists already in the UK under which the Secretary of the State authorises interception of communications.

It is now a known fact that the data communication draft bill is not under consideration anymore. However the UK government is now trying to adopt a middle course for the legitimate law enforcement access of communications data.

4. 8 Regulators of the surveillance and communication interception strategies

As discussed under the Chapter 2 of literature review the RIPA 2000 RIPA established a framework for the use of surveillance and data collection techniques by the police, the security services, and other law enforcement agencies. In addition to criminalising the intercepting of a communication over a public network without consent or a warrant authorised by the Secretary of State, the Act set out the circumstances under which public authorities can engage in various types of surveillance activities. It provided a framework for the authorisation and review of those activities by the Office of Surveillance Commissioners (OSC) and the Intelligence Services Commissioner. Therefore the following crucial regulatory officers who were introduced by the RIPA 200 oversee the surveillance and data use. The Information Commissioner oversees and enforces the Data Protection Act 1998 (DPA 1998) and the Privacy and Electronic Communications Regulations, as well as the Freedom of Information Act 2000 (FOIA 2000). He promotes the protection of personal information by increasing public awareness and by providing guidance to individuals and organisations, and he takes remedial action when the DPA 1998 is breached. The Chief Surveillance Commissioner leads the OSC, which provides oversight of the conduct of covert surveillance and the use of covert human intelligence sources under the RIPA 2000 and the Police Act 1997. The Interception of Communications Commissioner keeps under review the issue and operation of warrants permitting interceptions and the acquisition of communications data under RIPA. The Intelligence Services Commissioner reviews the issue by the relevant Secretary of State of warrants and authorisations for operations by the Security Agencies and Mini