ICFAI LAW SCHOOL HYDERABAD

CYBER Newsletter

A Bi-monthly Newsletter of
The Centre of Excellence in Cyber Law and Data Protection

Upcoming Events

- Webinars
- Guest Lectures

Events Organized

- Webinars
- Guest Lectures

Rankings

- ICFAI Law School, Hyderabad ranked 1st among the top ten Law Schools in India according to The Academic Insights, 2020.
- ICFAI Law School, Hyderabad ranked 1st among the Best Promising Law School in India - Higher Education Review 2018 & 2019.
- ICFAI Law School, Hyderabad ranked 2nd among Top Law Schools of Southern India - CSR GHRDC 2018.
- ICFAI Law School, Hyderabad is ranked 3rd among top law schools. – India Today

Editorial Board

Dr. Md Akbar Khan

Dr. P L Jayanthi Reddy

Dr. Vinay Sharma

Mr. Suryadevara Rakesh

Students

Center Coordinator's Message

In present world where there is a constant and steady development in the Artificial Intelligence (AI), a lot of software products and applications like Facebook, Google etc. have been developed in such a way that they not only take the personal data from the user but also use it for further processing and for different purposes. For which there is a need to create awareness in Cyber Law and Data Protection to govern all aspects of transactions and activities involving internet and cyberspace.

The Centre for Cyber Law and Data Protection Law was established and constituted in the year 2019 under the able supervision and guidance of Dr. A V Narsimha Rao, Director, ILS, IFHE, Hyderabad with the following objectives:

• To enhance the awareness about the ever-increasing cyber-crimes in the society and provide inputs to the students and general public about safe and efficient handling of the social media.

• To provide inputs to use of internet, mobile phones, ATM Cards and confidential information securely.

• To understand and enlighten the problems and critical issues that are emerging with the growth of information technology.

• To promote research in the area of cyber and data protection law and make suggestions for Cyber and Data Protection Policy, updating the existing laws.

• To arrange and organize the conferences, workshops, training and awareness programs for capacity building of academic institutions, investigating agencies and knowledge bank.

• To develop technically skilled manpower in the area of cyber law and Cyber forensics.

• To arrange the frequent interactions of students and faculty with the cyber computer forensic experts and cyber-crime investigators.

• To arrange the quiz and essay writing competitions to the students and working groups to highlight the problems that are cropping up in the area of cyber-crimes and data protections.

• To encourage the research scholar to undertake their research on the topics of 'social media and infringement of rights' etc.

• To undertake minor and major projects in the area of Cyber law and Data Protection. To organize the Hackathons to promote the creative idea generations and grounding the start-ups in the area of Cyber law and Data Protection.

Recent Events

1. **Webinar on "Cyber Crime Investigation: Forensic Stratagems" on July 27th, 2020.**

   Speakers
   • Ms. Anjana. K, Cyber Forensic Scientific Officer, Telangana State, Forensic Science Laboratory, Hyderabad

   About the event:

   The speaker in her presentations spoke on cyber forensics, procedures and practices and the need for Laws in the area through which forensic issues could be resolved. There was also emphasis on the practical issues in the transfer of technology and a look at the other areas in which cyber forensics could be used to detect crimes and cybercrimes in particular during and post COVID-19.

2. **Webinar on "Artificial Intelligence: A conceptual contour" on July 31st, 2020**

   Speakers

   - Dr. Atul Negi, Professor of Computer and Information Science, University of Hyderabad
   - Mr. Raghu Boddu, Global Director, SAP Innovation and Automation, Toggle now Software Solutions Pvt.Ltd.
   - Professor A.V. Narsimha Rao, Director, ICFAI Law School, Hyderabad.

   About the event:

   The Speakers in their presentation spoke on the need and importance of Artificial Intelligence in the modern society. They also stressed on the need to improve the knowledge and reasoning models available for representing the diversity of the human intelligence process and there was hybridization of knowledge based reasoning with AI especially in the field of Decision Support Systems.

3. **Webinar on "Hacking and Network Intrusions: Techno-Legal Formulations" on August 9th ,2020**

   Speakers

   - Mr. U. Ram Mohan, SP(CID), Government of Andhra Pradesh
   - Mr. Ashok Ram Kumar, Senior IPR Attorney
   - Mr. Neeraj Arora, Advocate, Supreme Court of India

   About the event:

   The speakers stressed on the role of network security as a specialized field consisting of the provisions and policies to prevent and monitor unauthorized access, misuse, modification, or denial of a computer network and network-accessible resources as well as ensuring their availability through proper procedures. Many security devices are being developed and deployed to defend against cyber threats mainly due to network and to prevent unintended data breaches. In spite of all these efforts, the 'golden age' of cybercrime continues, as organizations around the world continue to suffer data breaches and security attacks on a regular basis.

4. **Webinar on "Data Protection and Cyber Laws in India", 17th December 2020.**

Speaker:

- Dr. A. Nagarathna, Associate Professor, NLSIU, Bangalore.

About the event:

The speaker talked about the provisions regarding protection of data, privacy of information, breach of data resulting in damages and compensation that are incorporated in IT, Act, 2000.

Case Law

Justice K.S. Puttaswamy (Retd) v. Union of India, (2017) 10 SCC 1

The nine-judge bench of the Supreme Court has unanimously delivered its judgment "Right to privacy is a part of the right to "life" and "personal liberty" enshrined under Article 21 of the Constitution but the said right is not an absolute right and it can be curtailed according to procedure established by law."

Consequential orders-

The requirement to mandatorily link Aadhaar numbers to PAN was held to be valid, since it was based on a law, serving a legitimate state interest and was proportionate.

The requirement to mandatorily link Aadhaar numbers to bank account numbers was held not to be valid since it did not meet the proportionality test.

The requirement to mandatorily link Aadhaar numbers to mobile numbers was held not to be valid since it did not serve a legitimate state aim and was disproportionate in its encroachment on individual liberties.

DATA LOCALISATION- A PARADIGM NEED FOR LAWS

Governments around the world have been trying to make a case that there should be data localization, so that local laws may apply, but this is proving elusive in the absence of cross-border enforceable legal agreements. Data residency and its localization refer to the physical or geographic location of an organization's data or information. The data of a company in India may be stored in a server that may be based out of say Europe or the Americas then the laws of India might not apply. If data is adjudged by an Indian court to be of critical or perverse evidence, then the data stored in that server may turn out be an important exhibit in that particular case. The company which maintains the data has to isolate the same within the server which it feels as critical evidence and "seal" the same electronically and the company which owns the server may not be ready to maintain and seal the data to be presented as evidence for a case in India.

In a world where data portability has moved into a space of copying and transferring personal data it has become imperative that companies and Governments do not compromise on the security of data. The

caveat in the Indian cyberspace has always been that such a data has been gathered from the user with or without his consent

There is a need to look into the legal framework of secure storage and secure portability of data. There is a need for Data Localization so that whenever the user wants to have permanent deletion of his data that facility should be given to him by making the data localization laws more stringent and available in the parent country and not in other places.

In view of this there is a need to understand and make the right moves on Data Localization and data Security by the Government enacting new laws so that the citizens at large in India do not have to seek different means of protecting their privacy. It is also to be seen in the context of the Government to enact the Data Protection Bill, 2019 so that the intent is shown with regard to data protection and localization.

 NEW MALWARE FOR SEARCH ENGINES- THE UNDERSTANDING AND SOLUTION

Google Chrome, Firefox, Microsoft Edge and Yandex have become the latest targets of an ongoing malware campaign, dubbed Adrozek, as revealed by Microsoft. The malware injects ads into search results and adds malicious browser extensions. The company claims that this virus has been at scale since at least May, with the attacks peaking in August, with the threat being noticed on more than 30,000 devices every day.

The main goal for Adrozek is to lead people to affiliate pages. It is doing so by silently adding malicious browser extensions and changing the browser settings to insert ads into webpages. It is also modifying the Dynamic Link Library (DLL) files per target browser, for example, it is turning of MsEdge.dll on Microsoft Edge, which is basically turning off the security controls of the browser.

The Adrozek malware is distributed through drive-by download, experts saw 159 unique domains used to distribute hundreds of thousands of unique malware between May and September 2020. Attackers relied heavily on polymorphism to evade detection.

Microsoft claims, Adrozek is in high concentration in Europe, South Asia and Southeast Asia, as of now. It could soon expand to other geographies soon.

The company recommends that users should use an antivirus solution like Microsoft Defender, which has endpoint protection and can block malware families.

MoU with Cyber Security Centre of Excellence:

We are pleased to inform that our Centre for Excellence at ILS, IFHE, Hyderabad has entered MoU with the 'Cyber Security Centre of Excellence', a joint venture of the Data Security Council of India and Government of Telangana.

The Cybersecurity Centre of Excellence (CCoE) is a glocal hub based in Hyderabad to catalyze innovation, entrepreneurship and capability building in cybersecurity and privacy. It is a joint initiative of the Government of Telangana and DSCI setup to fulfil DSCI's commitment towards creating a safe, secure and a trusted cyberspace. The objective is to build best practices, standards and execute initiatives in cybersecurity and privacy domain. It nurtures a culture of innovation by, incubating start-ups, conducting trainings/workshops/events, showcasing products in experience zone, hosting delegations and collaborating in local, national and international initiatives.

Comments

Data Protection Principles

The Supreme Court categorically recognized certain data protection principles such as Data-minimization, purpose limitation, data retention and data security as relevant factors in determining whether the provisions of particular legislation, including the Aadhaar Act, was in conformity with an individual's right to privacy.

Data Protection Legislation

The Right to Privacy declared as fundamental right by the Supreme Court has resulted and paved way for Personal Data Protection issues and the related harm that may be caused to the individual owing to its public disclosure.

Therefore, it is high time for the legislature to convert the Personal Data Protection Bill, 2019 into a full-fledged and comprehensive Act with the incorporation of relevant and compatible provisions adopted from GDPR and Personal Data Protection Bill, 2018.