# INTERNATIONAL JOURNAL FOR LEGAL RESEARCH AND ANALYSIS

Open Access, Refereed Journal Multi Disciplinary
Peer Reviewed

www.ijlra.com

**ISSN: 2582-6433**

# DISCLAIMER

ISSN: 2582-6433

# ABOUT US

The *International Journal for Legal Research & Analysis (IJLRA)* (ISSN: 2582-6433) is a peer-reviewed, academic, online journal published on a monthly basis. The journal aims to provide a comprehensive and interactive platform for the publication of original and high-quality legal research.

IJLRA publishes Short Articles, Long Articles, Research Papers, Case Comments, Book Reviews, Essays, and interdisciplinary studies in the field of law and allied disciplines. The journal seeks to promote critical analysis and informed discourse on contemporary legal, social, and policy issues.

The primary objective of IJLRA is to enhance academic engagement and scholarly dialogue among law students, researchers, academicians, legal professionals, and members of the Bar and Bench. The journal endeavours to establish itself as a credible and widely cited academic publication through the publication of original, well-researched, and analytically sound contributions.

IJLRA welcomes submissions from all branches of law, provided the work is original, unpublished, and submitted in accordance with the prescribed submission guidelines. All manuscripts are subject to a rigorous peer-review process to ensure academic quality, originality, and relevance.

Through its publications, the *International Journal for Legal Research & Analysis* aspires to contribute meaningfully to legal scholarship and the development of law as an instrument of justice and social progress.

ISSN: 2582-6433

# *PUBLICATION ETHICS, COPYRIGHT & AUTHOR RESPONSIBILITY STATEMENT*

The *International Journal for Legal Research and Analysis (IJLRA)* is committed to upholding the highest standards of publication ethics and academic integrity. All manuscripts submitted to the journal must be original, unpublished, and free from plagiarism, data fabrication, falsification, or any form of unethical research or publication practice. Authors are solely responsible for the accuracy, originality, legality, and ethical compliance of their work and must ensure that all sources are properly cited and that necessary permissions for any third-party copyrighted material have been duly obtained prior to submission. Copyright in all published articles vests with IJLRA, unless otherwise expressly stated, and authors grant the journal the irrevocable right to publish, reproduce, distribute, and archive their work in print and electronic formats. The views and opinions expressed in the articles are those of the authors alone and do not reflect the views of the Editors, Editorial Board, Reviewers, or Publisher. IJLRA shall not be liable for any loss, damage, claim, or legal consequence arising from the use, reliance upon, or interpretation of the content published. By submitting a manuscript, the author(s) agree to fully indemnify and hold harmless the journal, its Editor-in-Chief, Editors, Editorial Board, Reviewers, Advisors, Publisher, and Management against any claims, liabilities, or legal proceedings arising out of plagiarism, copyright infringement, defamation, breach of confidentiality, or violation of third-party rights. The journal reserves the absolute right to reject, withdraw, retract, or remove any manuscript or published article in case of ethical or legal violations, without incurring any liability.

ISSN: 2582-6433

# DIGITAL WELLBEING, ETHICS, AND DATA PRIVACY"

AUTHORED BY - DR.USHA PALHOEYA
Associate Professor
Oriental University Indore

CO-AUTHOR - AYUSHI JATTAPI

## Abstract

Today, we live in a digital world. As the economy changes, so too do society's needs. Following the computer revolution, we entered the digital world. Digital Well-Being: Digital well-being encompasses any changes in people, whether physical, emotional, or psychological, that result from the use of technology. With the advent of social media, smart phones, and other connected devices, users can experience both positive and negative impacts on society. Technology offers convenience and connectivity, but it also brings concerns like addiction, mental health problems, and digital overload. Finding digital balance involves understanding how much screen time is healthy, promoting digital deter practices, and using technology wisely. Misuse can have far-reaching consequences.

## Data Privacy

Data privacy means that people have the right to share their personal information on social media or elsewhere, but they also have the right to ensure that this data is protected. In today's digital age, a lot of data is collected. For example, if a company employs 200 employees, their personal data is shared with the company, but there is no guarantee that their personal data will remain secure. At a time when so much data is being collected continuously—often without user consent or knowledge—data privacy is compromised. Therefore, data privacy has become a central issue in discussions about trust and security. The public needs assurance that their data is not being misused, while organizations must be transparent about how they collect, store, and share data. Debates surrounding data privacy often focus on the balance between innovation and protecting personal freedom.

In the 21st century, technology has become a necessity. From online chats to the banking sector and the stock market, technology drives everything. Data privacy must be maintained alongside

ISSN: 2582-6433

the use of technology, as it is constantly evolving. Maintaining digital power and data privacy is a difficult task. Data should be used in a way that maximizes societal benefit. This research paper aims to shed light on digital data use and privacy. It aims to offer recommendations and actions that should be taken at the national and international levels to promote digital well-being, ethics, and data privacy.

The term 'database' generally refers to an agreement of information want to protect, you may want to combine Systematically arranged and stored in a computer system or in any other form.

Database 'means a collection of works, data or other materials arranged in another means. It includes the materials arranged in another means. It includes the material necessary for the operation and consolation of a data base, such as a tie a thesaurus and indexing.[1]

You restrict what users do in file by About protecting databases Requiring them to enter an account name and password when they attempt to open a file. The account name and password they enter determines which privilege set will be used to limit what they can do in a fickle.[2]

The privileges that you set up apply to a single file only and all tables within that file. If your databases solution consists of muliplefiles that you want to protect, you may want to combine all of these files into one. Multi-table file. then you can define privileges in only a single file to manage access to the entire database solutions if you don't want to combine the file into one file, then you should define privileges in each file they contains items you want to protect.[3]

If you have a multi file database solution, that includes multiple protected files you may want to consider using identical account names and passwords in each protected file. When one protected file attempt to access another protected file maker provincially attempts to open the second file with the same account name and password that was used to open the firth file. If there is a matching accounts name and password. File maker pro skips displaying theAccount/password dial box. If there is no machine account, then file make pro displays the account /password dialog box so the yes can enter accent information.[4]

[1] Dr.s.r. Myneni information technology law p-438 (5th ed. 2042-25).
[2] Dr.s.r. Myneni information technology law p-439 (5th ed. 2042-25).
[3] Dr.s.r. Myneni information technology law p-439 (5th ed. 2042-25).
[4] Dr.s.r. Myneni information technology law p-440(5th ed. 2042-25).

ISSN: 2582-6433

**Key Ward:** Digital Wellbeing, multi file, Data privacy, Computer system, Legislation.

# Introduction

**Introduction to Digital Wellbeing, Ethics, and Data Privacy**

In today's digital world, technology has become an important part of our daily lives. People use smart phones, computers, and the internet for communication, education, work, entertainment, and social interaction. While digital technology provides many benefits, it also raises concerns about digital wellbeing, ethics, and data privacy. Understanding these concepts helps individuals use technology responsibly and safely.

**Digital wellbeing** refers to maintaining a healthy relationship with digital devices and online platforms. Many people spend long hours on social media, gaming, or browsing the internet, which can lead to stress, sleep problems, reduced productivity, and mental health issues. Digital wellbeing encourages balanced technology use by setting screen-time limits, avoiding excessive social media usage, and taking regular breaks from devices. It helps individuals focus on their physical health, mental health, and real-life relationships.

**Digital ethics** involves the moral principles and guidelines that people should follow when using digital technologies. Ethical digital behavior includes respecting others online, avoiding cyber bullying, not spreading false information, and using digital resources responsibly. Environment.

**Data privacy** is another important aspect of the digital world. Every time people use websites, social media platforms, or online services, they share personal information such as names, email addresses, locations, and browsing history. If this information is not protected properly, it can be misused by hackers, companies, or other individuals. Data privacy focuses on protecting personal information from unauthorized access and misuse. People can protect their in conclusion, digital wellbeing, ethics, and data privacy is essential for creating a safe and responsible digital environment. As technology continues to evolve, individuals must learn to use digital tools wisely while protecting their health, respecting others, and safeguarding their personal information. By practicing responsible digital behavior, society can enjoy the benefits of technology while minimizing its risks.

ISSN: 2582-6433

## Meaning of Data

**After section 2(o) of the** information technology act, 2000, data means representation of information knowledge, facts concepts or instructions which are being prepared or have been prepared in a formalized manner, and is intended to be processed, is being processed or has been processed in a computer system or computer network. And may be in any form or stored internally in the memory of the computer"

Computer jeans any electronic magnetic, optical or other high-speed data processing device or system which performs logical, authentic, and memory functions by manipulations of electronic, magnetic or optical impulses, and includes all input, output, processing, storage, computer software, or communication facilities which are connected or related to the computer in a computer system or computer network sec-2(I) of Intact, 2000.[5]

Computer system means a device or collection of devices, including input and output support devices and excluding calculators which are not programmable and capable of being used in conjunction with external files which contain computer programs, electronic instructions, input data, and output data, that performs logic, arithmetic, data storage and retrieval communication control and other functions (sec.2 (I) of IT Act, 2000).

## "Computer network"

Means he inter connection of one, or more computer or computer systems or communication device through- The use of satellite, microwave terrestrial line, wire, wireless or other communication media; and Terminals or a complex consisting of two or more inter-connected computers or communication device whether or not the interconnection is continuously maintained (Sec 2(j) of ITAct, 2000).

Data is protected in computers through security system 'security system' means The right of privacy in the matter of personal life or of a trade and commercial activities is also a valuable right and cannot be permitted to be invaded by anybody, how strong he may be. Therefore with the advent of internet the demand came from various quarters for enactment of proper law so that cyber intrusion may be controlled.[6]

[5]Dr.s.r. Myneni information technology law p-625(5th ed. 2042-25).
[6] Dr.s.r. Myneni information technology law p-626(5th ed. 2042-25).

ISSN: 2582-6433

## Definition of personal data

Personal data is data which relates to a living individual who can be identified:

i) From that data, or

ii) From that data and other information which is in possession of or is likely to came into the possession of the data controller Sensitive personal dataconcerna the subject's race, ethnicity, politics, religion, trade union status, health, sex life or criminal records.[7]

**Protecting databases[8]**

You can restrict what use' can see and do in a database file by defining accounts and privilege set. For example, you can

1. Password-protect a file.
2. Allow data entry only,
3. Allow blousing but prohibit database changes.
4. Restrict access to specific tables, records, fields and layouts.
5. Give certain users full access to a file which allows them to define tables, fields, relationships data sources, and access privileges for other users.

You can also control access to a file' scheme (including its tables, layouts, scripts, and value lists and prevent versions of file market pro earlier than version 11 from opening the file.

## Protection of database by state

In has become very difficult very difficult task to individuals to protect the database. So there are international laws, the laws enacted by the states to protect the databases. There are legal enforcement authorities in every country, there are severe punishments and penalties against the wrongdoers[9].

International law relating to data protection and privacy.

The united nations commission on international trade and development(UNCITAD) adopted the model law on Electronic commerce in 1996.The resolution was carried in the general a Assembly of the UN on 30-1-1097 and it was expected from all nations to enact laws relating

[7] Dr.s.r. Myneni information technology law p-440(5th ed. 2042-25).
[8] Dr.s.r. Myneni information technology law p-438(5th ed. 2042-25).
[9] Dr.s.r. Myneni information technology law p-440 (5th ed. 2042-25).

ISSN: 2582-6433

to electronic commerce for equal legal treatment of used of electronic communications. Accordingly all nations.

## Legislation in the USA on Data protection and privacy

**In the USA the following Acts deal with the data protection and privacy;**

1) **The computer fraud and abuse ct (Cafe)**

   **The CFAA bans any access to a computer network system which is made without permission and prescribes penalty for any unauthorized access or** alteration of information. Of a virus within a protected computer for causing damage. CFAA provides both criminal and civil remedies and prescribes a limited period of two years from the date of violation or discovery of damage to lodge a suit.[10]

2) The child online privacy protection act 2012(COPPA) is a legislation aimed at safeguarding the privacy of children below the age of 13 while tee children use the internet. The act provides information that is allowed to be collected from a child including his/her name, residential address, telephone number and social security number. The act mandates that a website owner ought to procure the express consent of the parents before they collect, use or circulate sensitive personal information about children. It also stipulates that on the websites meant for children, disclosure of personal information should not be a prerequisite.[11]

3. Video privacy protection act 2012(VPPA).

4) Sarbanes-Oxley Act, 2002(sox).

5) Gramm-leach blileyAct, 212(GLBA).

6) Federal fair credit reporting Act, 1970(FFCRA).

7) Health insurance portability and Accountability act, 1996

Apart from these legislations few other enactments relevant to privacy protection enacted in the US include privacy Act, 1974, Electronic fund transfer act cable communications policy act, federal aviation act, the right to financial privacy act 1978(relating to bank records)and the driver's privacy protection act,1994.[12]

**Canada**

Canadian privacy law is governed by multiple, including the Canadian charter of Rights and

[10] Dr.s.r. Myneni information technology law p-440 (5th ed. 2042-25).
[11] Dr.s.r. Myneni information technology law p-440 (5th ed. 2042-25).
[12] Dr.s.r. Myneni information technology law p-440 (5th ed. 2042-25).

ISSN: 2582-6433

freedom; and the privacy act (Canada). Mostly the legislation concerns privacy infringement by government organization. Data privacy was first addressed with 'personal information protection and Electronic documents act and provincial level legislation also exist to account for more specific cases personal privacy protection against commercial organizations.[13]

**Australia**

In Australia there is the privacy act, 1988 the act applies to private sector organizations including (I)individuals who collect, use or disclose personal information in the course of a business;(ii)bodies corporate (iii) partnership, unincorporated associations and trusts any act or practice of a partner, committee member or trustee is attributed to the organization. Organization outside Australia must comply with the provisions in some circumstances. Sending information out of Australia is also regulated.

## National law relating to violation of privacy

**Privacy and constitution of India**

India has failed o incorporate any express Provision recognizing the right to privacy as fundamental right but the judicial pronouncements of the apex court provide the purposes and the content of the right of privacy.

In R rajgopalvs. State of Tamil Nadu (1994)65SCC632),the court has observed that "Citizen has a right to safeguard the privacy of his own, his family, marriage or prove creation, motherhood and child bearing and education among other matters. None cam publish anything concerning the above matters without his consent whether truthful or otherwise and whether laudatory or otherwise. It he does so, he would be violating the right to privacy of the person concerned and would b liable in action for damaged"

In people's Union for civil liberties vs. Union of India (1997) I SSC301), it has been held telephone tapping as violation of privacy right of a citizen which is protected under article 21 and also covered by Article 19(1)(a)of the constitution of India.[14]

In kharak Singh vs. state of UP (1964)1 SCR, 332), the court has held that the domiciliary visit at night of regulation 236 of UP Police regulation as violence do of article 21 and strike done

[13] Dr.s.r. Myneni information technology law p-440 (5th ed. 2042-25).
[14] Dr.s.r. Myneni information technology law p-440 (5th ed. 2042-25).

ISSN: 2582-6433

the provisions as unconstitutional in view of the fact that article 21 of the constitution of India guarantees the right to privacy as a fundamental right.

**Privacy protection under information technology act 2000**

Punishment for violation of privacy (Sec-66E)

Whoever, internationally or knowingly captures, published or transmits the image of a private area of any person without his or her consent, under circumstances violating the privacy of that person, shall be punished with imprisonment which may extend to three years or with fine not exceeding two laky rupees, or with both.[15]

**Sec-72 penalty for breach of confidentiality ad privacy**

Save as otherwise provided in this act or any other law for the time being in force, if any person who, in pursuance of any of the powers conferred under this act, rules or regulations made there under, has secured access to any electronic record, book, register, correspondence, information, document or other material with our the consent of the person concerned discloses such electronic record book, register, correspondence, information, document or other material to any other person shall be punished with imprisonment for a term which may extend to two years, or with fine which may extend to one laky rupees, or with both.

## Protection of database under copyright laws.

Most national systems have gradually moved in the direction of providing protection to computer software and database under copyright law. In principle, it is the skill, labor and judgment of the author that is protected irrespective of the from in which product appeaare. E.g. Whether one types a book on oil fashioned typewriter or transforms. It in a digitalized from or in hand written from. Any reproduction of the work including translations is considered a reproduction of the original.[16]

## Protecting personal information in databases.

These days many databases are established which contain the personal information about individual's e.g. Members of a library or business card holders. Such databases have risen issued regarding and misuse of personal information of individuals. Misuse may occur wherein

[15]Dr.s.r. Myneni information technology law p-447 (5th ed. 2042-25).
[16] Dr.s.r. Myneni information technology law p-440 (5th ed. 2042-25).

ISSN: 2582-6433

unwanted mail is dumped to individuals whose addresses are obtained from the computerized databases. Alternatively, if a database service misspelled the name of, an author in reference to one of the author's papers then the evaluated performance of the author measured in terms of the number of articles published may be lowered.[17]

Many countries have responded to privacy concerns of such database by introducing data protection legislation. The legislation allows individuals who are the subject of such databases the right to know what records there are about them and the contents of those records.

The issue whether data protection applies to data on CD-ROM is not yet settled. As a user of CD-ROM, one has no say in the content of the CD-ROM and can note, amend it. One is not liable to data protection law. Alternatively it is argued that as one could download CD-ROM database onto magnetic tape and then amend it, one is subject to the law about the data.[18]

## Protection of Databases by state

In has become very difficult task to individuals to protect the database. So there are international laws the laws enacted by the States to protect the databases. There are legal enforcement authorities in every country. There are severe punishments and penalties against the wrongdoers.

**Protection of databases under copyright law.**

Most national systems have gradually moved in the direction of providing protection to computer software and databases under copyright law. In principle, it is the skill labor and judgment of the author tutor that is protected irrespective of the from in which product appears .E.g.

A work is copyrightable if described as being fixed in a tangible medium of expression when its embodiment in a copy or phone record or otherwise communicated for a period of more than transitory duration. Computer databases, which are electronic files of information 'formed by the collection, assembly, and arrangement of pre-existing materials or data' are thus considered protected provide the resulting work as a whole constitutes original authorship.[19]

[17] Dr.s.r. Myneni information technology law p-441(5th ed. 2042-25).
[18] Dr.s.r. Myneni information technology law p-441 (5th ed. 2042-25).
[19] Dr.s.r. Myneni information technology law p-401 (5th ed. 2042-25).

ISSN: 2582-6433

## Discussion and challenges

The proposal for the new regulation is not final yet and discussed controversially. Amendments have been proposed. The single set of rules and the removal of administrative requirements are supposed to save money. But critics point out some issues,

a) The requirement to have a data protection officer ((DPO)in companies with more than 250 employees is new for many EU countries and criticized by some for its administrative burden, for other countries like Germany this is lowering the level of data protection since there is already a requirement for a DPO in smaller companies
b) The breach notification to the

## Digital Personal Data Protection Act, 2023.

**Sec** *2 (h*) "data" means a representation of information, facts, concepts, opinions or Instructions in a manner suitable for communication, interpretation or processing by Human beings or by automated means;

**Sec** 2((*I*) "Data Fiduciary" means any person who alone or in conjunction with other Persons determine the purpose and means of processing of personal data;

**Sec** 2(*k*) "Data Processor" means any person who processes personal data on behalf Of a Data Fiduciary;

**Sec** 2(*l*) "Data Protection Officer" means an individual appointed by the Significant Data Fiduciary under clause (*a*) of sub-section (*2*) of section 10;

**Sec 11.** (*1*) The Data Principal shall have the right to obtain from the Data Fiduciary to whom she has previously given consent, including consent as referred to in clause (*a*) of section 7 (hereinafter referred to as the said Data Fiduciary), for processing of personal data, upon making to it a request in such manner as may be prescribed,—(*a*) a summary of personal data which is being processed by such Data Fiduciary and the processing activities undertaken by that Data Fiduciary with respect to such personal data; (*b*) the identities of all other Data Fiduciaries and Data Processors with whom the personal data has been shared by such Data Fiduciary, along with a description of the personal data so shared; and(*c*) any other information related to the personal data of such Data Principal and its processing, as may be prescribed.

(*2*) Nothing contained in clause (*b*) or clause (*c*) of sub-section (*1*) shall apply in respect of the sharing of any personal data by the said Data Fiduciary with any other Data Fiduciary authorized by law to obtain such personal data, where such sharing is pursuant to a request

ISSN: 2582-6433

made in writing by such other Data Fiduciary for the purpose of prevention or detection or investigation of offences or cyber incidents, or for prosecution or punishment of offences.

**Sec 15.** A Data Principal shall perform the following duties, namely:—

*(a)* Comply with the provisions of all applicable laws for the time being in force while exercising rights under the provisions of this Act;(*b*) to ensure not to impersonate another person while providing her personal data for a specified purpose;(*c*) to ensure not to suppress any material information while providing her personal data for any document, unique identifier, proof of identity or proof of address issued by the State or any of its instrumentalities;(*d*) to ensure not to register a false or frivolous grievance or complaint with data Fiduciary or the Board; and(*e*) to furnish only such information as is verifiably authentic, while exercising the right to correction or erasure under the provisions of this Act or the rules made there under.

## DATA PROTECTION BOARD OF INDIA

**Sec 18.** (*1*) With effect from such date as the Central Government may, by notification, Appoint, there shall be established, for the purposes of this Act, a Board to be called the Data Protection Board of India.

(*2*) The Board shall be a body corporate by the name aforesaid, having perpetual Succession and a common seal, with power, subject to the provisions of this Act, to acquire, Hold and dispose of property, both movable and immovable, and to contract and shall, by The said name, sue or be sued. (*3*) The headquarters of the Board shall be at such place as the Central Government may notify.

**Sec 19.** (*1*) The Board shall consist of a Chairperson and such number of other Members as the Central Government may notify.

(*2*) The Chairperson and other Members shall be appointed by the Central Government in such manner as may be prescribed.(*3*) The Chairperson and other Members shall be a person of ability, integrity and standing who possesses special knowledge or practical experience in the fields of data governance, administration or implementation of laws related to social or consumer protection, dispute resolution, information and communication technology, digital economy, law, regulation or techno-regulation, or in any other field which in the opinion of the Central Government may be useful to the Board, and at least one among them shall be an expert in the field of law.

ISSN: 2582-6433

**Sec 20.** (*1*) The salary, allowances and other terms and conditions of service of the Chairperson and other Members shall be such as may be prescribed, and shall not be varied to their disadvantage after their appointment.(*2*) The Chairperson and other Members shall hold office for a term of two years and shall be eligible for re-appointment.

## PENALTIES AND ADJUDICATION

**Sec-33.** (*1*) If the Board determines on conclusion of an inquiry that breach of the provisions Of this Act or the rules made there under by a person is significant, it may, after giving the Schedule. (*2*) While determining the amount of monetary penalty to be imposed under Sub-section (*1*), the Board shall have regard to the following matters, namely:—

(*a*) the nature, gravity and duration of the breach;(*b*) the type and nature of the personal data affected by the breach;(*c*) repetitive nature of the breach;(*d*) whether the person, as a result of the breach, has realized a gain or avoided any loss;(*e*) whether the person took any action to mitigate the effects and consequences of the breach, and the timeliness and effectiveness of such action;

(*f*) Whether the monetary penalty to be imposed is proportionate and effective, having regard to the need to secure observance of and deter breach of the provisions of this Act; and (*g*) the likely impact of the imposition of the monetary penalty on the person.

**Sec-34.** All sums realized by way of penalties imposed by the Board under this Act, shall Be credited to the Consolidated Fund of India. In today's digital world, technology has become an important part of our daily lives. People use smart phones, computers, and the internet for communication, education, work, and entertainment. While digital technologies provide many benefits, they also raise important issues

**Suggestion**

- Limit screen time: Use built-in tools like Digital Wellbeing or Apple Screen Time to track and reduce usage.
- Take regular breaks: Follow the 20-20-20 rule (every 20 minutes look at something 20 feet away for 20 seconds).
- Avoid excessive social media use: Platforms like Integra and Tiptop can increase stress if used excessively.
- Set device-free time: For example, no phone use during meals or before sleep.
- Promote offline activities: Exercise, reading, hobbies, and face-to-face conversations.

ISSN: 2582-6433

- Respect others online: Avoid cyber bullying and harassment.
- Verify information before sharing: Prevent spreading fake news.
- Respect intellectual property: Do not copy or distribute copyrighted material illegally.

**Suggestions:**

- Use strong passwords: Combine letters, numbers, and symbols.
- Enable two-factor authentication (2FA): Especially on apps like Google Authenticator.
- Check privacy settings: Regularly review settings on social media and apps.
- Avoid sharing sensitive information online: Such as bank details, passwords, or personal documents.
- Use secure networks: Avoid public Wi-Fi for important transactions.

**Conclusion:**

By practicing digital wellbeing, ethical behavior, and strong data privacy measures, individuals can enjoy technology safely while protecting their mental health and personal information.