International Journal of Sociology and Political Science
www.sociologyjournal.in
Online ISSN: 2664-7745, Print ISSN: 2664-7737
Received: 10-05-2024, Accepted: 15-06-2024, Published: 29-06-2024
Volume 6, Issue 1, 2024, Page No. 89-94

The roots of the data protection movement: A global perspective

Bilal Ahmad Ganai
Assistant Professor, Department of Law, School of Legal Studies, Central University of Kashmir, Jammu and Kashmir, India

Abstract
This paper deals with the origins of the data protection movement that took place with the onset of computers in the world, which led to the digitization of various types of data. It explores the historical trajectories of the data protection movement, which started in some of the advanced democracies of the world.
The purpose of this article is to showcase the development of this movement across countries and how the importance of data was ultimately recognized by the legal, political, and administrative establishments of various nations. It highlights specific developments that occurred in around four countries and some international organizations and how those developments ultimately shaped the legal and administrative responses in the form of fair information principles that later came to determine the data protection and security related measures across the world.

Keywords: Informational privacy, privacy acts, data safety, OECD, fair information principles

Introduction

World has gone through many changes due to the onset of technology. Technology has given our world new directions. The impact of this computerization on our society and culture is, in many ways, very complex and far-reaching.
There are some experts who say the word "computer" is a misnomer given the fact that most computers do far more than compute. The computerization of our society has taken place at a tremendous speed.
In his book *Megatrends*, John Naisbitt [1] terms this phase of human history, where the computerization of our society is taking place at a very large speed, as the third important wave of civilization. He equates feudalism as the first wave of civilization and the emergence of industrialism as the second wave. Regarding this third wave of human civilization, he states that it has been giving rise to major societal transformations.
James N. Denziger [2], in one of his works, states that the computer package has been at the center of this third wave of human civilization. He says computer technology encompasses a complex interdependent system composed of people, which includes users, computer specialists, and managers; equipment, which includes hardware such as computer mainframes and peripherals; software, which includes operating systems and application programs; and data. The third important factor of this computer package he terms as techniques, which include procedures, practices, and organizational arrangements.
This computer package has been behind the instantaneous access to vast quantities of information from multiple and remote locations, and this access has changed the character of the modern organization and the society in which it is taking place.
One of the important transformations that we have seen in the world today because of the voracious onset of technology, is how many of our transactions and functions have turned online, given the rapid access to the internet in our day-to-day affairs. Many of our services that were previously available only in physical mode have now switched over to online platforms.
There are a number of citizen services that have become available to citizens through these online platforms. This change has facilitated many aspects of our public life, but these positive changes have also been accompanied by many negative consequences.
When it comes to the readiness of society to digest technology in the best possible way, this readiness has always been wanting, as technological changes have outpaced any considerations we can have regarding the goodness or badness of these technologies.
In the modern world, we have seen how online services have become available to citizens, enabling them to order items and shop for various necessities from the comfort of their homes. Various online platforms have created a buffet of products that citizens need.
We have also observed how citizens today can access online consultations with doctors for their needs and requirements. In fact, people can consult any doctor across the world through these online platforms.
Similarly, regarding land revenue-related facilities, we have seen a significant change. Previously, citizens had to visit various offices and stand in line to avail themselves of services. However, with the onset of online platforms, citizens can now access these services without going to the offices in person, allowing them to attend to their personal affairs simultaneously.
One of the negative fallouts of these changes that computers have brought to the fore is the challenge that computerization has posed to the privacy of individuals, or more specifically, the informational privacy of individuals. The challenges to the informational privacy of individuals have largely emerged as computers have developed an increased use in modern societies [3].
The use of computers and related phenomena has accelerated, and the world has seen significant growth of the internet over the last several decades. This growth has led to the datafication of individuals. Datafication is a phenomenon that refers to the conversion of an individual's identity into various parameters of data.

Today's system is more interested in understanding human beings from a data point of view, which means it tries to draw conclusions about individuals by analyzing their health-related data, focusing on their financial data, and scrutinizing their personal data. Thus, we have seen many proposals from various governments around the world today. In fact, some have already come to fruition. It has been proposed, and in some countries realized, that Personal Identification Numbers (PINs) are created for every citizen. This personal numerical code has come to be used for both identification and authentication.

The emergence of this arrangement has resulted in achieving the goals of efficiency in the management of the government services offered to citizens. For example, in India, the government has created a 12-digit unique identity number known as Aadhaar, which every citizen is supposed to have voluntarily to facilitate the dispersal of various services and facilities that the government offers to its citizens.

In order to ensure the smooth distribution of these unique identity numbers, the Government of India established the Unique Identification Authority of India (UIDAI) in January 2016 [4]. UIDAI is a statutory body that supervises the distribution of these UID cards, which have also come to be known as Aadhaar UID cards.

Thus, we can say that gigantic databases have come into existence, and large amounts of personal data have been fed into these databases increasing the risk of abuse and misuse of data.

Materials and Methods

In order to trace the origins of the data protection movement in the world, we will adopt a historical approach. In this approach, we will limit our case to the four important countries that have taken the lead in the development of data protection frameworks. These countries are Sweden, the United States, West Germany, and Britain. We only limited ourselves to the origins of these movements in these countries.

We can say that the four different models of data protection created in the world belong to these four important jurisdictions. We will focus on the licensing system in Sweden. We will analyze the emphasis on individual self-help and enforcement by courts in the United States of America. We will discuss the data commissioner model of West Germany, and finally, we will examine the British model, which has come to be known as the registration system.

We will analyze the important historical documents, acts, and committee reports that ultimately shaped the data protection ideas within these countries, and then we will juxtapose them with each other.

The Four Important Cases: Sweden, USA, West Germany and Britain.

The data protection movement in the world was mainly fueled by the common perception of the difficulties that countries across the globe began facing due to the emergence of technology, which left them feeling at a disadvantage in dealing with these challenges. There was no such problem they encountered earlier when computers and the internet did not exist. However, with the advent of these technologies, they suddenly started facing the risk of their data being unsafe due to the indiscriminate computerization of public affairs.

Thus, it was not only the existence of technology that forced them to confront this type of challenge. It was also the perception that the mysterious nature of computer technology posed to them, which led them to collaborate in addressing this new phenomenon.

Let us now try to chronologically and analytically explore some of the important milestone developments in the evolution of data protection-related legal measures that occurred across the world.

The Sweden Data Act, 1973

Sweden became the first country in the world wherein a Government Commission was setup in 1969 to look into the issues of data protection. It was in July, 1973 when the Swedish Data Act came into existence. Hondius has remarked that "if laws in other countries appear to be more sophisticated on certain points, is should be recognized that this would not have been possible without the Swedish prototype" [5]. Jan per Georg Haraldsson Freese played a very pivotal role in the development of this act. He was a Swedish jurist and held prominent positions in government agencies at that time. He was born on the 28th of October, 1933, in Stockholm, Sweden. He also served as the Director General of the Swedish Data Inspection Board from 1975 to 1986.

This act was important in many ways because it prepared the ground for the recognition of the importance of data safety. Its achievement was the acknowledgment of the various challenges that privacy would face, especially with the advent of computerized systems in the world. It highlighted the significance of informational privacy, which was going to be threatened by the increasing computerization of society. This act was 'preventive' in its orientation as it was mainly guided by the spirit of Jan Freese who proudly claimed that, "to me it is important to solve problems, and I prefer to do so before they occur" [6].

One important reason that led to Sweden becoming a fertile ground for data protection-related laws was the widespread computerized registration of its population. Sweden, at that point in time, was one of the most computerized countries in the world.

This act came up with an institutional control mechanism for the preservation of the informational privacy of the citizens. Concurrently with this act, a Data Inspection Board (DIB) was established and this board was authorized to oversee the safety of the personal data of citizens. Any recording of the personal data was only allowed if permitted by the DIB.

This act had a very strong impact on data protection laws worldwide. This strong impact of this act was largely due to Jan Freese, who was the chairman of the Data Inspection Board from 1974 until 1986. He made significant efforts to publicize the Data Act across the globe.

American Privacy Act, 1975

The United States of America formed a Commission for the study of data protection related issues in February, 1972 and finally the American Privacy Act was legislated in January, 1975. The American idea of privacy was mainly summed up by Samuel Warren and Louis Brandeis's million-dollar idea of "the right to be l *et al* one" [7]. The technologically empowered record-keeping systems had started ringing alarm bells in American society in the same way as they had done in America.

Senator Sam J. Ervin played a very important role in the development of this law in America. His role as Chairman of the Senate Judiciary's Sub-Committee on Constitutional Rights from 1970 to 1974 was of huge importance which ultimately fed into the vibrancy of the American Privacy Act, 1975. Senator Sam J. Ervin submitted the report in 1974 titled *Federal Data Banks and Constitutional Rights*. In this report Ervin specifically focused on the databanks in America which 'were littered with diverse information on just about every citizen in the country' [8].

As against the Swedish Privacy Act, American Privacy Act had a deep orientation of voluntary compliance and self-help. It had a deep imprint of individual agency. Senator Sam J. Ervin had tone down his insistence on a regulatory institutional arrangement for the protection of data. It laid down a more decentralized arrangement for the implementation of the privacy act.

West German Data Protection Act, 1977

It was in September, 1973 that a government commission was instituted to look into the issues of data protection in West Germany and the West German Data Protection Act was finally passed in January, 1977. Again the establishment of databanks and as well as the assignment of unique PINs to citizens for various administrative purposes was the drive which led to the emergence of concensus regarding data protection in West Germany. The free development of one's personality emerged as a chief constitutional value and the recognition of 'untouchable sphere of private life withdrawn from the influence of state power,' was given a special importance by the constitutional courts in West Germany [9].

Spiros Simitis was a prominent Greek-German jurist and legal scholar, and he played a significant role in the development of data protection law in West Germany. He was born on October 19, 1934, in Greece, but later became a German citizen. His name is associated with the world-famous leading figures in the development of modern data protection law in Europe.

He served as the data protection commissioner from 1971 in West Germany under the Hessian Data protection act and became one of the most respected and effective advocates for data protection in the world.

The German method of data protection surrounds around the institution of Data Protection Commissionership. The modal represented a rejection of the self-control model of implementation in favour of an institutional approach in the form of a complex and unusual agency [10].

British Data Protection Act, 1984

In the United Kingdom, a government commission to study the data protection related issues was instituted in 1970 and it took around 170 months for the UK government to give a formal shape to these deliberations and decisions in July, 1984.

Britishers settled with the system of registration as compared with the others options that were available. In Britain, interestingly, various periods of time every time of policy instrument were advocated in one way or the other. The idea of Data Registrar was mooted who was supposed to oversee the formulation of the public register of databanks to be located in the Home Office and ensure that registered data users would comply with data protection principles. It was this policy instrument that eventually found its way into the 1984 Data Protection Act [11].

The act of registration entails a commitment to processing personal data according to the data protection principles. Registration differs from licensing method only in the sense that the control agency would have no authority to block the creation of an information system.

The Hybridicity of Data Protection Models

But in practice, we see that the various ways of managing data and ensuring its protection at the ground level have important points that we need to take care of. There is a lot of hybridicity in these policy instruments, meaning that one way of data protection has the accompanying features of other methods of data protection. At the ground level, it is this hybrid nature of these methods of data protection that becomes important.

The fact remains that every policy instrument has a dominant approach to data protection to ensure the safety of the data. As far as the other accompanying, if we can use the word, 'alien' features from the other methods of data protection are concerned, they are only secondary to the dominant and unique approach of a model.

As we have discussed in the above paragraphs, Sweden licenses data protection, the United States relies on individual self-help and the courts, West Germany's policy operates through a data commissioner, and the British policy is implemented through a registration system.

Data Protection Movement: Some Core Convergent Principles.

So, from these four important models of data protection from four different countries, we can safely distill some core important fair information principles which characterized the data protection movement across the world. These principles were present in every case, although every case or model was different from every other model. The data protection movement from Sweden to America, from America to Germany, and from Germany to Britain originated within different contexts but still carries certain common characteristic features. These features later played very important roles in relation to data protection and data governance measures worldwide. Let's examine these principles one by one:

The Principle of Openness

The principle of openness means that, regarding record keeping, data collection, and the existence of any registers for storing data about various aspects of the people, everything should be open to public view. There should be no mystification of data. In fact, the data should be public.

We should arrange this data in such a way that it is accessible and known to the general public. All the models we have analyzed above emphasize this characteristic feature of openness and publicity concerning the collection and storage of data. No data or information should be hidden from the public eye.

The Principle of Individual Access and Correction

The principle of individual access and correction is another common feature present in all the models we have observed above. According to this principle, every human being, or data subject, should retain the right to access the information collected about them. They should be able to verify the authenticity of that information, which has been collected and stored by various data-collecting agencies. If

the need arises, they should also be able to correct that information.

This means that all the information and data collected about individuals should be arranged in such a way that it is accurate and complete. To ensure this completeness and accuracy, the data must be open, accessible, and rectifiable by the data subjects.

The Principle of Collection Limitation

Another important principle that has accompanied the data protection movement in the world is the principle of collection limitation. According to this principle, we are supposed to collect data not only through lawful and fair means, but there are also important considerations that we should take into account to limit the collection of personal data.

This means that after ensuring the consent of the data subjects, our focus should also be on limiting the collection of personal data. This principle emphasizes the need to check or discourage the indiscriminate collection of information about data subjects, which may be misused if it falls into the wrong hands or is used for inappropriate purposes.

The Principle of Use Limitation

The principle of use limitation has also been one of the important principles at the heart of the data protection movement. As far as this principle is concerned, it states that once any information is collected about the data subjects, we should put some limits on its use. We should specify the limits for the uses for which we can utilize it.

If we delve into this principle and try to unpack it, we see that the idea of relevance is at the very core of this principle. It asserts that if the information has been collected for a particular purpose and that purpose has been made clear at the time of data collection, we cannot use that data for any other purpose that we have not disclosed to the individuals from whom we collected this data. Therefore, information collected for one purpose cannot be used for any other unrelated purpose.

The Principle of Disclosure Limitation

The principle of disclosure limitation is, in many ways, limited and predicated upon the principle of use limitation. The principle of disclosure limitation states that any information collected from data subjects or individuals shall not be communicated externally to any other platform or agency unless we seek the consent of those individuals or any other authority established for this purpose.

This principle of disclosure limitation is another important principle that has been present in all the models and frameworks we have encountered regarding data protection measures. In fact, the case of Cambridge Analytica was one of the gross violations of this principle of disclosure limitation [12].

Cambridge Analytica was a controversial British political consulting firm, linked to the Facebook–Cambridge Analytica data scandal, which harvested personal data from millions of Facebook profiles without consent to build psychographic profiles for targeted political advertising, impacting elections like the 2016 US Presidential race and Brexit, before ceasing operations in 2018.

Security Safeguards Principle

The security safeguards principle is the final principle that we discussed with regard to the data protection movement. According to this principle, any information or personal data should be protected by reasonable security safeguards against risks such as loss, unauthorized access, destruction, use, modification, or disclosure of data [13]. As far as this security safeguards principle is concerned, we can see a direct reference to it in the Organization for Economic Cooperation & Development guidelines regarding data protection, an intergovernmental economic organization with 38 member countries (mostly democracies with market economies) that works to stimulate economic progress.

In his research, Colin J. Bennett has discussed that the convergence or similarization of data protection-related measures across these four important countries can be understood from multiple angles. To comprehend how this process of similarization regarding data protection measures was achieved, he lists some important factors that, according to him, have played a significant role in this process.

The first important factor that has persuaded these countries to adopt similar data protection measures is technological determinism. According to this deterministic factor, all these countries were compelled to implement these types of measures due to the uniformities that technology has created in otherwise diverse political, cultural, and economic contexts. Consequently, these countries were confronted with a common factor in the form of technology, which led to the increasing computerization of their political, social, and economic lives which in turn gave rise to many accompanying problems [14].

Another important factor is the process of lesson drawing, in which policy measures from one country were adopted by another. In this process, countries learned from each other various measures and frameworks that they created or utilized to address the challenges posed by technology. As we know, no country is self-sufficient when it comes to the challenges that the then emerging world presented. Thus, compelled by circumstances, countries seemed eager to benefit from each other's experiences, ultimately leading to the similarization of various techniques and models vis a vis data protection governance across the world.

Another significant factor in the data protection movement is the crucial role that internationally recognized policy experts played in shaping data protection measures. According to this idea, some well-known international experts took the lead as policymakers in various countries, working closely or collaboratively on these issues, which contributed to the similarization of data protection-related measures in these countries. For example: Spiros Simitis from Germany, Jan Freese from Sweden, Louis Joinet from France, Michael Kirby from Australia, Hans Peter Gassmann associated from OECD, Frits Hondius from Council of Europe, and Stefano Rodota from Italy were at the forefront of this process of data protection movement. They had also developed a network which enabled them to debate and discuss the relevant issues with each other.

Furthermore, the role of international organizations in formulating various data protection-related laws worldwide had also been significant in encouraging countries to align themselves with data protection frameworks. Among these organizations, the Council of Europe, established in 1949, and the Organization for Economic Cooperation and

Development established in 1961 are two important entities that have greatly contributed to the concretization and solidification of data protection measures globally. A brief discussion of the contribution of these organizations will not be out of place here.

The Council of Europe

The Council of Europe was a platform for increasing collaboration among various countries in Europe. This platform became an ideal place for discussing the various problems these countries faced, and the protection of data became one of the important focuses of analysis. Accordingly, this platform started discussing the impact of technology on society from the 1960s onwards.

This organization undertook various studies to dissect the problems that technology has created for the rights of human beings. The Council of Europe formed various groups of experts who tried to navigate the issues that technology had given rise to. The work of these experts under the banner of the Council of Europe found expression in two resolutions passed by the Council. The Council of Europe advised its member countries to incorporate these resolutions into their domestic laws.

The first of these resolutions addressed how the information collected by private sector data banks should be accurate, up-to-date, and relevant. This resolution also specified that these data banks should use the data only for the purpose for which it was collected. The resolutions emphasized the electronic security systems that these platforms should have to ensure their safety.

Subsequent resolutions of the Council of Europe further broadened awareness regarding data protection measures and the application of these principles not only to private sector enterprises but also to public sector [15]. In this way, the Council of Europe played a critical role in raising awareness about fair information principles worldwide. These are some of the initial and important measures that resulted from the Council of Europe, ultimately helping to shape future measures regarding data protection.

The Organization for Economic Cooperation and Development (OECD)

The Organization for Economic Cooperation and Development (OECD) played an important role by showing its early interest in the impact of technology on society and the resulting data communications related problems. This organization recognized the increasing importance of data as an essential commodity with the potential to be traded among various European countries. Accordingly, the OECD established various groups, for example, the Group on Computer Utilization, to investigate the interface that exists between emerging technology and the related economic and legal questions.

There was a significant symposium in 1977 titled "Trans-border Data Flows and the Processing and Protection of Privacy," held in Vienna, where important issues regarding this phenomenon were discussed. In the backdrop of this symposium, a group of government experts under the banner of the OECD began their work in 1978 on draft guidelines for the protection of privacy in the trans-border flow of personal data. The agreement on these guidelines was reached in 1979, and the recommendation in the form of these guidelines was adopted in September 1980. These guidelines, also known as OECD guidelines, constituted a parallel effort to that of the Council of Europe towards the harmonization of privacy protection rights and requirements.

Thus, we can say the OECD forum provided a much-needed opportunity for Europeans and Americans to focus their attention on safeguarding human rights after the emergence of computers [16]. Later on, the OECD guidelines, along with other international arrangements, became the main catalysts for preparing other countries to develop legislative, administrative, and political measures for designing various data protection-related laws. Governments across the world later developed a realization about the problems that computers posed to human rights, which ultimately led them to adhere to the lines of these international guidelines regarding data protection.

Conclusion

The present data protection-related awareness has a long history, although not that long. The fact remains that from the 1950s onwards, and even before that, we have seen how various countries have risen to these concerns. The emergence of computers and the process of computerization brought significant changes to the political, economic, legal, and administrative landscapes.

Every country, in its own way, tried to grapple with these challenges by contextualizing the responses within their unique constitutional, ideological, and administrative structures. At the same time, the equivalence of the challenges that technology posed to all the countries and societies, irrespective of their cultures and political structures, convinced them to respond to these challenges in a uniform manner. They pooled their intellectual, legal, and political resources to confront the challenges that technology had presented.

They learned from each other in developing various tools and techniques for dealing with the challenges of data protection and computerization, which some even believed had given rise to "*the naked society*," by emulating the responses from one another [17]. The role of experts in various countries and organizations, who took these challenges by the horns and did not shy away from learning from each other at the world level also bolstered the responses in a vibrant manner.

It is against this backdrop of initial measures and primordial frames that we should analyze modern-day data protection measures and data governance regimes.

References

1. Naisbitt, John. Megatrends, New York: Warner Books, 1982.
2. N James, *et al*., Computers and Politics: High Technology in American Local Governments. Columbia University Press, 1982.
3. Kumar, Anil. “Economic Development in India: A Response to the Information Technology (IT) Revolution,” ECONSPEAK: A Journal of Advances in Management, IT and Social Sciences,2011:1(1):105-109.
4. Unique Identification Authority of India (UIDAI). https://uidai.gov.in/en/my-aadhaar/about-your-aadhaar/aadhaar-enrolment.html.
5. Hondius, Frits. “Data Legislation on the March,” Information Privacy, 1978.

6. Freese, Jan. “Preserving the Open Flow of Information across Borders,” in OECD, Transborder Data Flows and the Protection of Privacy, Proceedings of a Symposium held in Vienna, 1977, 20-23.
7. Warren and Brandeis, the Right of Privacy, Harvard Law Review, 1890.
8. U.S. Senate, Federal Data Banks and Constitutional Rights, Report Submitted in, 1974.
9. Riccardi J Lee. ‘The German Federal Data Protection Act of 1977: Protecting the Right of Privacy?’ Boston College International and Comparative Law Review, 1983.
10. Bennet, Colin J. Regulating Privacy Data Protection and Public Policy in the Europe and the United States. Cornell University Press, 1992.
11. Bennet, Colin J. Regulating Privacy Data Protection and Public Policy in the Europe and the United States. Cornell University Press, 1992.
12. Boerboom, Carissa. “Cambridge Analytica: The Scandal on Data Privacy”. Augustana Center for the Study of Ethics Essay Contest, 2020. https://digitalcommons.augustana.edu/ethicscontest/18
13. OECD, Guidelines on the Protection of Privacy & Trans-border Flows of Personal Data, 1981.
14. Kumar, Anil. “Social Thinking to Scientific Social Theory: An Introduction to Sociology and Social Anthropology,” International Journal of Research in Sociology and Social Anthropology,2013:1(1):1-5.
15. Council of Europe, Resolution (73) 22 and Resolution (74) 29.
16. Bennett, Colin J. Regulating Privacy Data Protection and Public Policy in the Europe and the United States. Cornell University Press, 1992.
17. Packard, Vance. The Naked Society, New York: Pocket Books, 1964.