 ISSN: 2581-8503

WHITE BLACK LEGAL

LEGAL

VOLUME 1: ISSUE 8

||January 2020 ||

Email: editor@whiteblacklegal.co.in

Website: www.whiteblacklegal.co.in

 ISSN: 2581-8503

DISCLAIMER

EDITORIAL TEAM

 ISSN: 2581-8503

ABOUT US

WHITE BLACK LEGAL is an open access, peer-reviewed and refereed journal provide dedicated to express views on topical legal issues, thereby generating a cross current of ideas on emerging matters. This platform shall also ignite the initiative and desire of young law students to contribute in the field of law. The erudite response of legal luminaries shall be solicited to enable readers to explore challenges that lie before law makers, lawyers and the society at large, in the event of the ever changing social, economic and technological scenario.

With this thought, we hereby present to you

WHITE BLACK LEGAL: THE LAW JOURNAL

CYBER CRIMES AGAINST CHILDREN

Author: Joseph Ivan Michael

INTRODUCTION

'A digital India where cyber security becomes an integral part of national security' is one of the most important issue the legislature has to interfere in. The development of internet and other advanced technology have in many ways influenced the twenty first generation. It has sufficiently ensured to possess anything around the globe just with a touch of the hand. However, there are many threats influenced with this necessity evil. Today's children have become habitual victims of such abuses. The vulnerability and innocence of children are two important factors of being victims. Therefore, it is necessary that the legislature takes an active part to enforce the same. The paper ensures a promising approach inorder to protect the children from cyber bullying.

The case ***Ryan Halligon case of Vermot (2003)*** is the first ever that deals with cyber bullying. However, the judgement did not hold the accused guilty as the facts did not fall in the ambit of criminal law. However, the case classified cyber bullying into different kinds such as:

1) Humiliating the victim through any post
2) Sending vulgar and exploited content to the child
3) Acts of violence of threat of acts of violence
4) Invading in personal space – threatened calls or messages
5) Threat of child pornography

UNODC and CYBERCRIME AGAINST CHILDREN

UNODC recently published a Study on the Effects of New Technologies on the Abuse and Exploitation of Children. The document is based on open source research as well as the work of a UNODC Informal Expert Group Meeting on the subject, convened in Vienna in 2013.

This meeting brought together experts from international organizations, law enforcement, specialists on the subject and members of academia.A number of international legal instruments require States to take measures to protect children from abuse and exploitation, as well as engage in international cooperation in the investigation and prosecution of child abuse and exploitation crimes. A lack of consistent and appropriate legislation across countries globally, however, remains a major impediment to successful investigations and prosecutions. Individual states vary considerably in their definitions of child abuse andexploitation, and often cannot move fast enough to enact laws that keep pace with technology. To address these challenges, the Study covers the main forms of ICT-facilitated child abuse and exploitation, including the creation and distribution of child pornography, plus the commercial sexual exploitation of children, cyber-enticement, solicitation and grooming, cyber-bullying, cyber-harassment and cyber-stalking; as well as exposure to harmful content. This Study, one of UNODC's tools to help states prevent and combat cybercrime, is accompanied by a package of technical assistance which includes law enforcement and judicial training, activities for improved international cooperation and awareness raising tools.

1. Convention on the Rights of the Child

The Convention on the Rights of the Child11 (hereafter also referred to as "CRC") aims to ensure a wide range of human rights for children – including civil, cultural, economic, political, and social rights.

Article 1 of the CRC provides that "For the purposes of the present Convention, a child means every human being below the age of 18 years unless under the law applicable to the child, majority is attained earlier".

Article 34 of the CRC requires States Parties to take all appropriate measures to address the sexual exploitation and sexual abuse of children, including measures to prevent the exploitative use of children in pornographic performances and materials.

All of the 17 Asian countries analysed (Brunei Darussalam, 1995; Cambodia, 1992; China, 1992; Democratic People's Republic of Korea, 1990; India, 1992; Indonesia, 1990; Japan, 1994; Lao People's Democratic Republic, 1991; Malaysia, 1995; Mongolia, 1990; Myanmar, 1991; Philippines, 1990; Republic of Korea, 1991; Singapore, 1995; Thailand, 1992; Timor-Leste, 2003; and Vietnam, 1990) have ratified or acceded to the CRC as of October 24,

2014.12 Accession has the same legal effect as ratification by the terms of the Convention according to Article 49 of the CRC.

CHILD RIGHTS PROTECTION PROVIDES ONLINE COMPLAINT PLATFORM TO REPORT CYBER CRIME

With child abuse finding new forms and channels through mobile and digital technologies, victims of such cybercrimes can now lodge their complaints at National Commission for Protection of Child Rights (NCPCR)'s enhanced online platform 'POCSO e-box'.Considering the growing menace of cybercrimes targeting children, POCSO e-box has been enhanced to handle cyber bullying, cyber stalking, morphing of images and child pornography.

Such crimes can be reported by pressing the 'e-box' button available at the commission's website. Complaints can be sent to the e-mail address of pocsoebox -- ncpcr@gov.in or on the mobile number 9868235077.

"In India, about 134 million children have access to mobile phones. While this provides opportunities for accessing useful material for learning purposes, lack of digital literacy and online safety measures expose children to hazards of cybercrime," the statement said. It informed that the 'POCSO e-box' is an easy and direct medium for reporting of child sexual abuse under the Protection of Children from Sexual Offences (POCSO) Act, 2012. The platform was launched by Women and Child Development Maneka Gandhi in 2016.

CHILD PROSTITUITION – CYBER CRIME

It is the curse of the legal framework in India to be negligent enough on the issue of child prostitution despite the rising number of victims to this abuse.

In today’s world, pornography is readily available on the internet. To follow this example, if someone today was to purchase online pornography, it can be done in the privacy of their own home. No one needs to know and the natural deterrent is removed, seeing a marked increase in pornography use today. The ease in access to pornography has also created a

further market and demand for material, some of which is becoming more and more heinous in nature allowing individuals to carry out fantasies in virtual reality. The internet combined with factors such as this are providing a lucrative environment for traffickers to operate their business. Fight the New Drug claim that 25% of all search engine requests are for pornographic material.

How child prostitution is related with cybercrime is quiet simple- the victim (child) is threatened by sexual needs and forced to sell their body

Elements

a) Consent of the child is immaterial as it is noted that no child has a stable maturity to decide whether or not to engaged themselves in prostitution

b) Malafide intention from the side of the abuser

c)Deals with selling/transporting/receiving the child for the purpose of prostitution

The abuser commits the crime using various methods like:

1.) By providing remuneration or any kind of consideration in return

2.) Using the threat of defaming the child if he/she denies

3.)Engaging the child into trafficking

ROLE OF UNICEF AND CYBERSPACE

UNICEF India today launched the Child Online Protection in India Report which provides a comprehensive overview of the current risks and threats faced by children when using the internet and social media. (Download Report) Digital technologies offer significant developmental and educational benefits for children. They offer new spaces for learning, play, socialization and entertainment. Most importantly, ICT and social media can offer incredible opportunities for children's active participation and empowerment, via digital citizenship, and ultimately contribute to the wider efforts towards meeting child-focused development goals. However, the lack of digital literacy and online safety measures mean that children are also exposed to the risk of online crimes, abuse and exploitation. Cyber offences against children are spreading and diversifying across India as new methods are used to harass, abuse and exploit children.

Addressing the gathering, Dr. Ajay Kumar, Additional Secretary, Ministry of Electronics and Information Technology (MeitY), said "I compliment UNICEF and NASSCOM Foundation for organizing the event as Child Online Safety is one of the most important of challenges arising in an internet world. Ministry of Electronics and IT is taking steps to block sites depicting child abuse. However, given the nature of the menace, this requires a collective effort from all stakeholders, including service providers, content providers, civil society and regulatory authorities." The report launched today states that offline forms of crime and violence against children are finding new forms of expression in the online world and their effects on children are amplified. Being able to stay anonymous online and impersonate others may embolden people into offensive and criminal acts and lower the deterrent potential of laws. Cyber-crimes against children have many forms including sex-texting, online grooming, production and distribution of child harmful material, cyber bullying, etc. However, to date cyber-crimes against children in India are under-reported and have received very little attention and are not included in the National Crime Records Bureau statistics as a separate category. "This Report is an important step in the direction of child online protection and safety and will go a long way in improving child online protection measures in our country," said Stuti Kacker, Chair of NCPCR. The report is a useful resource for child protection actors, law enforcement agencies, Information and Communication technology (ICT) companies, government ministries, media and anybody concerned about children's online safety including parents and teachers. It is a resource that should help any organization working with children to enhance their awareness of the issue and understand both where to improve their own interventions and where to strengthen collaboration and coordination with other stakeholders. "Globally, child online protection is much recognized and discussed agenda but sadly India is a little late to realize it. NASSCOM Foundation appreciates the efforts by UNICEF to bring the right people together to address this burning issue and we are glad to be a Technology for Good partner for this report which should act as a wake-up call," said Shrikant Sinha, NASSCOM Foundation Head. The Report also stress the importance to empower parents, professionals and policymakers to play an active role in preventing and protecting children from child online abuse and exploitation. A safe online ecosystem for children requires technical solutions and a high degree of preparedness, collaboration and coordination among stakeholders. "No single agency or government institution can ensure the safety of children from online threats and violence. This calls for all relevant government institutions, the private sector, international organizations, media, academia and civil society to work together to build structures, mechanisms and capacities to prevent and respond to the specific threats and risks posed to children," said Louis-Georges Arsenault, UNICEF India

Representative. The Report's launch event provided a forum for multiple-stakeholders to discuss the complex nature of child online violence and the need for a multi-sectoral response. During the launch senior representatives from key government institutions, the ICT sector, national and international experts, media, academia and civil society discussed the way forward for child online safety, including prevention and response to online violence and abuse. Representatives from 10 States across India participated and estimated international experts contributed to the event including Patrick Burton, Director, Centre for Justice and Crime Prevention – Cape Town (South Africa) and Marie-Laure Lemineur, Head of Programmes for ECPAT International – Bangkok (Thailand). Young people from Delhi, Mumbai and Chennai had the opportunity to talk about what online safety means to them in an interactive session with radio jockeys from New Delhi. Breakthrough India also shared their adolescent #bemysafespace initiative led by young people that promotes online safety for children and adolescents.

From the report presented and the discussion at the launch, recommendations were put forward on the following seven areas for action:

1. Leadership and partnership for child online safety in India
2. Evidence, research, data on child online safety
3. Education for digital literacy, citizenship and safety
4. Legislation and policies to protect children from online abuse and exploitation
5. Reporting and removing online child sexual abuse material
6. Legal investigation and prosecution of online sexual abuse and exploitation
7. Services for victims of the worst forms of child online abuse and exploitation

Currently there are about 400 million Internet users in India and growing with access to mobile Internet use. There are 306 million mobile Internet users in India with 219 million from urban India and 87 million from rural India. The majority of these users are youth. UNICEF India encourages all stakeholders to come together under a common 'Child Online Safety National Framework and Multi-agency Action Plan' to ensure that all Indian children can benefit from safe digital spaces.

TECHNOLOGY TO PROTECT CHILDREN FROM CYBER CRIMES

"Cybercrime is happening against children and it has pervaded into our system and we have to be very careful."The smartphones have contributed to rise in offences against women and children, and expressed concern over increasing cases of Internet crime against children. In a nation with a lot of small children but unfortunately we are careless in managing our human wealth. Children are our future, but unfortunately we are not investing enough in our children by way of time, resources and safety. Emphasises on the importance of professionalism in the field of cybercrime investigation and leveraging technology to protect the interests of children has to be executed. Due to an increase in the use of Internet by children, online child sexual abuse and cyber radicalisation instances are on the rise. Cybercrime is happening against children and it has pervaded into our system and we have to be very careful. Cyber space is being used to get hold of children and change their minds and referred to a case wherein Internet groups approached young girls and persuaded them to commit suicide. Smartphones have become a status symbol but device has a negative side too. The smartphone has improved our lives and made communication easy but in a way it has become our nemesis and creates problems for us. smartphones have contributed to rise in crime against women and children as one can do all the things that a computer can do including downloading porn films/clips.

due to extensive use of Internet-based home control systems, hackers/online predators are accessing electronic gadgets like webcams, computers and collecting data compromising privacy/safety of people, especially children. NCPCR has set up an online complaint management system called ‘POCSO e-box’ for children to report any cases of sexual assault/abuse or harassment. Stating that children stalked by the (online) predators suffer a lot mentally and constantly live in fear. We need to protect our children and also their minds. If we don’t protect them and they have access and see all this filth then we are not incubating good individuals.

The internet is also becoming a place of choice for traffickers to sell the services theyforce upon their victims. One can readily access the services of escorts and prostitutiononline with just a few clicks using services like Backpage, Craigslist, Facebook and the manychatrooms dedicated to these services.Online advertising is not the only method traffickers use to sell their wares but it is akey component with many traffickers ensuring online listing happens in as many places aspossible. Some even force their victims to spend time online advertising

themselves withboth real and different photo identities. False photos are often used to hide under ageexploitation.

Thorn, a NGO set up by Aston Kutcher and Demi Moore to drive tech innovation tofight child trafficking and the sexual exploitation of children, commissioned a survey ofsexual exploitation victims to find out the role of technology in trafficking. 63% of thesurvey participants reported being sold online.

Cybercrime Counter Human Trafficking Efforts

There are some good advances in tools to fight cybercrime on the surface web and thedark web that should be noted. Spotlight is a tool created by Thorn in partnership with Digital Reasoning. Spotlightscraps publicly available information from the internet, analyses it and uses it to helpprioritise cases for law enforcement. It focuses on child trafficking data and essentiallyincreases the response time of police by providing concentrated data to work with.

Lieutenant Chad Gremillion of the Louisiana State Police reported:

"Seeing Spotlight in action reinforces the idea that we can use technology for good.This is such an incredibly powerful tool in our effort to locate trafficking victims andget them connected to services. It's also made our jobs easier in finding offenders,which is exactly what we did after identifying Karina. With the help of Spotlight, wenot only arrested her trafficker, but he's now looking at 30 years to life in prison. Wecouldn't have asked for a better outcome for her and for this case."

With cybercrime being fairly recent, new groups are being established to monitor and provideaccountability at a global effort. This is especially important as no one group owns theinternet. In January 2014 the Global Commission on Internet Governance was established toarticulate and advance strategic vision for the future of Internet governance. Its key focusesinclude ensuring human rights online, freedom of expression and cybercrime cooperation.

CONSTITUITIONAL PROVISIONS

Article 19- protection against all forms of abuse and effort to prevent creation and neglect

Article 34- includes sexual online child abuse images, sexual grooming, etc

Article 36- online dimension of child trafficking

Article 17(e)- protection from material injuries

Article 13- child's freedom of expression

Article 15- freedom of association

CONCLUSION

Any legislation proposed should:

- Be rights-based, with the best interests of the child (all children involved) as a primary consideration
- Focus on prevention including responsible digital citizenship
- Provide for the establishment of school codes of conduct, anti-bullying action plans, child friendly reporting mechanisms and appropriate consequences, remedies and appeal processes, which Involve children directly in the development of related codes, policies, consequences, remedies and action plans and ensure they are fully informed of them
- Focus on accountability for duty-bearers
- Use the most severe penalties only as a last resort, with a focus on progressive discipline
- Be adequately resourced

RECOMMENDATIONS

1.Informing your teen of the various cybercrimes in existence: A number of actions are categorised as cybercrimes. However, cybercrimes themselves can be divided into three basic categories – crimes against persons, crimes against property and crimes against the government.

Crimes against persons would include actions such as cyber stalking and cyber bullying which is common among teenagers.

Crimes against the government include actions such as cyber terrorism and sedition. While you may not think that children and teenagers are capable of carrying out such serious crimes, it is important to keep in mind that several terrorist outfits spread their propaganda over social media and influence impressionable individuals to support them and share their posts.

Probably the most common type of cybercrime committed is crime against property. While teenagers may lack the expertise or motive to create and spread software viruses, very often they download movies, songs and games from illegal Internet sites for free. This act of downloading pirated versions of these literary works is a form of infringement of the intellectual property rights of the creators of these works. Another common crime against property is hacking, by which an individual gains access to another's system without their consent.

Apart from the instances mentioned above, there are many more specialised actions that are classified as cybercrimes and are prohibited for this reason.

2. Educating you teen on cyber laws and penalties for cybercrimes: The Indian Information Technology Act, 2000 (amended in 2008) is the main law dealing with cybercrimes and technology-related issues. It lists various crimes and their punishments. Many of these crimes are also punishable under other statutes such as the Indian Penal Code. For example, cyber terrorism is punishable both under S. 69 of the IT Act and any other law on terrorism that is applicable. These offenses and their penalties are under constant discussion due to the rate of development of technology.

3. Monitoring Internet use of pre-teens: Nowadays children are exposed to gadgets and technology as early as primary school. Though children below 18 years are not allowed to create profiles on many of the more popular social media platforms, many children below this age limit create profiles on such social media platforms either with or without the knowledge of their parents. Children may be influenced by the content available on such sites or may themselves become victims of cybercrimes. Placing the right checks and balances with your child at an early age will allow him to develop his own sense of responsibility when he is old enough to be on social media.

4. Teaching your child to respect property, privacy and persons: While this may seem a rather general guideline, it goes a long way in ensuring that your child respects cyber laws. Many cybercrimes relate to the infringement of property rights, privacy rights and other personal rights of individuals. Inculcating a general awareness of these rights in your child will help her apply the same in a virtual environment as well.

5. Keeping yourself updated with technological developments: Another important way to ensure that your child is not breaking any cyber law is to keep yourself updated on new developments in technology. Due to the fast-developing nature of technology, cyber laws need to be adapted to regulate these developments. By keeping yourself informed of the basic developments and trends, you can be aware of not only the new laws but also the new cybercrimes that come up. In doing so, you will be better able to advise your child on these issues as well as keep him informed of the punishments he might attract for the contravention of cyber laws.

To sum up, though a crime free society is perfect and exists only in illusion, it should be constant attempt of rules to keep the criminalities lowest. Especially in a society that is dependent more and more on technology, crime based on electronic law-breaking are bound to increase and the law makers have to go the extra mile compared to the impostors, to keep them at bay. Technology is always a double-edged sword and can be used for both the purposes – good or bad. Steganography, Trojan Horse, Scavenging (and even Dos or DDos) are all technologies and per se not crimes, but falling into the wrong hands with an illicit intent who are out to exploit them or misuse them, they come into the array of cyber-crime and become punishable offences. Hence, it should be the tenacious efforts of rulers and law makers to ensure that technology grows in a healthy manner and is used for legal and ethical business growth and not for committing crimes.

It should be the duty of the three stake holders viz. i) the rulers, regulators, law makers and agents ii) Internet or Network Service Suppliers or banks and other intercessors and iii) the users to take care of information security playing their respective role within the permitted limitations and ensuring obedience with the law of the land.