IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

RIGHT TO PRIVACY IN THE CONTEXT OF APPLICATION SOFTWARE (APPS) IN INTERNATIONAL LAW

K. M. FIROZ

Advocate, High Court of Kerala
Kochi, India

Abstract: The privacy right seeks to protect a person's private as well as his family affairs and confidentiality. In the case of Application Software [Apps], privacy rights shield the secrecy of communication and other emerging rights taking within its ambit the use of personal information and data in the process. The data protection rights jealously guard the rights of individuals in the matter of personal data processing. Normally emerging data protection rights do not apply if the subject matter dealt with is not personal. It clearly, deals with an area narrower than privacy rights. It is confined only to individual rights. We find a dearth of effective deliberations in International law about Application Software. No effective steps are taken to improve international privacy rights in this ever-widening area. The right to privacy visualised in Article 12 of the *Universal Declaration of Human Rights* as well as Article 17 of the *International Covenant on Civil and Political Rights* do not address such emerging issues adequately. Regrettably, the norms of International Laws in this respect appear to have failed to address the development in the area, particularly in respect of Application Software. Existing laws in different countries encompass only regional privacy issues giving scant attention to emerging international issues, especially in the case of enforcement of rights. The International Application Software developers, breach privacy laws with impunity. No control mechanism has evolved to mitigate the situation. This study highlights some salient features of privacy rights and seeks remedial measures.

Key Words: Privacy -Application Software - International Law

I. INTRODUCTION

Currently, there is software application for everything on earth. This has changed the ways of the world in a big way. No wonder, one can access the whole world in a few taps. As everybody knows, hardware is the physical component of computer. Software of computers operates in two different ways. One is system software which governs the way of computer hardware functioning, for instance operating system. Application software, on the other hand, is a set of rules that are framed by users for accomplishing specific tasks. A few years ago, computers functioning in mobile devises started outselling normal computers. Software Applications are part of normal life. As its use continues to expand, privacy right violations are rampant.[1]

[1] Robert V. Hale II, "*Recent Developments in Mobile Privacy Law and Regulation*" the Business Lawyer, Vol.69.

In the explosive digital age, it is not practical to precisely define privacy.[2] Increase in online activities as well as artificial intelligence has raised the recognition of importance of privacy as well as data protection. Privacy rights may safeguard personal dignity.[3] Even though privacy rights and data protection rights appear to be similar, they deal with different activities. The Right to privacy is wider than the concept of data protection.[4] Such rights even extend to interception of communication, relating to family, sexual preferences, religious, political etc.[5] In the circumstances, it is essential to provide legal guarantee for personal dignity. The emerging situation encompasses every aspect of individual life as well as personal data processing by private persons or agencies or Governments. It can be seen that privacy is the genus. Protection of data is its species.[6] For instance privacy right is the right that protects confidentiality of a communication even if it does not include any personal data or information. But data protection right will apply to processing of personal data of an individual. Therefore normally data protection rights will not apply if data is not personal in character. However, new trends are developing by which the scope of personal data rights is expanded and the protection is extended to data that has become public. Even if it is not confidential, still they need to be protected, if the same comes under the scope of personal data. Obviously, it is a personal privacy right against misuse or unauthorised use of personal data. It intends to protect the privacy of individual at the risk for collection of personal data misuse. In a broad perspective, personal data means data relating to identification of living persons. It includes data provided actively by individuals themselves, data collected by the software application providers through tracking technologies, metadata, inferred and derived data by software application providers, combination of known personal data which may lead to identifying individuals, sensitive data regarding personal status etc.

Few jurisdictions, as in the case of Russia Federation, Saudi Arabia, European Union etc. are very strict regarding transferring of personal data outside their territory. Such jurisdictions permit processing of personal data in their territories alone unless there are effective safeguards and undertaking from the third country to which the data is purported to be transferred to the effect that they will provide effective protection in relation to such rights.[7]

Confidentiality agreements become relevant in the circumstances. This is more so when software application developers outsource various functions to third parties. A non-disclosure agreement (NDA) is a common method adopted to protect data. But normally it is confined to protection of information revealed during development of Software Applications. The primary method for addressing the right of privacy of software application users is by framing and accepting privacy policy. Privacy policies will govern the right of end users regarding privacy as well as data. It will have to be accepted at the threshold of the use of the software application. It should be clear and transparent. There should be international norms and guidelines which would make terms of Privacy Policy clear, transparent and fair. End-user license agreements will also cover some issues concerning privacy and data protection. The invasion of privacy as well as personal data in relation to application software is a serious concern in international law.

Privacy Rights and International Conventions

United Nations Declaration of Human Rights (UDHR), 1948[8] is apprehensive against possible arbitrary interferences with privacy.[9] Article 12 of the Declaration declares that nobody should be

[2] Nuala O' Connor and Aletha Lange, '*Privacy in the Digital Age'*, Great Decisions, 2015, JSTOR, Foreign Policy Association Page 17-28

[3] As recognised by nine member Constitution Bench of the Hon'ble Supreme Court of India in *Justice K.S. Puttaswamy and Another. vs. Union of India and Others 2017 (10) SCC 1.*

[4] Dimitra Kamarinou, "*A Guide To Data Protection In Mobile Applications" , World Intellectual Property Organisation, 2021*

[5] *Supra note 3*

[6] *Supra note 4*

[7] Habeas data is a kind of action which could be taken before the courts of law to gain protection of individual data and privacy. It gives the aggrieved to raise grievance before the judicial system to restrain the misuse of personal data. It operates as an access right into personal information within the territory of personal data.

[8] India is a signatory

[9] Article 12

interfered arbitrarily with a person's correspondence, his home or his family affairs. It further declares that there should not be attacks on once reputation as well as honour. It asserts that everybody will have the right to be protected by law against privacy interference and attacks.

The European Convention on Human Rights[10] deals with privacy aspects in its Article 8. It states that everybody will have the right to respect for his private as well as family life, his correspondence as well as his home. Article 8(2) further declares that there shall not be interference from the part of a public authority with the exercise of that right save except as per the law. Such interference by law can only be to the limit admissible in a democratic society in the interest of national security, economic well being, safety of public, for the prevention of disorder as well as crime, for protection of freedoms rights of others, morality, health etc.

Similar protection is offered by the *International Covenant on Civil and Political Rights (ICCPR), 1966.*[11] Article 17 of that International Covenant declares that nobody should be put to unlawful and arbitrary interference with his/her privacy. His/ her home, family or correspondence shall not be subjected to such illegal interference. It further declares that there should not be illegal attacks on honour as well as reputation. It assures that everyone will have the right to be protected by law against such attacks as well as interferences.

Article 16 of the *Convention on Rights of Child* gives emphasis to the privacy of children. It declares that a child shall not be put to unlawful as well as arbitrary privacy interference. It states that home, family or correspondence of the child shall not be arbitrarily interfered and child's reputation and honour shall not be attacked unlawfully. It guarantees that every child will have the right to law's protection against all such interferences and attacks.

International Convention on the Protection of the Rights of All Migrant Workers and Members of their Families in its Article 14 declares that migrant worker or member of his family shall not be interfered arbitrarily with her privacy. The *American Convention on Human Rights* in its Article 11 protects right to privacy.

The aforesaid declarations, covenants and conventions make it clear that right to privacy is not an absolute one.[12] The Government can interfere with the privacy for various reasons including safety of public, security of nation etc. Furthermore, privacy rights will rarely override higher rights regarding life, health etc. of others. However it is regrettable indeed that those international declarations and covenants are not sufficient enough to cover new digital developments including application software.

National legislations with International ramifications

About 137 nations have enacted or implemented national legislations in their respective jurisdictions to safeguard the protection of privacy as well as protection of personal data. It is gratifying to note that legislations empower and authorize various authorities in those nations to investigate data protection violations and to impose punishments and compensations, if so necessary. On an analysis of various laws enacted by various nations, it is evident that the international privacy laws regarding data protection will continue to evolve ensuring personal data protection.

Some laws so enacted have international ramifications and their attempt to rigorously protect citizens from international privacy attacks or misuse. Such legislations have extra territorial operations that are effective in a broad sense such laws apply not only within the territorial limits but they govern international activities targeting misuse, if any. These laws in this new area are evolving and developing gradually. They are governed by five globally accepted privacy principles namely:

[10] Came into force on 3-9-1953.

[11] India is a signatory

[12] *Anjum Ansari*, "*International Perspective of Right To Privacy*" , DPU, Dr.D.Y.Patil Unitech Society, Pune, 2022

1. Advising and giving notice to users to protect personal information.
2. Providing choices and consent regarding use, storage, management and collection of personal data
3. Ensuring use of data by proper and correct people with proper security protocol
4. Ensuring prohibition of unauthorized access
5. Regulating enforcement compliance

General Data Protection Regulation (GDPR)

The *European Convention on Human Rights* recognised right to privacy and ensures its enforcement since 1950. When the technology progressed, the European Union realised the necessity for innovative protections regarding privacy rights and moved forward for a comprehensive approach. Accordingly, *General Data Protection Regulation* was passed through European Parliament. From 25th May 2018 the said Regulation was implemented in European Union and thereafter data controllers in relation to European Union have to be GDPR compliant. The Regulation had effective impact on international privacy law regarding data protection since the same affected every organisation or person who processed personal data inclusive of biometrics from citizens of any European Union organisation. The said Regulation had considered modern trends and had set various standards leading to protection on right of privacy and data usage outside territory. Moreover many countries including Peoples Republic of China, Japan, Brassil, Kinea, Nigeria etc. seems to have drafted their national data protection legislation in tune with the basic principles of GDPR.

The various privacy rights of data subjects as per GDPR are the following:

- Right to be informed
- Right to access
- Right to rectify
- Right to erase
- Right to restrict processing
- Right to portability of data
- Right to object
- Right regarding profiling automated decision making

As per Article 6 of GDPR, processing of data is considered to be legal in two cases. First one is when it is found necessary for the performance of a contract, for compliance with legal obligation and also for the purposes of legitimate interests etc. Other one is when the user provides consent for processing of his or her personal data for one or more specific purposes. Such consent is usually referred to as secondary consent. The consent for storing data is necessary for fulfilling other contractual requirements as well as legal obligations.

It is pertinent to note that Data Protection, Privacy, and Electronic Communications (DPPEC) Regulations of 2019 altered the DPA 2018 with the GDPR. The UK-specific data protection system that applies to the UK is introduced which is known as the UK GDPR. Even though the rights as well as fundamental principles remain unaffected, the UK GDPR departs from the EU GDPR in some key areas. For instance, there are deviations regarding provisions pertaining to exemptions for certain public authorities, provisions regarding appointments of data protection officers, data breach notification requirements etc. Cross-border data transfers are controlled by the said provisions and they have international impacts.

India's *Digital Personal Data Protection Act, 2023* (DPDPA)

India's *Digital Personal Data Protection Act*, 2023 is more flexible when compared to GDPR. GDPR also applies to offline data. Cross-border data transfers to areas and jurisdictions outside India are not prohibited by DPDPA, 2023. The Act applies to processing of digital personal data even outside the territories of India, provided that such processing should be in connection with activities connected

to offering of services or goods to Data Principals within territories within India.[13] However, transfer of personal data outside India can be restricted by the Central Government of India by issuing a notification. Therefore such transfers are not permissible to jurisdictions expressly identified by Government of India[14]. The DPDPA does not necessitate implementation of transfer mechanism. The DPDA on the other hand makes it clear that said provision in the Act shall not restrict the applicability of any law in force in territory of India which afford a higher degree of restriction or protection upon transfer of any personal data by a fiduciary of data outside India in relation to any data fiduciary or personal data or classes thereof.[15] The Act further exempts personal data[16] of Data Principals which are not within Indian Territory which are processed based on any contract entered with any person beyond Indian Territory by any person based in India.[17]

Legislations in other nations and their international impacts.

Regulations of other nations are also being constantly changed in accordance with and adapting to varying trends as well as International best practices.

Even though the United States of America had not introduced formal laws on data protection at Federal level, federal legislations were introduced to protect data on a general level. Several states in the US had enacted data protection legislations. The *California Consumer Privacy Act*[18] (CCPA) as amended by the *California Privacy Rights Act*[19] give sufficient protection to privacy and better control over personal information. The said Act permits the individuals to establish how their personal data is collected and for what purpose they are being used for. Recently, many other States in the US have also come forward with similar legislations such as the *Colarado Privacy Act* [20], the *Connecticut Personal Data Privacy and Online Monitoring Act*[21], the *Delaware Personal Data Privacy Act*[22], the *Indiana Consumer Data Protection Act*[23], the *Lowa Consumer Data Protection Act*[24], the *Montana Consumer Data Privacy Act*[25], the *Oregon Consumer Privacy Act*[26], the *Tennessee Information Protection Act*[27], the *Texas Data Privacy and Security Act*[28], the *Utah Consumer Privacy Act*[29], the *Virginia Consumer Data Protection Act*[30].

The South Africa had enacted the Protection of Personal Information Act (POPIA) with meticulous personal data protection controls. These laws have gone through a series of changes according to changing trends and times.

The State of Brazil had implemented *General Data Protection Law* (*Lei Geral de Proteção de Dados)* (LGPD) supplementing various data privacy laws that had been in force in that country. The aforesaid law in the Brazil reduces the conflicts between the different laws prevailing there. The law insists on personal data protection, regardless of where the data processor is located. These laws prescribe for data protection officers with sufficient security measures for ensuring compliances.

---

[13] Section 3(b) of the DPDPA, 2023
[14] Section 16(1) of the DPDPA, 2023.
[15] Section 16(2) of the DPDPA, 2023.
[16] Exempts from Chapter II except Section 8(1) and (5) and Chapter III as well as section 16 of DPDPA
[17] Section 17 of the DPDPA, 2023.
[18] *Effective from 1st January, 2020.*
[19] *Effective from 1st January, 2023.*
[20] *Effective from 1st July 2023*
[21] *Effective from 1st July 2023*
[22] *Effective from 1st January, 2025*
[23] *Effective from 1st January, 2026*
[24] *Effective from 1st January, 2025*
[25] *Effective from 1st October, 2024*
[26] *Effective from 1st July 2024*
[27] *Effective from 1st July 2025*
[28] *Effective from 1st July 2024*
[29] *Effective from 1st December, 2023*
[30] *Effective from 1st January, 2023*

Canada has enacted its *Personal Information Protection and Electronic Documents Act* (PIPEDA) protecting consumers regarding their personal information. It upholds the five global privacy principles. The Digital Charter Implementation Act (DCIA) was also introduced on 17-12-2020 intending to control protection of personal information and deal with various issues regarding disclosure of information during the course of commercial activities. Bahrain is one among the nations which had initially introduced a Data Protection Law in the Middle East. The law protects the rights of Bahrain citizens beyond its territory. The Philippines had enacted its *Data Privacy Act* in the year 2012. The said Act ensures the protection of personal information by organizations.

Other countries such as Denmark, Australia, Finland, Angola, Nigeria, Israel, British Virgin Islands etc have also introduced and implemented privacy laws for data protection. All such laws and legislations have definite impact on Cross-border data transfers and they have definite international impact and dimensions.

Need for International consensus

Regulations enacted by various countries and unions all over the world are being changed constantly and consistently to adapt to changing global advancements in technologies. In making regulations, some nations are stricter than others. Each regulation has different methods and mechanisms when it comes to the field of operation with consent.

There is wide concern internationally regarding the sharing as well as use of various personal information to outside parties beyond the territory of various countries. Unlike other laws, data protection laws and privacy laws especially concerning software applications have very huge impact internationally since they have extra-territorial consequences.

A software application developer or provider cannot rely on the privacy and data protection law of a single nation for framing the privacy policies, user agreements etc. Therefore a common and well accepted international data protection law regarding fair and transparent processing is indispensible and essential due to the increased use of mobile applications all over the world. A common guideline regarding legal ground to process data and the norms for obtaining consent of individuals has to be framed and approved internationally.

The guidelines should contain various norms and declarations internationally accepted regarding fairness considering individuals reasonable expectations without unfair discrimination and bias. Further, guidelines should contain effective provisions for transparency providing processing information to individuals in accessible, understandable and clear manner. Such a common and accepted declaration of international regulations is required since such declarations and guidelines will protect valuable personal data from loss and leaks. The common international guidelines will increase trust, credibility as well as confidence in users. It will result in highly developed and improved transformation as well as innovations.[31]

Common and generally accepted principles or guidelines is inevitable since the software application providers as well as developers will be able to frame the privacy policies and terms based on common principles applicable and accepted in majority of the countries. Therefore, if an international treaty or covenant could be framed and signed internationally it will support and help software application providers also to know the well accepted common principles in majority of nations and they can frame their affairs and norms according to those internationally accepted guidelines rather than searching for the different norms applicable in different territories. If an international guideline is not framed, the software application providers will have to consider and frame their policies based on the data protection and privacy law of respective countries wherein the provider is operating from as well as the laws of the nations were the individual users of the software application are located. The conflicting national laws will be an impediment for effective software application development.

[31] Beyond GDPR; Data Protection Around The World, Thales Headquarters

Conclusions

A flexible international guideline which aligns with changing global requirements is inevitable in light of the apprehensions stated in the preceding paragraphs. Rigid international common guidelines are not practical, feasible or workable. The international guidelines will certainly cause rigidity and they will not be effective in the light of regional variations. It is an undeniable fact that privacy concerns are variable and sensitivity will be different from region to region. Moreover, data-collecting software and applications are drastically changing and improving day by day. So the prevailing international guidelines may not be able to suit changing trends and evolving needs. The rigid international guidelines will only open up several hurdles on the way which will not be able to be filled up easily and effectively. The guidelines should insist that in addition to providing a general privacy policy before a software application is put to use, the software application developers should also provide "special notices" that would alert users in advance to unrelated data practices or functions involving sensitive information granting opportunity to the users to correct or prevent the misuse, if any.

For framing an international guideline or common norms, it is essential to conduct an international privacy or data protection impact assessment (DPIA) expeditiously. An International DPIA will lead to understanding the international processing operations and identifying associated harms and potential sources of risk internationally. It can also assess the steps which could be taken to prevent and mitigate the damage which is likely to be caused from an international perspective. The guidelines regarding the obligations of the controller, as well as the processor to keep records of processing activities will have to be framed by international consensus. For that purpose, a data protection impact assessment regarding the maintenance of records will also have to be conducted with an international perspective. It is also essential to evolve a body or authority internationally to monitor and implement the various international norms and guidelines which will be framed as agreed between the signatory nations. Such an international authority should be given powers by consensus to implement the various norms and guidelines through the implementing agencies and authorities in the signatory nations. General modal forms to be adopted by the software application providers, which are accepted and agreed upon internationally and framed in a transparent and fair manner, will have to be prescribed for privacy policies as well as user agreements based on consensus between the signatory nations.

The implementation of data protection internationally by design and by default can be cast on controllers by consensus. Even though it is impossible to prescribe the exact format or guidelines in which the privacy policies have to be framed or agreement has to be drafted or terms of fairness and transparency has to be prescribed, a broad guideline can be framed through consensus internationally. Such guidelines can be implemented by signing treaties, covenants etc. Therefore, it is essential to enter into an international treaty or covenant with the consensus of various nations across the world. It remains a stark reality that a data protection user will not be able to get speedy and efficacious relief or remedy in case of a breach of the privacy policy or user agreement by a software application provider in another country, in the absence of an effective common implementation mechanism at international level. The norms of International Laws have failed to address these important aspects. An effective mechanism has to be evolved to mitigate the situation.