ALLIANCE UNIVERSITY
Private University established in Karnataka State by Act No.34 of year 2010
Recognized by the University Grants Commission (UGC), New Delhi
Alliance School of Law

ACIPR
ALLIANCE CENTRE FOR INTELLECTUAL PROPERTY RIGHTS

Volume 01 Issue 02

ACIPR Bulletin

COVER STORY

Alliance Centre for Intellectual Property Rights (ACIPR) is established with an aim to evolve as a Centre of excellence in IPR Research and innovation. It intends to engage academicians, jurists and practitioners in research and training on the promotion and protection of IP rights. The Centre is an initiative of Alliance School of Law, Alliance University for making active research contribution in the niche areas of all forms of IP rights. It aims to give special emphasis in fostering research & development in the unexplored areas of IP. ACIPR strives to evolve into a breeding ground for innovators & creators, thereby making a positive change in the development of these rights at national & regional levels.

Central Library, Alliance University

Disclaimer: The opinions expressed in these articles are the personal opinions of the author. The facts and opinions appearing in the article do not reflect the views of Alliance University and the university does not assume any responsibility or liability for the same.

MESSAGE FROM THE EDITOR-IN-CHIEF

The globalization of technology is bolstering up every single industry in the world. With the advent of development of technologies such as Artificial Intelligence which have unprecedented applicability and inherent power, the world is undergoing a phase of metamorphosis. In the wake of the COVID-19 pandemic, social interaction has been confined to the boundary's virtual platforms. In this time, it has become important to understand the repercussions of over-reliance on such technologies.

I am proud to present the second edition of the ACIPR Bulletin Newsletter. Based around the theme of Artificial Intelligence and Data Privacy, it is our aim to highlight the developments of such technology and discuss in detail the consequences of its use, or misuse. The Newsletter covers the interplay of Artificial Intelligence and Data Privacy, and the consequential interaction with Intellectual Property Rights.

Once again, I would like to express my gratitude to all the contributors, editors and reviewers who have worked tirelessly to uphold the quality of content, and towards the release of the second edition of this Newsletter.

Dr. Kiran Dennis Gardner
Professor & Dean
Alliance School of Law

CONTENTS

FROM THE EXPERTS

Mr. Harpreet Singh Hora
Advocate
Supreme Court of India, New Delhi

Why do you think data protection laws are required and what is the Constitutional standpoint about it?

It was almost one and a half decade ago that the famous British mathematician Mr. Clive Humby shouted from the rooftops, "Data is the new oil." and today, the world is in solemn agreement with him. The need for data protection laws is intrinsic in the concept of Fundamental freedom guaranteed to us in the Constitution of India and with the Right to Privacy having been held to be a part of Fundamental Rights by the Supreme Court of India in the Justice Puttuswamy judgment, the data protection laws are urgent and should be an urgency. As far as the Constitutional perspective is concerned, it is needless to state that the void of a robust data protection framework would render the right to privacy futile and pointless. Any violation of "Informational Privacy" of an individual/corporation shall frustrate the very concept of guarantees under Articles 19 and 21 of the Constitution of India and thus, sturdy legislative provisions are required for every step including (but not limited to) the collection, processing, retention, disposal and sharing of data to protect the said guarantees in "letter and spirit".

What is the legal stance of India towards data privacy challenges and data protection?

On a formal scale, India still needs to have a freestanding law on the issue of data privacy and the constitution of Justice B.N. Srikrishna Committee of experts was the first major step recognizing the said void in the year 2017.

The current legislation under section 43A of the Information Technology Act, 2000. Section 43A (that relates to compensation for Failure to Protect Data and enables the enactment of reasonable security practices and procedures for the protection of sensitive personal data) has been criticized to be inadequate and insufficient. The Information Technology (Reasonable Security Practices and Sensitive Personal Data or Information) Rules, 2011 known as SPDI Rules relate to requirements for the collection of information, organizations to have a detailed privacy policy and prohibition of disclosure without consent of the individual. The said rules have been termed as inadequate as they leave the government entities out of its ambit and are restricted only to the "sensitive personal data".

With the introduction of the PDP Bill 2019, several issues will be addressed, and it is a welcome step, although it should have come a long way back. The categorization of information (into personal, sensitive personal and critically personal), the inclusion of state actors, the provisions on the restriction of data outside India and the formation of the Data Protection Authority (DPA) shall prove to be a steppingstone in the field.

How far do you think individual participation rights and data as intellectual property are intrinsic to the fundamental rights of a person?

An individual's consent, expectation and control strike at the heart of his data privacy rights and, thus, individual participation rights and data as an intellectual property form an inseparable part of a person's fundamental rights. There have been instances where individuals have complained of losing control over the information that they had once provided. Instances include the use of information provided for a particular purpose being misused by other agencies or for other purposes, the lack of information on the way his information is being used, the refusal by agencies/corporations to remove information when the purpose is fulfilled. This not only puts the individual information at risk but also paves way for violation of integrity of the information provided and the ultimate sufferer is the individual, for no fault of his own. From an Indian perspective, the insufficient infrastructure, lack (or I'd say absence) of wide-scale expertise, non-availability of effective redressal mechanism would make the task more challenging for the citizens.

What are your views on the right to be forgotten having a place in India's data protection law? Are we at international parity in this aspect?

Right to be forgotten as a standalone right does not find a mention in the laws in place till date. The PDP bill 2019 introduces the said right and states that an individual has the right to restrict and prevent the disclosure of the information it in a situation when the information is no longer necessary for the purpose it was collected for, the consent of the individual is withdrawn and when the retention of such information is in contravention to PDP or any other law. The recent interim order of the Delhi High Court (name of the Petitioner not disclosed) recognizes the said right in view of the "irreparable prejudice" that may be caused to the Petitioner's "social life and his career prospects" despite him having been ultimately acquitted and his acquittal having been upheld by the Delhi High Court. Although the High Courts have taken different approaches on the said issue, the observations of the Odisha HC are relevant here, the Hon'ble Court had remarked as:

"information in the public domain is like toothpaste, once it is out of the tube one can't get it back in and once the information is in the public domain it will never go away"

In the case before the Court of Justice of the European Union (CJEU) titled as "Google Spain SL, Google Inc. v Agencia Española de Protección de Datos, Mario Costeja González (2014)", it was held that an Internet search engine operator is responsible for the processing that it carries out of personal information which appears on web pages published by third parties. Like the grounds as mentioned above in PDP bill, the grounds of the said removal include the circumstances where the information "appear to be inadequate, irrelevant or no longer relevant or excessive in the light of the time that had elapsed."

Argentina's Right to be forgotten as it finds place under Article 43 of the Constitution of Argentina which gives the right to "any person" to file action demanding the "suppression, rectification, confidentiality, or updating" of the information or data held in public registries, data banks, private registers etc. Hence, it would be fair to say that we are far from achieving parity on what exists on an international level.

FROM THE EXPERTS

Ms. Savitha K. Jagadeesan
Senior Resident Partner
Kocchar & Co., Chennai

How do data privacy work in conjugation with data security in Indian perspective and the legal stand on it?

Data privacy and data security are two different ambits that require different aspects of law addressing its challenges, however, in India data privacy is interlinked with data security. To hold the personal data collected and to ensure the non-leakage of the same requires that considerable measures are in place to avoid any format of infringement of privacy rights of an individual. India's data security and privacy laws are covered under its technology law- the Information Technology Act, 2000 ("IT Act") and the rules thereunder, more specifically the Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011. At the other end of the spectrum, we also have Section 43-A of the IT Act which imposes damages for negligence while implementing and maintaining the security practices to avoid data leakage/theft. Further Section 72-A – puts an embargo on service providers to disclose materials containing personal information of any person without their consent and treats this as a breach of contract.

The archaic telegraph laws of India still have a say especially when it comes to espionage where Sections 5 & 24 of the Telegraph Act, 1885 – regulates the interception of messages by the Central Government and the State Governments of India, which can only be done by following the Telegraph Rules, 1951

The PDP Bill recognised the importance of data privacy and the need to secure the data collected and brought to the fore procedural safeguards to prevent any violation of the privacy rights of an individual.

What is your opinion about the Personal Data Protection Bill, 2019? Do we stand at international parity in this information era?

One of the biggest concerns of the PDB Bill is that it is yet another instance of a sporadic piece of law which has not come to terms with aspects of citizen privacy. According to Tsaaro, a data protection services provider who surveyed peoples' expectations on the PDP Bill, stated that as per their survey over 51 per cent of respondents thought the upcoming Personal Data Protection Bill 2019 was at par with other global privacy laws such as the General Data Protection Regulation, California Consumer Privacy Act and the Personal Information Protection Law.

Globally the data protection laws have a common thread but still contrasting models. For example, the EU model provides a comprehensive data protection law for the processing of personal data in contrast to the US model that holds privacy paramount vis-à-vis state intervention. The Indian model has tried to combine the two elements, but for privacy experts, the fact that government intervention is given a free hand remains a cause of concern and criticism. If we were to study the IAPP comparative analysis by and large the laws are similar but administrative wise, as well as enforcement wise the PDP, is more stringent including it gives the government a lot more leeway, however, on a significant spectrum the PDP bill can be considered to be at par with its international counterpart. The Tsaaro survery also echoes this thought where the majority of participants were worried that the drafted Bill does not guarantee the same rights to Data Subjects as privacy legislation such as the GDPR do.

What impact this bill will have in situations where the data is processed or transmitted to other country impacting the security and privacy of the country?

Keeping the above in mind the bill has some very positive features such as the setting up of the Data Protection Authority to be at par with its European counterpart as well it seeks to improve data handling and data privacy. The bill enables data collection to be done only with customers consent including it enables the withdrawal of the given consent at any time. It also enables the consumers to access, correct and erase their data after it is processed, and the businesses will have to enable policy and practice to allow the customers to be in charge. The bill provides for data localisation where certain data can be stored on Indian servers only. Sensitive personal data includes “special categories of personal data” including data relating to health, religion, sex life, etc, but does not include passwords. Personal data that are not considered “sensitive” or “critical” can be stored entirely outside of India and no transfer restrictions apply to this data, however, if the personal data falls into the sphere of Critical personal data” then this cannot be transferred outside India.

How can legal agencies help in protecting the data and privacy of the people especially after the advent of artificial intelligence?

Artificial intelligence is the source of big data and therefore is likely to accelerate the trend towards data collection and processing and its technology enables the same where search algorithms, search engines, all are driven by machine learning and decisions are driven through algorithms. Therefore, with the evolution of artificial intelligence, the use of personal information will be magnified so much so its scope of the intrusion into privacy space of an individual might be lost due to its magnificent quality to quickly collect and process data, therefore, leading to complete intrusion of an individual's privacy interests. Users allow for the AI applications to simply collect their data without realising that the application permissions allow them to scrape and mine the data to be used for future purposes. This concern requires to be addressed in the present laws but has not been recognised. The PDP bill has in fact a carve-out provision which allows that for the purposes of encouraging innovation in artificial intelligence, machine learning or any other emerging technology in the public interest to create a Sandbox. Therefore, the present laws have failed to envisage the impact of AI on privacy concerns and have not addressed the concerns surrounding AI applications. There is, thus, a need to understand and resolve the scope of data protection law and principles in the rapidly changing context of AI.

FROM THE EXPERTS

Dr. Mathew Thomas
Advocate and Author

Is AI going to be a game-changer in this info-centric world and what are the scope and limitations of AI in the contemporary world?

Artificial Intelligence is today an umbrella term that encompasses so many diverse application fields, such as networks, medical, finance, telecommunications, satellites, transportation, entertainment, military, cartography, education, security, energy etc., that it touches so many disciplines either directly or indirectly. AI has many techniques such as Logic programming, Fuzzy logic, Probabilistic reasoning, Ontology engineering and Machine learning and its diverse branches. The advancement in the field of AI is rapid and fast-changing. With Facebook having rebranded itself as Meta, is on its way to creating a Meta universe, a digital twin of the real world, with 10,000 engineers working on the project. As it is, smartphones use AI (most of us are unaware of this AI) and that is how they are able to answer questions posed to them, Siri (Apple) is one such example. Many of the service providers use low-end AI and BOTs to answer questions during chats with customer service.

The implications for humans with the advancement of AI techniques are mindboggling and at times raises fears of it surpassing human intelligence and cognitive abilities. Some AI machines have been deemed to be sentient, that is to say, that they emote like humans with feelings. AI systems at present have the capability to rationalize and choose between alternatives. Many of the common utility items that we use today use some form of inbuilt AI.

The area which is of concern in the near future would be as to how to control AI machines when they achieve 'Singularity'. This would happen when machines surpass human intelligence. Machines have the capability to work continuously without tiring and its output is huge. As it is, many services use AI and repetitive jobs are being assigned to AI, for example, painting in a car factory. Surgical robots also use some form of AI, and once data is fed in, they precisely operate upon the patient with little human intervention. AI is being used to diagnose/detect pathological slides/radiology for cancer. Limitations of AI are dependent on the validity of data being used to train AI. Biases often creep in due to various factors such not being able to generate clean data that is devoid of biases due to skewed data being fed in.

Artificial intelligence is one of the most debated topics in our generations and what kind of impact would AI have in the next 20 years in India regarding data protection.

The Personal Data Protection Bill was introduced in the Parliament in 2019 and was referred to the Joint Parliamentary Committee for detailed examination. With a huge increase in the availability of data due to penetration of the internet and usage of smart devices, there is a copious amount of data that is being generated as data waste. Data is any data that is used to work with internet-connected devices. This is classified into personal data and non-personal data. Personal data is one where the individual identity of the individual using a smart device can be identified such as age, sex, orientation, religion, race, preferences, marital status, etc. Non-personal data is data which though generated by an individual, cannot identify the individual with the data. What is of concern is when a State may use data to identify individuals on their political leanings and thoughts. Authoritarian states use such data to clamp down on dissent or bring in harsh measures against civil society. There are a number of countries that use data to identify individuals on their political leanings from the data exhaust created when a smart device or internet is used.

While on one hand there is a need for large amounts of data for training AI, there is a need to anonymize and randomize data so that individual identity is not revealed. While many countries have AI policies in place yet it is the organizations that use AI that could spell danger to individual liberty and thought. Privacy is at the helm of individual freedom within the bounds of modern society. The Supreme Court in KS Puttuswamy has opined that measures restricting privacy must be backed by law must be legitimate, proportionate to the objective of the law and above all must have procedural safeguards against abuse. AI if used could easily vet conversations that use words such as integrity, sovereignty, public order, state security, public order, which could be interpreted as inimical to state interests if a state would like to clamp down on individual liberty. So, exemptions to agencies in the Personal Data Protection Bill may be counterproductive to individual liberty and freedom but at the same time needs to balance. The use of AI in data protection could be a counterbalance against exploitation by state agencies. But at the same time, the hard lessons learnt from social media agencies, India policy, on selective removal of communally sensitive posts may be a hard lesson in protecting personal data with larger use of AI. Whether there is the increased use of AI in data protection or not, the key is the consent of the individual on fairgrounds, unlike the present terms and conditions of take it or leave it, as in the case of online contracts, where the individual is forced to agree to terms of the service provider.

ARTIFICIAL INTELLIGENCE AND COPYRIGHTS

Intellectual Property is an intangible innovation created by the human mind which includes artificial intelligence (AI). While AI is the study and development of computer systems and software that can reproduce human behavior.

Although there is no particular act that governs and regulates AI, the Copyright Act, 1957 affects the AI systems in India. Certain provisions of this Act acts as a hindrance in the development of AI and also deny protection to the works produced by the machines operated by such systems.

Under the Copyright Act, 1957, two doctrines define the originality of the work which comes under this act:

1. The sweat of the Brow:

According to this doctrine, an author is only entitled to get a copyright on his work based on the efforts put and expenses incurred by him in the creation of such work.

2. The modicum of Creativity:

This doctrine provides that the degree of creativity need not be high, but a reasonable level of creativity should be incorporated for the work to be able to get copyright protection. This doctrine was adopted in the case Eastern Book Company v. D. B. Modak. The Supreme Court in this case held that AI systems can achieve the modicum of creativity and thus, any work produced by such machines can pass the test of originality.

Section 2 (d) of the Copyright Act, 1957 defines the term 'author' which poses to be a roadblock for copyright protection of the works produced by AI. According to the definition, an author is a person who causes work to be created. Here, such a person is a human or a legal person. Therefore, the present copyright act does not include works created by artificial intelligence systems.

One such example of protection of a copyrightable work created by a non-human is the famous 'Monkey Selfie' case. It was held in this case that while monkeys can take selfies, only a human can own the copyright.

The main issues with the copyrights of the work created by AI are, firstly, who would be the rightful owner of such copyrighted work – the natural, legal person, who created the AI or the person who owns it? Secondly, if an AI infringes some other person's copyright without any human command, then who would be held liable?

It is evident that the changes and developments in the technological field have not yet been adopted by the legislation. Seeing that it is important for the laws to go hand in hand with the developments in society, the acts that regulate AI and IPR should be amended and updated accordingly.

Artificial Intelligence, OXFORD LEANER'S DICTIONARIES, (November 20th, 2021, 12:03 AM) URL: https://www.oxfordlearnersdictionaries.com/definition/english/artificial-intelligence

The Copyright Act 1957

Eastern Book Company v. D. B. Modak, 2008 1 SCC 1

The Copyright Act 1957 § 2 cl. d

Susannah Cullinane, Monkey does not own selfie copyright, appeals court rules, CNN, (Novem 19th, 2021, 1:18 AM) URL: https://edition.cnn.com/2018/04/24/us/monkey-selfie-peta-appeal/index.html

Ajinkya Malgaonkar
Student
Alliance School of Law

QUICK FACTS

Apple’s Patent Application for Metaverse

Metaverse or 3-D virtual environment is next up on list in the Apple’s technology world. Application titled “Method and Device for Attenuation of Co-User Interactions in Simulated Reality (SR) Space” has been filed with the U.S. Patent Office, however, the accessibility of this endeavour is still a long-term work in process. With this technology bringing your own avatars in real environment would no more be a dream!

ISSUES CONCERNING BIOMETRIC-BASED AI INNOVATIONS IN TERMS OF DATA PRIVACY LAW AND INTELLECTUAL PROPERTY

Consumers have seen an increase in the usage of biometric data in place of passwords and other forms of identification in today's era of mobile devices and always-on Internet access. As technology advances, mobile devices are increasingly using fingerprints, iris scans, or even full-face recognition to "unlock" locked devices. Therefore, biometrics-based Artificial Intelligence (AI) technologies are on the increase. While the Intellectual Property (IP) potential for such developments is enormous, concerns about the usage of biometric data may arise in light of recently adopted and growing data privacy laws and regulations.

Biometrics data relates to physical characteristics of the human body or behavioral traits of human beings, according to the International Organization for Standardization (ISO), the word "biometrics" referring to the "automated recognition of individuals based on their biological and behavioral characteristics." Therefore, anything relating to the measuring of people's bodily traits and attributes is referred to as biometric data. This data is used to prove a person's uniqueness and verify that they are who they say they are in terms of digital identification. Previously, biometric data was only used to get access to restricted areas or facilities, such as high-tech laboratories or classified government buildings. Today, however, a wide range of devices, including but not limited to cellular phones, mobile tablets, and laptop computers, make use of this information.

Biometrics data is very valuable for AI advancements. This is because AI is primarily a data-driven technology that uses unique information to train AI computer models for specific tasks. Biometric datasets from a variety of people might be gathered and utilized to train a biometric-centric AI model. Once trained, the biometric-centric AI computer model may use new data as input to forecast, categorise, or generate output findings for use in a range of applications, including security choices. Patents can give wide protection for AI technologies that use biometrics data in terms of intellectual property. Apple, for example, has hundreds of patents covering its Face ID technology. A set of patent claims for a biometric-centric AI invention may generally correlate to its work flow, which may comprise pre-processing gathered biometrics data, training an AI model using the pre-processed biometrics data, and employing the AI model to produce a security or identification result (e.g., like Face ID).

Biometrics data is being dragged into the data privacy legal and regulatory environment due to its highly individualised character. The regulatory landscapes formed by the European Union (EU) are discussed in this article.

General Data Protection Regulation (GDPR) is a European Union rule that aims to safeguard "natural people with relation to the processing of their personal data." The GDPR went into effect on May 25, 2018, and it applies to firms that process personal data of EU people and are based in any of the EU member states (e.g., France, Germany, Italy, Spain, etc.). While the GDPR is a European Union rule, it has worldwide implications. This is because the GDPR puts requirements on organisations that target or collect data about EU people, even if they are not based in the EU. As a result, and considering that the combined EU member states' territories account for a significant chunk of the global economy, the GDPR is widely seen as a critical legal framework, particularly for businesses based in or looking to grow into Europe. The GDPR has influenced other countries' privacy laws. While the number of nations affected by or taking notes from the GDPR is long, it's vital to remember that protecting consumer privacy when dealing with biometrics, Big Data, and AI is a worldwide concern and opportunity.

AI and the use of Big Data and biometric data in everyday life have an impact on a wide range of people and organisations. AI may access a consumer's personal information, which is typically very sensitive. Business firms are held liable for misappropriation or breaches of such information. Governments all across the world are attempting to establish which, if any, restrictions to enact in order to safeguard AI, as well as the extent of any regulations.

The regulatory framework controlling biometrics data is projected to continue to expand. As a result, businesses should exercise caution while creating new biometrics-based goods or services, even if they are located outside of states or countries that have data privacy legislation. While data privacy laws vary by country, many of them have similar regulatory elements. Developing written rules covering how the organisation will collect, use, distribute, and delete biometric data might help a corporation using biometric data prepare for data privacy concerns that may occur. Putting in place procedures to track workers' and consumers' informed permission for the usage of their biometric data; biometric data encryption and security. Companies creating novel biometrics-based goods and services will want to collaborate with legal counsel that is familiar with both IP and data privacy laws and regulations to protect their inventions and keep up with the evolving data privacy landscape.

Data privacy is a part of consumer law and basic rights in the United States and England, respectively. In India, "data privacy" is not severely enforced as a legislation, but under Article 21, the right to "life" includes the right to "privacy" as well. Working hand in hand with global legislation, India is likewise grappling with a lack of legal frameworks to protect personal data and privacy, and has already begun the process of drafting a comprehensive set of codified data protection and privacy laws. India requires a conducive climate in which to promote technological knowledge and proficiency, to foster collaboration between public and private organisations, and to provide a comprehensive legal framework for future technologies.

ISO, https://www.iso.org/obp/ui/#iso:std:iso-iec:tr:24741:ed-2:v1:en (last visited Nov 6, 2021).

Christina Bonnington, APPLE PATENT EXPANDS ON BIOMETRIC IDENTIFICATION IMPLEMENTATIONS WIRED (2012), https://www.wired.com/2012/10/apple-patent-biometric/ (last visited Nov 6, 2021).

Matt Burgess, WHAT IS GDPR? THE SUMMARY GUIDE TO GDPR COMPLIANCE IN THE UK WIRED UK (2020), https://www.wired.co.uk/article/what-is-gdpr-uk-eu-legislation-compliance-summary-fines-2018 (last visited Nov 8, 2021).

Arthita Halder
Student
Alliance School of Law

THALER VS COMMISSIONER OF PATENT AUSTRALIA

On July 30th, 2021, the federal court of Australia made a landmark decision in respect of patents and became the first court to recognize that anything other than a natural person i.e. (AI) Artificial Intelligence can be an inventor.

Dr Stephen Thaler filed this lawsuit on behalf of DABUS, an artificial intelligence system he designed. DABUS is an acronym for "Device for the Autonomous Bootstrapping of Unified Sentience". By submitting patent applications to Australia and other countries around the world, Dr. Thaler named the AI machine DABUS as the inventor, and himself as an assignee, applicant, and attorney. This application was rejected by the courts and the patent offices of the United Kingdom, the United States and Europe, even in Australia. However, the Australian Federal court overruled the decision of the Commissioner of Patents in the case of Australian Patent Application No 2019363177. This invention relates to a container for food products that uses a series of fractal elements to allow multiple containers to be interconnected, thereby improving gripping and heat transfer into and out of the container.

The Delegate of the Commissioner of Patents, in rejecting the Patent Application, noted that the Australian Patent Act lacks a definition for the term "inventor." However, at the time the Act was passed (in 1991), there could have been no doubt that inventors were natural persons, and machines were tools for inventors. However, machines now do such a vast array of things that it is reasonable to claim that machines could be inventors with artificial intelligence. Given section 15 of the Act, a patent can only be granted to the inventor or to the person who entitles the invention to the inventor. A person can be a natural person or a legal person, such as a corporation. Section 15 makes it clear rights of the patentee flow from the inventor, and if the patentee does not devolve, the inventor will be the patentee. This implies that the inventor must also be a physical person, and an inventor who is not a person cannot be granted a patent.

According to the United States Patent and Trademark Office, it has determined the meaning of "inventor" based upon terms in the statute such as "whoever", "himself" and "herself", which relate to humans. Most other jurisdictions have determined the issue by concluding that only a natural person has the ability to transfer or assign inventor rights, and as a matter of statutory interpretation this is a necessary characteristic for the definition of an inventor. so all other applications were rejected based on these contentions.

In this particular case court justified how DABUS is considered to be a inventor in most of the places. As there is no definition of "inventor" in either the Australian Patents Act or the Regulations, the word has its ordinary meaning: "In that regard, the word "inventor" is an agent noun. Then the words like computer, controller, regulator, lawnmower, dishwasher and so on are all agent nouns. Each example shows that agents can be people or objects. If an artificial intelligence system is the agent that invents, then it can be described as an "inventor". According to the Court, antiquated dictionary definitions of "inventor" are unhelpful, which means it may adopt a definition incorporating artificial intelligence. A non-human inventor, such as an AI, is not excluded from the provisions of Section 15 which deal with inventorship and ownership.

Section 15(1)(b) provides that a patent may be granted to someone who would be entitled to hold the patent if a patent for the invention were granted. This provision does not explicitly require that there be an inventor. Additionally, the provisions of this section are not limited to an assignment by the inventor or an earlier vesting of title in the inventor. As a matter of definition, it covers situations where a machine has made an invention, rather than a human, that was the subject of contract, or that was misappropriated. This gives rise in either case to an equitable or legal right of assignation.

According to section 15(1)(c), a patent may be granted to a person who "derives title to the invention from the inventor or from a person mentioned in (b)". Based on the Court's reasoning, Dr Thaler prima facie falls under s 15 (1) (c) since he inherited title to the invention from the inventor, DABUS. Therefore, section 15(1)(c) clearly defines an AI as an inventor.

The Court went on to rationalize this finding by stating: While DABUS, as an artificial intelligence system, is not a legal person and cannot assign the invention, this does not mean that title cannot be derived from DABUS. Under s 15(1)(c), a person who inherits an invention from an inventor has additional rights in addition to those granted by an assignment.

In the end, the Court determined that, as the owner and controller of DABUS, Dr Thaler would own any inventions developed by DABUS. In this respect, title may derive from the inventor even if it does not vest ab initio in the inventor. This case had opened a Pandora box of new dimensions of interpretation by the courts and its emphasis on the acceptance of AI.

Patents Act 1990(Australia)
Section 15, Patents Act 1990
[2021] FCA 879 ,para 120

Bharatee Preeya
Student
Alliance School of Law

IS YOUR VOICE ASSISTANT LISTENING TO YOU? AN INSIGHT INTO DATA PRIVACY LAW

There isn't a day that goes by when our voice assistants don't help us with a simple task by providing ready answers or playing our favourite music. It is startling that Google Assistant, Apple's Siri, Amazon's Alexa, and Microsoft's Cortana all respond to a single voice command, which makes it a possibility that they are always listening to us. A vast number of terms and restrictions, which are often disregarded because of twisted wording and ambiguity, always accompany these technologies.

Chatbots and other applications based on artificial intelligence process various amounts of personal data, in particular also for training purposes. Therefore, they often fall within the scope of data protection laws. In technical terms, often known as the Virtual Private Voice Assistant (VPVA), are so widely popular that by the end of 2020 there were 4.2 billion of them being in use. However, the flexibility of using them does not eradicate the point of data privacy and cybersecurity. Through eavesdropping, hackers can easily gain access to the smart cameras or speakers operated by these VPVAs. Another issue with eavesdropping is that it detects voice recognition. Google Assistant or Siri, in particular, responds to registered speech, raising the potential that they are always listening even when not in use.

Each smart device is potentially another way into your home- to access data, abscond with your money, or steal your identity. Researchers recently uncovered the absence of potent user authentication systems in most digital assistants. Hence, hackers can meddle with a variety of smart cars, smart home systems, and other devices. Inaudible voice commands with high ultrasonic sound or laser rays from a distance of 110 m is enough to tap into these devices.

In a recent case of California, the plaintiffs approached the court with a complaint of violation of users' privacy by Siri. The contentions were Siri routinely recording the private conversations because of accidental activation and disclosing it to third parties. Although the case was dismissed on grounds that the private setting alone is enough to show a reasonable expectation of privacy.

Another case involving Google Assistant previously surfaced in July, in which the plaintiff claimed that Google had no right to use their conversations for targeted advertising. It was contended that the device was eavesdropping them. However, the plaintiffs failed to establish that they were harmed or that Google had breached its contractual obligations, so the case was dismissed once more. U.S. District Judge, Beth L. Freeman said “it does not sufficiently apprise users that it will use recordings made in the absence of manual activation or a hot word utterance.”

However, consumers can take some precautions to protect their safety. Adding additional authentications to compensate for the lack of end-to-end encryption, avoiding connecting all devices, and creating a tenable Wi-Fi network are just a few of the foundations. The issue is how our privacy is breached. Therefore, as long as the dangers are known and mitigation measures are implemented, using these smart assistants poses relatively little risk.

Part 1: What should be considered under data privacy law with voice assistants?, Voicetechhub.com (2021), https://www.voicetechhub.com/what-should-be-considered-under -data-privacy-law-when-implementing-voice-assistants-or-chatbots (last visited Oct 31, 2021).

Cybersecurity: How Safe Are Voice Assistants? Kiuwan, Kiuwan (2021), https://www.kiuwan.com/safety-voice-assistants/ (last visited Nov 1, 2021).

Lopez et al. v. Apple Inc. (2019) U.S. District Court, N.D. Cal 04577

Ipsita Sarkar
Student
Alliance School of Law

QUICKFACTS

Any change to an existing idea can be patented, but this does not ensure your rights to commercialise your product. You may still need permission to utilise anything patented by a third party in your device.

AI AND LEGAL PERSONALITY: THE ACCOUNTABILITY GAP?

The concept of legal personality is a construct of law. Legal personality intrinsic to the idea of legal personhood arises from what is known as natural persons. Natural persons, the best example being human beings have their intellect, emotions, ideas, manifestations, so on and so forth. The legal personality that we commonly equate to corporations was introduced in the legal system to limit the liability of the founders or shareholders of the corporation. This construct endows on the corporation a set of rights and liabilities. It includes civil and, in some cases, criminal liability.

A question that has been looming in the international platform is whether Artificial Intelligence (AI) should be granted legal personality. Theoretically speaking, there is no bar to recognizing AI's legal personality. But there exist technical difficulties in actually implementing this construct. This is due to the lack of a clear consensus with regards to the future of AI and the fact that not all AI's have independent and complex functioning. In a report requested by the European Parliament, a new form of personality, i.e., electronic personality has been discussed. Electronic personality, in its general sense, as argued should be given to a specific kind of AI under three functional grounds provided it is applicable only when it is deemed to be more appropriate than other legal remedies.

It has been argued, that electronic personality is not in its entirety different from legal personality and is kind of a way to refer to the same legal construct. This concept has been immensely criticized across the global, but what is imperative to note here is that there exists a huge accountability gap for any action of an AI that is complex and have an independent functioning via machine learning. In such a situation, wherein, an AI gains a certain level of autonomy, attaching liability to the inventor(s) of the AI seems to be futile. In most situations, tracing back to the actual person behind the AI is feasible. But with an increase in complexity and use of AI in almost every area, it has become questionable as to for how long the same can be done. However, granting AI legal personality does not in its entirety solve the issue of accountability. This is because the extent of rights or the liability that could be attached is still an issue of debate. The author believes that considering AI a legal person would be a stepping stone in addressing the pertinent accountability issue.

With the technological advancements in recent times, it would be fallacious to hold the originator or group accountable, when in certain circumstances due to machine learning the AI can arrive at a different outcome than what the natural persons' intended. AI has also been recognized as an inventor in recent times by jurisdictions like South Africa and Australia, although this may seem futuristic at this juncture in the Indian jurisprudence, there is a need to address these issues.

Karolina Ziemianin, Civil legal personality of artificial intelligence. Future or utopia?, 10(2) IPR 1, 8 (2021), < https://policyreview.info/pdf/policyreview-2021-2-1544.pdf>

Shubham Singh, Attribution of Legal Personhood To Artificially Intelligent Beings, July-September BLR 194, 198-199 (20117) < http://docs.manupatra.in/newsline/articles/Upload/7E399602-D4A0-4364-BE11-F451330BFDB5.pdf>

ANDREA BERTOLINI, ARTIFICIAL INTELLIGENCE AND CIVIL LIABILITY 33, (PE 621.926, 2020)

Jayed Wood and Jennifer A Marles, Recent wins for DABUS- Patenting in an era of Artificial Intelligence, MONDAQ (Oct. 25, 2021), https://www.mondaq.com/canada/patent/1124222/recent-wins-for-dabus-patenting-in-an-era-of-artificial-intelligence-

Ashmita Mitra
Student
Alliance School of Law

QUICKFACTS

The usual procedural procedure for patents can take three to five years to reach the stage of a fully granted patent. Inventors frequently fail to realise that they may be required to retain an application for that long before they may consider selling the patent.

ARTIFICIAL INTELLIGENCE AND DATA PRIVACY

The amount of data created by various electronic devices and apps has increased dramatically in recent years. Today's businesses receive enormous benefit from 'big data' analysis, and they also outline their business strategy based on it. Although the commercial efficiency is undeniable, the burning question is 'do individuals have any influence over how information about them is gathered and managed by others?' Every data management program must include Intellectual Property Rights (IPR) management. The creator of a database or other data resource will be interested in who owns it and how it might be used by others. Anyone who intends to use the tool with data given in part by others should make sure that any legal, ethical, or professional obligations to the data supplier are addressed as well as fulfilled. Individual liberty is emphasised by data protection, and this individual's freedom is challenged by stranger intervention.

By all means required, it is important to put a halt to the stranger's action on the person's activities. Because personal information reflects an individual's individuality, Indian courts, including the Supreme Court of India, have recognised that the right to privacy is an integral aspect of the right to life and personal liberty, which is guaranteed to every citizen under the Indian Constitution. As a result, the Indian judiciary places a premium on the right to privacy, which can only be strengthened for justifiable reasons like as national security and public interest. There are, however, a variety of different legal frameworks that discuss data security, such as the IT Act, 2000, The Indian Copyright Act, 1957 and Credit Information Companies Regulation Act, 2005.

How does IPR ensure data privacy?

The balance between "data protection" and "intellectual property legislation" must be examined as the best approach to the functioning of computer-related databases. Anyone who is aware of an illegal copy of the application on a computer is responsible for infringement under Section 63B of the Indian Copyright Act. The characteristics of 'effort, ability, and judgement' underpin an individual's claim to intellectual property. The protection of the owner's right to that work is vital in the case of legislation on specific works of literature, fiction, music, art, and cinema.

However, the Copyright Act makes it impossible to distinguish between data privacy and database security. The aim of data protection is to safeguard individual privacy, but the purpose of database security is to protect the creativity and investment made in the gathering, verification, and display of databases. Access, anonymity, ownership, and facts are all legal concepts that apply to all interactions.

The necessity to keep identifying information over time in order to establish rights and duties must be balanced with privacy protection. The author and receiver, data subjects, and third parties, all of whom are equally significant in the online world, are assigned duty for the production, recording, and preservation of evidence using the rights and duties approach. Similarly, 'data security' and 'intellectual property rights' are issues about rights.

Mutaman Amir Ahmed Abdalla
Student
Alliance School of Law

QUICKFACTS

Self-plagiarism occurs when we choose to replicate our own previously circulated work, in whole or in part, without noting that they have previously been distributed. Almost everything, including works not covered by copyright, can be plagiarised. Obtaining permission to use a work, on the other hand, makes the usage non-infringing, albeit it may still be considered plagiarism.

AI AND PATENT LAWS: REVIEW OF THE PARLIAMENTARY STANDING COMMITTEE REPORT

Recently, South Africa had become the first country to grant patent to an AI "DABUS". But while applying for multiple jurisdictions, the United Kingdom was one of the countries to reject it stating that patents can only be granted to human inventors. Artificial Intelligence (hereinafter AI) has been gaining more and more importance in various fields as it has a high economic impact. Due to this, the Parliamentary Standing Committee Report (hereinafter The Report) of 23rd July, 2021 recommended a series of amendments and changes to be made to the Indian Intellectual Property laws in order to accommodate and extract benefits arising from AI.

The Report stated that the current Patents Act, 1970 (hereinafter the Act) is not sufficient to deal with inventorship and ownership by AI. In this regard it recommends that the Act has to be modified to expand its protection to both AI generated works and AI solutions. Firstly, Section 6(1)(a) of the Act, which provides the human inventor condition by using the term "by any person", has to be changed to include innovations by AI. The Report also recommends the amendment of Section 3(k) of the Act. The Report also proposed that by granting patent protection to AI induced inventions, the creator of the AI will also be incentivized and encouraged which will also increase overall creativity and innovation in AI solutions. the most apparent issue with regard to AI is its lack of legal personality. For this the Report observed that AI and humans have different attributes and therefore it is better to provide a different type of legal status to it. It was suggested that a separate set of rights may be provided for AI induced inventions and their protection.

The main criticism of the Report is that, while it recommended necessary improvements and amendments to be made, it does not specifically deal with the real issues that occur with AI generated works. It doesn't address issues on purpose of ownership pf AI, incentives for AI, negotiation of patent terms by AI, the role of the creator of the AI and so on. This shows that the current IP regime is not in consonance with the rapid development of AI technology. Therefore, there is a need for a far more flexible and dynamic IP framework that can assist the current and future developments in AI.

Erika K. Carlson, Artificial Intelligence Can Invent But Not Patent—For Now, 6 ENGINEERING 1212, 1212 (2020), https://www.sciencedirect.com/science/article/pii/S209580992030254X?via%3Dihub.

Review of the Intellectual Property Rights Regime in India, Report No. 161, DEPARTMENT RELATED PARLIAMENTARY STANDING COMMITTEE ON COMMERCE (2021).

Indra Priyadarshini
Student
Alliance School of Law

QUICK FACTS

A parody or an exaggerated replication of the work for comic or critical purposes is permissible under the fair use doctrine if the parody is transformative. A derivative work that simply exploits copyrighted names, concepts, characters, and ideas is not a parody; however, a work that twists them in such a way that the consumer gains a new understanding of the original is. Sometimes the new knowledge is as simple as being able to chuckle at how the parody mocks the original.

THE INTERPLAY OF NFTS AND INTELLECTUAL PROPERTY

The buzz around the term "crypto-currency" has made it a part of our daily vocabulary. It is only a matter of time before it becomes an inherent part of the business ecosystem as well, considering the strong upsurge of the block chain technology/based systems. With the arrival of virtual ecosystems like Metaverse, the concept of a "Non-Fungible Token" is starting to attract a lot of attention.

In layman's terms, "Non-Fungible Tokens" are tokens acting as a unique identifier of information existing on a blockchain. Unlike the traditional crypto-currencies such as Bitcoin, which have a permanent, equivalent and fractional value (also known as Fungible Tokens), a Non-Fungible Token acts as a seal of authorization, verifying the authenticity of an intangible item due to its unique value. In other words, an NFT, in a manner, certifies the originality of content.

There already exists an inherent need and use for these tokens in the enforcement of intellectual property rights. Intellectual property such as copyrights and trademarks, which require some form of originality or distinctiveness to be enforceable, will clearly benefit from the introduction of NFTs.

Several industries make predominant use of intellectual property and depend on its licensing or assignment to generate profits. The media and entertainment industry cardinally revolves around the licensing of copyrights and other intellectual property. The implementation of NFTs, along with self-executable contracts (smart-contracts), will revolutionize the licensing component of several trades.

Copyrighted material such as original artwork, sound recordings or other commercially exploitable resources require the drafting of extensive and complex agreements - which often require several stages of litigation to be enforceable. Furthermore, once an NFT is marketed on an online platform, the creator or licensed vendor can derive economic profits from its sale without the existence of a physical deed or agreement, as the NFT attributes ownership to the buyer upon the fulfilment of the contract of sale.

Recent developments in the NFT marketplace have seen NFT associated artwork being sold for several million dollars. A digital artist going by the name "Beeple", in the month of March, sold his original work for a reported amount of $69 million. The introduction of NFTs will significantly propel the accessibility of artwork and other copyrighted resources globally, and will definitely act as a golden tool for upcoming artists. The concept, although in its genesis phase, is one that demands a lot of attention and regulation. The development of a reasonable regulatory framework will have a pronounced effect on the accessibility of information and resources, which at the end of the day, is what the regulation of intellectual property aims to achieve.

Bharat Sharma, Metaverse is No Joke, As Someone Just Paid $650,000 For A Digital Yacht NFT, India Times, (Nov. 30, 2021), https://www.indiatimes.com/technology/news/metaverse-yacht-nft-555550.html

Dragan Bosovic, How nonfungible tokens work and where they get their value – a cryptocurrency expert explains NFTs, The Conversation, (Mar. 31, 2021), https://theconversation.com/how-nonfungible-tokens-work-and-where-they-get-their-value-a-cryptocurrency-expert-explains-nfts-157489

Regner, Ferdinand & Schweizer, André & Urbach, Nils, "NFTs in Practice – Non-Fungible Tokens as Core Component of a Blockchain-based Event Ticketing Application." 2019, (Presented at the 40th International Conference on Information Systems [ICIS 2019] at Munich)

Paarth Samdani, "Blockchain and its relevance in the field of Intellectual Property", ACIPR Bulletin Vol. I Issue 1., 2020, https://www.alliance.edu.in/uploads/pdf/ACIPR-Newsletter.pdf

Jacob Kastrenakes, Beeple sold an NFT for $60 million, THE VERGE, (Mar. 11, 2021), https://www.theverge.com/2021/3/11/22325054/beeple-christies-nft-sale-cost-everydays-69-million

Paarth Samdani
Student
Alliance School of Law

DATA PROTECTION, BIOMETRICS AND INTELLECTUAL PROPERTY LAW

Biometrics-based Artificial Intelligence (AI) technologies are on the rise. While the Intellectual Property (IP) potential for such developments is enormous, concerns about the usage of biometric data may arise in light of recently adopted and developing data privacy laws and regulations. The volume of data created by various electronic devices and apps has increased dramatically in recent years. Today's businesses receive enormous benefits from 'big data' analysis, and they also outline their business strategy based on it. Although the business efficiency is undeniable, the burning question is 'do individuals have any influence over how information about them is gathered and managed by others? The evolution of technology and the dynamism of the legal system provide insight into modern privacy and data security problems. As a result of technological advancement, privacy has become a worry for everyone, while data security has received less attention. Every data management programme must include Intellectual Property Rights (IPR) management. The creator of a database or other data resource will be interested in who owns it and how it might be used by others. Anyone who intends to use the tool with data provided in part by others should make sure that any legal, ethical, or professional obligations to the data supplier are honoured.

Biometrics data relates to physical characteristics of the human body or behavioural traits of human beings, according to the International Organization for Standardization (ISO), with "biometrics" referring to the "automated recognition of individuals based on their biological and behavioural characteristics." The phrase "biometric characteristic" refers to a "biological and behavioural characteristic of an individual from which distinctive, repeatable biometric features for biometric recognition can be retrieved." Fingerprints, DNA, face recognition, palm prints, iris recognition, hand geometry, retina, gait analysis, voice, body geometry, and other biometric data can be used to characterise an individual's human traits. Biometrics data, on the other hand, defines specific human features for each individual. As a result, biometrics data is highly individualised data that provides each person with a unique signature. Biometric data can now be used in a variety of security and personal identification applications. It also raises concerns about data privacy in light of new and evolving data privacy rules and regulations. Biometrics data is very useful for AI advancements. This is because AI is primarily a data-driven technology that uses unique information to train AI computer models for specific tasks. Biometric datasets from a variety of people could be gathered and utilised to train a biometric-centric AI model. Once trained, the biometric-centric AI computer model can use new data as input to forecast, categorise or generate output findings for use in a range of applications, including security choices.

Patents can give wide protection for AI technologies that use biometrics data in terms of intellectual property. Apple, for example, has dozens of patents covering its Face ID technology. A set of patent claims for a biometric-centric AI innovation may generally correlate to its workflow, which may comprise pre-processing gathered biometrics data, training an AI model with the pre-processed biometrics data, and employing the AI model to produce a security or identification result.

The Indian Copyright Act stipulates that infringements of intellectual property must be prosecuted regardless of the severity of the offence. According to Section 63B of the Indian Copyright Act, anyone who willfully uses an unauthorised copy of a computer programme on a computer faces a minimum of six months in prison and a maximum of three years in prison5. It's worth noting that Indian courts accept data as having copyright. It has been argued that collecting a list of clients/customers by investing time, resources, effort, and talents to the task constitutes "literary work" for which the author holds copyright under the Copyright Act. The balance between "data protection" and "intellectual property legislation" must be examined as the best approach to the functioning of computer-related databases. Anyone who is aware of an infringing copy of the programme on a computer is responsible for infringement under Section 63B of the Indian Copyright Act. The characteristics of 'effort, ability, and judgement' underpin an individual's claim to intellectual property.6 The preservation of the owner's right to that work is vital in the case of legislation on specific works of literature, fiction, music, art, and film. However, the Copyright Act makes it impossible to discern between data privacy and database security.

The government tabled the Personal Data Security Bill (DPB) in Parliament in December 2019 to create India's first cross-sectoral data protection regulatory structure. Rather than protecting the privacy of the information with a view to the possible harm of a violation of that privacy, the law attempts to protect the privacy of individuals through a protective mechanism governing the acquisition and use of information by corporations. It focuses on data use activity control in particular. The Committee, chaired by Justice B.N. Srikrishna, published research on the legislative structure for data security as well as Personal Data Protection Bill (2018). This model will allow the Indian economy to benefit from developments in personal data processing within a more precise and realistic framework for personal data protection. Only through a genuine cost-benefit analysis for India can a more complete and realistic regulatory framework be built. Data protection measures are desperately needed in India, and even if they are imperfect, they are preferable to no data protection regulations. This bill is a solid first step toward establishing explicit regulatory principles, and comprehensive laws and regulations should, in theory, continue to be properly balanced.

Ryan N. Phelam, Data Privacy Law and Intellectual Property Considerations for Biometric-Based AI Innovations, SECURITY MAGAZINE, (June,12, 2020, 10 AM), Data Privacy Law and Intellectual Property Considerations for Biometric-Baseed AI Innovations | 2020-06-12 | Security Magazine

Vinita Jindal, Implementing Information Security Using Multimodal Biometrics, Handbook of Research on Cyber Crime and Information Privacy, PP. 1-18, 2021.

Hazel Moir, Empirical Evidence on Patents and Data Protection, SSRN Electronic Journal, pp.1-135, 2016.

Vinita Jindal, Implementing Information Security Using Multimodal Biometrics, Handbook of Research on Cyber Crime and Information Privacy, PP. 1-18, 2021.

Daniel J. Gervais, Exploring the Interfaces Between Big Data and Intellectual Property Law, Journal of Intellectual Property, Information Technology and Electronic Commerce Law (JIPITEC) , 11-12, 2019.

Chanvi Gaur
Student
Alliance School of Law

THE ADVENT OF DATA PRIVACY IN INDIA

The resource that revolutionised the world post-industrial revolution was oil, however, in this era of technological revolution, it is often said that data has replaced oil to be the most valuable resource. Oil as a natural resource fuelled the industrial revolution but data is revolutionising society technologically and psychologically. Data is nothing but facts about an individual but these set of facts when collected from millions of users tends to show a pattern and behaviour, it creates a personality of the individual with the small packets of information provided by us through the usage of apps, consumption of content, browsing of the internet, reading of news, spending time over social media, types of entertainment resources and the most important our expenditure of money. The voluntary and involuntary sharing of our data has created enough digital footprints and information for these data aggregators to hurt our life and privacy. The threat is more real than ever.

The year 2017 was a historic year for our nation as privacy became indispendsible to the right to life as a fundamental right. This fumed the debate of data privacy and protection in India. The central government prepared a draft of the data protection bill in the year 2019 (yet to be passed) to cover the gaps in data protection in the country. Yes, we have arrived in the debate of data protection, but we are way behind most of the developed nations in the world, the first instance of data protection law can be traced back to Sweden in the year 1973 wherein they passed an act called "The Data Act" followed by Germany in the year 1977 wherein it passed federal legislation for the protection of data and privacy. These acts were passed due to the advent of the computer revolution in these developed democracies.

The European Union followed suit in the year 1995 by enacting a directive of data protection in the EU. In the year 2000, the European Union and the United States of America joined hands intending to regulate the data privacy laws and overcome the disparities in their respective jurisdiction. This was the infamous 'the Safe Harbor Accord' which granted unlimited access of EU data to US intelligence and was struck down. The very next year the gold standard of data protection laws in the world was enacted in the European union termed as General Data Protection Regulation or as popularly known as GDPR.

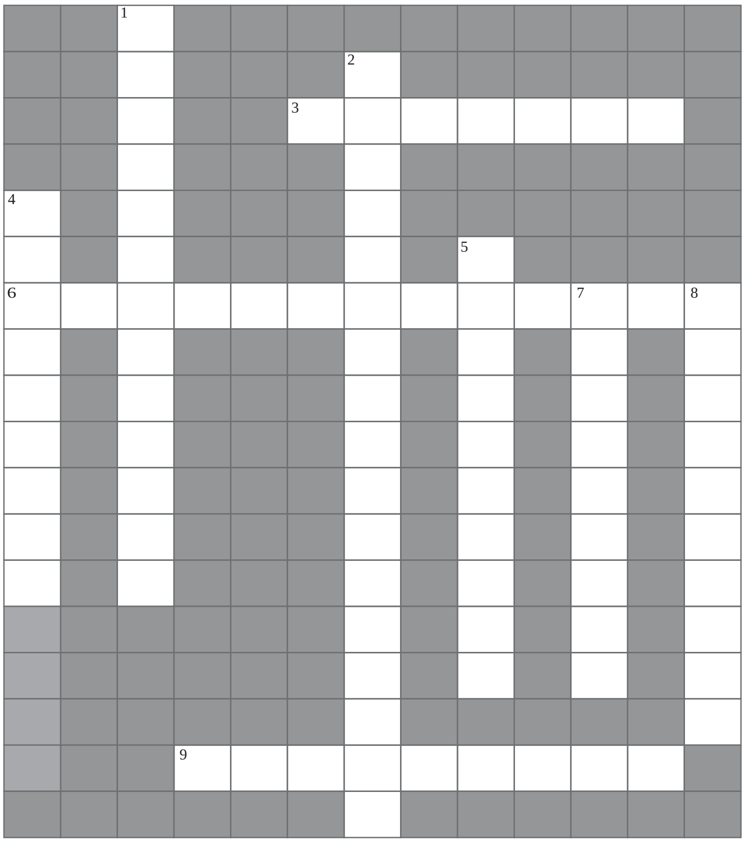
The Indian data protection bill of 2019 has many similarities with the GDPR of Europe. The legislator intends to narrow the trough between the Goliaths of technologies and the Davids, the common man. The authorities in India have recognised the need for and importance of data privacy in modern times. It is trying to tighten the noose on the free reign of the data mongers. The government has issued directives concerning localising the data and its maintenance in the Indian geographical location. This has been a steppingstone in the development of the data protection regime in India but we have miles to go to secure the right to privacy and ensure effective implementation of the data protection laws in Indian cyberspace.

KS Puttuswamy v Union of India, (2017) 10 SCC 1

Maximillian Schrems v Data Protection Commissioner, C-362/14, Court of Justice of the European Union (2015). It was struck down by the European Court of Justice in the year 2015.

Prof. Rohit Ranjan
Assistant Professor
Alliance School of Law

TRIVIA



Across:

3 The first criteria for patentability

6 Which is the first product that was given GI protection in India?

9 This protects the confidential information of a business or enterprise

Down:

1 Unauthorised and fake replicas of an original product

2 A type of statutory license that authorises a third party to make, use, or sell a patented invention without the permission of the patent holder

4 International treaty that deals with deposition of microorganisms with regards to patent protection

5 A relief that is available in suits of patent infringement

7 The IP right that protects the brand logos

8 The whole or partial transfer of an IP right by the holder to another person

QUIZ

1) Which IP right Protects software and computer codes?
   a) Patents
   b) Copyrights
   c) Trade secrets
   d) Industrial designs

2) Which Statute or treaty extended the protection of Berne convention to cover computer codes?
   a) The Copyright Act 1957
   b) The Paris convention
   c) The Rome Convention
   d) The WIPO Copyright Treaty

3) When a software is developed for a particular hardware alone to give a technical result then which IP Right protects the same
   a) Copyright
   b) Patents
   c) Both a & b
   d) None of the above

4) Which licence allows copyrighted works available without restrictions by anyone while avoiding the complications of the assignment or compatibility with other licenses?
   a) Statutory license
   b) Compulsory license
   c) Public Domain Dedication License
   d) Open Database license

5) Which section under the Indian Copyright Act renders a person liable who has mere awareness of an infringing copy of a program on a computer?
   a) S. 63 A
   b) S. 63 B
   c) S. 65
   d) S. 66

6) Big Data which is important for research and growing can be protected by which of the following?
   a) Copyrights
   b) Trade secrets
   c) Patents
   d) All of the above

7) Which of following has a broader coverage in terms of protection of IP rights?
   a) The Berne Convention
   b) The Paris convention
   c) The TRIPS agreement
   d) The Rome Convention

Answers:

Crossword - 1.Counterfeit | 2.Compulsory license | 3.Novelty | 4.Budapest | 5.Injunction | 6.Darjeeling tea | 7.Trademark | 8.Assignment | 9.Trade secrets

Quiz - 1.Copyrights | 2.The WIPO Copyright treaty | 3.Patents | 4.Public domain dedication license | 5.S. 63 B | 6.All of the above | 7.TRIPS agreement

ALLIANCE UNIVERSITY

Private University established in Karnataka State by Act No.34 of year 2010
Recognized by the University Grants Commission (UGC), New Delhi

Celebrating 25 YEARS OF ALLIANCE EDUCATION

ADMISSIONS OPEN 2022

QS I·GAUGE INDIAN UNIVERSITY RATING DIAMOND

Alliance University was appraised with Diamond Rating for Teaching, Employability and Facilities in the QS I·GAUGE rating system, 2019

nirf #39 Management Institution in India (including IIMs), 2020

Alliance University Awarded the QS I·GAUGE E-Learning Excellence for Academic Digitisation in 2020

Courses Offered

Alliance School of Business	Alliance College of Engineering and Design	Alliance School of Law	Alliance Ascent College
BBA (Hons.) B. Com. (Hons.) MBA Ph.D. in Management Executive PGDM	B. Tech. M. Tech. Ph.D. in Engineering and Sciences	B.A. LL.B. (Hons.) B.B.A. LL.B. (Hons.) LL. M. Ph.D. in Law	BBA B. Com. MBA

SALIENT FEATURES OF ALLIANCE UNIVERSITY

50+	50+	200+	400+	30000+
Acres of Lush Green Campus	Study-Abroad Options in Global Universities	World-Class Faculty from India and Abroad	Recruiting Partners in 2021	Global Alumni in 50+ Countries

ALLIANCE UNIVERSITY
Chikkahagade Cross, Chandapura - Anekal Main Road, Anekal, Bengaluru – 562 106
Phone: +91 96200 09825, +91 98860 02500,+91 80461 99000 / 9100 / 9200
Website: www.alliance.edu.in, E-mail: admissions@alliance.edu.in