Sri Lanka Journal of Social Sciences 2021 ***44*** *(1): 27-32*
DOI: https://dx.doi.org/10.4038/sljss.v44i1.7942

RESEARCH ARTICLE

Recognising protection of personal data under the Fundamental Rights (Constitutional Rights) perspective in Sri Lanka

Komanda Kankanamge Gimhani Anuththara

Department of Legal Studies, Faculty of Humanities & Social Sciences, The Open University of Sri Lanka, Nawala, Sri Lanka.

Abstract: Use of data in unprecedented scale and flow of data among irrelevant users would affect the personal life of any person. Most of the countries all over the world already addressed the issue by introducing laws for personal data protection. While countries like Portugal and Chile recognised this under the Constitution as 'Right to Personal Data Protection', some other countries recognised it under a specific piece of legislation as 'Personal Data Protection Act'. This article is based on an analysis of possibilities for recognising protection of personal data under the Constitutional Right perspective in Sri Lanka.

Keywords: Personal data, personal life, protection of personal data, constitutional right, legal framework.

INTRODUCTION

> "Rapid technological developments and globalization have brought new challenges for the protection of personal data. The scale of the collection and sharing personal data has increased significantly. Technology allows both private companies and public authorities to make use of personal data on an unprecedented scale in order to pursue their activities."[1]

Use of data in unprecedented scale and flow of data among irrelevant users would affect the personal life of any person. Most countries all over the world already addressed the issue by introducing laws for personal data protection. While countries like Portugal and Chile recognised this under the Constitution as 'Right to Personal Data Protection', some other countries recognised it under a specific piece of legislation as 'Personal Data Protection Act'. This article is based on an analysis of possibilities for recognising protection of personal data under the Constitutional Right perspective in Sri Lanka. This will be discussed under the sub-headings: 1) Distinguish right to personal data protection from right to privacy; 2) Possibilities of guaranteeing right to personal data as a Constitutional right in Sri Lanka; 3) Suggestions for an Act of personal data protection which provides the legal framework for this Constitutional right (fundamental right) to be exercised.

DISTINGUISH RIGHT TO PERSONAL DATA PROTECTION FROM RIGHT TO PRIVACY

Previously, 'right to privacy' was treated as an umbrella clause which included most of the concepts relating to the personal life of an individual. Protection of personal data was one among those. Attempts to recognise protection of personal data as an independent concept which is no longer dependent on 'right to privacy' was emerged. Interestingly, a tendency to recognise these concepts as two different concepts which have their own way of independency can be witnessed recently. Famous scholarly discussions with this regard mostly depend on opinions of De Hert & Gutwirth (2007). These scholars propose an ingenious way to illustrate the differences in scope, rationale and logic between these two rights. They characterise privacy as a "tool of opacity" and data protection as a "tool of transparency". In connecting the invention and elaboration of these legal tools to the development of the democratic constitutional state and its principles, the above mentioned authors state that:

*Corresponding author (kkanu@ou.ac.lk; https://orcid.org/0000-0002-9147-5815)

> "the development of the democratic constitutional state has led to the invention and elaboration of two complementary sorts of legal tools which both aim at the same end, namely the control and limitation of power. We make a distinction between on the one hand tools that tend to guarantee non-interference in individual matters or the opacity of the individual, and on the other, tools that tend to guarantee the transparency/accountability of the powerful" (De Hert & Gutwirth, 2007).

In developing the fundamental differences between these tools, the authors explain that:

> "The tools of opacity are quite different in nature from the tools of transparency. Opacity tools embody normative choices about the limits of power; transparency tools come into play after these normative choices have been made in order still to channel the normatively accepted exercise of power. While the latter are thus directed towards the control and channelling of legitimate uses of power, the former are protecting the citizens against illegitimate and excessive uses of power." (De Hert & Gutwirth, 2007)

> "Through the application of these ideas, governments try to reconcile fundamental but conflicting values such as privacy, free flow of information, governmental need for surveillance and taxation, etc... keeping in mind the societal need to collect, store and process data, along with the relative ease through which entities collecting such data can abuse power and infringe privacy, data protection seems to assume an administrative role. In fact, and as Blume notes, this is one of the functions of traditional administrative law that has been extended to data protection law." (De Hert & Gutwirth, 2007).

Privacy is a concept which is introduced to ensure the non-interference in individual matters, including interference by government or by private sector, which would make obstacles for personal autonomy. Data protection is not always so private. According to De Hert & Gutwirth (2007) it is a 'tool of transparency' which would ensure the processing of personal data. After all, the data protection is procedural while privacy is substantive in the face of rights. A matter of data protection is based on the procedural way of protecting the personal data. The major discussion of this article includes that the concepts of "personal data" and "data relating to personal life" are not the same and should not be confused as same concepts. The phrase "information relating to the personal life" describes any information which holds the credibility of damaging the dignity of any person if the information is revealed or might affect his or her private life in a significant manner and it is considered as the information which is protected under concept of "Right to Privacy". After all, privacy is about 'deciding yourself who will get which information about you'. Apart from that, any information which is connected with any natural person but not in the stage of damaging him or her private life, such identified or identifiable information can be recognised as "personal data". Furthermore, "identifiable person" means a person who can be easily identified through a given data.

According to Article 2 of the European Union (EU) Directive 95/46, the enlarged idea of "personal data" clarifies that those data are treated as any information relating to an "identifiable natural person" who can be identified directly or indirectly, in particular, by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity. This means that the information is directly about a person, or can be traced back to this person; most importantly, the name, email address, and contact numbers etc. The basic argument is that there is a significant amount of information identifiable to us that we do not deem as private but we deem a significant amount of protection.

Recently, the difference between the 'right to privacy' and 'right to personal data' was recognised by the Chilean Constitution on 16th June of 2018 through an amendment Law No. 21.096. By this amendment, it was purposed to distinguish right to personal data from the right to privacy. It ensures the possibility of imposing legal duties on third parties which control personal data more effectively. They included a new provision for personal data protection. This was recognised as a fundamental right which is granted by the Constitution of Chile.

With the above mentioned amendment, Article 19 of the Chilean Constitution is as follows,

> "The Constitution ensure to every person:
>
> The respect and protection of private life and the honor of the person and family, and furthermore, the protection of personal data. The treatment and protection of this data will be put into the form and condition by law".

This has exemplarily revealed that Right to privacy and right to personal data has their own perspectives and should be treated as two different rights. It is clear that privacy, itself a fundamental right, is a value that the right to data protection seeks to protect (McDermott, 2017).

POSSIBILITIES OF GUARANTEEING RIGHT TO PERSONAL DATA AS A FUNDAMENTAL RIGHT (CONSTITUTIONAL RIGHT) IN SRI LANKA

Rights are recognised as such because they protect particular values of a polity, and whilst rights violations often result in serious harm to claimants, this is not a necessary component of a claim because a breach of those rights is an attack on the values underpinning the legal system, and that is the harm that human rights jurisprudence seeks to protect against (McDermott, 2017).

Fundamental rights are defined as "rights contain in a Constitution or in a certain part of it, or if the right in question are classified by a Constitution as fundamental rights" (Tzanou, 2017). More specifically fundamental right is a basic or foundation, derived from law; a right be deemed by the Supreme Court to receive the highest level of Constitutional protection against government interference.

Possibilities of recognising personal data protection as a fundamental right should be considered with more relevant examples. Charter of Fundamental Rights of the European Union would be the best example to be used. While international law instruments normally use the term 'human rights', the EU (and national legal orders) speak of 'fundamental rights'. According to the preamble of the Charter, "it is necessary to strengthen the protection of fundamental rights in the lights of changes in society, social progress and scientific and technological development by making those rights more visible"[2]. Furthermore, they admitted the fundamental rights as a result of constitutional traditions and also as international obligations which are common to the Member States of the European Union.

The recognition of Data Protection as a Fundamental Right in the EU seems to broadly satisfy the criteria employed by international human rights scholars for the introduction of new human rights: Data Protection reflects fundamental social values in the era of the rapid advancement of the technologies; it has been relevant for some time in national, international and transnational systems.; it is consistent with the existing body of laws in the field; it achieved a high degree of consensus at least in the EU; and it gives rise to 'identifiable rights and obligations[3].

According to the EU Network of Independent Experts on Fundamental Rights, finally there is a pragmatic reason for the elevation of data protection to the status of a fundamental right: individuals must be aware of its existence and be conscious of the ability to enforce it in the light of the new challenges arising from the rapid development of information and communication technologies[3].

This article treated fundamental rights and Constitutional rights as same. Constitutional rights have gradually been applied in horizontal relationships, their origin lies in regulating the vertical relationship, between citizen and state. Constitutional rights provide citizens with the freedom from governmental interference, for example in their private life or freedom of expression[4].

The values constitutional rights protect are seen as particularly weighty and essential to human dignity or personal freedom; they concern matters such as privacy and freedom of expression, but also lay down procedural rules that regulate the state and its organs, such as the separation of powers, the authority of the different powers and the democratic voting process. The constitution is literally the constitution of a state which provides the fundaments on which the nation is based. Although the provisions in the constitution can generally be changed, it is often more difficult to alter those than non-constitutional rights. Many countries require a qualified majority to change the constitution and demand that two parliaments in a row, after elections having taken place, must agree on altering the constitution. This research would also include the possibilities of introducing the "right to protection of personal data" under the Constitution of Sri Lanka.

The best example for introducing right to personal data in a fundamental right manner is Article 7 and Article 8 of the European Union Charter of Fundamental Rights[2].

As mentioned in the Article 7: Respect for private and family life:

> "Everyone has the right to respect for his or her private and family life, home and communication"[2].

This has separately stated that the 'right to privacy' by means of protection of information relating to a private life.

Article 8 of the Charter has given the recognition of right to protection of personal data as mentioned below[2].

1. Everyone has the right to protection of personal data concerning him or her.

2. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law.

3. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified.

4. Compliance with these rules shall be subject to control by an independent authority.

The concept of personal data protection in a constitutional right manner is not a novel thing. 'Right to data protection' has been recognised by Constitution in many countries. Article 35 of the Portugal Constitution stated that specifically based on computerised data[5]:

1. Every citizen has the right to access to all computerized data that concern him, to be informed of the purpose for which they are intended, all as laid down by law, and to require that they be corrected and updated.

2. Computers shall not be used to process data concerning political affiliation, religion, or private life, except where the processing of data is done for the purpose of processing statistical data that cannot be individually identified.

This has proven that right to personal data protection can be recognised also under the Constitution of Sri Lanka and this can be done as same as how Sri Lanka introduced 'right to information' under Article 14A of the Constitution.

SUGGESTIONS FOR AN ACT OF PERSONAL DATA PROTECTION WHICH PROVIDES THE LEGAL FRAMEWORK FOR THIS FUNDAMENTAL RIGHT TO BE EXERCISED

As mentioned above the introduction of 'right to information' under the Constitution was enabled by a piece of legislation named 'Right to Information Act 2016' and, it is obvious that any right which has the Constitutional status may have the practical significance through an enabling Act. Likewise, 'Protection of Personal Data Act' can be suggested as the procedural way of formulating the processing of personal data both private companies and public authorities use. Mainly this must prohibit the unnecessary processing of collected data.

The concept, 'processing' means any operation or set of operations which is performed on personal data or on a set of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

This can be guided by Article 5 of the General Data Protection Regulation (GDPR) 2016/679[6]. It provided that principles relating to processing of personal data under six categories as mentioned below.

Personal data shall be:

a. Processed lawfully, fairly and in a transparent manner in relation to the data subject (lawfulness, fairness and transparency).

b. Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in public interest, scientific or historical research purposes or statistical purpose shall, in accordance with the Article 89(1), not be considered to be incompatible with the initial purpose (purpose limitation).

c. Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed (data minimisation).

d. Accurate and where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay (accuracy).

e. Kept in a form which permits identification of data subjects for no longer than necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with the Article 89(1), subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedom of the data subject (storage limitation).

f. Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures (integrity and confidentiality).

Furthermore, it requires the establishment of an Authority which regulate each and every entity that engages with data collecting and processing; Data Protection Authority. The main duty of the said Authority should be investigating the conformation of above mentioned rules proposed by General Data Protection

Regulation (GDPR) 2016/679. Therefore, a new designation as Data Protection Officer can be introduced to work in any private or public authority as mentioned in the Article 37, 38 and 39 of GDPR[7] with the basis of professional qualities and the knowledge of data protection laws and practice. His/her task shall consist of informing and advising the controller or the processor of any data to carry out the processing in accordance with the regulations mentioned in the above proposed Act.

CONCLUSION

The purpose of introducing a law for personal data protection should ensure the freedom of the persons related to that data. The law should facilitate possibilities that the person remains in control of their data. The owner of the data should be the one who decides with whom he needs to share their information, including who has access to it, for how long and for what purposes. The major argument based on the discussions of introducing a law for data protection is, to update law to prevent both private companies and public authorities use personal data on an unprecedented scale in order to pursue their activities.

END NOTES

1. Council Regulation (EU) 2016/679 of European Parliament and of the Council, Article 06, *Official Journal of the European Union* [Online] Available from: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679.

2. The European Parliament, the Council and the Commission (2012) Charter of Fundamental Rights of the European Union 2012/C 326/02, *Official Journal of the European Union.*

3. The EU Network of Independent Experts on Fundamental Rights presents its Report on the situation of fundamental rights in the European Union in 2004 [Online] Available from: https://ec.europa.eu/commission/presscorner/detail/en/MEMO_05_260 [Accessed: 12th February 2019].

4. See further: Vicki C. Jackson & Mark Tushnet, *Comparative constitutional law* (St. Paul: Foundation Press 2014); Michel Rosenfeld & András Sajó, *The Oxford Handbook of Comparative Constitutional Law* (Oxford: Oxford University Press 2012); Walter F Murphy & Joseph Tanenhaus, *Comparative Constitutional Law: Cases and Commentaries* (London: Macmillan 1977).

5. Article 35 of the Portugal Constitution, viewed 13th of June 2019, http://www.legislationline.org

6. Council Regulation (EU) 2016/679 of European Parliament and of the Council, Article 05, *Official Journal of the European Union* [Online] Available from: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679 [Accessed: 1st February 2019].

7. Council Regulation (EU) 2016/679 of European Parliament and of the Council, *Official Journal of the European Union* [Online] Available from: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679 [Accessed: 25th March 2019].

REFERENCES

Abeyratne, S. D. B. (2008) *Introduction to information and communication technology law*, Rajagiriya: Golden Graphics.

Boyd, D. & Crawford, K. (2012) Critical questions for big data: Provocations for a cultural, technological, and scholarly phenomenon, *Information, communication & society*, 15(5), pp: 662–679.

DOI: https://doi.org/10.1080/1369118X.2012.678878

Computer Crimes Act No 24 of 2007, Colombo: Parliament of the Democratic Socialist Republic of Sri Lanka.

Constitution of the Portuguese Republic [Online] Available from: https://www.legislationline.org/searchn2/runSearch/1/key/Portugal+Constitution/rows/10 [Accessed: 13th June 2019].

Council Regulation (EU) 2016/679 of European Parliament and of the Council, *Official Journal of the European Union* [Online] Available from: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679 [Accessed: 25th March 2019].

Council Regulation (2016) General Data Protection Regulation (GDPR) 2016/679, *Official Journal of the European Union.*

de Andrade, N. N. G. (2010) Data Protection, Privacy and Identity: Distinguishing Concepts and Articulating Rights, In *IFIP PrimeLife International Summer School on Privacy and Identity Management for Life*, pp: 90–107, Berlin, Heidelberg: Springer [Online] Available from: https://link.springer.com/chapter/10.1007/978-3-642-20769-3_8 [Accessed: 13th January 2019].

DOI: https://doi.org/10.1007/978-3-642-20769-3_8

De Hert, P. & Gutwirth, S. (2007) Privacy, data protection and law enforcement. Opacity of the individual and transparency of power, *Privacy and the Criminal Law*, In Claes, E., Duff, A. & Gutwirth, S. (eds.) *Privacy and the Criminal Law*, Antwerpen-Oxford: Intersentia, pp: 61-104 [Online] Available from: http://www.justiciarestaurativa.org/www.restorativejustice.org/articlesdb/articles/7635 [Accessed: 12th February 2019].

De Hert, P. & Gutwirth, S. (2009) Data protection in the case law of Strasbourg and Luxemburg: Constitutionalisation in

action, In *Reinventing data protection?*, pp: 3–44, Dordrecht: Springer [Online] Available from: https://link.springer.com/chapter/10.1007/978-1-4020-9498-9_1 [Accessed: 25th April 2019].

DOI: https://doi.org/10.1007/978-1-4020-9498-9_1

European Parliament & Council Directive (EU) Article 2 of Directive 95/46/EC of The European Parliament and of The Council, *Official Journal of the European Union* [Online] Available from: https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:EN:HTML [Accessed: 25th March 2019].

Flaherty, D. H. (1990) On the utility of constitutional rights to privacy and data protection, *Case Western Reserve Law Review*, 41(3), pp: 831–855 [Online] Available from: https://scholarlycommons.law.case.edu/cgi/viewcontent.cgi?article=2048&context=caselrev [Accessed: 11th March 2019].

Fuster, G. G. & Gellert, R. (2012) The fundamental right of data protection in the European Union: In search of an uncharted right, *International Review of Law, Computers & Technology*, 26(1), pp: 73–82 [Online] Available from: https://www.tandfonline.com/doi/abs/10.1080/13600869.2012.64679 [Accessed: 24th January 2019].

DOI: https://doi.org/10.1080/13600869.2012.646798

Grossman, M. (2011) *Technology Law*, India: Universal Law Publishing.

Information and Communication Technology Act No. 27 of 2003, Colombo: Parliament of the Democratic Socialist Republic of Sri Lanka.

Kokott, J. & Sobotta, C. (2013) The distinction between privacy and data protection in the jurisprudence of the CJEU and the ECtHR, *International Data Privacy Law*, 3(4), pp: 222–228.

DOI: https://doi.org/10.1093/idpl/ipt017

Lynskey, O. (2014) Deconstructing data protection: The added-value of a right to data protection in the EU legal order, *International and Comparative Law Quarterly*, 63(3), pp: 569–597. DOI: https://doi.org/10.1017/S0020589314000244

McDermott, Y. (2017) Conceptualising the right to data protection in an era of Big Data, *Big Data & Society*, 4(1), 2053951716686994.

DOI: https://doi.org/10.1177/2053951716686994

Morscher, C. (2014) Serge Gutwirth, Ronald Leenes, and Paul De Hert (Eds): Reloading data protection: multidisciplinary insights and contemporary challenges- Book Review, *International Review of Economics*, 61(4), pp: 417–421 [Online] Available from: https://link.springer.com/article/10.1007/s12232-014-0218-4#citeas [Accessed: 10th March 2019].

DOI: https://doi.org/10.1007/s12232-014-0218-4

The European Parliament, the Council and the Commission (2012) Charter of Fundamental Rights of the European Union 2012/C 326/02, *Official Journal of the European Union.*

Tzanou, M. (2017) *The Fundamental Right to Data Protection*, 1st Ed., Oxford and Portland, Oregon: Hart Publishing [Online] Available from: https://media.bloomsburyprofessional.com/rep/files/9781509901678sample.pdf [Accessed: 29th March 2019].