INTERNATIONAL JOURNAL OF DIGITAL LAW – IJDL
ano 01 · n. 01 · janeiro/abril 2020 - Publicação quadrimestral
DOI: 10.47975/digital.law.vol.1.n.1
01
ISSN 2675-7087

# IJDL

# International Journal of DIGITAL LAW

NUPED
Núcleo de Pesquisas em Políticas Públicas e Desenvolvimento Humano da PUCPR

FORUM

# IJDL – INTERNATIONAL JOURNAL OF DIGITAL LAW






Luís Cláudio Rodrigues Ferreira
Presidente e Editor

Av. Afonso Pena, 2770 – 15º andar – Savassi – CEP 30130-012 – Belo Horizonte/MG – Brasil – Tel.: 0800 704 3737
www.editoraforum.com.br / E-mail: editoraforum@editoraforum.com.br

Impressa no Brasil / Printed in Brazil / Distribuída em todo o Território Nacional





IN61 International Journal of Digital Law – IJDL. – ano 1, n. 1 (abr. 2020) –.– Belo Horizonte: Fórum, 2020-.

Quadrimestral; Publicação eletrônica
ISSN: 2675-7087

1. Direito. 2. Direito Digital. 3.Teoria do Direito. I. Fórum.

CDD: 340.0285
CDU: 34.004

Coordenação editorial: Leonardo Eustáquio Siqueira Araújo
Aline Sobreira
Capa: Igor Jamur
Projeto gráfico: Walter Santos

DOI: 10.47975/IJDL/1nagarathna

# Cybercrime regulation through laws and strategies: a glimpse into the Indian experience

## *Regulamentação do crime cibernético por meio de leis e estratégias: um vislumbre da experiência indiana*

**Annappa Nagarathna***
India University (Bangaluru, Karnataka, India)
nagarathna@nls.ac.in
https://orcid.org/0000-0001-8874-508X

**Recebido/Received:** 02.03.2020/ March 2nd, 2020
**Aprovado/Approved:** 21.04.2020/ April 21st, 2020

**Abstract:** Cybercrimes in India are increasing at an alarming rate. Though various legal provisions under the conventional criminal laws including form the Indian Penal Code, could be used to regulate the cybercrimes, yet the changing nature of these crimes necessitated adoption of a new law framework. Thus, the Indian Information Technology Act was enacted in 2000 but seldom could regulate cybercrimes since it focused on promoting and facilitating e-commerce and e-governance. This Act underwent amendment in 2008 to accommodate provisions essential to regulate cybercrimes as well as protect data and privacy on cyber space. In addition to the law, other strategies were designed and adopted to better regulate cyber offences including announcing cyber security policies, constituting institutions to take care of certain concerns including those relating to critical infrastructure information, etc. This paper aims to provide an overview of the approach adopted in India primarily the legal approach adopted to regulate cybercrimes. Additionally, other strategies adopted by India is also reviewed in brief. Despite these, since cybercrimes are technical as well as dynamic in nature, there is a need to constantly review and revise nation's strategies, which is also one of the objects of this paper.

**Keywords:** Cybercrime. India. Strategy. IT Act. Challenges.

**Resumo:** Os crimes cibernéticos na Índia estão aumentando a uma taxa alarmante. Embora várias disposições legais sob as leis criminais convencionais, incluindo o Código Penal Indiano, pudessem ser usadas para regular os crimes cibernéticos, a natureza mutável desses crimes exigia a adoção

Como citar este artigo/*How to cite this article*: NAGARATHNA, Annappa. Cyber crime regulation through laws and strategies: a glimpse into the Indian experience. *International Journal of Digital Law*, Belo Horizonte, ano 1, n. 1, p. 53-64, jan./abr. 2020.

* Doctor, Associate Professor & Chief Coordinator, Advanced Centre on Research, Development and Training in Cyber Laws & Forensics, National Law School of India University (Bangaluru, Karnataka, India).

de uma nova estrutura legal. Portanto, a Lei de Tecnologia da Informação da Índia foi promulgada em 2000, mas raramente poderia regular os crimes cibernéticos, uma vez que se concentrava na promoção e facilitação do comércio eletrônico e da governança eletrônica. Esta lei foi alterada em 2008 para acomodar as disposições essenciais para regulamentar os crimes cibernéticos, bem como proteger os dados e a privacidade no espaço cibernético. Além da lei, outras estratégias foram elaboradas e adotadas para melhor regulamentar os crimes cibernéticos, incluindo o anúncio de políticas de segurança cibernética, constituindo instituições para cuidar de certas questões, incluindo aquelas relacionadas a informações de infraestrutura crítica, etc. Este artigo tem como objetivo fornecer uma visão geral da abordagem adotada na Índia, principalmente a adotada para regular os crimes cibernéticos. Além disso, outras estratégias adotadas pela Índia também são revistas brevemente. Apesar disso, uma vez que os crimes cibernéticos são de natureza técnica e também dinâmica, é necessário revisar e revisar constantemente as estratégias do país, o que também é um dos objetos deste artigo.

**Palavras-chave:** Cybercrime. Índia. Estratégia. Lei de TI. Desafios.



## 1 Introduction

As dependence on cyber technology is fast expanding, so it the abuse of it, leading to increase in the number of cybercrimes across the world. Cybercrimes today pose a challenge to State's administration of justice. Additionally, cybercrime is also changing its form day by day thereby necessitating a stronger and an updated law framework. India, like other nations, too is striving to better combat cybercrimes.

> There is a greater dependence on digital payment platform due to reduced cash handling and greater data sharing is happening online and presence on social media have also increased. While we are able to manage our affairs online to a certain extent, malicious actors also found in it, a new opportunity. Shri. Ajith Doval, India's National Security Adviser.[1]

Dependence on this technology though indicates its advantage yet increase its abuse has always been a concern for nations. In India, from 2012 to 2018, there were over 90 thousand cybercrime incidents registered across the country, out of which, over 27 thousand cases were registered in 2018 alone, marking an increase of more than 121 percent since 2016.[2] According to the Federal Bureau of Investigation's Internet Crime Compliant Centre [ICS], India is the third country to be victimised with cybercrimes.[3]

1 THE WIRE...
2 KEELERY, Sandhya...
3 Report on Internet Crime for 2019, quoted by: PINTO, Deepak...

## 2 Indian law framework

While Indian conventional criminals' laws, most importantly, the Indian Penal Code of 1860 could to an extent regulate cybercrimes, but new forms of crimes committed through this novel technology could not be comprehensively and effectively dealt with under the then existing law. On the other hand, expansion of usage of cyber technology for commercial and governance related transactions, necessitated enacting a law specifically to deal with issues that arose with such use as well as abuse of cyber technology. Government of India hence in 2000 enacted its first cyber legislation, the Information Technology Act of 2000.

Indian Information Technology Act of 2000[4] primarily focused on promotion of e-commerce and e-governance. For this, the law provided legal recognition to electronic documents, electronic contracts, and digital signatures. This original Act hardly had focused on regulating cybercrimes and it had very few provisions through which some forms of cybercrimes could be regulated. Such cybercrimes included hacking, alternation or deletion of computer source code and cyber pornography. No specific provisions then existed to deal with offences such as phishing, malware attacks, etc. This 2000 Act also did not specifically recognise other crucial concerns such as offences affecting data and privacy protection, child's online protection, etc. Further abuse of cyber technology for terrorist and other extremist's activities was also not taken care of.

In 2008, the Indian Information Technology Act underwent extensive changes vide Information Technology Amendment Act, thereby becoming more a comprehensive law than before. The 2008 Act specifically deals with various forms of cybercrimes. Certain provisions thereunder are so worded that it facilitates wider legal interpretation so as to cover under its ambit wide variety and forms of cybercrimes, though some are not expressly named.

### 2.1 Cyber crimes and Information Technology Act 2000

The current Information Technology Act vide its 2008 Amendment deals with various forms of cybercrimes. Section 66 read with Section 43 recognises following as offences:1) Hacking and unauthorised access, that is, accessing or securing access to any computer, computer system or computer network or computer resource; 2) Data stealing – by way of downloading, coping or extracting any data, computer data base or information from a computer, computer system or computer network including information or data held or stored in any removable storage medium; 3) Malware or Virus and worm attacks – committed by way of introducing or causing to be introduced any computer contaminant or computer virus

[4] Henceforth referred to as IT Act, 2000.

into any computer, computer system or computer network; 4) Data diddling or data destruction or destruction of a computer system, that is causing any damage to any computer, computer system or computer network, data, computer data base or any other programmes residing in such computer, computer system or computer network; 6) Causing disruption to the working of any computer, computer system or computer network; 7) Denial of service attacks or Distributed denial of Service Attacks or any other offences due to which a person is denied of his access to a computer, computer system or computer network, which is wide even to include ransom ware attacks; 8) Abetting a person to hack a system, by way of providing him assistance to access any computer, computer system or computer network; 9) Charging illegally to a person, for the services availed by another by way of tampering or manipulating any computer, computer system, or computer network; 10) Destroying, deleting or altering of any information residing in a computer resource; 11) Doing any act which diminishes the value or utility of information residing in a computer or doing any act with which such information is affected injuriously; 12) Stealing or concealing or destroying or altering directly or through another any computer source code used for a computer resource with an intention to cause damage.

It is important to note that the above offences are dealt with under Section 43 as civil wrongs and as "criminal offences" under Section 66, provided they are committed with 'fraudulent' or 'dishonest' intention. Section 65 of the IT Act criminalises acts of knowingly or intentionally concealing, destroying or altering any computer source code used for a computer, computer programme, computer system or computer network provided such computer source code is required to be kept or maintained by law for the time being in force. This provision can also be extended to acts of its abetment. Section 66B criminalises dishonest receiving or retaining of any stolen computer resource or communication device. Hence procuring stolen computers and communication devices as well as pirated software programmes can be dealt with under this provision.

Impersonation or Identity theft on cyber space is dealt with under Section 66C according to which this offence is said to be committed when a person fraudulently or dishonestly makes use of another person's electronic signature, password or any other unique identification feature. Further, cheating by personation on cyber space can be regulated through Section 66D of the IT Act, according to which if a person by using any communication device or a computer resource, cheats by personation can be punished with criminal sanctions.

## 2.2 Crimes against women and children

Indian IT Act also aims to regulate cybercrimes committed against women and children. Section 66E deals with voyeurism. According to this provision, criminal

liability is imposed upon a person who intentionally or knowingly captures, publishes or transmits the image of a private area of any person without his or her consent, under circumstances violating the privacy of that person. This section however is not just limited to protecting women as it's a gender-neutral provision. Parallel to this, Section 354C of the Indian Penal Code specifically protects women against the offence of voyeurism. According to this provision, any man who watches or captures the image of a woman engaging in a private act in circumstances where she is expecting of not being observed either by the accused or any other person, at the behest of the accused commits the offence of voyeurism. The offence is also committed when a person disseminates such images or contents.

According to Section 67, publication or transmission of "any material which is lascivious or appeals to the prurient interest or if its effect is such as to tend to deprave and corrupt persons who are likely, having regard to all relevant circumstances, to read, see or hear the matter contained or embodied in it" in an electronic form constitutes to be the offence of Cyber obscenity. Further according to Section 67A publication or transmission of "any material which contains sexually explicit act or conduct" amounts to be an offence of cyber pornography.

Child pornography is dealt with under Section 67B. According to this provision, Child pornography includes the following: (a) publication or transmission of any material in any electronic form which depicts children engaged in sexually explicit act or conduct; (b) act of creating text or digital images, collecting, seeking, browsing, downloading, advertising, promoting, exchanging or distributing any material in electronic form and depicting children in obscene or indecent or sexually explicit manner; or (c) cultivating, enticing or inducing children into online relationship with one or more children for and on sexually explicit act or in a manner that may offend a reasonable adult on the computer resource; or (d) facilitating online abuse of children or (e) Recording in any electronic form one's own abuse or that of others pertaining to sexually explicit act with children.

In addition to the IT Act, the Protection of Children from Sexual Offences Act of 2012 also deals with online abuse of children. According to Section 11, Sexual harassment includes uttering any word or making any sound, or making any gesture or exhibiting any object or part of body with the intention that such word or sound shall be heard, or such gesture or object or part of body shall be seen by the child; or making a child exhibit his body or any part of his body so as it is seen by such person or any other person; or showing shows any object to a child in any form or media for pornographic purposes; or repeatedly or constantly follows or watches or contacts a child either directly or through electronic, digital or any other means or threatening threatens to use, in any form of media, a real or fabricated depiction through electronic, film or digital or any other mode, of any part of the body of the

child or the involvement of the child in a sexual act; or enticing a child for pornographic purposes or gives gratification therefor. The acts included under this provision even if committed on cyber space or through the usage of cyber technology, can be dealt with under this provision.

According to Section 13 using a child for pornographic purposes includes using a child in any form of media (counting programme or advertisement telecast by TV canals or internet or any other electric form or printed form, whether or not such programme or commercial is intended for personal use or for distribution), for the purposes of sexual gratification, which includes: (a) representation of the sexual organs of a child; (b) usage of a child engaged in real or imitation sexual acts (with or without penetration); (c) the indecent or obscene representation of a child.

Using a child or children for pornographic purposes is specifically punished under Section 14. Section 15 makes the law more comprehensive by addressing issues such as possession of child pornographic material. According to this provision, storing or possessing any pornographic material in any form involving a child and failing to delete or destroy or report the same to the designated authority is an offence, if it is done with an intention to share or transmit such child porn material. Further, if a person stores or possesses pornographic material in any form involving a child for transmitting or propagating or displaying or distributing in any manner at any time unless it is for the purpose of reporting or using as evidence in court, can also be punished under this provision. In addition, if a person stores or possesses pornographic material in any form involving a child for commercial purpose is also made punishable under this provision.

Procedurally this Act provides for provisions that are child friendly and also facilitate easier prosecution by way of providing presumption-based liability in certain cases. While section 29[5] reduces prosecution's burden of proof by providing presumption of men's rea in cases falling under Section 3, 5, 7 and 9 of the Act, Section 30 also provides for presumption of existence of state of mental state for commission of offences that culpable mental state. In the latter case, the burden is rather shifted upon the accused to rebut such presumption, by way of proving that he had no such mental state. Even though these provisions of imposing liability based on presumption have come under criticism, it continues to currently exist in the law framework.

Amendments made to Indian Penal Code in 2013 have added few provisions that aim at regulating some forms of cybercrimes committed against women. As

[5] According to this provision – "Where a person is prosecuted for committing or abetting or attempting to commit any offence under sections 3, 5, 7 and section 9 of this Act, the Special Court shall presume, that such person has committed or abetted or attempted to commit the offence, as the case may be unless the contrary is proved".

earlier mentioned, section 354C deals with voyeurism. Section 354A which deals with the offence of sexual harassment, includes under its ambit the offence of "showing pornography against the will of a woman" and "making sexually coloured remarks" and these committed on cyber space can also be dealt with under this provision. Cyber stalking to an extent is dealt with under Section 354D of the Code, according to which if a person "monitors the use by a woman of the internet, email or any other form of electronic communication" can be punished for the offence of stalking. Further according to Section 509, IPC, if a person with the intention to insult the modesty of a women, utters any words, makes any sound or gesture or exhibits any object, intending that such word or sound be heard or that such gesture or object shall be seen by such women, or intrudes upon the privacy of such women, can be held liable for causing 'insult to the modesty of a women".

Apart from widening the law framework, the Government of India also taken additional measures to check cybercrimes committed against women and children. In order to facilitate filing of a Complaint of cybercrimes, especially anonymously, the Government of India has launched a National Cyber Crime Reporting Portal that 'caters to complaints pertaining to cybercrimes only with special focus on cyber-crimes against women and children.[6]

## 2.3 Cyber Crimes against security of state

Offences against State such as cyber terrorism, cyber warfare and offences on critical infrastructure are also dealt with under the Act to an extent. Section 66F of the Act defines cyber terrorism quite widely. According to the provision, a person can be charged with the offence of cyber terrorism if he with an intention to "threaten the unity, integrity, security or sovereignty of India" or in order to "strike terror in the people or any section of the people" does any act and thereby: (a) denies or cause the denial of access to any person authorised to access computer resource; or (b) attempts to penetrate or access a computer resource without authorisation or exceeding authorised access; or (c) introduces or causes to introduce any computer contaminant and by means of such conduct, "causes or is likely to cause death or injuries to persons or damage to or destruction of property or disrupts or knowing that it is likely to cause damage or disruption of supplies or services essential to the life of the community or adversely affect the critical information infrastructure".

A person can also be charged with the offence of cyber terrorism if he knowingly or intentionally "penetrates or accesses a computer resource without authorisation or exceeding authorised access, and by means of such conduct obtains access to

[6] INDIA. Ministry of Information and Broadcasting. *News*. Available at: https://cybercrime.gov.in/

information, data or computer data base that is restricted for reasons of the security of the State or foreign relations; or any restricted information, data or computer data base, with reasons to believe that such information, data or computer data base so obtained may be used to cause or likely to cause injury to the interests of the sovereignty and integrity of India, the security of the State, friendly relations with foreign States, public order, decency or morality, or in relation to contempt of court, defamation or incitement to an offence, or to the advantage of any foreign nation, group of individuals or otherwise".[7]

Section 70 of the Act defines a protected system as the one declared to be so by the appropriate Government, that is, Central or State government, through a notification in the Official Gazette, provided such computer resource is the one which can directly or indirectly affects the facility of Critical Information Infrastructure. The same provision also clarifies that the "Critical Information Infrastructure" means the computer resource, the incapacitation or destruction of which, shall have debilitating impact on national security, economy, public health or safety.

Government of India has laid down the Information Technology (National Critical Information Infrastructure Protection Centre and Manner of Performing Functions and Duties) Rules, 2013.[8] Government has constituted the National Critical Information Infrastructure Protection Centre (NCIIPC) to take care of the Critical Information Infrastructure Protection. The Centre is the National Nodal Agency in relation to this infrastructure protection and aims to provide "all necessary measures to facilitate protection of Critical Information Infrastructure, from unauthorized access, modification, use, disclosure, disruption, incapacitation or distraction through coherent coordination, synergy and raising information security awareness among all stakeholders".[9] The NCIIPC has also issued guidelines for the Protection of National Critical Information Infrastructure.[10]

## 2.4 Offences relating to data and data privacy

Indian IT Act also deals with data protection to an extent. It apart from protecting data through section 43 and 66, also obligates stakeholders except government agencies, to protect personal and sensitive data. According to Section 43A and rules[11] laid thereunder, non-compliance to these rules and breach of personal data

7 Section 66F of IT Act.

8 INDIA. Ministry of Communications and Information Technology. Department of Information Technology. *Public Opinion and Public Grievances*. Available at: http://meity.gov.in/sites/upload_files/dit/files/GSR19(E).pdf.

9 NATIONAL CRITICAL INFORMATION INFRASTRUCTURE PROTECTION CENTRE...

10 INDIA. National Critical Information Infrastructure Protection Centre...

11 INDIA. Ministry of Communications and Information Technology...

privacy leading to wrongful loss or wrongful gain can lead to imposition of civil liability upon such stakeholder. However a new law called Personal Data Protection Bill, is underway and it aims to extend clearer and wider protection to data privacy in the country.[12] Since the Supreme Court of India in the case of Justice K S Puttaswamy (Retd.) v. Union of India[13] apart from reiterating that the right to privacy is integral to right to life has also specifically recognised information privacy, that is, data privacy as a part of right to privacy. Hence the Bill intends to extend wider protection to data privacy.

## 3 Other legal aspects dealt with under IT Act

IT Act imposes liability for abetment and attempt to commit cybercrimes under Section 84B and 84C respectively. Additionally if the offence is committed by a company, corporate liability is imposed under Section 85 upon both the company as well as officers running the affairs of such company unless it is shown that such offence was committed without their knowledge and despite their adherence to due diligence. Further an internet intermediary can also be held liable for wrongs committed on their platform provided such intermediary is involved in commission of such offence. However, if such offences are committed by a third party, an internet intermediary cannot be held liable for such offences committed without their knowledge and despite their compliance to due diligence.[14]

## 4 Challenges affecting implementation of laws in India

Cyber-crimes are largely technical in nature. Conventional police officer often finds it difficult to deal with digital crimes and digital evidence. Law enforcement agencies hence require continuous training on both legal as well as technical aspects. Since these crimes also involve digital evidence it is important to utilise digital forensics process in the course of investigation and at time during its trial process.

Establishing jurisdiction for crimes committed by a foreigner or from a foreign country becomes complicated due to clash of jurisdictions. Unless a regional or international convention or multilateral or bilateral agreements are in place it becomes difficult to investigate as well as try such cases. Currently the legal procedure to be complied for collection of evidence from abroad should be as per conventional criminal procedural rules, prescribed by Criminal Procedure Code.

12 See for the copy of bill: INDIA. Ministry of Communications and Information Technology...
13 INDIA. Supreme Court of India. *Judgement, 24 Aug...*
14 Section 79, IT Act.

This often fails to take note of the specific concerns in relation to cyber space, cybercrimes, and digital evidence.

Lack of cooperation by internet intermediaries has often posed a challenge to effective investigation of cybercrimes. Since most of the intermediaries are based in abroad, procuring evidences and essential information on time becomes difficult. The Supreme

Court of India in the case of Re Prajwal a Letter dated 18.2.2015[15] which was a Public interest litigation relating to online abuse of children, directed the Government and internet intermediaries including Facebook, WhatsApp, Google, Microsoft, etc., to "remove the videos of rape, gang rape and child pornography from the internet."[16] Such an approach lacks in relation to other cybercrimes.

Often cyber space is used to spread unwanted and false propaganda, sometimes even leading to incidences of mob violence, mob lynching, disturbance to law and order and also at times affecting communal harmony. India Spend, a data journalism outlet, pegs the figure at 33 killed in 69 incidents of mob violence between January 2017 and July 2018.[17]

It may be noted that during the covid-19 epidemic situation, false messages sent in its regard created huge a concern for the state to address. The Supreme Court of India had raised this concern in the case of A lakh Alok Srivastava v. Union of India[18] by stating: "Panic was created by some fake news that the lock down would last for more than three months……. A further direction was sought to prevent fake and inaccurate reporting whether intended or not, either by electronic print or social media which will cause panic in the society…. It is therefore not possible for us to overlook this menace of fake news either by electronic, print or social media".[19] Currently Indian IT Act lacks specific provision to deal with such abuse of technology, though some provisions of the Indian Penal Code may be used in such cases by giving wider interpretation so as to extend it to cyber space.

Government of India announces its first national cyber security policy in 2013. The policy recognises a need "to build a secure and resilient cyberspace for citizens, businesses and Government" as the vision of the nation and this policy.[20] It lays down various strategies including those essential to create a cyber secured ecosystem. The government has recently announced the draft of the new Cyber

---

15 INDIA. Supreme Court of India. *The Registrar*...

16 DHAMIJA, Alabhya...

17 MCLAUGHLIN, Timothy...

18 MCLAUGHLIN, Timothy...

19 INDIA. Ministry of Information and Broadcasting. *News*. Available at: https://mib.gov.in/sites/default/files/OM%20dt.1.4.2020%20along%20with%20Supreme%20Court%20Judgement%20copy.pdf.

20 INDIA. Ministry of Communications and Information Technology. Department of Information Technology. *National Cyber Security Policy - 2013*...

Security Policy [in 2020] which recognises the need to "ensure a safe, secure, trusted, resilient and vibrant cyber space for our Nation's prosperity" as its vision.[21]

## 5 Conclusion

India like many other countries is striving to combat cybercrimes with laws, policies, and other strategies. However, unless challenges of jurisdiction, non-cooperation of intermediaries, complexities caused due to technical nature of the offence is effectively resolved with effective implement of these laws, policies and strategies can't be ensured. Like other nations, India is moving towards making its approach a more comprehensive and effective.

## References

DHAMIJA, Alabhya. *SC Directs Govt, Facebook, WhatsApp, Google to remove child porn, rape videos.* Available at: https://tilakmarg.com/news/sc-directs-govt-facebook-whatsapp-google-to-remove-child-porn-rape-videos/.

INDIA. Ministry of Communications and Information Technology. Department of Information Technology. *Public Opinion and Public Grievances.* Available at: http://meity.gov.in/sites/upload_files/dit/files/GSR_19 (E).pdf.

INDIA. Ministry of Communications and Information Technology. Department of Information Technology. *National Cyber Security Policy - 2013.* Available at: https://www.meity.gov.in/writereaddata/files/downloads/National_cyber_security_policy-2013%281%29.pdf.

INDIA. Ministry of Communications and Information Technology. Department of Information Technology. *Notification*. New Delhi, the 11th April 2011. Available at: https://www.meity.gov.in/writereaddata/files/GSR313E_10511%281%29_0.pdf.

INDIA. Ministry of Communications and Information Technology. Department of Information Technology. *The Personal Data Protection Bill,* 2018. Available at: https://www.meity.gov.in/writereaddata/files/Personal_Data_Protection_Bill,2018.pdf.

INDIA. Ministry of Information and Broadcasting. *News.* Available at: https://cybercrime.gov.in/.

INDIA. Ministry of Information and Broadcasting. *News.* Available at: https://mib.gov.in/sites/default/files/OM%20dt.1.4.2020%20along%20with%20Supreme%20Court%20Judgement%20copy.pdf.

INDIA. *National Critical Information Infrastructure Protection Centre.* Available at: https://nciipc.gov.in/documents/NCIIPC_Guidelines_V2.pdf.

INDIA. National Informatics Centre, Ministry of Electronics & IT. *National Cyber Security Strategy 2020 (NCSS 2020).* Available at: https://ncss2020.nic.in/.

INDIA. Supreme Court of India. *Judgement, 24 Aug.* 2017. Available at: https://main.sci.gov.in/supremecourt/2012/35071/35071_2012_Judgement_24-Aug-2017.pdf.

INDIA. Supreme Court of India. *The Registrar.* Available at: https://sci.gov.in/supremecourt/2015/6818/6818_2015_Order_22-Oct-2018.pdf.

[21] INDIA. National Informatics Centre, Ministry of Electronics & IT…

KEELERY, Sandhya. *Total number of cybercrimes reported in India 2018.* Available at: https://www.statista.com/statistics/309435/india-cyber-crime-it-act/#:~:text=Total%20number%20of%20cyber%20crimes%20reported%20in%20India%202018&text=From%202012%20to%202018%2C%20there,than%20121%20percent%20since%202016.

MCLAUGHLIN, Timothy. *How WhatsApp Fuels Fake News and Violence in India:* The messaging app owned by Facebook has become a major channel for hate speech and false stories in India. The government is demanding changes. Available at: https://www.wired.com/story/how-whatsapp-fuels-fake-news-and-violence-in-india/.

NATIONAL CRITICAL INFORMATION INFRASTRUCTURE PROTECTION CENTRE. *A unit of National Technical Research Organisation.* Available at: https://nciipc.gov.in/.

PINTO, Deepak. *India stands third among top 20 cybercrime victims.* FBI report. Available at: https://www.newindianexpress.com/nation/2020/feb/23/india-stands-third-among-top-20-cyber-crime-victims-says-fbi-report-2107309.html.

THE WIRE. *Financial Fraud Rising Because of More Digital Payments:* Ajit Doval. Available at: https://thewire.in/tech/financial-fraud-rising-because-of-more-digital-payments-ajit-doval.

Informação bibliográfica deste texto, conforme a NBR 6023:2018 da Associação Brasileira de Normas Técnicas (ABNT):

NAGARATHNA, Annappa. Cyber crime regulation through laws and strategies: a glimpse into the Indian experience. *International Journal of Digital Law*, Belo Horizonte, ano 1, n. 1, p. 53-64, jan./abr. 2020.

# Sumário
# *Contents*

# EDITORIAL Nº 1

É com satisfação que apresentamos à comunidade profissional e acadêmica o *International Journal of Digital Law*. Procuramos criar um periódico científico novo, com a pretensão de suprir uma lacuna que ainda é existente na tratativa do tema, tanto em nível local quanto global.

O *International Journal of Digital Law* consiste em periódico científico eletrônico de acesso aberto e periodicidade quadrimestral promovido pelo NUPED – Núcleo de Pesquisas em Políticas Públicas e Desenvolvimento Humano do Programa de Pós-Graduação em Direito da Pontifícia Universidade Católica do Paraná – um grupo de pesquisa filiado à REDAS – Rede de Pesquisa em Direito Administrativo Social.

A publicação foi encampada pela Editora Fórum, sem dúvida a mais renomada casa editorial do Direito Público brasileiro – o que por si só já é um atestado de qualidade conferido ao projeto.

O Conselho Editorial é composto por renomados juristas vinculados a instituições de ensino superior do Brasil, Argentina, Austrália, Colômbia, Espanha, Egito, França, Holanda e Índia. O enfoque da revista é o estudo crítico das instituições jurídico-políticas típicas do Estado de Direito, notadamente, as voltadas à inovação e ao desenvolvimento humano por intermédio da revolução digital. Agradecemos muito a franca disponibilidade dos professores que aceitaram compor tanto o Conselho Editorial quanto o Conselho Especial de Pareceristas.

O NUPED se insere na área de concentração do PPGD/PUCPR intitulada "Direito Econômico e Desenvolvimento". Por sua vez, a área congrega duas importantes linhas de pesquisa: 1. Estado, Economia e Desenvolvimento e 2. Direitos Sociais, Globalização e Desenvolvimento.

A revista irá dar destaque a este marco teórico. Entretanto, transversalmente ao tema da economia, do desenvolvimento, da globalização e dos direitos sociais, as palavras-chave que melhor definem o escopo da revista implicam a tratativa de temas como: acesso à informação, *Big data*, *Blockchain*, Cidades inteligentes, Contratos inteligentes, *Crowdsourcing*, Cibercrimes, Democracia digital, Direito à privacidade, Direitos fundamentais, *E-business*, Economia digital, Educação digital, Eficiência administrativa, *E-Government*, Ética, *Fake news*, *Gig economy*, Inclusão digital, Infraestrutura, Inovação, Inteligência artificial, Interesse público, Internet, Internet das coisas, Jurimetria, *Lawfare*, Novas tecnologias, Perfilamento digital, Pesquisa em multimeios, Processo administrativo eletrônico, Proteção de dados, Regulação administrativa, Regulação econômica, Risco, Serviços públicos,

Sistemas de informação, Sociedade da informação, Transparência governamental e Telecomunicações.

E o escopo da revista é, portanto, fortemente interdisciplinar e transdisciplinar. Espera-se que estudiosos dos mais diferentes campos de pesquisa possam enviar seus trabalhos, que serão muito bem recebidos, podendo ser escritos em português, inglês ou espanhol. Já neste primeiro número, além dos artigos dos pesquisadores brasileiros, temos textos oriundos de três diferentes países e continentes: Argentina, Espanha e Índia.

Os artigos passarão pelo sistema de avaliação em *doble blind peer review*. A ideia é que rapidamente o *International Journal of Digital Law* torne-se uma referência em termos de seriedade acadêmica e impactação na sociedade. Para isso, procuraremos nos enquadrar nas diretrizes das mais importantes bases de indexação nacionais e internacionais.

**Emerson Gabardo**
**Alexandre Godoy Dotta**
**Juan Gustavo Corvalán**

# EDITORIAL Nº 1

We are pleased to present the *International Journal of Digital Law* to the professional and academic community. We seek to create a new scientific journal, with the intention of filling a gap that still exists in dealing with the topic, both at the local and global levels.

The *International Journal of Digital Law* consists of an open-access electronic scientific journal and published every four months by NUPED – Center for Research in Public Policies and Human Development of the Postgraduate Law Program at the Pontifical Catholic University of Paraná – an affiliated research group to REDAS – Research Network in Welfare State Administrative Law.

The Editorial Board is composed of renowned professors linked to higher education institutions in Brazil, Argentina, Australia, Colombia, Spain, Egypt, France, and India. The journal's focus is the critical study of the legal-political institutions typical of the rule of law, notably those aimed at innovation and human development through the digital revolution. We are grateful for the frank availability of the professors who agreed to compose both the Editorial Board and the Special Peer Review Bord.

NUPED is part of the PPGD/PUCPR Concentration area entitled "Economic Law and Development". In turn, the area brings together two important lines of research: 1. State, Economy and Development and 2. Social Rights, Globalization and Development.

The magazine will highlight this theoretical framework. However, transversely to the theme of economics, development, globalization and social rights, the keywords that best define the scope of the magazine involve dealing with topics such as access to information, Big data, Blockchain, Smart Cities, Smart contracts, Crowdsourcing, Cybercrimes, Digital democracy, Right to privacy, Fundamental rights, E-business, Digital economy, Digital education, Administrative efficiency, E-Government, Fake News, Gig economy, Globalization, Digital inclusion, Infrastructure, Innovation, Artificial intelligence, Public interest, Internet, Internet of things, Jurimetrics, Lawfare, New technologies, Digital profiling, Multimedia research, Electronic administrative process, Data protection, Administrative regulation, Economic regulation, Risk, Public services, Information systems, Information society, Government transparency, and Telecommunications.

And the journal's scope is, therefore, strongly interdisciplinary and transdisciplinary. It is expected that scholars from the most different fields of research will be able to send their works, which will be very well received and can be written in Portuguese, English or Spanish. In this first issue, in addition to articles by

Brazilian researchers, we have texts from three different countries and continents: Argentina, Spain and India.

All articles will go through the evaluation system in double-blind peer review. The idea is that the *International Journal of Digital Law* will quickly become a reference in terms of academic seriousness and impact on society. For that, we will try to fit in the guidelines of the most important national and international indexing bases.

**Emerson Gabardo**
**Alexandre Godoy Dotta**
**Juan Gustavo Corvalán**