UNIVERSITY OF ESSEX **DISSERTATION**

SCHOOL OF LAW/HUMAN RIGHTS LAW

LLM/MA: LLM
STUDENT'S NAME: Hayriye Keser
SUPERVISORS'S NAME: Nikolaidis Charilaos
DISSERTATION TITLE: Article 8 of European Convention on Human Rights (ECHR) and the Protection of Personal Data .. European Court of Human Rights' New Approaches to the Mass Data Processing

SUPERVISOR'S COMMENTS: (PLEASE WRITE BELOW YOUR COMMENTS)

MARK:	
SIGNATURE:	**DATE:**

UNIVERSITY OF ESSEX

SCHOOL OF LAW / HUMAN RIGHTS CENTRE

SCHOOL OF LAW

LL.M / MA in (insert your DEGREE COURSE)

LLM

Insert your ACADEMIC YEAR

2018/2019

Supervisor:

Nikolaidis Charilaos

DISSERTATION

Article 8 of European Convention on Human Rights (ECHR) and the Protection of Personal Data .. European Court of Human Rights' New Approaches to the Mass Data Processing

Name: Hayriye Keser

Registration Number (optional): 1802950

Number of Words: 16012

Date Submitted: 02/09/2019

1. Introduction

In recent years, data processing has evolved rapidly at short notice with computer-based technologies. These technologies can be used to examine the attitude of large groups or populations as well as the tendency of the consumers and likings of a specific individual. Personal data is being gathered, stored, processed and pervaded the world in many of our daily habits by using the technologies. Similarly, banks and insurance companies rely on risk profiles of customers to take certain decisions, and internet companies like Google and Facebook use such profiles for advertising purposes. On the other hand, it is irrefutable that the increase of data processing is pivotal to advance in the security, efficiency, and convenience of contemporary life in an information rich world. These technologies have supplied considerable developments in terms of the detection and prevention of crime, coordination of medical services, impacts of the public.[1]

Therefore, there are many benefits of technological development as well as harm related to personal data. It is obvious that personal data is wide open to abuse without protection in this digital era. Privacy interests every single human being in his or her most personal and private matters. It is a fundamental human right, however, it is almost constantly in the line of fire due to contemporary technological advancement. In the last decade, the law in Europe and the United States has managed to reinforce the ability of the States to obtain communications data at the expense of privacy.[2] Privacy questions have become an integral part of the international agenda, turning individuals' data protection into a serious global issue. The extent of the exposed surveillance program by the public authorities led to reconsiderations of current policies and technologies. Individuals now fear that both legal and technological means constituted with legitimate purposes, such as counter-terrorism and crime control, are also increasingly used for total social control.[3] While some claim that privacy is dead, others feel that it is now more than ever that privacy needs protection.[4] Thus, the advancement of digital technologies has raised main questions about the role of courts from a fundamental rights approach.[5]

As is common knowledge, the basic document of the European human rights framework is undeniably the European Convention for the Protection of Human Rights[6] (ECHR). Concluded in 1950 within the framework of the Council of Europe, it was designed to protect individuals'

[1] Christopher Kuner, 'Regulation of Transborder Data Flows under Data Protection and Privacy Law: Past, Present, and Future' *TILT Law & Technology Working Paper,* (2010) 331.
[2] Joel R. Reidenberg, 'The Data Surveillance State in the United States and Europe' *Wake Forest Law Review* (2013) 2.
[3] Ilina Georgieva, 'The Right to Privacy under Fire Foreign Surveillance under the NSA and the GCHQ and Its Compatibility with Art. 17 ICCPR and Art. 8 ECHR' *Utrecht J. Int'L & EUR. L,* vol 31(2015) 104.
[4] Bart van der Sloot, 'Privacy as Human Flourishing: Could a Shift towards Virtue Ethics Strengthen Privacy Protection in the Age of Big Data' *J. Intell. Prop. Info. Tech.and Elec. Com. L*,vol 5 (2014) 230.
[5] Evangelia Psychogiopoulou and Maja Brkan, 'Introduction: Courts, Privacy and Data Protection in the Digital Environment' in M. Brkan and E. Psychogiopoulou (eds), *Courts, Privacy and Data Protection in the Digital Environment* (EE Publishing, UK Edward Elgar Publishing, UK 2017) 1.
[6] *European Convention for the Protection of Human Rights and Fundamental Freedoms* (adopted in Council of Europe 4 November 1950, entered into force 1953) ECHR

fundamental rights and freedoms.[7] Individuals may appeal the European Court of Human Rights (ECtHR, the Court) for the breaches of rights that are guaranteed in the ECHR.[8] Therefore, the numerous cases related to the personal data have been brought before the Court. Accordingly, existing law has been needed to interpret in order to conclude these cases. Since, 'The ECHR is a living instrument which … must be interpreted in the light of present-day conditions'[9]. Moreover, the Court has sought to protect fundamental rights by reviewing the interference in the light of public interests as the prevention of disorder or crime or national security. In this regard, the ECtHR is the crucial body to reflect a perspective to the State Parties.[10]

The Court has evaluated the personal data under article 8 of ECHR, in the scope of privacy. However, the concept and value of privacy need careful reconsidering, as the traditional approach to privacy seems unfit to resolve cases which include the threats posed by Big Data which is defined as collecting huge amounts of data without a pre-established goal or purpose, about an undefined number of people.[11]

In this study, firstly, personal data will be examined in its general meaning and background. Then the scope of the personal data will be set out and analysed in terms of the ECtHR's jurisprudence. In the sense of article 8 of the ECHR, the classic cases of the ECtHR which are issued regarded with the protection of personal data will be evaluated. Besides, this study will argue the ECtHR's perception in terms of access to personal data, collection, storage, and disclosure of personal data as important underlying values while discussing cases under Article 8 ECHR. Moreover, it will be addressed how the Court has assessed the proper rationales in order to limit such right. Thereafter, the innovations of the ECtHR will be discussed concerning the complicated cases such as mass data and surveillance. Coping with these challenges how the ECtHR has applied the relevant principles in practice under article 8 of the ECHR. In addition, the Court's role as guardian of the ECHR is particularly vital to scrutiny and assess the Contracting Parties' surveillance activities via the applications, thus, the last part will argue whether the ECtHR's approach could be adequate to resolve these challenging cases.

1.1 The Protection of Personal Data and in more General Extent and its Background

The appearance of data protection laws is not long past. With the emergence of data technology during the 1960s, there was a growing requirement for more specific rules to protect individuals by

[7] Paul De Hert, 'Balancing Security and Liberty within the European Human Rights Framework. A Critical Reading of the Court's Case Law in the light of Surveillance and Criminal Law Enforcement Strategies after 9/11' *Utrecht Law Review*, vol 1 (September, 2005)
[8] Psychogiopoulou and Brkan (n 5) 1.
[9] *Tyrer v the UK* App no 5856/72 (ECtHR, 25 April 1978) para 31.
[10] Psychogiopoulou and Brkan (n 5) 1.
[11] Sloot, *'Privacy as Human Flourishing: Could a Shift towards Virtue Ethics Strengthen Privacy Protection in the Age of Big Data'* (n 4) 230.

safeguarding their personal data.[12] Thus, it is with some justification that data protection laws have been characterised as regulatory reactions to technological advancements.[13] The pieces of legislation in the area emerged at early 1970s. The international measures, particularly for the aim of guarding privacy interests against the risk of misusing data by automatic means, was conducted by regional bodies, notably European ones.[14]

However, there are large number of legal instruments on data protection currently. Moreover, several international instruments have introduced data protection. Particularly, two international data protection instruments are addressed as primary sources. Since they include the main principles of data protection which are present in national data protection laws and they are referred to effective models by international and domestic initiatives concerned data protection. These instruments are the Council of Europe's Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (CoE Convention) and the EC Directive on the Protection of Individuals with regard to the Processing of Personal Data (EC Directive).[15]

CoE Convention is the hereto unique international treaty particularly related to data protection. It remains important as it has impacted and materialised the main principles of most countries' current data protection laws along with the EC Directive.[16] It has three basic elements: it formulates major orders for data protection measures to be adopted by contracting States, it establishes special rules about transborder data flows and it sets out mechanisms for advisory.[17] Personal data is defined in article 2(a) of the CoE Convention as[18] 'any information relating to an identified or identifiable individual.'

The EC Directive is the most extensive and complex of the instruments. It establishes a set of rules capable of broad effect and application. Similar but more comprehensive definition compared to the CoE Convention, article 2 (a) of the EC Directive introduces the personal data as: 'any information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or one or more factors specific to his physical, physiological, mental, economic, cultural or social identity.' The purpose of the CoE Convention is addressed in article 1 as: 'to secure in the territory of each Party for every individual ... respect for his rights and fundamental freedoms, and in particular his right to privacy, with regard to automatic processing of personal data relating to him.'

---

[12] Handbook on European Data Protection Law (2018) < *https://fra.europa.eu/sites/default/files/fra_uploads/fra-coe-edps-2018* > accessed 01 July 2019

[13] Lee A. Bygrave, *Data Protection Law: Approaching Its Rationale, Logic, and Limits* (Kluwer Law International, 2002) 94.

[14] James Michael, *Privacy and Human Rights: an International and Comparative Study, with Special Reference to Developments in Information Technology* (UNESCO, 1994) 32.

[15] Bygrave, *Data Protection Law: Approaching Its Rationale, Logic, and Limits* (n 13) 30.

[16] ibid 31.

[17] Michael (no 14) 35.

[18] Bygrave, *Data Protection Law: Approaching Its Rationale, Logic, and Limits* (n 13) 41.

The core principles of data protection are manifest in article 5 of the CoE Convention[19] and article 6 (1) of the EC Directive[20]. These principles can be sum up as:

'(i) personal data should be gathered by fair and lawful means; (ii) the amount of personal data gathered should be limited to what is necessary to achieve the purpose(s) of gathering the data; (iii) personal data should be gathered for specified and lawful purposes and not processed in ways that are incompatible with those purposes; (iv) use of personal data for purposes other than those specified should occur only with the consent of the data subject or with legal authority; (v) personal data should be accurate, complete and relevant in relation to the purposes for which they are processed; (vi) security measures should be implemented to protect personal data from unintended or unauthorized disclosure, destruction or modification; (vii) data subjects should be informed of, and given access to, data on them held by others, and be able to rectify these data if inaccurate or misleading; and (viii) parties responsible for processing data on other persons should be accountable for complying with the above principles.'[21]

The breaches of the CoE's core obligations could induce the violation of the right to respect private life in many cases of the ECtHR. Moreover, the jurisprudence of ECtHR plays a role in designating the meaning of the provisions in the EC Directive.[22] In this sense, the Court's former president, Rolv Ryssdal's expression is remarkable in order to evaluate the influence of these instruments on the ECtHR:

'For our part, we in Strasbourg should not ignore the basic principles laid down in the Data Protection Convention in addressing ourselves to those issues which do come before us. Those basic principles are a sectoral implementation of Article 8 of the ECHR in the context of automatic data processing and may therefore [be employed] in aid in interpreting that provision.'[23]

1.2 Personal Data within the Scope of the Right to Respect for Private Life

The ECHR is one of the main instruments in the human rights system in Europe. Thus, a search into how this convention evaluates data protection right is an essential step of any analysis of data protection from a human rights approach. The ECHR does not explicitly acknowledge the right to data protection.[24] At this point, it should be needed to assess the ECtHR's jurisprudence in order to reach the Court's perspective. Personal data protection plays a primordial role in the exercise of a person's right to respect for his private life enshrined in Article 8 of the Convention. The ECtHR

[19] *Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data* (adopted in Council of Europe 28 January 1981, entered into force 01 October 1985) the CoE Convention
[20] Bygrave, *Data Protection Law: Approaching Its Rationale, Logic, and Limits* (n 13) 58.
[21] Lee A. Bygrave, 'Data Protection Pursuant to the Right to Privacy in Human Rights Treaties' *Int'L J.L. & Info. Tech.,* Vol.6 (1998) 250.
[22] Bygrave, *Data Protection Law: Approaching Its Rationale, Logic, and Limits* (n 13) 35.
[23] Ryssdal, 'Data Protection and the European Convention on Human Rights', in Data Protection, Human Rights and Democratic Values, Proceedings of the 13th Conference of Data Protection Commissioners held 2-4 October 1991 in Strasbourg (Strasbourg: CoE, 1992), 42.
[24] Nadezhda Purtova, *Property Rights in Personal Data, A European Perspective* (Wolters Kluwer Law and Business 2012) 224.

repeatedly stated that data protection fell under the protective scope of article 8 of the ECHR. Moreover, the ECtHR expressed that it is impossible and unnecessary to attempt an exhaustive definition of what "private life" in Article 8 means, thus the concept of private life has been widely interpreted.[25]

Article 8 (1) of the ECHR sets out the substantive scope of the right to respect for private and family life as: 'Everyone has the right to respect for private and family life, his home and his correspondence.' Therefore, it provides little guidance in terms of responding to the question whether data protection interests enjoy the ECHR's protection.[26]

Although ECHR does not explicitly include personal data protection, the necessity of personal data protection is expressed in the jurisprudence of the ECtHR. In the *S. and Marper v UK* case, two applicants claimed that the retention by the authorities of their fingerprints, cellular samples and DNA profiles after their acquittal or discharge induced the violation of the right to respect private life.[27] The ECtHR has stated that: 'The protection of personal data is of fundamental importance to a person's enjoyment of his or her right to respect for private and family life, as guaranteed by Article 8 of the Convention.'[28]

The ECtHR introduced personal data as 'any information relating to an identified or identifiable individual'.[29] That broad interpretation is conformed with article 2(a) of the CoE Convention and its purpose as previously mentioned.[30]

Therefore, it should be needed to draw the line of the distinction between private and public in order to determine which information can be assessed as 'relating to an individual's private life.' The ECtHR has emphasized that private life is not restricted to the inner circle of the individual since the improvement of individual's personality is the keystone of the protection granted by article 8 (1) of ECHR.[31] This approach is reflected in *Shimovolos v Russia* Case which is related to the police listing and surveillance on applicant's account of membership in a human rights organisation.[32] The ECtHR noted that: 'Article 8 is not limited to the protection of an "inner circle" in which the individual may live his own personal life as he chooses and to exclude therefrom entirely the outside world not encompassed within that circle. It also protects the right to establish and develop relationships with other human beings and the outside world.'[33]

---

[25] Bart van der Sloot, Legal Fundamentalism: Is Data Protection Really a Fundamental Right? in R. Leenes, R. van Brakel, S. Gutwirth, P. De Hert (eds), *Data Protection and Privacy: (In)visibilities and Infrastructures* (Springer International Publishing, 2017) 3.
[26] Purtova (n 24) 224.
[27] *S and Marper v UK* App no 30562/04 (ECtHR, 04 December 2008) para 9-25.
[28] ibid para 103.
[29] *Amann v Switzerland* App no 27798/95 (ECtHR, 16 February 2000) para 69.
[30] Maria Tzanou, *The fundamental Right to Data Protection:Normative Value in the Context of Counter-Terrorism Surveillance* (Hart Publishing 2017) 45.
[31] Psychogiopoulou and Brkan (n 5) 33.
[32] *Shimovolos v Russia* App no 30194/09 (ECtHR, 21 June 2011) para 5-20.
[33] ibid para 64.

The other remarkable example is the *Von Hannover v. German* case in which a Monegasque national, Princess Caroline von Hannover, and a German national, Prince Ernst August von Hannover's ("the applicants") photos are taken in the public place and published in the German's magazines[34], the Court expresses that '… the concept of private life extends to aspects relating to personal identity, such as a person's name, photo, or physical and moral integrity; the guarantee afforded by Article 8 of the Convention is primarily intended to ensure the development, without outside interference, of the personality of each individual in his relations with other human beings. There is thus a zone of interaction of a person with others, even in a public context, which may fall within the scope of private life. Publication of a photo may thus intrude upon a person's private life even where that person is a public figure.'[35]

However, drawing a clear line between private and public activities is sometimes difficult.[36] In some cases, the Court found that there had been no violation of the right to respect the private life, as the data had been reached from the public official documents or the information was general knowledge due to the concerning person's notoriety and regarded with such person's public life. In this regard, it might be that obtaining of publicly accessible data or information concerning records or subjects in the public domain would exclude the scope of article 8. Though, while gathering this information, specific or intrusive measures should not be used and a specific person should not be targeted or such data should not be stored long term in a secret file as well. [37]

Besides, drawing the line of the distinction between private and public, the other essential inquiry is assessing which information could be evaluated as personal data. In the *S and Marper v UK* case, ECtHR assesses cellular samples and DNA profiles differently according to the fingerprints. Since the Court expresses that 'the retention of cellular samples and DNA profiles has a more important impact on private life than the retention of fingerprints.' Thus, the ECtHR notes that '…the retention of both cellular samples and DNA profiles discloses an interference with the applicants' right to respect for their private lives, within the meaning of Article 8 (1) of the Convention.'[38] However, in terms of the fingerprints, the ECtHR states as: '… the retention of fingerprints on the authorities' records in connection with an identified or identifiable individual may in itself give rise, notwithstanding their objective and irrefutable character, to important private-life concerns.'[39]

Private life also covers the physical and psychological integrity of a person due to the broader concept of article 8 (1). For instance, in the case of *Mikulic v. Crotoatia* the claimant alleged that the

[34] *Von Hannover v German* App no 59320/00 (ECtHR, 24 June 2004) para 10-53.
[35] ibid para 95.
[36] Bernadette Rainey, Elizabeth Wicks, and Clare Ovey, Jacobs, White, and Ovey: *The European Convention on Human Rights*,(Oxford University Press 2017) 418.
[37] Karen Reid, *A practitioner's Guide to the European Convention on Human Rights* (Thomson/Sweet & Maxwell, 2012) 876.
[38] *S and Marper v UK* App no 30562/04 (ECtHR, 04 December 2008) para 77.
[39] ibid para, 85.

proceedings concerning her paternity allegation had failed due to the excessive length of the paternity proceedings.[40] In the present case, the ECtHR states that: 'Private life … includes a person's physical and psychological integrity and can sometimes embrace aspects of an individual's physical and social identity. Respect for "private life" must also comprise to a certain degree the right to establish relationships with other human beings.'[41]

The applicant claimed that his proposed expulsion from the United Kingdom to Algeria may make him confronted with the inhuman and degrading treatment, and threatened his physical and moral integrity in the *Bensaid v. The United Kingdom* case.[42] Although the applicants' claim regarded to article 8 (1) was rejected by the Court, the ECtHR's notion was remarkable in order to determine the scope of personal data as: '… elements such as gender identification, name and sexual orientation and sexual life are important elements of the personal sphere protected by Article 8. Mental health must also be regarded as a crucial part of private life associated with the aspect of moral integrity.'[43] Similarly, collection and storage of medical data and other medical records are evaluated as personal data in terms of the ECtHR's jurisprudence. A related case is *L.H. v Latvia* in which Ms L.H. asserted that the collection of her personal medical data by a State agency had given rise to a violation of the right to respect for her private life.[44] The indiscriminate gathering of medical data by the public organ responsible for following the quality of medical care was assessed as an infringement of article 8 (1) of the ECHR.[45] The Court emphasizes that: '… the protection of personal data, not least medical data, is of fundamental importance to a person's enjoyment of the right to respect for his or her private life as guaranteed by Article 8 of the Convention. Respecting the confidentiality of health data is a vital principle in the legal systems of all the Contracting Parties to the Convention. It is crucial not only to respect the sense of privacy of a patient but also to preserve confidence in the medical profession and in the health services in general.'[46]

In addition, the Court accepted the individual's ethnic identity within the scope of the personal data. As an illustration, in the *Ciubotaru v. Moldova* case, the applicant alleged that the authorities refused his demand in order to record his ethnicity as stated by him, accordingly, such refusal induced a breach of his right to respect for private life.[47] The Court determined that '… ethnic

[40] *Mikulic v. Crotoatia* App no 53176/99 (ECtHR, 7 February 2002) para 8-32.
[41] ibid para 51.
[42] *Bensaid v. The United Kingdom* App no 44599/98 (ECtHR, 6 February 2001) para 7-21.
[43] ibid para, 47.
[44] *L.H. v. Latvia* App no 52019/07 (ECtHR, 29 April 2014) para 3.
[45] David Harris, Michael O'Boyle, Ed Bates, and Carla Buckley, Harris, O'Boyle, and Warbrick: *Law of the European Convention on Human Rights* (Oxford University Press 2018) 540.
[46] *L.H. v. Latvia* App no 52019/07 (ECtHR, 29 April 2014) para 56.
[47] *Ciubotaru v. Moldova* App no 27138/04 (ECtHR, 27 April 2010) para 5-13.

identity was a detail pertaining to the individual's identity falling within the ambit of Article 8 … an individual's ethnic identity constitutes an essential aspect of his or her private life and identity.'[48]

Moreover, in the other cases related with the bank accounts' data, the ECtHR determines that banking documents should be evaluated as personal data, even if such data is concerned professional activities. In *M.N. and others v San Marino* case, the applicants' banking data documents were seizure and copied in the context of criminal proceedings. The applicants were notified about the measure applied to them about one year after the adoption of the search and seizure decisions.[49] The applicants then lodged a complaint in terms of such decision which was rejected. In the present case, the ECtHR highlighted that: '… information retrieved from banking documents undoubtedly amounts to personal data concerning an individual, irrespective of it being sensitive information or not. Moreover, such information may also concern professional dealings and there is no reason of principle to justify excluding activities of a professional or business nature from the notion of "private life".[50]

In the light of evaluated cases related with the consent of personal data, it could be constituted that, even if the ECHR does not cover an explicit definition of the personal data, the ECtHR is trying to broaden the scope of 'private life' in order to fill this gap. Furthermore, the Court emphasises some pivotal notions which are essential to be dependent and free individuals in the society such as personal development, relationships with other human beings and the outside world, individual autonomy, integrity, and identity. In this respect, the diversity of data which is included in the related cases proves such an approach.

2. Personal Data

2.1 Access to Personal Data

In particular circumstances, individuals and governments could conflict due to the citizens' demands for accessing their files related to their private life.[51] The ECtHR has usually been favour of the individuals who tries to reach information in the context of their origins.[52] The principal case is *Gaskin v UK* in which the applicant was received into care as a child when attaining the age of majority, he tried to learn his past to cope with his problems, though, his demand in order to access his files is rejected by the local authority.[53] The Court found that: "respect for private life requires that everyone should be able to establish details of their identity as individual human beings and

[48] ibid para 49-53.
[49] *M.N. and Others v San Marino* App no 28005/12 (ECtHR, 07 July 2015) para 7-19.
[50] ibid para 51.
[51] Reid (n 37) 876.
[52] Harris, O'Boyle, Bates, and Buckley (n 45) 541.
[53] *Gaskin v the United Kingdom* App no 10454/83 (ECtHR, 07 July 1989) para 10-12.

that in principle they should not be obstructed by the authorities from obtaining such very basic information without specific justification".[54]

The ECtHR also expressed that '…, persons in the situation of the applicant have a vital interest, protected by the Convention, in receiving the information necessary to know and to understand their childhood and early development. On the other hand, it must be borne in mind that confidentiality of public records is of importance for receiving objective and reliable information, and that such confidentiality can also be necessary for the protection of third persons.'[55]

A similar approach has taken place in the *Godelli v. Italy* case. In the concrete case, the applicant could not reach information concerning her birth, since the registered office did not share information with. Accordingly, she had no opportunity to learn her origin.[56] The court reiterated that: '…the child has a right to know its origins, that right being derived from the notion of private life… the right to an identity, which includes the right to know one's parentage, is an integral part of the notion of private life…'[57]

In certain situations, access to information could be crucial for the individual in order to eliminate or minimize the risks on life and health.[58] In *Roche v. the United Kingdom* case, the Court was asked to evaluate a complaint about a member of the British Army who suffered from some respiratory diseases due to nerve and mustard gas tests in the Medical Assessment Programme of the army and he had not obtained the essential information from the governments, which would have allowed him to be treated.[59] The ECtHR expresses that '… the State has not fulfilled the positive obligation to provide an effective and accessible procedure enabling the applicant to have access to all relevant and appropriate information that would allow him to assess any risk to which he had been exposed during his participation in the tests.[60]

In the *K.H. and Others v. Slovakia* case, the applicants demanded to take photocopies of their medical documents by the authorities in order to find out reasons for their infertility and possible treatment, however, they have not been permitted to access the documents.[61] The Court held that there had been a violation of Article 8 of the Convention and stated as: 'The complaint in issue concerns the exercise by the applicants of their right of effective access to information concerning their health and reproductive status. As such it is linked to their private and family lives within the meaning of Article 8.[62] The ECtHR also added that the exercise of the right under Article 8 to

[54] ibid para 39.
[55] ibid para 49.
[56] *Godelli v Italy* App no 33783/09 (ECtHR, 25 September 2012) para 5-12.
[57] ibid para 50-52.
[58] Harris, O'Boyle, Bates, and Buckley (n 45) 541.
[59] *Roche v The United Kingdom* App no 32555/96 (ECtHR, 19 October 2005) para 9-33.
[60] ibid para 167.
[61] *K.H. and Others v Slovakia* App no 32881/04 (ECtHR, 28 April 2009) para 7-10
[62] ibid para 44.

respect for one's private and family life must be practical and effective, thus the Contracting Parties' positive obligations should extend, in particular such cases where personal data are concerned, to the making available to the data subject of copies of his or her data files.

A specific principle of access to information has also emerged in the context of the security files. For instance, in the *Turek v. Slovakia* the applicant was recorded by the StB as their "agent", due to such registration, the applicant was confronted with a negative security clearance, accordingly, his reputation and good name and reputation were brought into disrepute. He could not have the opportunity to correct his registration, since he had not had full access to his file.[63]

The ECtHR notes that 'particularly in proceedings related to the operations of state security agencies, there may be legitimate grounds to limit access to certain documents and other materials. However, in respect of lustration proceedings, this consideration loses much of its validity…, if a State is to adopt lustration measures, it must ensure that the persons affected thereby enjoy all procedural guarantees under the Convention in respect of any proceedings relating to the application of such measures. In the present case, the applicant was asserting his rights in the context of an interference with them which had been occasioned by State power and arguably without his knowledge. The courts considered it crucial for the applicant to prove that the interference was contrary to the applicable rules. These rules were, however, secret and the applicant did not have full access to them. On the other hand, the State did have full access. In those circumstances, and irrespectively of whether the placing of the burden of proof on the applicant was compatible with domestic law, that requirement placed an unrealistic burden on him in practice… It was thus excessive. The applicant's proceedings therefore cannot be considered as offering him effective protection of his right to respect for his private life.'[64]

As a result, when individuals try to obtain data about their origin and the Contracting States do not share concerning information, the ECtHR generally takes the part of the individuals. ECtHR also highlights that information which should be reached to prevent the risks on health and life, should also be given the individuals order to protect them. The data in the security files is the other specific type of information which the ECtHR may evaluate the issue for the sake of the complaints.

2.2 Collection, Storing and Disclosure of Personal Data

Personal data processing as the collection, storing and disclosure of data by the state related an individual will interfere with his right to respect for his private law in terms of the Court.[65] Therefore, the ECtHR is seeking for effective procedures, checks and oversight mechanisms related to data

[63] *Turek v Slovakia* App no 57986/00 (ECtHR, 14 February 2006) para 3-13.
[64] ibid para 115-116.
[65] Harris, O'Boyle, Bates, and Buckley (n 45) 583.

processing. Moreover, the Court is looking for the published framework which the State acts concerning these mechanisms.[66]

In *Leander v Sweden* case, it is set out that the storage of data is capable of resulting in a violation of the right to respect for private life, though in the case, it did not due to the appropriate safeguards.[67] The applicant complained that he had been fired from his work in the civil service since in the police record he had been seen as a security risk. The Court noted that '…where the implementation of the law consists of secret measures, not open to scrutiny by the individuals concerned or by the public at large, the law itself, as opposed to the accompanying administrative practice, must indicate the scope of any discretion conferred on the competent authority with sufficient clarity, having regard to the legitimate aim of the measure in question, to give the individual adequate protection against arbitrary interference.'[68]

In the more recent case of *Aycaguer v. France*, the applicant complained that he refused to undergo a biological test during the prosecution because the result of these tests is stored in the national computerised DNA database. Thus, he alleged that identifying his DNA and storing the corresponding data amounted to a disproportionate interference with his private life. The Court emphasized that: '… the national authorities can legitimately set up databases as an effective means of helping to punish and prevent certain offences, including the most serious types of crime, such as the sex offences for which the national computerised DNA database was originally created. However, such facilities cannot be implemented as part of an abusive drive to maximise the information stored in them and the length of time for which they are kept. Indeed, without respect for the requisite proportionality vis-à-vis the legitimate aims assigned to such mechanisms, their advantages would be outweighed by the serious breaches which they would cause to the rights and freedoms which States must guarantee under the Convention to persons under their jurisdiction.'[69]

In *Z v Finland* case, the disclosure of personal data is issued concerning medical information. The applicant complained about the failure of the Finnish authorities to prevent the disclosure by the press of her identity and her medical condition as an HIV carrier during the court process regarded with her husband's sexual offences. The ECtHR notes that 'Respecting the confidentiality of health data is a vital principle in the legal systems of all the Contracting Parties to the Convention. It is crucial not only to respect the sense of privacy of a patient but also to preserve his or her confidence in the medical profession and in the health services in general.'[70] However, non-disclosure of medical personal data may not be considered as an absolute right, the Court

[66] Gordon Nardell QC, 'Levelling up: Data Privacy and the European Court of Human Rights' in Serge Gutwirth, Yves Poullet, Paul De Hert (eds), *Data Protection in a Profiled World* (Springer, Belgium 2009) 47.
[67] Rainey, Wicks, and Ovey (n 36) 418.
[68] *Leander v Sweden* (1987) Series A no 28 para 51.
[69] *Aycaguer v France* App no 8806/12 (ECtHR, 22 June 2017) para 51.
[70] *Z v Finland* App no 22009/93 (ECtHR, 25 February 1997) para 95.

highlights that: ‘As to the issues regarding access by the public to personal data, the Court recognises that a margin of appreciation should be left to the competent national authorities in striking a fair balance between the interest of publicity of court proceedings, on the one hand, and the interests of a party or a third person in maintaining the confidentiality of such data, on the other hand. The scope of this margin will depend on such factors as the nature and seriousness of the interests at stake and the gravity of the interference.’[71]

Numerous cases emerged the disclosure of the personal information by the police in the scope of the criminal investigations.[72] In *Craxi v Italy*, the applicant was the former Prime Minister of Italy and there was a criminal procedure against him. The consent of telephone conversations which obtained with the wiretapping by the police was released into the media. The applicant claimed that such act was given rise a violation of his right to respect for his private life. The ECtHR expresses that ‘… Such persons inevitably and knowingly lay themselves open to close scrutiny by both journalists and the public at large. However, public figures are entitled to the enjoyment of the guarantees set out in Article 8 of the Convention on the same basis as every other person. In particular, the public interest in receiving information only covers facts which are connected with the criminal charges brought against the accused… The Court also added that some of the conversations published by the press did not correspond to a pressing social need. Therefore, the interference with the applicant's rights under Article 8 (1) of the ECHR was not proportionate to the legitimate aims which could have been pursued.’[73]

In some cases, the disclosure of personal data without the individuals’ content may be constituted interference of the right to respect for private life. For instance, in *Brito Ferrinho Bexiga Villa-Nova v. Portugal* case, while inspecting the accounts of the applicant’s law firm, the tax authorities realized that she had not paid value-added tax, the applicant refused to share her personal bank statements with the authorities due to the professional confidentiality and bank secrecy. The local court lifted her professional confidentiality and bank secrecy in the prosecution of tax fraud. Thus, she alleged that this decision gives rise to a violation of article 8 (1) of the Convention. The ECtHR expressed that ‘… the proceedings for lifting the professional confidentiality binding on the applicant in her capacity as a lawyer had admittedly been conducted before a judicial body, but without her participation. She had not become aware that professional confidentiality and bank secrecy had been lifted with regard to her bank statements. Thus, she had not therefore been involved in the proceedings at any time and had thus been unable to submit her arguments. … Having regard to the lack of procedural guarantees and effective judicial control of the measure complained of, the

[71] ibid para 99.
[72] Harris, O'Boyle, Bates, and Buckley (n 45) 539.
[73] *Craxi v Italy* App no. 25337/94 (ECtHR, 17 July 2003) para 64-65.

Court considered that the Portuguese authorities had failed to strike a fair balance in the present case between the demands of the general interest and the requirements of the protection of the applicant's right to respect for her private life. Accordingly, there had been a violation of Article 8 of the Convention.'[74]

Besides, the level of interference to the right for respect private life may vary according to aims for which it is being collected, stored or disclosed. Therefore, while the collection of personal data may constitute to a justified interference in terms of private life, the context of its retention may not be justified.[75] In *S and Marper v. United Kingdom* case, the ECtHR expresses that: '…the Court will have due regard to the specific context in which the information at issue has been recorded and retained, the nature of the records, the way in which these records are used and processed and the results that may be obtained.'[76]

In sum, collection, storing and disclosure of personal data for purposes of criminal investigation generally will concern private life but may be justified in the interests of public safety and prevention of crime in the ECtHR jurisprudence. Similarly, the interference involved the collection, storage, and retention of personal data may be justified in serious offences.[77] In addition, medical personal records, taking and storing by the police of public data, storage by tax authorities are the other relevant issues may be amounted to an interference with private life if the adequate safeguards are absent.

3. Justification for Interference

Most incidents of the violation with regard to article 8 (1) by the Contracting State authorities' collection, storage or disclose of personal data have been evaluated by the ECtHR as justified under article 8(2). Thus, it is crucial to absorb the context of this provision, as interpreted by the Court. Article 8(2) establishes three main criteria in order to justify an interference with a person's right for respect to private life.[78] The interference must be: (i) 'in accordance with the law'; (ii) 'necessary in a democratic society'; and (iii) in furtherance of at least one of the aims listed in paragraph 2 of article 8 as: 'national security', 'public safety', 'economic well-being of the country', 'prevention of disorder or crime', 'protection of health or morals' or 'protection of the rights and freedoms of others'.

Prescribed by law requires the principle of legality and has two basic elements. Primarily, the interference must be compatible with national law.[79] Secondly, 'domestic law must provide

[74] <https://hudoc.echr.coe.int/eng-press#{"fulltext":["BRITO FERRINHO BEXIGA VILLA"]} > accessed 08 July 2019
[75] Nora Ni Loideain, 'Surveillance of Communications Data and Article 8 of the European Convention on Human Rights' in Serge Gutwirth, Ronald Leenes and Paul de Hert (eds), *Reloading Data Protection* (Springer, 2014) 193.
[76] *S and Marper v UK* App no 30562/04 (ECtHR, 04 December 2008) para 67.
[77] Reid (n 37) 878.
[78] Bygrave, *'Data Protection Pursuant to the Right to Privacy in Human Rights Treaties'* (n 21) 270.
[79] Loideain (n 75) 188.

protection against arbitrary interference with an individual's right under Article 8.'[80] In the *Taylor-Sabori v. the United Kingdom* case, the applicant alleged that the interception of his pager messages by the police and subsequent reference to them at his trial given rise to an unjustified interference. The Court has emphasized that: '… the phrase "in accordance with the law" not only requires compliance with domestic law but also relates to the quality of that law, requiring it to be compatible with the rule of law.'[81]

The legality requirement includes two key tests: accessibility and foreseeability.[82] These elements have been expressed by the ECtHR as: '… the law to be accessible to the person concerned, who must, moreover, be able to foresee its consequences for him…, the requirement of foreseeability implies that the domestic law must be sufficiently clear in its terms to give citizens an adequate indication as to the circumstances in and conditions on which public authorities are empowered to take any such measures.'[83] Moreover, 'the law must indicate the scope of any … discretion conferred on the competent authorities and the manner of its exercise with sufficient clarity, …, to give the individual adequate protection against arbitrary interference.'[84]

Moreover, if the interference to the rights under article 8 (1) is serious, it is needed for comprehensive regulation of the activities that incur the interference.[85] For an illustration, in *Kruslin v. France* case in which the applicant complained about the evidence from telephone tapping in connection with other proceedings, the Court underlines that: 'Tapping and other forms of interception of telephone conversations represent a serious interference with private life and correspondence and must accordingly be based on a "law" that is particularly precise. It is essential to have clear, detailed rules on the subject, especially as the technology available for use is continually becoming more sophisticated.'[86]

The interference must be 'necessary in a democratic society' which has often arisen from the greater dispute.[87] The notion of necessity has been held by the ECtHR as 'the interference corresponds to a pressing social need and, in particular, that it is proportionate to the legitimate aim pursued.'[88] The Court has admitted three main justifications for restricting the right to privacy: security, morality, and economic well-being, while application of the 'necessary in a democratic society' test to Article 8 ECHR. Next, it evaluates whether a particular interference has been

[80] *Khan v United Kingdom* App no 35394/97 (ECtHR, 12 May 2000) para 26.
[81] *Taylor-Sabori v The United Kingdom* App no 47114/99 (ECtHR, 22 October 2002) para 18.
[82] Loideain (n 75) 188.
[83] *Valenzuela Contreras v Spain* App no 27671/95 (ECtHR, 30 July 1998) para 46.
[84] *Malone v The United Kingdom* App no 8691/79 (ECtHR, 02 August 1984) para 68.
[85] Bygrave, *'Data Protection Pursuant to the Right to Privacy in Human Rights Treaties'* (n 21) 272.
[86] *Kruslin v France* App no 11801/85 (ECtHR, 24 April 1990) para 33.
[87] Loideain (n 75) 190.
[88] *Leander v Sweden* (1987) Series A no 28 para 55.

necessary by determining the general interest involved with the violation.[89] In this regard, the Court has expressed that powers of authorities may be tolerated under the Convention only in so far as strictly necessary for safeguarding the democratic institutions.[90] 'In practice, this means that there must be adequate and effective guarantees against abuse. The assessment depends on all the circumstances of the case, such as the nature, scope and duration of the possible measures, the grounds required for ordering them, the authorities competent to authorise, carry out and supervise them, and the kind of remedy provided by the national law.'[91] Thus, the Court evaluates the complaints a case by case such guarantees that the State Parties have implemented governing the related measures.[92]

Besides, when assessing the standard 'necessary in a democratic society' under the second paragraph of article 8, the ECtHR will invoke the margin of appreciation doctrine.[93] ECtHR expresses in the *Buckley* case: 'As is well established in the Court's case-law, it is for the national authorities to make the initial assessment of the "necessity" for the interference, as regards both the legislative framework and the particular measure of implementation. Although a margin of appreciation is thereby left to the national authorities, their decision remains subject to review by the Court for conformity with the requirements of the Convention. The scope of this margin of appreciation is not identical in each case but will vary according to the context. Relevant factors include the nature of the Convention right in issue, its importance for the individual and the nature of the activities concerned.[94]

As a consequence, when limiting the rights to respect for private life, the Contracting States must meet three conditions: the breach should be prescribed by law, it should purpose of the rationales designated in the article 8 (2) of ECtHR, and it should be necessary in a democratic society. The first criterion is generally referred to as the 'rule of law test'. It stipulates that there must be a law on which the interference is based and in which the authorities are provided with the specific competence to act by the democratic law-maker. These legal regulations must be accessible to the individuals and be sufficiently clear and precise to enable a person to reasonably foresee the outcomes of his actions. Lastly, the law must provide effective guarantees against arbitrary interferences and the abuse of power by the executive authorities. The second criterion is not a test in itself, not only because utter arbitrary interferences will commonly not be provided for by law, but also primarily since it is subsumed in the 'democratic necessity test'. In this test, the Court assesses

[89] Bart van der Sloot, 'How to Assess Privacy Violations in the Age of Big Data? Analysing the Three Different Tests Developed by the ECtHR and Adding for a Fourth One' *Information & Communications Technology Law, vol.24.1*, (2015) 85.
[90] *Klass and others v Germany* App No 5029/71 (ECtHR, 06 September 1978) para 42.
[91] *Kennedy v The United Kingdom* App no 26839/05 (ECtHR, 18 May 2010) para 140.
[92] Bygrave, *'Data Protection Pursuant to the Right to Privacy in Human Rights Treaties'* (n 21) 274.
[93] Yukata Arai-Takahashi, *The Marjin of Appreciation Doctrine and the Principle of the Proportionality in the Jurisprudence of the ECHR* (Intersentia, Antwerp, Oxford, New York 2002) 9.
[94] *Buckley v UK* App no 20348/92 (ECtHR, 29 September 1996) para 74.

whether a specific interference is 'necessary in relation to the aims pursued'. Therefore, second and third steps are merged into one test.[95]

4. Protection of Privacy in the Digital Age

As it is seen in terms of mentioned cases, it is easy to determine the infringement in the classic privacy incidents or clarify the justifications. Since, the time and the place of the violation, the individual harm and the victim could be identified simply in such cases. However, while many people were monitoring and the mass data was collecting with the secret surveillance measures due to the technological developments, pivotal questions are arising when resolving related numerous cases. Firstly, the individual who appeals to the ECtHR related with these surveillance activities, how could prove his personal interest and individual harm. The other concern is to identify whether these data processing systems are all necessary and proportionate in terms of security. Moreover, it may be asked to what extent these systems are efficient. While concluding these cases, how the ECtHR can make the proper balance between individual harm and the importance of interest. Thus, in this part, these questions are tried to be answered in the light of the Court's approach. In addition, it will be evaluated that while resolving such cases which innovator tests the ECtHR accepts.[96]

4.1 The ECtHR's Efforts to Relax Admissible Standards against Current Issues

The ECtHR emphasizes the individual harm by natural persons when assessing the admissibility of cases under article 8.[97] The Court expresses that 'the individuals bringing applications before the Court must be able to show that they were "directly affected" by the measure complained of.'[98] This expression emerges from article 34 of the ECHR, which provides: 'The Court may receive applications from any person, …up of individuals claiming to be the victim of a violation by one of the High Contracting Parties of the rights set forth in the Convention or the Protocols thereto. The High Contracting Parties undertake not to hinder in any way the effective exercise of this right.'

A conclusion of such emphasis on the individual interests and the personal injury of the complaint is that *in abstracto* claims, in which an applicant makes a complaint about a practice or a law as such, without it being implemented or otherwise have an effect on the claimant himself, are proclaimed inadmissible. This manner is similar for the *actio popularis* or class action, in which a societal organization challenges a law or policy not from a personal perspective, but with an eye on the public interest. Lastly, hypothetical complaints and a priori applications, in which the case regards a

[95] Sloot, *'How to Assess Privacy Violations in the Age of Big Data? Analysing the Three Different Tests Developed by the ECtHR and Adding for a Fourth One'* (n 89) 77.
[96] Bart van der Sloot, 'Is the Human Rights Framework Still Fit for the Big Data Era? A Discussion of the ECtHR's Case Law on Privacy Violations Arising from Surveillance Activities' in Serge Gutwirth, Ronald Leenes and Paul de Hert (eds), *Data Protection on the Move* (Springer International Publishing, 2016) 413-414.
[97] Bart van der Sloot, 'Privacy in the Post-NSA Era: Time for a Fundamental Revision' *J. Intell. Prop. Info. Tech. and Elec. Com. L.,* Vol.5.2 (2014) 4.
[98] *Trivkanov v Croatia* App no 12986/13 (ECtHR, 06 July 2017) para 49.

possible, future violation by the Contracting State, without any damage having occurred yet, are also announced inadmissible.[99] The Court expresses that 'It is only in highly exceptional circumstances that an applicant may nevertheless claim to be a victim of a violation of the Convention owing to the risk of a future violation.'[100]

This induces a serious problem with it for complaints related to mass data collections, whether they are taken action on by secret services or by big internet companies because individuals are often unknowing that they have been filmed, followed by cookies or subjected to internet monitoring. Therefore, merely a few individuals will file a legal complaint. These few people will have problems about indicating any individual harm. Moreover, the individual damage arising from data collection practices is many times rather hypothetical, since the collection itself generally has little effect on the personal autonomy or dignity of an individual and the damage that could result from the hypothetic possibility of, for instance, a data breach or the abuse of the data by a future regime. Accordingly, complaints related to Big Data process which is introduced as collecting massive data without a pre-established aim, about an undefined number of people, will often have a theoretical and abstract character.[101]

First examinations regarded to the victim-requirement and surveillance measures by the State Parties have to begin with *Klass and others v. Germany* case.[102] In this case, the applicants complained about the contested German legislation, since it allowed surveillance activities without requiring the authorities to inform the persons concerned is not informed of the surveillance measures when such measures are terminated. They also claimed that there is no remedy before to court due to the ordering and implementation of these measures.[103] Although the Court admitted that the victim of an alleged breach may bring the complaint, in the concrete case, the applications, stated that they may be or may have been subject to secret surveillance, for example, in course of legal representation of clients who were themselves subject to surveillance, and that persons have been the subject of secret surveillance are not always subsequently informed of the measures taken against them. Therefore, the Court assessed that the applicants have to be evaluated as victims.[104]

The governments claimed that, 'in order to be able to claim to be the victim of an interference with the exercise of the right conferred on him by article 8 (1), it should suffice that a person is in a

[99] Sloot, *'Privacy in the Post-NSA Era: Time for a Fundamental Revision'* (n 97) 4.
[100] *Noel Narvii Tauria and others v France* App no 28204/95 (ECtHR, 4 December 1995) para 130.
[101] Sloot, *'Privacy in the Post-NSA Era: Time for a Fundamental Revision'* (n 97) 4.
[102] Sloot, *'Is the Human Rights Framework Still Fit for the Big Data Era? A Discussion of the ECtHR's Case Law on Privacy Violations Arising from Surveillance Activities'* (n 96) 419.
[103] *Klass and others v Germany* App No 5029/71 (ECtHR, 06 September 1978) para 10.
[104] ibid para, 26.

situation where there is a reasonable risk of his being subjected to secret surveillance.'[105] At this point, the Court's approach was significant, it expresses that: 'an individual may, under certain conditions, claim to be the victim of a violation occasioned by the mere existence of secret measures or of legislation permitting secret measures, without having to allege that such measures were in fact applied to him. The relevant conditions are to be determined in each case according to the Convention right or rights alleged to have been infringed, the secret character of the measures objected to, and the connection between the applicant and those measures.'[106] In this way, the ECtHR adopted an *in abstracto* claim, in place of a hypothetical claim, only the existence of a law may constitute a violation of the right to respect for private life.[107]

In the more recent case of *Weber and Saravia v. Germany*, the applicants complained about the certain provisions of the Fight Against Crime Act amending the G 10 Act, in their versions as interpreted and modified by the Federal Constitutional Court.[108] The first applicant is a freelance journalist who works for various German and foreign newspapers, radio and television stations on a regular basis. She investigates matters related to surveillance activities. The second applicant took messages for the first applicant when she was on assignments, both from her telephone and from his own telephone. He then transmitted these messages to wherever she was.[109] The ECtHR permits *in abstracto* claims as: 'The mere existence of legislation which allows a system for the secret monitoring of communications entails a threat of surveillance for all those to whom the legislation may be applied. This threat necessarily strikes at freedom of communication between users of the telecommunications services and thereby amounts in itself to an interference with the exercise of the applicants' rights under Article 8, irrespective of any measures actually taken against them.'[110]

Thus, the Court's acceptance of *in abstracto* claim was vital in order to assess the surveillance measures. Besides such abstract test, the ECtHR accepted the reasonable likelihood test in particular cases. In these cases, the applicant does not know whether a certain surveillance practice implemented himself and has no opportunity to determine whether this was so, and cases in which an applicant is merely impacted by a law of its all-embracing scope, may be proclaimed admissible by the ECtHR under specific situations. At this point, it has to be a possibility that someone was impacted by a specific practice, that the complaint was part of a particular group of

[105] ibid para, 31.
[106] ibid para, 34.
[107] Sloot, *'Is the Human Rights Framework Still Fit for the Big Data Era? A Discussion of the ECtHR's Case Law on Privacy Violations Arising from Surveillance Activities'* (n 96) 420.
[108] *Weber and Saravia v Germany* App no 54934/00 (ECtHR, 29 June 2006) para 73.
[109] ibid para, 5-6.
[110] ibid para, 78.

people classified in the law or had taken place on the activities that could induce such people to monitor and surveillance.[111]

Therefore, the ECtHR ignore the applications which rely on mysterious clicking noises during phone calls. However, it accepted when the applicants are members of a group actively campaigning against a particular issue, from which a reasonable fear of active monitoring may be deduced.[112] For instance, in *Kennedy v. The United Kingdom* case, the Court reflects this approach clearly. In the present case, the applicant alleged that his communications were being unlawfully intercepted in order to intimidate him and undermine his business activities due to his high profile case and his subsequent involvement in campaigning against miscarriages of justice.[113] The Court expresses that: 'The applicant has alleged that the fact that calls were not put through to him and that he received hoax calls demonstrates a reasonable likelihood (hypothetical harm) that his communications are being intercepted. The Court disagrees that such allegations are sufficient to support the applicant's contention that his communications have been intercepted. Accordingly, it concludes that the applicant has failed to demonstrate a reasonable likelihood that there was actual interception in his case.'[114] However, the ECtHR accepts the application in light of his other allegations as: '… any interception is taking place without lawful basis in order to intimidate him, the Court considers that it cannot be excluded that secret surveillance measures were applied to him or that he was, at the material time, potentially at risk of being subjected to such measures.'[115]

Though, the Court requires the applicants to prove, at least, a reasonable likelihood when the security activities are taken place in the narrower scope. In this sense, *Hilton v. the United Kingdom* case was indicative. In the concrete case, the applicant complains that the obtaining, retention and application of personal information by the BBC and the Security Service so as adversely to affect her prospects of being appointed to a particular post, without any opportunity for her to know or to comment on the accuracy of the information. The Court notes that ' The *Klass and others v. Germany* case falls to be distinguished from the present case in that there existed a legislative framework in that case which governed the use of secret measures and that this legislation potentially affected all users of postal and telecommunications services. In the present case the category of persons likely to be affected by the measures in question is significantly narrower. On the other hand, the Commission considers that it should be possible in certain cases to raise a complaint such as is made by the applicant without the necessity of proving the existence of a file of personal information. To fall into the latter category the Commission is of the opinion that applicants

[111] Sloot, *'Privacy in the Post-NSA Era: Time for a Fundamental Revision'* (n 97) 5.
[112] ibid
[113] *Kennedy v The United Kingdom* App no 26839/05 (ECtHR, 18 May 2010) para 6-7.
[114] ibid para 125.
[115] ibid para 128.

must be able to show that there is, at least, a reasonable likelihood that the Security Service has compiled and continues to retain personal information about them.'[116]

The other principle is the chilling effect (future harm) which the Court is also willing to embrace in particular cases regarded with article 8 of the ECHR, mainly when they concerned surveillance activities, and besides, related with laws that distinguish or stigmatize particular groups in society. This effect induces people to limit their behaviour and avert from specific acts which they consider as possibly inciting negative outcomes. At this point, the ECtHR is willing to admit that even no damage has been done yet to a complaint, he might still allege his priori claim if it is probably that he will be effected from the harm in the future. Since he is curtailed in his right for respect to private life by the authorities or he will invoke in the limitation of using his rights.[117]

In this context, the case of *Michaud v. France* could be evaluated as an instance. The applicant claimed that as a lawyer he was obliged, subject to disciplinary action, to report people who came to him for advice because lawyers were required to report suspicious operations. He assessed this to be incompatible with the principles of lawyer-client privilege and professional confidentiality.[118] The Government asserted that the applicant could not claim to be a "victim". They discussed that his rights had not actually been affected in practice, emphasizing that he did not allege that the legislation in question had been applied to his detriment, but simply that he had been requested to organise his practice accordingly and introduce special internal procedures. Therefore the Government warned against the extensive application of this concept, which would open the door to class actions.[119]

The Court noted that 'in order to be able to lodge an application a person must be able to claim to be a "victim" of a violation of the rights enshrined in the Convention … It is, however, open to a person to contend that a law violates his rights, in the absence of an individual measure of implementation, and therefore to claim to be a "victim" …, if he is required to either modify his conduct or risk being prosecuted, or if he is a member of a class of people who risk being directly affected by the legislation.'[120]

The ECtHR stresses that 'if the applicant fails to report suspicious activities as required he will expose himself by virtue of this text to disciplinary sanctions up to and including being struck off. The Court also considers credible the applicant's suggestion that, as a lawyer specialising in financial and tax law, he is even more concerned by these obligations than many of his colleagues and exposed to the consequences of failure to comply. In fact he is faced with a dilemma

[116] *Hilton v The United Kingdom* App no 12015/86 (ECtHR, 6 July 1988)
[117] Sloot, *'Is the Human Rights Framework Still Fit for the Big Data Era? A Discussion of the ECtHR's Case Law on Privacy Violations Arising from Surveillance Activities'* (n 96) 423.
[118] *Michaud v France* App no 12323/11 (ECtHR, 06 December 2012) para 47.
[119] ibid para 49.
[120] ibid para 51.

comparable, … either he applies the rules and relinquishes his idea of the principle of lawyer-client privilege, or he decides not to apply them and exposes himself to disciplinary sanctions and even being struck off. Thus, the Court accepts that the applicant is directly affected by the impugned provisions and may therefore claim to be a "victim" …'[121]

The Court tries to abandon its approach as strictly focusing on personal harm when cases related to potential discrimination and stigmatization of weaker groups in society. For instance, in *S.A.S v. France* case in which the applicant complained about the ban on wearing clothing designed to conceal one's face in public places, deprived her of the possibility of wearing the full-face veil in public.[122] The ECtHR determines that: 'Furthermore, the applicant admittedly does not claim to have been convicted – or even stopped or checked by the police – for wearing the fullface veil in a public place. An individual may nevertheless argue that a law breaches his or her rights in the absence of a specific instance of enforcement, and thus claim to be a "victim", if he or she is required either to modify his or her conduct or risk being prosecuted, or if he or she is a member of a category of persons who risk being directly affected by the legislation. This is the case … for women who, like the applicant, live in France and wish to wear the full-face veil for religious reasons. They are thus confronted with a dilemma comparable …: either they comply with the ban and thus refrain from dressing in accordance with their approach to religion; or they refuse to comply and face prosecution.[123]

This attitude is becoming increasingly crucial in cases concerning surveillance activities by the Contracting Parties, in which the ECtHR is also willing to accept chilling effects and surveillance activities. Sample case may be *Colon v. the Netherlands*.[124] In the present case, the applicant claimed that the designation of a security risk area by the Burgomaster violated his right to respect for privacy as it enabled a public prosecutor to conduct random searches of people over an extensive period in a large area without this mandate being subject to any judicial review.[125] Contrary to this, the Government argued that the designation of a security risk area or the issuing of a stop-and-search order had not in itself constituted an interference with the applicant's private life or liberty of movement. Since the event complained of, several preventive search operations had been conducted; in none of them, apparently, had the applicant been subjected to further attempts

[121] ibid para, 52.
[122] *S.A.S. v France* App no 43835/11 (ECtHR, 1 July 2014) para 3.
[123] ibid para 57.
[124] Martha Peeters, The Connection between Liberty and Bulk Interception of Data Legal Discourse on the Visuality of Liberalism and Neo-republicanism in Current Jurisprudence Regarding Bulk Interception of Data <*http://arno.uvt.nl/show.cgi?fid=145718*> accessed 28 July 2019, 32.
[125] *Colon v The Netherlands* App no 49458/06 (ECtHR, 15 May 2012) para 46.

to search him. This was enough to show that the likelihood of an interference with the applicant's rights was so minimal as to deprive him of the status of victim.[126]

The ECtHR emphasized that: 'In principle, it is not sufficient for individual applicants to claim that the mere existence of the legislation violates their rights under the Convention; it is necessary that the law should have been applied to their detriment. Nevertheless, Article 34 entitles individuals to contend that legislation violates their rights by itself, in the absence of an individual measure of implementation, if they run the risk of being directly affected by it; that is, if they are required either to modify their conduct or risk being prosecuted, or if they are members of a class of people who risk being directly affected by the legislation. The Court is not disposed to doubt that the applicant was engaged in lawful pursuits for which he might reasonably wish to visit the part of Amsterdam city centre designated as a security risk area. This made him liable to be subjected to search orders should these happen to coincide with his visits there. The events of 19 February 2004, followed by the criminal prosecution occasioned by the applicant's refusal to submit to a search, leave no room for doubt on this point. It follows that the applicant can claim to be a "victim" within the meaning of Article 34 of the Convention and the Government's alternative preliminary objection must be rejected also.'[127]

Therefore, the Court's approach was more flexible in terms of complaints about legislation authorising surveillance programmes. Such as, *Lordachi v. Moldavia* case, the Court has pointed out that[128]: 'The mere existence of the legislation entails, for all those who might fall within its reach, a menace of surveillance; this menace necessarily strikes at freedom of communication between users of the postal and telecommunications services and thereby constitutes an 'interference by a public authority' with the exercise of the applicants' right to respect for correspondence.'[129]

In sum, the Court's approach related to the notion of the victim has changed in certain types of cases, commonly cases concerning surveillance activities and data retention, either by secret services or other governmental institutions. The ECtHR tries to make it's standards flexible in terms of admissibility criteria. It is occasionally willing to permit the hypothetical complaints if there is a reasonable likelihood that the applicant has been harmed, it is sometimes willing to admit a priori claims, particularly when the mere existence of acts and policies forced the applicant to restrict using his right to privacy.[130] The reaction of the ECtHR refrains from the current evolvement known as Big Data which is introduced as collecting massive data without a pre-established aim, about an

[126] ibid para 58.
[127] ibid para 60-61.
[128] Sloot, *'How to Assess Privacy Violations in the Age of Big Data? Analysing the Three Different Tests Developed by the ECtHR and Adding for a Fourth One'* (no 89) 102.
[129] *Iordachi and Others v Moldova* App no 25198/02 (ECtHR, 10 February 2009) para 118.
[130] Sloot, *'Is the Human Rights Framework Still Fit for the Big Data Era? A Discussion of the ECtHR's Case Law on Privacy Violations Arising from Surveillance Activities'* (n 96) 429-430.

undefined number of people. [131] In these conditions, the ECtHR seems to find new formulations in the different areas of its jurisprudence when evaluating the right to privacy.[132]

4.2 Balancing Test whether the Approach of the ECtHR is Adequate in the Era of Mass Data

Even if surveillance activities and data retention were evaluated under the article 8 of the ECHR, and even if the related cases were announced admissible, it is still highly controversial whether the ECtHR would conclude the cases in favour of the applicants. Previously mentioned, privacy restrictions are permitted when they are in accordance with the law and necessity in a democratic society in connection to, among others; national security, public health, and economic-wellbeing in terms of article 8 (2). The authors of the ECHR kept in mind that the consequences of a case must be determined by an evaluation of the necessity of a breach, inter alia by assessing the effectiveness, proportionality, and subsidiary of a specific measure. Besides, using this intrinsic test occasionally, the ECtHR has been moved to the background and is increasingly supplemented by a 'balancing test'.[133]

Setting out that the regulation is necessary in a democratic society includes indicating that the action taken is in response to a pressing social need. Moreover, the interference with the rights safeguarded is no greater than is necessary to address that pressing social need. At this point, the latter requirement is referred to as the test of proportionality. The Court should take into account the balance between the severity of the restriction placed on the individual and the importance of the public interest.[134]

Therefore, to determine the outcome of a case, the ECtHR balances the damage a particular privacy violation has done to the individual interest of an applicant against its instrumentality towards protecting a social interest as national safety. However, with data processes, the relation between the data collection and processing of personal data of a certain person, and the useful results for the promotion of national security is mostly ambiguous and abstract, not in the last place, since the data collection begins before a particular suspicion has emerged, not afterwards. Namely, data are collected and processed, merely to assess at a later legal point which data are precious and for what aim they may be used. Particularly in legal cases, it is commonly difficult to decide what beneficial results the data collection of this specific person has had on the promotion of national safety. These situations are different from classic privacy breaches where, for instance, data was collected about a particular person to understand whether he had committed a crime.[135]

---

[131] ibid 413.
[132] Sloot, *'How to Assess Privacy Violations in the Age of Big Data? Analysing the Three Different Tests Developed by the ECtHR and Adding for a Fourth One'* (n 89) 95.
[133] Sloot, *'Privacy in the Post-NSA Era: Time for a Fundamental Revision'* (n 97) 7.
[134] Rainey, Wicks, and Ovey (n 36) 410.
[135] Sloot, *'How to Assess Privacy Violations in the Age of Big Data? Analysing the Three Different Tests Developed by the ECtHR and Adding for a Fourth One'* (n 89) 75.

Besides, the other question may be emerged as to how effective these data processing systems are. Since it is difficult to sort out these mass data in order to use the related information for security purposes.[136]

'As a result, during the past four decades the United States of America national security agency has dramatically increased the amount of the raw material that it collects, even while it has produced less and less intelligence information … in the 1980s, agency processed, analysed, and reported approximately 20 percent of the communications traffic it intercepted. Today, that number has dropped to less than 1 percent.'[137] Thus, it is obvious that the effectiveness of data processed activities is controversial in order to maintain public security.

In the light of these challenges, balancing test seems unfit for the cases related to surveillance activities.[138] In this regard, The Big Brother Watch and Others v. the United Kingdom is the core case in terms of mass data issue, this is the first time that the Court has been asked to consider the Convention compliance of an intelligence sharing regime.[139] In this case, 'the applicants complained about the scope and magnitude of the electronic surveillance programmes operated by the Government of the United Kingdom. The applicants accepted that the bulk interception regime had a basis in domestic law. However, they argued that it lacked the quality of law because it was so complex as to be inaccessible to the public and to the Government, reliance was placed on arrangements which were substantially "below the waterline" rather than on clear and binding legal guidelines, and it lacked sufficient guarantees against abuse.'

As it is seen in this case, the intelligence services of many other States, collect and process a large amount of personal information to, among other things, fight against terrorism. Though it might occasionally be difficult to prove the general interest served with these types of process, the ECtHR permit a wide margin of appreciation to countries in which the rationale of national safety is evoked, which is permitted by the ECtHR when it is relevant to issues of terrorism. Therefore, the Court does leave some room to the governments when it comes to determining the social interest included with big data processes.[140]

However, the ECtHR's permission related to the wide margin of appreciation does not mean, the Court will not leave its role as European supervisor. Moreover, the Court will continue to assess the

[136] Sloot, *'Privacy in the Post-NSA Era: Time for a Fundamental Revision'* (n 97) 7.
[137] Matthew Aid, The Secret Sentry Declassified <*https://nsarchive2.gwu.edu/NSAEBB/NSAEBB278/*> accessed 23 July 2019.
[138] ibid 99.
[139] *Big Brother Watch and Others v the United Kingdom* App no 58170/13, 62322/14 and 24960/15 (ECtHR, 13 September 2018) para 416.
[140] Sloot, *'Privacy in the Post-NSA Era: Time for a Fundamental Revision'* (n 97) 8-9.

activities of the state. Initially, it should be underlined that the ECtHR is trying to focus on procedural conditions.[141]

Therefore the ECtHR expresses that 'In its case-law on secret measures of surveillance, the Court has developed the following minimum safeguards that should be set out in statute law in order to avoid abuses of power: the nature of the offences which may give rise to an interception order; a definition of the categories of people liable to have their telephones tapped; a limit on the duration of telephone tapping; the procedure to be followed for examining, using and storing the data obtained; the precautions to be taken when communicating the data to other parties; and the circumstances in which recordings may or must be erased or the tapes destroyed.'[142] Moreover, the Court adds that: '… the bulk interception regime, itself, did not violate the Convention, but noted that such a regime had to respect criteria set down in its case-law.'[143]

However, it should be emphasized that, though the requirement that a privacy breach must be prescribed by law also applies to the activities of secret services, it is precisely related with the intelligence organizations that a separate and rather restricted legal regulations exist, thus generally neither the ordinary citizens nor the governments will aware exactly what activities are conducted and with which specific aims. From this respect, again, the balancing test does not seem suitable for mass data systems.[144]

Accordingly, it may be encouraging to look at the necessity case in order to address issues related with the complaint about the act of British secret services, since this test is developed for cases as relevant to security interests. Moreover, it seems logical to apply a necessity test when a data gathering is executed with a specific goal in mind; for instance, a certain person, group, or institution is suspected of making plans for criminal activity and data are gathered about them and their plans to obstruct these activities or prosecute them. Whenever there is at least a slight suspicion that a particular person or group may be planning to commit a crime, there is an adequately clear general interest the government can refer.[145]

However, at this point, another problem emerges regarded with mass data processes. Indeed, data are not gathered for a particular aim or reason, rather they are obtained, stored, and analysed to find patterns, statistical correlations, and for the formulation of group profiles.[146] Merely

---

[141] Sloot, *'Privacy in the Post-NSA Era: Time for a Fundamental Revision'* (n 97) 8.
[142] *Weber and Saravia v Germany* App no 54934/00 (ECtHR, 29 June 2006) para 95.
[143] *Big Brother Watch and Others v the United Kingdom* App no 58170/13, 62322/14 and 24960/15 (ECtHR, 13 September 2018) para 389.
[144] Sloot, *'Privacy in the Post-NSA Era: Time for a Fundamental Revision'* (n 97) 8.
[145] Sloot, *'How to Assess Privacy Violations in the Age of Big Data? Analysing the Three Different Tests Developed by the ECtHR and Adding for a Fourth One'* (n 89) 100.
[146] Narwaria Mamta, Arya Suchita, "State-of-the-art in Privacy Preserving Data Mining", 2016 3rd International Conference on Computing for Sustainable Global Development), Computing for Sustainable Global Development, 2016 3rd International Conference on, p. 2108, <*http://0-search.ebscohost.com.serlib0.essex.ac.uk/login.aspx?direct=true&db=edseee&AN=edseee.7724638&site=eds-live*> accessed 18 July 2019

subsequently it becomes clear what data are essential and for what goals they may be used. As the applicants related with mass data processes, such as the one submitted recently, usually do not regard the particular use of the data for determined goals, but the data collecting as such, it will be hard to impossible for data collectors, such as the state, to clarify at that point what public interest is served with the data gathering and to what extent. In consequence, the necessity test requires a clear societal interest, which is usually not easy to prove in mass data processes.[147]

Therefore, perhaps, it is more encouraging to apply the unreasonable burden test. In this test, the most important advantage is that the societal interest is assumed by the Court, which is a benefit in respect to the necessity test. Though, the individual interest needs to be shown, which, previously mentioned, substantiate difficultly in big data processes. Still, the ECtHR does not oblige harm or a setback to interest as such but only a 'burden', which is applied by the Court as a rather flexible term. Moreover, particularly the ECtHR has done something in these types of cases, namely, it has adopted as main notion whether the 'quality of life' of the applicant has been harmed. The challenge related with numerous environmental cases, like the cases concerning Big Data, the context of harm is so problematic. What harm causes noise pollution for the individual in terms of private or family life? How can one prove, for instance, that illnesses have arisen from smog or air pollution? Even if individual harm can be shown, the causal connection between environmental pollution and individual harm is often not easy to demonstrate. This is exactly why the ECtHR has used the notion of 'quality of life', as to whether the 'quality of life' is diminished can in principle merely be determined by the subject itself. Therefore, the notion of harm becomes a subjective, rather than an objective, matter.[148]

In this sense, the first case is *Branduse v. Romania*[149] in which the applicant complained among others about the offensive smells created by a former refuse tip situated about 20 metres away from the prison he was jailed, alleging that its quality of life and its welfare were affected by the respective smells. Though at the starting point it was evaluated that the applicant will not win this case, the Court determined that there had been a violation of Article 8 of the ECHR since the Romanian authorities failed to take the adequate measures to solve the problem.[150]

Similarly, the other significant example is *Ledyayeva, Dobrokhotova, Zolotareva and Romashina v. Russia* case in which the applicants claimed that the operation of a steel-plant in close proximity to

---

[147] Sloot, *'How to Assess Privacy Violations in the Age of Big Data? Analysing the Three Different Tests Developed by the ECtHR and Adding for a Fourth One'* (n 89) 100.
[148] ibid.
[149] *Branduse v Romania* App no 6586/03 (ECtHR, 7 April 2009)
[150] Laura Cristiana Spataru-Negura, 'The European Court of Human Rights and its Case-Law on Environmental Matters' Challenges of the Knowledge Society. Public Law 558. <http://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=6&cad=rja&uact=8&ved=2ahUKEwiCvsf7vr7jAhUUqXEKHd7eCH0QFjAFegQIABAC&url=http%3A%2F%2Fcks.univnt.ro%2Fuploads%2Fcks_2017_articles%2Findex.php%3Fdir%3D03_public_law%252F%26download%3DCKS_2017_public_law_032.pdf&usg=AOvVaw097K1yulOFkjNJLCODSd3X> accessed 19 July 2019

their homes endangered their health and well-being. Moreover, they complained that the government's failure to protect their private lives and homes from severe environmental nuisance arising from this steel plant's industrial activities. [151]

The Governments submitted that the domestic courts had never examined the influence of industrial pollution on the applicants' health nor assessed the damage caused by it, because the applicants had not raised these issues in the domestic proceedings. Numerous examinations of the state of environmental pollution in the town did not reveal any extreme cases of environmental pollution. The applicants have failed to use the means prescribed by the Russian legislation for assessing environmental hazards… The Government stressed that the environmental monitoring carried out by State agencies revealed an improvement in the overall environmental situation throughout the town, and that the pollution levels near the applicants' houses did not differ significantly from the average levels across the town.[152]

The ECtHR expressed that: '… in many cases the existence of an interference with a Convention right is evident and does not give rise to any discussion, in other cases it is a subject of controversy. The present four applications belong to this second category. There is no doubt that serious industrial pollution negatively affects public health in general. However, it is often impossible to quantify its effects in each individual case, and distinguish them from the influence of other relevant factors, such as age, profession etc. The same concerns possible worsening of the quality of life caused by the industrial pollution. The "quality of life" is a very subjective characteristic which hardly lends itself to a precise definition.'[153]

Therefore, within this term, the Court could announce that the case is admissible. Though the idea of relatively abstract public interests and subjective personal interests is a very promising beginning step, it is not adequate to enable the ECtHR to deal with current privacy breaches arising from mass data processes. Since it still focuses on the burden on particular individual claimants, while big data processes do not concern persons or small groups, but rather have an impact on everyone.[154]

In sum, it is not clear how the Court may approach these controversial issues related with the Big Data processes in a satisfactorily way. The ECtHR has usually applied three tests it has evolved to cope with different privacy questions, one in which the Court has considered the balance between the severity of the limitation placed on the individual and the importance of the public interest, other in which it has focused the necessity of the restriction, and a third in which it has applied the

[151] *Ledyayeva, Dobrokhotova, Zolotareva and Romashina v Russia* App no 53157/99, 53247/99, 56850/00 and 53695/00 (ECtHR, 26 October 2006) para 74.
[152] ibid para 79-81.
[153] ibid para 90.
[154] Sloot, *'How to Assess Privacy Violations in the Age of Big Data? Analysing the Three Different Tests Developed by the ECtHR and Adding for a Fourth One'* (n 89) 101.

unreasonable burden test it balances both interests. However, neither of these tests is adequate in order to resolve concerning cases.[155] Thus, a new test or approach needs to be improved, in which both interests weighed are formulated on a general and abstract level. Since there are already lacks of such an approach available in the Court's jurisprudence.[156]

5. Conclusion

To summarize briefly, although ECHR does not contain any provision which refers explicitly to the right for the safeguarding of personal data, data privacy falls within the scope of article 8 of ECHR according to the Court. The ECtHR has closed this gap by a broad interpretation of the concept of private life.[157]

The Court expresses that the collection, storage and disclosure by the Contracting Parties of information and data related to individuals with or without their consent, as well as their accessibility, will always concern a person's private life.[158] In this regard, for instance, person's name, photo, or physical and moral integrity[159], recording of fingerprints, images, cell samples, DNA profiles[160], medical data,[161] ethnic identity,[162] banking documents[163] are evaluated as personal data in the jurisprudence of the Court within its wide interpretation.

Article 8 (2) of the ECHR expresses that the protection of the right to respect for private life is not absolute and this article provides the conditions in which the Court allows the State Parties to limit such rights.[164] In this regard, the Contracting States should take into account three situations: the interference should be prescribed by law, it should purpose of the rationales designated in the article 8 (2) of ECtHR, and it should be necessary in a democratic society. The first criterion is generally accepted as the 'rule of law test'. It implies that there must be a law on which the interference is based and in which the authorities are provided with the specific competence to act by the democratic law-maker. This law must be accessible to the individuals and be sufficiently clear and precise to enable a person to reasonably foresee the outcomes of his actions. Finally, the law must provide effective guarantees against arbitrary interferences and the abuse of power by the executive authorities.[165]

---

[155] Sloot, *'How to Assess Privacy Violations in the Age of Big Data? Analysing the Three Different Tests Developed by the ECtHR and Adding for a Fourth One'* (n 89) 103.
[156] ibid 113.
[157] Psychogiopoulou and Brkan (n 5) 60.
[158] Ivana Roagnavana, Protecting the Right to Respect for Private and Family Life under the European Convention on Human Rights, *Council of Europe Human Rights Handbooks*, (Council of Europe, 2012) 19.
[159] *Von Hannover v German* App no 59320/00 (ECtHR, 24 June 2004) para 95.
[160] *S and Marper v UK* App no 30562/04 (ECtHR, 04 December 2008) para 85.
[161] *L.H. v Latvia* App no 52019/07 (ECtHR, 29 April 2014) para 56.
[162] *Ciubotaru v Moldova* App no 27138/04 (ECtHR, 27 April 2010) para 49-53.
[163] *M.N. and Others v San Marino* App no 28005/12 (ECtHR, 07 July 2015) para 51.
[164] Psychogiopoulou and Brkan (n 5) 34.
[165] Sloot, *'How to Assess Privacy Violations in the Age of Big Data? Analysing the Three Different Tests Developed by the ECtHR and Adding for a Fourth One'* (n 89) 77.

These criteria could be adequate to ascertain the infringement in the traditional privacy cases or it is easy to justify the violations as the personal harm and the victim could be clarified simply in these cases. The ECtHR could provide a balance between individual harm and the importance of interest while resolving such cases. Thus, balancing test is an effective tool in terms of determining the classic privacy cases by the ECtHR.[166]

However, personal computing and the internet have made it possible for a wider range of people – involving scholars, marketers, secret services, governmental agencies, educational institutions, and motivated individuals – to produce, share, interact with, and organize data.[167] At a time when it is easier than ever to monitor the attitude of persons, governments now rely on collecting all sorts of data from their citizens for the detention of criminal activities. While older forms of surveillance included monitoring only those suspected of offences (for instance, through wiretapping their phones or following their movements), new techniques involve collating massive amounts of personal data – regarding, for instance, phone calls, e-mail use and social media interactions – from large numbers of people, most of whom governmental institutions officials have no reason to believe are guilty of anything. The resulting data sets are then analysed in order to uncover potential criminal threats. These programs, however, are highly debated.[168] Therefore, in our current World, the types of cases related to the personal data are not as simple as these classic cases due to the developments in the technology and particularly advance in the internet area. Accordingly, key questions are arising when resolving these new types of cases.

As highlighted above, in Big Data processes, it becomes rather difficult to designate harm to an individual's interests. Usually, an individual is simply unaware that his personal data is collected by either his fellow citizens (e.g. via the use of their smartphones), by companies (e.g. by following cookies), or by governments (e.g. through covert surveillance). But even if a person has the awareness of these data gatherings, given the fact that data collection and processing is so omnipresent and common, it will unlikely be possible for him to keep up with every data processing which involves his data, to evaluate whether the data controller complies with the legal standards applicable, and if not, to file a legal complaint. And if a person does apply to the court to protect his rights, he has to demonstrate an individual interest, that is personal harm, which is a significantly challenging notion in Big Data processes. While the traditional approach is centered upon individual rights and individual interests, data processing is usually related with structural and societal issues.

---

[166] Sloot, *'Is the Human Rights Framework Still Fit for the Big Data Era? A Discussion of the ECtHR's Case Law on Privacy Violations Arising from Surveillance Activities'* (n 96) 413-414.

[167] Danah Boyd and Kate Crawford, 'Critical Questions for Big Data' *Information, Communication and Society*, vol15(5) (2012) 664.

[168] Isaac Taylor, 'Data Collection, Counterterrorism and the Right to Privacy' *Politics, Philosophy & Economics,* vol 16(3) (2017) 327.

Connecting these types of processes to personal harm to individual's autonomy, dignity, or negative freedom demonstrates increasingly difficult.[169]

Therefore, how the Court handles the emergence of an era of Big Data is critical as a paramount human right body. To deal with these issues, the Court has been willing to adopt a slight relaxation of the requirement of personal harm and individual interest. Regarding presumed surveillance activities about which no insight was given by the secret services, the Court expressed that it is not acceptable[170] that "the assurance of the enjoyment of a right guaranteed by the convention could be thus removed by the simple fact that the person concerned is kept unaware of its violation."[171]

Likely, in some cases, the ECtHR has also been prepared to accept a broader interpretation regarding to the complaints about law authorizing surveillance regimes, which is drafted in very broad and common terms. Moreover, cases in which the applicant does not know whether he was subjected to a specific surveillance activity and has no opportunity to detect whether this was so, and cases in which a plaintiff is solely affected by law by way of its all-encompassing scope, may be announced admissible by the ECtHR under certain situations. On this point, it must be plausible that someone was influenced by a specific practice, that the applicant is part of a particular group of people designated in the law or had engaged in activities that could lead to monitoring and surveillance. Thus, the ECtHR acknowledges as a matter of principle that to be granted a right of complaint, there must be the existence of a "reasonable likelihood" that the applicant has been subjected to a surveillance or monitoring practice.[172] In this regard, the Court is sometimes willing to allow the hypothetical complaints or future harm if there is a reasonable likelihood that the applicant has been harmed, it occasionally willing to adopt a priori claims, particularly when the mere existence of law and policies obliged the applicant to limit using his right to privacy.[173]

The other problematic issue is to make a proper balance of interests in this type of Big Data regimes as in these systems, both the public and personal interest are rather hypothetical and abstract, as indicated earlier. To handle with these issues, in data processing cases the ECtHR has tried to stay focused on the quality of the Contracting States' law and governmental activities.[174] 'The Court must be satisfied that there exist adequate and effective guarantees against abuse.'[175] 'According to the Court's case-law, the fact that persons concerned by such measures are not apprised of them while the surveillance is in progress or even after it has ceased cannot by itself

[169] Sloot, *'Privacy as Human Flourishing: Could a Shift towards Virtue Ethics Strengthen Privacy Protection in the Age of Big Data'* (n 4) 240.
[170] Sloot, *'Privacy in the Post-NSA Era: Time for a Fundamental Revision'* (n 97) 4.
[171] *Klass and others v Germany* App. no 5029/71 (ECtHR, 06 September 1978) para 36.
[172] Sloot, *'Privacy in the Post-NSA Era: Time for a Fundamental Revision'* (n 97) 5.
[173] Sloot, *'How to Assess Privacy Violations in the Age of Big Data? Analysing the Three Different Tests Developed by the ECtHR and Adding for a Fourth One'* (n 89) 95.
[174] Sloot, *'Privacy in the Post-NSA Era: Time for a Fundamental Revision'* (n 97) 8.
[175] *Association and European Integration and Human Rights and Ekimdzhiev v Bulgaria* App. no 62540/00 (ECtHR, 28 June 2007) para 77.

warrant the conclusion that the interference was not justified under the terms of paragraph 2 of Article 8, as it is the very unawareness of the surveillance which ensures its efficacy. However, as soon as notification can be made without jeopardising the purpose of the surveillance after its termination, the information should be provided to the persons concerned.'[176]

The Court has generally used three tests it has evolved to deal with different privacy issues. In the balancing test, the Court has taken into account the balance between the seriousness of the restriction taken placed on the individual and the importance of the public interest. The other test is the necessity test in which it has focused the necessity of the limitation. In the third test, the Court has applied the unreasonable burden test it balances both interests. However, these tests are not efficient in order to resolve concerning cases.[177]

In this respect, The *Big Brother Watch and Others v. the United Kingdom* is the landmark case. The Court expresses that: '… the bulk interception regime, itself did not violate the Convention, but noted that such a regime had to respect criteria set down in its case-law.'[178] The ECtHR's judgment is a vital step towards safeguarding individuals from unjustified intrusion as it has serious implications not only for the UK's data process, but also for the mass surveillance activities of the Council of Europe's other member states, and for such practices in other parts of the world.[179]

However, the ECtHR's these affords are not adequate in order to cope with the Big Data process challenge. Although a set of principles to counter data protection interferences are applied in different ways and generate different species of legal protection, the case-specific approach of the Court to all these interferences reflects the complex systems to assess the violations.[180] Moreover, given the difficulty in dealing with all these interferences related to mass data, it is clear that innovator approaches and tests are needed to implement in a systematic way in order to assure the individuals that the Big Brother is not watching them.

---

[176] ibid para 90.
[177] Sloot, *'How to Assess Privacy Violations in the Age of Big Data? Analysing the Three Different Tests Developed by the ECtHR and Adding for a Fourth One'* (no 89) 103.
[178] ibid para 389.
[179] A brief history of the '10 Human Rights Organisations v. the United Kingdom' legal case (12 September 2018) <*https://privacyinternational.org/feature/2264/brief-history-10-human-rights-organisations-v-united-kingdom-legal-case*> accessed 28 July 2019
[180] Antonella Galetta and Paul De Hert, 'Complementing the Surveillance Law Principles of the ECtHR with Its Environmental Law Principles: An Integrated Technology Approach to a Human Rights Framework for Surveillance ' Utrecht L Rev, vol 55 (2014) 74.

Bibliography

Primary Sources

Cases

Amann v Switzerland App no 27798/95 (ECtHR, 16 February 2000)

Association and European Integration and Human Rights and Ekimdzhiev v Bulgaria App. no 62540/00 (ECtHR, 28 June 2007)

Aycaguer v France App no 8806/12 (ECtHR, 22 June 2017)

Bensaid v The United Kingdom App no 44599/98 (ECtHR, 6 February 2001)

Big Brother Watch and Others v the United Kingdom App no 58170/13, 62322/14 and 24960/15 (ECtHR, 13 September 2018)

Branduse v Romania App no 6586/03 (ECtHR, 7 April 2009)

Buckley v UK App no 20348/92 (ECtHR, 29 September 1996)

Ciubotaru v Moldova App no 27138/04 (ECtHR, 27 April 2010)

Colon v the Netherlands App no 49458/06 (ECtHR, 15 May 2012)

Craxi v Italy App no. 25337/94 (ECtHR, 17 July 2003)

Gaskin v the United Kingdom App no 10454/83 (ECtHR, 07 July 1989)

Godelli v Italy App no 33783/09 (ECtHR, 25 September 2012)

Hilton v the United Kingdom App no 12015/86 (ECtHR, 6 July 1988)

Iordachi and others v Moldova App no 25198/02 (ECtHR, 10 February 2009)

Kennedy v the United Kingdom App no 26839/05 (ECtHR, 18 May 2010)

K.H. and others v Slovakia App no 32881/04 (ECtHR, 28 April 2009)

Khan v United Kingdom App no 35394/97 (ECtHR, 12 May 2000)

Klass and others v Germany App No 5029/71 (ECtHR, 06 September 1978)

Kruslin v France App no 11801/85 (ECtHR, 24 April 1990)

Leander v Sweden (1987) Series A no 28

Ledyayeva, Dobrokhotova, Zolotareva and Romashina v Russia App no 53157/99, 53247/99, 56850/00 and 53695/00 (ECtHR, 26 October 2006)

L.H. v Latvia App no 52019/07 (ECtHR, 29 April 2014)

Malone v the United Kingdom App no 8691/79 (ECtHR, 02 August 1984)

Michaud v France App no 12323/11 (ECtHR, 06 December 2012)

Mikulic v Crotoatia App no 53176/99 (ECtHR, 7 February 2002)

M.N. and others v San Marino App no 28005/12 (ECtHR, 07 July 2015)

Noel Narvii Tauria and others v France App no 28204/95 (ECtHR, 4 December 1995)

Roche v the United Kingdom App no 32555/96 (ECtHR, 19 October 2005)

Ryssdal, 'Data Protection and the European Convention on Human Rights', in Data Protection, Human Rights and Democratic Values, Proceedings of the 13th Conference of Data Protection Commissioners held 2-4 October 1991 in Strasbourg (Strasbourg: CoE, 1992)

S and Marper v UK App no 30562/04 (ECtHR, 04 December 2008)

S.A.S. v France App no 43835/11 (ECtHR, 1 July 2014)

Shimovolos v Russia App no 30194/09 (ECtHR, 21 June 2011)

Taylor-Sabori v the United Kingdom App no 47114/99 (ECtHR, 22 October 2002)

Trivkanov v Croatia App no 12986/13 (ECtHR, 06 July 2017)

Turek v Slovakia App no 57986/00 (ECtHR, 14 February 2006)

Tyrer v the UK App no 5856/72 (ECtHR, 25 April 1978)

Valenzuela Contreras v Spain App no 27671/95 (ECtHR, 30 July 1998)

Von Hannover v German App no 59320/00 (ECtHR, 24 June 2004)

Weber and Saravia v Germany App no 54934/00 (ECtHR, 29 June 2006)

Z v Finland App no 22009/93 (ECtHR, 25 February 1997)

Conventions

Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (adopted in Council of Europe 28 January 1981, entered into force 01 October 1985) the CoE Convention

European Convention for the Protection of Human Rights and Fundamental Freedoms (adopted in Council of Europe 4 November 1950, entered into force 1953) ECHR

Secondary Sources

Books

Arai-Takahashi Y, *The Marjin of Appreciation Doctrine and the Principle of the Proportionality in the Jurisprudence of the ECHR* (Intersentia, Antwerp, Oxford, New York 2002)

Bernadette Rainey B, Wicks E, and Ovey C, Jacobs, White, and Ovey: *The European Convention on Human Rights* (Oxford University Press 2017)

Bygrave L, A, *Data Protection Law: Approaching Its Rationale, Logic, and Limits* (Kluwer Law International, 2002)

Harris D, O'Boyle M, Bates E, and Buckley C, O'Boyle H, and Warbrick: *Law of the European Convention on Human Rights* (Oxford University Press 2018)

Michael J, *Privacy and Human Rights: an International and Comparative Study, with Special Reference to Developments in Information Technology* (UNESCO, 1994)

Purtova N, *Property Rights in Personal Data, A European Perspective* (Wolters Kluwer Law and Business 2012)

Reid K, *A practitioner's Guide to the European Convention on Human Rights* (Thomson/Sweet & Maxwell, 2012)

Roagnavana I, *Protecting the Right to Respect for Private and Family Life under the European Convention on Human Rights* (Council of Europe, 2012)

Tzanou M, *The fundamental Right to Data Protection:Normative Value in the Context of Counter-Terrorism Surveillance* (Hart Publishing 2017)

Contributions to Edited Books

Nardell QC,G, 'Levelling up: Data Privacy and the European Court of Human Rights' in Serge Gutwirth, Yves Poullet, Paul De Hert (eds), Data Protection in a Profiled World (Springer, Belgium 2009)

Ni Loideain N, 'Surveillance of Communications Data and Article 8 of the European Convention on Human Rights' in Serge Gutwirth, Ronald Leenes and Paul de Hert (eds), *Reloading Data Protection* (Springer, 2014)

Psychogiopoulou E, and Brkan M, 'Introduction: Courts, Privacy and Data Protection in the Digital Environment' in M. Brkan and E. Psychogiopoulou (eds), *Courts, Privacy and Data Protection in the Digital Environment* (EE Publishing, UK Edward Elgar Publishing, UK 2017)

Van der Sloot B, Legal Fundamentalism: Is Data Protection Really a Fundamental Right? in R. Leenes, R. van Brakel, S. Gutwirth, P. De Hert (eds), *Data Protection and Privacy: (In)visibilities and Infrastructures* (Springer International Publishing, 2017)

Van der Sloot B, 'Is the Human Rights Framework Still Fit for the Big Data Era? A Discussion of the ECtHR's Case Law on Privacy Violations Arising from Surveillance Activities' in Serge Gutwirth, Ronald Leenes and Paul de Hert (eds), *Data Protection on the Move* (Springer International Publishing, 2016)

Journal Articles

Boyd D and Crawford K, 'Critical Questions for Big Data' *Information, Communication and Society*, vol 15.5 (2012)

Bygrave L,A, 'Data Protection Pursuant to the Right to Privacy in Human Rights Treaties' *Int'L J.L. and Info. Tech.* vol 6 (1998)

De Hert P, 'Balancing Security and Liberty within the European Human Rights Framework. A Critical Reading of the Court's Case Law in the light of Surveillance and Criminal Law Enforcement Strategies after 9/11' *Utrecht Law Review,* vol 1 (September, 2005)

Galetta A, and De Hert P, 'Complementing the Surveillance Law Principles of the ECtHR with Its Environmental Law Principles: An Integrated Technology Approach to a Human Rights Framework for Surveillance ' *Utrecht Rev*, vol 55 (2014)

Georgieva I, 'The Right to Privacy under Fire Foreign Surveillance under the NSA and the GCHQ and Its Compatibility with Art. 17 ICCPR and Art. 8 ECHR' *Utrecht J. Int'L & EUR. L.*, vol 31(2015)

Kuner C, 'Regulation of Transborder Data Flows under Data Protection and Privacy Law: Past, Present, and Future', *TILT Law and Technology Working Paper* (2010)

R. Reidenberg J, 'The Data Surveillance State in the United States and Europe' *Wake Forest Law Review*, (2013)

Taylor I, 'Data Collection, Counterterrorism and the Right to Privacy' *Politics, Philosophy and Economics,* vol 16(3) (2017)

Van der Sloot B, 'Privacy as Human Flourishing: Could a Shift towards Virtue Ethics Strengthen Privacy Protection in the Age of Big Data' *J. Intell. Prop. Info. Tech. and Elec. Com. L,.* vol 5 (2014)

Van der Sloot B, 'How to Assess Privacy Violations in the Age of Big Data? Analysing the Three Different Tests Developed by the ECtHR and Adding for a Fourth One' *Information & Communications Technology Law*, vol 24.1 (2015)

Van der Sloot B, 'Privacy in the Post-NSA Era: Time for a Fundamental Revision' *J. Intell. Prop. Info. Tech. and Elec. Com. L.,* Vol 5.2 (2014)

Websites

A brief history of the '10 Human Rights Organisations v. the United Kingdom' legal case (12 September 2018) <*https://privacyinternational.org/feature/2264/brief-history-10-human-rights-organisations-v-united-kingdom-legal-case*> accessed 28 July 2019

Handbook on European Data Protection Law (2018) <*https://fra.europa.eu/sites/default/files/fra_uploads/fra-coe-edps-2018* > accessed 01 July 2019

<https://hudoc.echr.coe.int/eng-press#{"fulltext":["BRITO FERRINHO BEXIGA VILLA"]} > accessed 08 July 2019

Laura Cristiana Spataru-Negura, 'The European Court of Human Rights and its Case-Law on Environmental Matters' Challenges of the Knowledge Society. Public Law 558. <*http://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=6&cad=rja&uact=8&ved=2ahUKEwiCvsf7vr7jAhUUqXEKHd7eCH0QFjAFegQIABAC&url=http%3A%2F%2Fcks.univnt.ro%2Fuploads%2Fcks_2017_articles%2Findex.php%3Fdir%3D03_public_law%252F%26download%3DCKS_2017_public_law_032.pdf&usg=AOvVaw097K1yulOFkjNJLCODSd3X*> accessed 19 July 2019

Martha Peeters, The Connection between Liberty and Bulk Interception of Data Legal Discourse on the Visuality of Liberalism and Neo-republicanism in Current Jurisprudence Regarding Bulk Interception of Data <*http://arno.uvt.nl/show.cgi?fid=145718*>accessed 28 July 2019

Matthew Aid, The Secret Sentry Declassified <*https://nsarchive2.gwu.edu/NSAEBB/NSAEBB278/*> accessed 23 July 2019.

Narwaria Mamta, Arya Suchita, "State-of-the-art in Privacy Preserving Data Mining", 2016 3rd International Conference on Computing for Sustainable Global Development), Computing for Sustainable Global Development, 2016 3rd International Conference on, p. 2108, <*http://0-search.ebscohost.com.serlib0.essex.ac.uk/login.aspx?direct=true&db=edseee&AN=edseee.7724638&site=eds-live*> accessed 18 July 2019