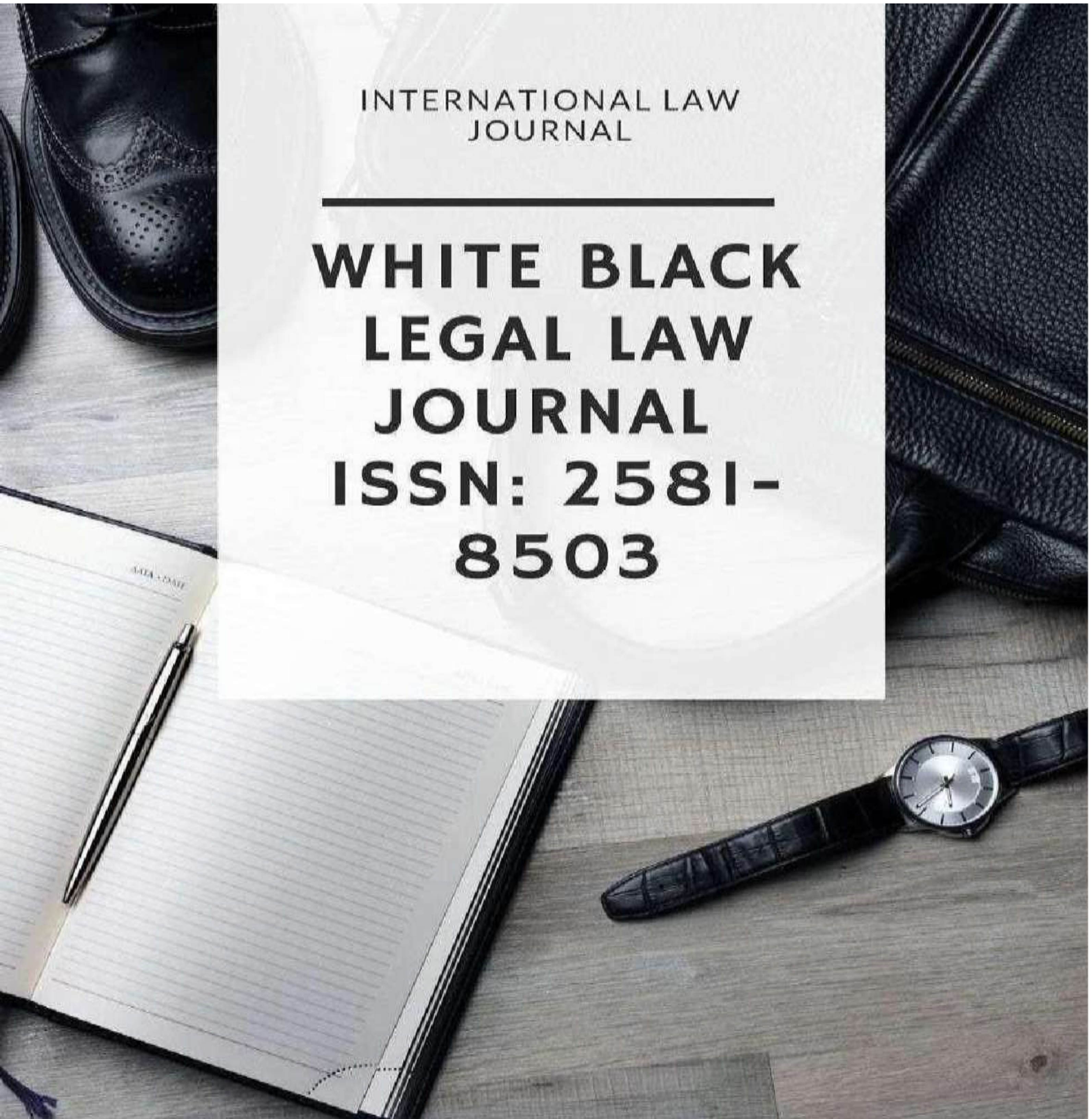

INTERNATIONAL LAW
JOURNAL

WHITE BLACK LEGAL LAW JOURNAL

ISSN: 2581-8503

Peer - Reviewed & Refereed Journal

The Law Journal strives to provide a platform for discussion of International as well as National Developments in the Field of Law.

WWW.WHITEBLACKLEGAL.CO.IN

DISCLAIMER

No part of this publication may be reproduced or copied in any form by any means without prior written permission of Editor-in-chief of White Black Legal – The Law Journal. The Editorial Team of White Black Legal holds the copyright to all articles contributed to this publication. The views expressed in this publication are purely personal opinions of the authors and do not reflect the views of the Editorial Team of White Black Legal. Though all efforts are made to ensure the accuracy and correctness of the information published, White Black Legal shall not be responsible for any errors caused due to oversight or otherwise.

EDITORIAL TEAM

Senior Editor

Dr. Neha Mishra

Dr. Neha Mishra is Associate Professor & Associate Dean (Scholarships) in Jindal Global Law School, OP Jindal Global University. She was awarded both her PhD degree and Associate Professor & Associate Dean M.A.; LL.B. (University of Delhi); LL.M.; PH.D. (NLSIU, Bangalore) LLM from National Law School of India University, Bengaluru; she did her LL.B. from Faculty of Law, Delhi University as well as M.A. and B.A. from Hindu College and DCAC from DU respectively. Neha has been a Visiting Fellow, School of Social Work, Michigan State University, 2016 and invited speaker Panelist at Global Conference, Whitney R. Harris World Law Institute, Washington University in St. Louis, 2015.

Ms. Sumiti Ahuja

Ms. Sumiti Ahuja, Assistant Professor, Faculty of Law, University of Delhi,
Ms. Sumiti Ahuja completed her LL.M. from the Indian Law Institute with specialization in Criminal Law and Corporate Law, and has over nine years of teaching experience. She has done her LL.B. from the Faculty of Law, University of Delhi. She is currently pursuing PH.D. in the area of Forensics and Law. Prior to joining the teaching profession, she has worked as Research Assistant for projects funded by different agencies of Govt. of India. She has developed various audio-video teaching modules under UGC e-PG Pathshala programme in the area of Criminology, under the aegis of an MHRD Project. Her areas of interest are Criminal Law, Law of Evidence, Interpretation of Statutes, and Clinical Legal Education.

Dr. Navtika Singh Nautiyal

Dr. Navtika Singh Nautiyal presently working as an Assistant Professor in School of law, Forensic Justice and Policy studies at National Forensic Sciences University, Gandhinagar, Gujarat. She has 9 years of Teaching and Research Experience. She has completed her Philosophy of Doctorate in ‘Intercountry adoption laws from Uttranchal University, Dehradun’ and LLM from Indian Law Institute, New Delhi.

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

THE ROLE OF CYBER FORENSICS IN INVESTIGATING ONLINE CHILD EXPLOITATION IN THE UK

AUTHORED BY - SWESTHIGA KUMAR & DHANUSH RAVIKUMAR

ABSTRACT

As online child exploitation has become more common, cyber forensic techniques have had to evolve in order to successfully investigate and convict criminals. Based on a doctrinal methodology, the paper examines both primary and secondary legal sources, such as academic publications, statutes, and case law. According to the theory, the full potential of cyber forensic tools is impeded by legal and technical constraints, even though they greatly improve the detection and prosecution of online child exploitation. The study looks at the steps involved in a forensic investigation, such as gathering data, preserving digital evidence, and analysing encrypted communications and darknet activity. It evaluates the judicial system in the United Kingdom (UK). It also looks at moral conundrums, such as how to strike a balance between individual rights and law enforcement surveillance. The paper adds to the growing body of knowledge about digital forensics and child protection by providing guidance to legislators, law enforcement, and attorneys on how to improve the use of cyber forensics in cases involving online child exploitation.

INTRODUCTION

The growing popularity of digital technologies and the internet has changed how we communicate, work, and live. Online child exploitation occurs when a person uses the internet to take advantage of a child's innocence, tricking or forcing them into illegal or sexual activities.[1] Cyber forensics, a vital branch of forensic science, focuses on the examination, extraction, and processing of data from electronic devices for use in criminal investigations. Online child exploitation is one of the many illegal risks associated with this digital revolution. Online harassment of children and exploitation, as well as the creation, promotion, and possession of child abuse content, have increased in frequency and intensity. Identifying and

[1] 'Online Exploitation' (*Hampshire Safeguarding Children Partnership*) <www.hampshirescp.org.uk/professionals/toolkits/child-exploitation/what-is-child-exploitation/online-exploitation/>

punishing offenders can be challenging due to the internet's invisibility, the use of encryption and other evasion tactics, and the vast amount of digital information. Addressing online child exploitation requires the use of cyber forensics, a branch of digital forensics. In cyber forensics, data is collected from various sources, including computers, mobile devices, networks, and online platforms, which are then examined and preserved. Investigators can pinpoint criminals, analyse online activity, and gather evidence to support verdicts using cyber forensic techniques.

The purpose of this study is to critically analyse how cyber forensics can be applied to investigate online child exploitation. The procedures and steps of a forensic investigation, including data collection, digital evidence preservation, and analysis of encrypted communications and dark web activities, are also examined in this study. The paper advocates for stronger legislative frameworks, expanded forensic capabilities, and ethical oversight to ensure effective and equitable investigations. By providing recommendations to lawmakers, law enforcement, and legal professionals on enhancing the application of cyber forensics in cases involving online child exploitation, this study contributes to the growing body of knowledge regarding digital forensics and child protection in the United Kingdom.

THE EMERGENCE OF CYBER FORENSICS

The usage of digital media, gadgets, and social media has increased significantly during the last ten years. Few could have foreseen the degree to which digital technology would permeate daily life twenty years ago. Many people today take for granted electronic gadgets that can be operated remotely, mobile phones that act like compact computers, and residences with cameras that are more sophisticated than those found in the majority of business buildings in the early 2000s. The way that police respond to crimes, assist victims, and gather evidence from various digital devices—now referred to as digital forensics—has unavoidably been influenced by these technological breakthroughs[2].

Since its inception, digital forensics has made great strides in addressing traditional criminal investigations, including cybercrimes. As technology continues to develop, it presents both new possibilities and challenges. Forensic procedures need to be updated and improved on a regular basis due to the increasing complexity of digital systems and the usage of

[2] 'An inspection into how well the police and other agencies use digital forensics in their investigations' (HMICFRS, 1 December 2022) <https://hmicfrs.justiceinspectorates.gov.uk/publication-html/how-well-the-police-and-other-agencies-use-digital-forensics-in-their-investigations/> accessed on 18 March 2025

anonymisation techniques by criminals. Data encryption is a significant challenge in digital forensics. Although this procedure is essential for safeguarding sensitive data, it poses significant challenges for forensic investigators, as it converts data into a coded format that prevents unauthorised access. Advanced technical knowledge and specialised equipment are required to crack encryption, which makes the investigation process more difficult. Additionally, these difficulties have been exacerbated by the growth of cloud computing. Users can store their data remotely using cloud storage, which is available from any device with an internet connection. Digital forensic specialists must adapt their techniques to effectively gather and examine evidence from the cloud while making sure it satisfies legal requirements for admissibility, as a result of this evolution, which makes data acquisition and preservation more difficult[3].

Numerous digital forensic examinations are carried out by intelligence and law enforcement organisations for a range of investigative objectives. These studies could help find missing people, clear suspects by bolstering alibis, or reveal proof of criminal activities, such as terrorist attack preparations. Private businesses also use digital forensic techniques to probe information security breaches and conduct internal investigations. Digital forensic exams are either conducted in-house by law enforcement organisations in the UK or contracted out to for-profit forensic service firms. Since digital forensics is not covered by the government-managed national forensic procurement framework, this outsourcing is usually done through a tendering procedure. The National Technical Assistance Centre, a branch of GCHQ, may also be able to help agencies. Nevertheless, there is still a lack of publicly accessible information regarding agency spending on forensic services.

The main source of forensic science in the United Kingdom prior to 2012 was the Home Office-funded Forensic Science Service. However, police departments began obtaining forensic services from private firms or managing them in-house after the closure in 2012. Certain fields, such as toxicology, are dominated by the commercial sector, whereas police departments typically handle other services, including fingerprint analysis and digital forensics.

In 2013, the Science and Technology Committee of the House of Commons emphasised the dearth of financing for forensic science research in the United Kingdom and reaffirmed its

[3] Sigurður Ragnarsson, 'The Role of Digital Forensics in CSAM Scanning' (Videntifer, 17 February 2024)< https://www.videntifier.com/post/the-role-of-digital-forensics-in-csam-scanning> accessed on 20 March 2025

proposal that the government create a forensic strategy. This strategy was scheduled for release by the Home Office in 2016. The Home Office had also started collecting information on the use of digital forensics by police departments in Wales and England. The Government Chief Scientific Adviser examined forensic science, particularly digital forensics, and its various applications in their 2015 annual report[4].

Recently, the UK government has come up with a new strategy to combat cybercrimes. The UK Cyber Security Strategy 2022-2030 is primarily concerned with increasing national resilience against cyber threats, safeguarding key infrastructure, and boosting collaboration between the public and commercial sectors. It highlights the need for increased capabilities in cyber investigations, digital evidence handling, and cooperation between law enforcement and intelligence organisations, even though it does not specifically focus on cyber forensics. An essential component of these goals is cyber forensics, especially when it comes to combating cybercrime and improving the UK's capacity to respond to cyber incidents.

This strategy recognises the vital role that cyber forensics plays in preventing crime and ensuring national security. The UK intends to keep ahead of changing cyber risks by investing in advanced forensic tools, expert training, and cross-sector collaboration, as well as ensuring strong digital evidence processing in court procedures.

HOW DOES CYBER FORENSICS INVESTIGATE ONLINE CHILD EXPLOITATION?

Online child exploitation involves a wide range of abuse, such as the distribution of child sexual abuse material (CSAM), minor grooming, live-streamed abuse, and trafficking. Cyber forensic methods are crucial for identifying and prosecuting these crimes since criminals frequently use anonymity and encryption technology to conceal their identity.

The National Crime Agency targets those who engage in any kind of sexual abuse or exploitation of children. This includes individuals who directly sexually abuse children as well as those who engage in cybercrimes, including grooming or blackmailing minors online or producing, disseminating, or watching pornographic photographs of children. Cases involving

[4] Lydia Harriss & Kathryn Boast, 'Digital Forensics and Crime' (UK Parliament, 09 March 2016) <https://post.parliament.uk/research-briefings/post-pn-0520/> accessed on 20 March 2025

the streaming of recorded and live abuse are also handled by the organisation. The work of the National Crime Agency is not limited to crimes that are committed in the United Kingdom. It keeps track of child sex offenders who enter the UK with the intention of abusing children or who travel elsewhere to do so. The organisation also offers specific guidance and experience to support law enforcement investigations both domestically and abroad[5]. The National Crime Agency, as the principal reporting body for industry and international law enforcement, receives a significant amount of information about child sex crimes. With the main objectives of detecting criminals and guaranteeing the safety of children and youth, this intelligence is used to direct and assist law enforcement activities across the globe.

Collection of digital evidence

Forensic investigators use software like EnCase, Autopsy, and AccessData FTK to retrieve data from digital devices like PCs, mobile phones, and external storage devices. By producing forensic pictures, which are precise duplicates of storage devices, these techniques guarantee data integrity and preserve metadata, which is essential for creating timelines. Online predators frequently interact with youngsters through gaming forums, messaging applications, and social media sites. Investigators use forensic tools like Cellebrite UFED and Magnet AXIOM to follow communications and recover deleted texts. Sophisticated computers recognise grooming behaviours by analysing chat patterns. To find offenders, cyber forensic experts employ metadata analysis and IP address tracing. Offenders' digital traces make it easier to identify who they are in real life. Network data is analysed by programs like Wireshark and XRY to find questionable activity.

Identifying the Perpetrators

Anonymisation techniques are frequently used by offenders in an effort to conceal their identities. To find them, cyber forensic specialists use the following methods:

The dark web is the site of many online child exploitation activities, where criminals utilise Tor (The Onion Router) to remain anonymous. Investigators use blockchain analysis, honeypots, and Open Source Intelligence tools to track illegal activity and penetrate criminal networks. By comparing fresh photos to a database of known abusive content, AI-powered forensic technologies like PhotoDNA and Project VIC assist in identifying CSAM. Images'

[5] 'Child sexual abuse and exploitation' (National Crime Agency) <www.nationalcrimeagency.gov.uk/what-we-do/crime-threats/child-sexual-abuse-and-exploitation> accessed on 22 March 2025

extracted metadata, such as EXIF data, aids in identifying the material's location and place of origin. To identify grooming techniques, machine learning systems examine online patterns and behaviours. Forensic specialists can anticipate and stop exploitation before it escalates by examining the language patterns and engagement strategies employed by perpetrators.

Recently, the Child Abuse Image Database (CAID) has announced the world's first statewide deployment of Cyacomb Forensics' mobile device capability, which will allow UK police forces to scan devices for known child sexual abuse material (CSAM) in seconds. CAID was created by the Home Office in partnership with law enforcement, business partners, and both domestic and foreign technology companies as a key aspect of the national IT strategy to combat child sexual abuse and exploitation, a top priority threat in the UK. The Home Office has kept improving and investing in its capabilities since its initial launch in December 2014 across all UK territorial police forces and the National Crime Agency[6].

In 2019, the then-Home Secretary stated that Cyacomb's quick forensic triage technology would be integrated into CAID, making the UK the first nation to do so nationwide. To keep UK law enforcement at the forefront of combating CSAM, the contract was extended for an additional two years in August 2024, adding Cyacomb's mobile device scanning capabilities to the project. Using a quick and easy scanning method, Cyacomb Examiner acts as a "digital breathalyser" for law enforcement, detecting child abuse content on suspect devices up to 100 times quicker than traditional forensic tools. In addition to speeding up investigations, this cutting-edge digital forensic triage allows for quick kid safety precautions and relieves strain on digital forensic labs. Instead of restricting access to forensic labs, Cyacomb Examiner in the UK uses data from CAID through a highly secure Contraband Filter, enabling frontline cops and search teams to use the technology.

Cyber forensics is an essential component in combating online child exploitation. Law enforcement can track criminals and rescue victims with the use of tools like CAID and Cyacomb Forensics. However, persistent difficulties necessitate constant development in legal frameworks and forensic technology. Society can better safeguard vulnerable children and hold offenders accountable by enhancing forensic capabilities and raising public awareness.

[6] Alan McConnell, 'UK Home Office rolling out new technology to detect Child Sexual Abuse on suspect's devices' (Cyacomb, 5 December 2024) < www.cyacomb.com/resources/news/2024/december/uk-home-office-rolling-out-new-technology-to-detect-child-sexual-abuse-on-suspects-devices/> accessed on 22 March 2025

A CRITICAL EXAMINATION OF THE JUDICIAL PERSPECTIVE IN THE UK

Computer Misuse Act 1990

The Act[7] focuses on protecting computer systems and data from unauthorised access or alteration and establishes the related legal provisions. Online child exploitation involves hackers misusing the children through the internet, and this will be an offence of unauthorised access under the Act.

The Act aims to protect computer systems and data by making unauthorised access a criminal offence. Its framework includes ensuring law enforcement agencies have all necessary authority to investigate and take action against online hackers, and whether the law remains effective with the growth in technologies since the act was introduced.[8]

Protection of Children Act 1978

The Act[9] focuses on preventing child exploitation by banning the creation, promotion, and sharing of indecent and abusive images and provides punishments to the offenders.[10] Under this Act, criminal proceedings and investigations can be taken against the defendant for online child exploitation.

Investigatory Powers Act 2016

The Act[11] talks about the regulations on how authorities can collect and use people’s communication data by covering interception, equipment interference, or acquisition. The Act also establishes the Investigatory Powers Commissioner and other Judicial Commissioners to use those investigatory powers responsibly.

Police, Crime, Sentencing and Courts Act 2022

Chapter 3 of the Act[12] talks about the extraction of information from electronic devices for the purpose of the investigation of crime.

[7] Computer Misuse Act 1990.
[8] Department of Crime, justice and law, *Consultation outcome Review of the Computer Misuse Act 1990: consultation and response to call for information (accessible)* (2023).
[9] Protection of Children Act 1978.
[10] Protection of Children Act 1978.
[11] Dr Janice Goldstraw-White, LEGAL AND POLICY FRAMEWORK FOR DIGITAL FORENSICS: A RESOURCE FOR PRACTITIONERS A Policy and Practice Briefing from the Digital Forensics and Social Media project funded by the Dawes Trust (2022).
[12] Police, Crime, Sentencing and Courts Act 2022.

Online Safety Act 2023

The Act[13] sets out the laws to protect children and adults from abuse while using the internet. The Act makes sure that people are safe while surfing the internet. It protects the users by targeting social media companies and search engines, which mandates them to take steps to prevent harm.[14] The Act also punishes different content, including illegal content and content that is harmful to children. Importantly, the Act requires the online platforms to think carefully about how their algorithms might expose users, especially children, to harmful or illegal content.

Regina v Oliver[15]

In this case, the defendant was convicted of taking indecent photographs of prepubescent girls engaging in explicit sexual actions with adult males, with 20,000 indecent images and 500 child abuse computer movie files obtained. Considering the request for a community rehabilitation order, the judge issued a three-year jail term, citing the severe nature of the crimes, the huge number of photos involved, and the lack of proper rehabilitation programs. The Court of Appeal upheld the sentence, highlighting the necessity of evaluating the type of indecent material, the offender's commitment, and any commercial advantage to determine the seriousness of the behaviour at issue. Imposed a three-year sentence.

SUGGESTIONS & CONCLUSION

CURRENT STATUS

1. **Worcestershire**

   The Online Child Sexual Exploitation Team of West Mercia Police found that a 62-year-old man from Worcestershire tried to abuse a child. In his car, the police officers found cable ties, handcuffs, a whip, lubricant, amphetamine drugs, Viagra, and baby wipes. On the West Mercia Police webpage, a picture of these items was shown, and it looks very scary. Fortunately, the police officers discovered this incident before the man attempted to commit the offence, and they also punished him.[16]

[13] Online Safety Act 2023.

[14] 'Online Safety Act: explainer' (*GOV.UK*) <www.gov.uk/government/publications/online-safety-act-explainer/online-safety-act-explainer#the-new-offences-that-the-act-has-introduced> accessed 23 March 2025

[15] *Regina v Oliver* [2002] EWCA Crim 2766.

[16] 'Man jailed for trying to facilitate sexual activity with a child', *West Mercia Police* (West Mercia, 6 January 2025) <www.westmercia.police.uk/> accessed 23 March 2025

2. **The Bolton Crown Court**

   In this case, a 27-year-old man was arrested because he used different AI tools, and he encouraged the rape of children through the internet. He also spoke to other like-minded people through online for his own sexual satisfaction. Later, he was sentenced to 18 years in prison, with an additional six years of supervised release upon completion of his sentence. He also received an indefinite Sexual Harm Prevention Order.[17]

3. **Northern Ireland**

   In this case, a 26-year-old man from Northern Ireland was given a life sentence with a minimum of 20 years in jail for extreme online sexual abuse of children and the manslaughter of a 12-year-old girl by catfishing. From his home in Northern Ireland, he used a computer to inflict widespread fear and devastation on thousands of children globally. He mainly targeted victims on Snapchat, occasionally using Instagram and Kik. He exploited 64 devices to pose as a young girl, coercing victims into sending intimate photos. This abuse escalated to forcing children to involve their younger siblings, as well as family pets and various objects. According to the court, McCartney caused "unquantifiable" harm, sexually gratifying himself by "degrading and humiliating" his victims. Unfortunately, many of these child victims are still unidentified, but their lives have been permanently changed.[18]

SUGGESTIONS

At present, we are living in a digital age where we cannot function without electronic devices, and AI is increasingly dominating our lives. Children utilise online resources to study, play, or learn new things. Therefore, a parent or guardian should always monitor their children's activities and track the purposes for which they are using these devices, ensuring it is solely for educational and entertainment purposes, rather than anything beyond that. General awareness should also be provided to parents, children, police, and officials regarding the darker aspects of these devices, and the police and investigation teams should consistently ensure that children are not adversely affected by such offences through the use of cyber forensics. Furthermore, it is essential that not only children but also adults receive training, ensuring that their minds remain pure and devoid of criminal intent. As law students, we understand what actions to take

[17] 'Man who used AI technology to create child sexual abuse images jailed' (*Crown Prosecution Service*, 28 October 2024) <www.cps.gov.uk/cps/news/man-who-used-ai-technology-create-child-sexual-abuse-images-jailed> accessed 23 March 2025.

[18] F Murray, P Coulter and C Campbell, 'Abuser in 'UK's largest catfishing case' jailed for life' (*BBC*, 25 October 2024) <www.bbc.co.uk/news/articles/cj4d40922xvo> accessed 23 March 2025.

when encountering injustice. However, what about those without a legal background? Therefore, through awareness camps and education, they should learn how to be vigilant in advance to prevent future crimes and be informed about the legal provisions available in this area. Many children hesitate to report incidents and may not share their experiences. Parents or guardians should ensure that their children feel comfortable being open with them about any incidents that occur. Therefore, both children and parents or guardians should learn how to seek help. Additionally, with advancements in technology, the role of cyber forensics should likewise evolve to enhance the detection and prevention of crimes.

CONCLUSION

In a nutshell, cyber forensics is critical in the investigation of online child exploitation in the United Kingdom, providing key digital evidence to bring criminals to the penal system. Cyber forensics professionals use innovative tools and procedures to discover hidden digital tracks, track down criminals, and protect vulnerable youngsters. However, the ever-changing nature of cybercrime requires ongoing innovation and coordination among law enforcement, forensic professionals, and legislators to keep ahead of emerging threats. This study has looked at the origins of cyber forensics, its investigative techniques, and the UK's legal approach to online child exploitation, highlighting important issues and possible answers. Effective cyber forensics helps protect children and hold abusers accountable, highlighting its importance in the UK's efforts against online child exploitation. When all these measures are effectively implemented, we can strongly believe that we can prevent such child exploitation and create a safer environment for children.