VOLUME 4 | ISSUE 2

INTERNATIONAL JOURNAL OF ADVANCED LEGAL RESEARCH

DIGITAL EVIDENCE IN DIGITAL CRIME IN CONSENSUS WITH DPDP ACT, 2023

- Sthryna Saragadam, Sanjana Ravichandran & Annu Kumari[1]

"The problem isn't data protection, the problem is data collection" - Edward Snowden

Maybe the government is spying on your boring emails, hoping to find a secret recipe for turning plain toast into a national delicacy… While breeding an idea of upholding justice and preserving data privacy, an individual's personal life has been overshadowed. Justice K. S Puttaswamy v Union of India Judgement gave leeway to the Constitution to recognize the right to privacy as a fundamental right. The Digital Personal Data Protection Act is a subset of such right. A man on trial is adjudicated based on evidence presented in a court of law for a digital crime. The ecumenical nature of digital records is in conflict with legislation such as The Indian Evidence Act, of 1872 and the Information Technology Act, of 2000 creating a domino of irregularities. The act tried to give cognitive protection to the stakeholders by ensuring data is protected from fiduciaries such as the government, companies and third-party data processors. The development of concepts like "deemed consent' might have grave repercussions while dealing with digital crimes due to the exemptions consigned, albeit the term isn't strictly defined under the act. The significant issue that arises is, whether committing a crime absolves one from its right to protect personal data and privacy. This paper is set to analyse the need for protective clauses for individuals whose rights are being violated under the pretext of legitimate purposes under the act. It also contextualizes terms like "data fiduciary" and the need for establishing centralised authority to regulate such data.

[1] Students at IFIM Law School

Keywords: Data Privacy - Personal Data - Legitimate Purposes - Data Fiduciary - Evidence

INTRODUCTION

The development of computers and the Internet provided unprecedented convenience to humans, but it also spawned new unlawful and criminal activities related to computers and the Internet, which became an increasingly global problem at the same time. According to estimates, the economic loss caused by computer and network crime on a global scale has reached billions of dollars each year, with the figures rising year after year.

Hence, various legislations went through amendments to address the social changes and needs of the society and the Indian Evidence Act [2]was no exception it.

PART-I

Eventually, the courts realized the importance of electronic evidence in substantiating the case of the parties. Hence, the legislatures came up with the Information Technology (Amendment) Act, of 2000 which introduced two major changes in the Evidence Act, of 1872. Firstly, it amended section 3 of the Indian Evidence Act by widening the ambit of evidence to oral, documentary and electronic. Secondly, section 65A and 65B was added in the act that further elaborates on the conditions required to prove electronic evidence in a court of law.

ADMISSIBILITY OF EVIDENCE

Section 65B entails the conditions required for admissibility which are as follows:-

- The computer in which electronic evidence is stored must be in regular use
- Information was regularly and ordinarily fed into computer
- Computer was operating properly
- Duplicate copy must be reproduction of original electronic record.

In the case of Daubert v. Merrell-Dow Pharmaceuticals, Inc. the four-part reliability test was laid down which establishes a reasonable scientific link to the investigation as a precondition to admissibility. Firstly, whether the scientific theory on which the testimony is based on has been

[2] The Evidence Act, 1872, No. 1, Acts of Parliament, 1872 (India).

tested empirically; Secondly, the amount of potential error rate that exists. Thirdly, whether the scientific theory of technique has been subjected to peer review and publication Lastly, the expert's qualifications and opinions in the scientific community.

The dictum states that it is the obligation of the judge to ensure the digital evidence is both relevant and reliable. Therefore, reliability is a prerequisite for admitting evidence.[3]

LOOPHOLES EXISTING IN THE LAW:

These electronic evidence can be referred to as those clues or the traces that are curated due to the involvement of digital data in the commission of crime.[4] As a human beings in this technology-driven world we are a part of different sets of activities both online and offline which eventually results in the formation of a chain of online transactions such as browsing history, social media activities, digital files and much more.[5] And this trail of data creates the foundation of the electronic evidence of the legal case under investigation.

The fact that there are a number of things in the crime scene and there is an interchange of huge amounts of data makes it extremely crucial for the investigators and the court to understand the dynamics involved in the same. Hence, digital evidence is considered way more complicated and fragile in the framework of the Internet of Things because it becomes a daunting task to recognize the crime scene and its sophisticated interconnectivity with the devices at the crime scene. This further adds on to various consequences such as delayed and misled investigation processes, and privacy concerns due to the vast amount of data interconnectivity.[6]

In addition to this, another important challenge that courts and the forensics involved in the case face is protecting the safety and privacy of individuals participating in the process.

National Coordinator Ports Policing of the UK came up with a report which stated that nowadays 90% of criminal investigations have digital elements, and identifies standardization and automation as the key factors for the development of digital forensics.[7] Thus, the authenticity of

[3] Daubert v. Merrell Dow Pharmaceuticals, Inc., 509 U.S 579 (1993)
[4] E. Casey. Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet. Academic press, 2011.
[5] M. Harbawi and A. Varol, "The Role of Digital Forensic in Combating Cybercrimes," IEEE – The 4th International Symposium on Digital Forensics and Security (ISDFS 2016), pp. 138-142, 2016.
[6] M. Harbawi, "The Internet of Things Forensics: Opportunities and Trends," Unpublished.
[7] Digital evidence - unaddressed threats to fairness and the presumption of innocence - Rabina Stoykova

technology used in the investigation is also one of the crucial factors in determining the safety ensured for the individuals involved in the judicial process As per the Article 6 of ECHR the right to a fair trial is impaired due to the improper use of the technology that is below par.[8] Overreliance on these technologies not only weakens the position of suspects in the judicial process but also affects the presumption of innocence. The complexity involved in these digital investigations gives immense access to a chunk of data that may not be examined by the court but will have a serious impact on the parties involved in the case. It is contended so because it barges into the privacy rights of the individual and may lead to datafication. Hence, it becomes essential to ensure that the concept of digital preservation is met. It is a crucial aspect in ensuring authenticity, traceability and auditing in this process [8] due to the increasing intricacies of the digital elements

In contrast to the above, it's a given fact that in the context of the Internet of Things, the major chunk of data is captured digitally at the source and the data captured and transferred during a process might not cause any privacy issues on its own. However, when these fragmented data from various devices are gathered, processed, and analysed, might offer sensitive information about people's locations or living patterns, for instance.[9]

Therefore, it is clearly evident that the whereabouts of the data collected is of extreme importance.

PART-II

DATA AND ITS ASSEMBLY

The concept of privacy-respecting digital investigation with digital evidence is said to self contradictory[10]. The use of collected data in an investigation process is exponential and rather intrusive. Once a user consents to give his data, he has limited power over it. The principal aim of any data protection legislation is to protect a person's private information available in a

[8] Council of Europe, European Convention for the Protection of Human Rights and Fundamental Freedoms, as amended by Protocols Nos. 11 and 14, 4 November 1950, Article 6 - Right to a fair trial.

[9] Cameron Hashemi Pour, Ivy Wigmore, Internet of things privacy (IoT privacy), TECHTARGET, (Oct 31, 2023, 5.15PM)

[10] Ali Dehghantanha & Katrin Franke, *Privacy-Respecting Digital Investigation*, *in* 2014 Twelfth Annual International Conference on Privacy, Security and Trust 129 (2014), http://ieeexplore.ieee.org/document/6890932/ (last visited Sep 8, 2023).

public forum[11]. Data under the Digital Personal Data Protection Act, of 2023 signifies any representation of information, facts, concepts, opinions and instructions which can be interpreted communicated or processed by human beings, such as a data fiduciary.

The processing of Data for a lawful purpose according to the Act includes collection, storage, sharing, using, disclosing and dissemination and also includes erasure[12]. It is important to note that during the process of collecting data, the investigator must collect only such data which is relevant to the case[13]. The challenge that occurs is the accumulation of relevant information without being intrusive. Data which is available to the public has the ability to be a private data if it is systematically collected and stored in files by authorities[14].

The juxtaposition of an evidence-based trial and data collection without a privacy breach is not resolved in any data protection legislation. The intrusive measures which can be used by the investigator to collect data are through phone tapping, email interception[15] and prying into a person's social media life as such things have become an integral part of life. To combat invasion of privacy while collecting data for gathering evidence, the test of proportionality must be followed[16]. The collection must be strictly necessary and proportional to the crime involved as it should also safeguard the human rights of the accused[17]. The Court of Justice of the European Union in the case of Tele2Sverige[18] principally held that collection of data in the name of combating crime is not in line with EU's Data Privacy Policy and the collected data must be limited to what is strictly necessary and proportionate. However, the said proportionality test is impractical when it is brought to the current legal regime where every piece of evidence makes

[11] Colin J. Bennett, Regulating Privacy: Data Protection and Public Policy in Europe and the United States (1992).
[12] The Digital Personal Data Protection Act, 2023, No. 22, Acts of Parliament, 2023 (India)
[13] R. M. Malkani vs. State of Maharashtra 1973 AIR 157.
[14] 54733/16 Rotaru v. Romania [2000] ECHR 2923
[15] Radina Stoykova, *Digital Evidence: Unaddressed Threats to Fairness and the Presumption of Innocence*, 42 Comput. Law Secur. Rev. 105575 (2021).
[16] Ian Brown & Douwe Korff, *Terrorism and the Proportionality of Internet Surveillance*, (2008), https://papers.ssrn.com/abstract=1261194 (last visited Sep 10, 2023).
[17] Council of the European Union, 9554/17 Technical document: Measures to improve cross-border access to electronic evidence for criminal investigations following the adoption of the Council Conclusions on Improving Criminal Justice in Cyberspace, Brussels, 22 May 2017, part V.C., p.46.
[18] C 203/15; C-698/15 Tele2 Sverige AB v Post- och telestyrelsen and Secretary of State for the Home Department v Tom Watson and Others

or breaks the case. Therefore, there should be a model that assesses and regulates excessive search and seizure of digital evidence which is reasonable and practical in nature[19].

The analysis models currently use techniques such as skin detection, face recognition and DNA data sets. The analysis should be such that it fulfils the principles of fair trial while also accumulating everything that is required in order to ensure the accused is the perpetrator.

The DPDP Act, 2023 does not distinguish between sensitive personal data and personal data available in public. The IT Act and Rules of 2013 broadly protect the privacy of those sensitive personal data and information gathered through computer sources. The objective of the act is to process personal data in such a manner that recognizes both the rights of the individual and the processing of data in a lawful manner.[20] Sensitive Personal Data, as per the General Data Protection Regulation of the EU includes racial, political, religious, trade union members, genetic, biometric, sexual orientation and health details of individuals from the EU.[21] These sensitive data are prohibited from processing unless mentioned otherwise. Moreover, the processing of sensitive data is allowed in cases where there is a matter of public interest or as per laid down by the constitutional law or public international law.[22] In India, the generalization of personal data can only lead to assumptions that personal data entails sensitive data.

CONSTRAINTS WITH DATA COLLECTION:

Processing of Data does not stop at the collection of personal data, it also includes the multiplication of the data, i.e. sharing, organizing, adaptation and erasure as well. This means that a data that has been collected for a specific purpose lives on the stored device for time immemorial. This produces a risk of non-updation of data in cases where the data principal revokes her consent. The storage of data in criminal proceedings must be subjected to a particular time period and the individual must have the opportunity to challenge the data

[19] Ilyoung Hong et al., *A New Triage Model Conforming to the Needs of Selective Search and Seizure of Electronic Evidence*, 10 Digit. Investig. 175 (2013).
[20] The Digital Personal Data Protection Act, 2023, No. 22, Acts of Parliament, 2023 (India)
[21] What personal data is considered sensitive?, https://commission.europa.eu/law/law-topic/data-protection/reform/rules-business-and-organisations/legal-grounds-processing-data/sensitive-data/what-personal-data-considered-sensitive_en (last visited Sep 10, 2023).
[22] General Data Protection Regulation, art .55, 2016 O.J (L.119)

retention[23] just like how its done in traditional cases. Furthermore, it should be kept in check that while collecting data, there should not be surplus information interfering the evidence purpose[24], thereby creating a "function creep"[25]. Function creep is formed when the collected data might be used for some other purpose than the one intended, in this case, a fair investigation. To protect the data principally from impractical use of her data, there needs to be a procedural application for investigation warrants to access private information[26].

The next significant issue in the processing of data is the reliability or originality of the data and the truthfulness of the data. The evidence must fulfil the reliability test which states that it is absolutely necessary for the evidence accessed to be relevant and reliable. The digital evidence must not be tampered with and should be traced back to its different sources and origin[27]. The chain of custody gets interrupted when digital evidence is tampered with, and the question of whom to hold liable becomes unanswered. This further becomes a complicated procedure when there is a foreign jurisdiction involved[28]. Collection of evidence from one jurisdiction and processing in another requires data synchronization on multiple devices, backups and cloud storage which annihilates the reliability of the evidence.

Another form of collecting data, also known as the most intrusive form is through the surveillance of computer devices[29]. "Computer surveillance makes it possible to capture data that is not even intended to be transmitted and has not been stored, such as encryption keys and passwords".[30] This surveillance is done by the police and other law enforcement authorities to prevent crimes from happening. The crucial aspect of intrusion of privacy is left out in the name of the greater good and gives the Data Protection Act an undermining value. In the case of United States v. Jones[31], it was declared that monitoring a person for a short-term period would

[23] 30562/04. Marper v. The United Kingdom, [2008] ECHR 1581.
[24]30562/04 Marper v. the UK [2008] ECHR 1581,and no. 27798/95 Amann v. Switzerland, no. (2000) 30 EHRR 843
[25] Bert-Jaap Koops, *The Concept of Function Creep*, 13 Law Innov. Technol. 29 (2021).
[26] Bart W. Schermer, *The Limits of Privacy in Automated Profiling and Data Mining*, 27 Comput. Law Secur. Rev. 45 (2011).
[27] Stoykova, *supra* note 13.
[28] Transnational Cooperation in Criminal Matters and the Guarantee of a Fair Trial: Approaches to a General Principle - Utrecht Law Review, https://utrechtlawreview.org/articles/10.18352/ulr.244 (last visited Sep 10, 2023).
[29] Stoykova, *supra* note 13.
[30] André Årnes, Digital Forensics (2017).
[31] United States v. Jones 565 U.S (2012).

be considered reasonable, but in the longer term, it would be an illegal invasion of privacy and requires a statutory provision to curb it.

EXEMPTIONS TO DATA PRIVACY

No right is absolute. The data privacy regulation promises to cater for an individual but in reality it protects the privacy of the society as a whole, publicly[32]. The DPDP Act, 2023 provides for exemptions to when the law prevails the right to privacy. Section 17 of the Act mentions that in cases of law enforcement, such as investigation of offences, enforcement of legal rights and claims or for the matters of public interest, right to privacy can be exempted. Once the data principal gives consent to extract data,when there is a legal prosecution is going on based on digital evidence, such person cannot revoke consent. In furtherance to that, he does not have the right to erasure or rectification.

The lack of proportionality in assessing one's fundamental right and protecting the demands of society creates a lacuna in the law.

CONSENT IS A MYTH

As per section 6 of the DPDP Acts[33], the consent shall be free, specific, informed, unconditional and unambiguous with a clear affirmative action, and shall signify an agreement to the processing of her personal data for the specified purpose and be limited to such personal data as is necessary for such specified purpose. However, through the plain reading of the Act, it can be understood that the consent obtained is not purely unconditional. The deemed consent aspect of the act suggests that for legitimate purposes, the data fiduciary has the right to obtain private information regarding a person without his consent. The paradigm shift to use personal data for specific purposes gives the law an upper hand in not protecting individual rights.

Although consent is essential, it is not undivided. On the principles set out by the law, multiple jurisdictions across the globe have a veto-consent concept, similar to the deemed consent aspect of data protection. The Court of Justice of the European Union has opined that in the absence of

[32] P. Balboni et al., *Legitimate Interest of the Data Controller New Data Protection Paradigm: Legitimacy Grounded on Appropriate Protection*, 3 Int. Data Priv. Law 244 (2013).
[33] The Digital Personal Data Protection Act, 2023, No. 22, Acts of Parliament, 2023 (India)

a data subject's consent, and processing of personal data for a legitimate purpose, the data subject's fundamental rights and freedom must be respected and the data should be publicly available[34].

According to the 'principle of legitimacy' followed by the EU in its GDPR, the legitimate purpose must not just be lawful, but also fair and should respect the fundamental rights and freedoms of the data principal[35]. The concept of consent gives the data a habeas status, which implies that the data principal has the absolute power to object to the data processing whenever he wants.

While assessing consent as a fluctuating principle, the question of whether the right to data protection is an absolute right arises. The interference of legitimate purpose in this aspect makes it clear that the right to data protection is a relative right[36], which is sacrificed in the instances where there is an absolute right[37]. Right to data protection is a pivotal right albeit only to the extent where it helps in the functioning of the society[38].

India stirs away from the notion of protecting individual fundamental rights and freedoms. The right to fair trial prevails over the right to privacy[39]. If an evidence is collected in a manner that is violative of the fundamental rights of the accused, it would still be admissible in the name of the right to trial and the "right to privacy must yield the right to a fair trial"[40].

The concept of Data equity which means that there must be a fair and just treatment of an individual or group must be followed to govern a digital evidence based trial. There must be utmost transparency and accountability measures to hold the data fiduciaries liable in cases of malpractice. The data principals should be empowered to engage more closely where their data is being utilized and the process of the transfer chain must be transparent[41]. Similarly, the concept of data stewardship allows people to engage with the personal data shared and take control over

[34] C 468/10 and C 469/10, Asociacio´n Nacional de Establecimientos Financieros de Cre´dito (ASNEF) (C 468/10), Federacio´n de Comercio Electro´nico y Marketing Directo (FECEMD) (C 469/10) v Administracio´n del Estado, 2011, ECR I-00000.
[35] Balboni et al., *supra* note 29.
[36] C-275/06, Productores de Música de España (Promusicae) v. Telefónica de España SAU, [2008] ECR I-271.
[37] C-553/07, College van burgemeester en wethouders van Rotterdam v. Rijkeboer, [2009] ECR I-3889.
[38] C-92 & 93/09, Volker und Markus Schecke GbR and Hartmut Eifert v. Land Hessen, [2010] ECR I-11063.
[39] M. P. Sharma v. Satish Chandra 1954 AIR 300.
[40] Deepti Kapur v. Kunal Jhulka 2020 SCCOnLine Del 672.
[41] Astha Kapoor & Richard S. Whitt, *Nudging Towards Data Equity: The Role of Stewardship and Fiduciaries in the Digital Economy*, SSRN Electron. J. (2021), https://www.ssrn.com/abstract=3791845 (last visited Sep 8, 2023).

its use. The principle behind data stewardship is that the citizens have the final say in how the data is being processed than any other way[42]. It can be concluded that data equity and data stewardship is a step ahead to giving unconditional consent. Transparency and accountability of data processing ensures that the digital evidence collected is not fabricated and misused.

One of the main aspect of the Act is the role data fiduciaries play in figuring data privacy violation. The holders of data have the utmost control over the data and the law should keep check whether justice is served rightfully.

PART-III

WHO IS A DATA FIDUCIARY

The term 'fiduciary' comes from the Latin term 'fiduciarius', and refers to 'one who holds anything in trust'.[43] Fiduciary relationships frequently involve a special blending of levels of risk, trust, and degree of entrustment. It arises from a consensual setting under which the fiduciaries have committed to a set of obligations.[44]The structure is however being battered down due to the digital economy where the fleece of liability is applied on parties that are using ubiquitous data collection. The concept of data fiduciary was first introduced in India through the Justice Srikrishna Committee Report[45] which illustrated terms like "data principal", "data fiduciaries" in the Indian context.

It is deduced that though both parties have a mutual benefit arising out of this setup, the power imbalance is clear when the subject matter is regarding forensics in digital crime, the fiduciary being the government. Here the government has to abide by "showing good faith and candour, where such other person reposes trust and special confidence in the person owing or discharging the duty"[46]. The Supreme Court of India has also pointed out the necessary tests for establishing

[42] *Id.*
[43] Evan Fox-Decent, *Sovereignty's Promise*, (2011), https://papers.ssrn.com/abstract=2729412 (last visited Sep 6, 2023).
[44] Edelman, J., 2014. The role of status in the law of obligations. In *Philosophical Foundations of Fiduciary Law* (pp. 21-38). Oxford University Press.
[45] COMMITTEE OF EXPERTS UNDER THE CHAIRMANSHIP OF JUSTICE B.N. SRIKRISHNA, https://www.meity.gov.in/writereaddata/files/Data_Protection_Committee_Report.pdf.
[46] Central Board of Secondary Education and Anr. v. Aditya Bandopadhyay and Ors. (2011) 8 SCC 497.

a fiduciary relationship between parties, such as the level of vulnerability and dependence of the parties[47] where they usually asses through a method of extension by association.[48]

The Indian courts have predominantly looked at facts even if it doesn't fit into the definition of relationship under data fiduciaries but rather stated that even an act would suffice for it to be deemed as a fiduciary relationship with the party.[49]

DUTIES OF A DATA FIDUCIARY

The data fiduciary has the innate responsibility to be loyal towards its data principals in terms of protecting their data and ensuring there is data localisation but when the government takes the data of its citizens during the trial, the aspect of acting in the best interests of the data principal is tethered due to various factors such as accountability and vulnerability. The state being a fiduciary has been discussed even in the Indian courts with respect to the government-citizen relationship.[50]Though there is no specific standard of loyalty due to the degree of the relationship between the data principal and the data fiduciary, it is important to ensure this is not taken advantage of. In a case, the Delhi High Court was of the opinion that the the rules might not be suited according to the needs of the parties for it be be treated as a fiduciary relationship but is still considered as a data fiduciary.

There is a strict standard of care in areas like company law, trust law and the medical law where the companies and the medical practitioners have the liability to ensure that the data of an individual evaluated has to be protected and disclosed at the right time.[51] They are also bound to have greater repercussions if there is a breach of fiduciary duties which acts as a deterrent in their power play.[52]

In terms of the type of data that falls under the jurisdiction of a data fiduciary, it is made to be broad by the Indian Courts with an inclusive of confidentiality i.e information not disclosed to the public, unlike the GDPR which only focuses on the misuse of “personal data”. When it

[47] Id
[48] Treesa Irish w/o Milton Lopez v. Central Information Commission and Ors. 2010
[49] Canbank Financial Services Ltd. v. Custodian and Ors ILR 2010 (3) Ker 892
[50] Kapila Hingorani v State of Bihar (2003) 6 SCC 1
[51] Sameer Kumar v. State of Uttar Pradesh (2014) All 48
[52] Leonard I Rotman, *FIDUCIARY LAW’S “HOLY GRAIL”: RECONCILING THEORY AND PRACTICE IN FIDUCIARY JURISPRUDENCE*, 91 BOSTON Univ. LAW Rev.

comes to the responsibility of fiduciary the state is not solely held responsible, even the entities involved such as the data processing units also have the duty to give access, provide and disclose.

While it is important to note that the present bill tries to bring in ex-ante measures by acting as a deterrent in privacy issues of the users and also ensuring the users or parties do not have to prove to the court that there exists a fiduciary relationship to come to court[53], it however, fails to address the extent of monopolisation of data while dealing with digital evidence.

The Act also provides for a "guardian data fiduciary"[54] aimed at safeguarding the rights of the children in cases of non-consensual advertisements or anything that causes 'significant harm' to the child. Another category called "special data fiduciary"[55] are aimed at safeguarding data users who is need of appointing a data protection officer due to its sensitivity or the kind of information that might impact the sovereignty and integrity of India or cause disruption in the public order.[56]

PART-IV

RECOMMENDATIONS

The need for protection of data is of paramount importance, especially in the field of digital forensics. Crimes have a way of surpassing the law at any given point in time and digital crimes are not far behind and constant development of technologies has made it easier for criminals to use the data of individuals irrevocably and to an extent which is impossible for the investigators to trace back. Hence we propose the need for decentralized blockchain technology which does not remain just in the hands of the data fiduciary i.e in this case, the state should also have a semi-open network system which can be accessed by an authorized individual during the trial such as the advocates and not just investigators.

[53] Fiduciary relationships as a means to protect privacy: Examining the use of the fiduciary concept in the draft Personal Data Protection Bill, 2019, https://blog.theleapjournal.org/2020/01/fiduciary-relationships-as-means-to.html (last visited Sep 10, 2023).
[54]The Digital Personal Data Protection Act, 2023, No. 22, Acts of Parliament, 2023 (India)
[55]The Digital Personal Data Protection Act, 2023, No. 22, Acts of Parliament, 2023 (India)
[56]The Digital Personal Data Protection Act, 2023, No. 22, Acts of Parliament, 2023 (India)

Therefore, cloud-based forensics is an important addition that needs to be applied by the current government to ensure there is vertical use of the DPDP Act 2023. Through various studies, it is understood that the cloud-based forensics analysis[57] integrates with evidences modelling[58] to assist the state agencies.[59]

The reason for advocating a blockchain system is due to its nature of being a non-transgressional product which not only eliminates the supervision but commodifies itself into a ledger system ensuring transparency, self-verification during investigations and verifiable evidence.[60]

There are however few challenges of using digital forensics, such as lack of international standards posed by the UN or any other international regulatory body. To remove this a blockchain framework called Block4Forensic[61] was created which helped in the interageration of various steps involved in the investigation. There was another similar platform that was introduced based on the Ethereum model[62] which not only helped in the ease of investigation for the legal community but also the ease of using these applications.

The decentralized ledger system ensures the protective framework of creating an investigation file that is linked back to its sources, giving an encyclopedic view of the items in one go. This also gives leeway to audit the case after it's completed. As discussed previously in the paper the application of a semi-open network system can only be controlled by a fool-proof system created by the Internet of Things forensics chain(IoTFC). Hence anything that is chained to this system cannot be tampered with by a third party. This protective layer also ensures there is an option of

[57] Big Data Forensics: Hadoop Distributed File Systems as a Case Study, springerprofessional.de, https://www.springerprofessional.de/en/big-data-forensics-hadoop-distributed-file-systems-as-a-case-stu/16571216 (last visited Sep 10, 2023).

[58]Shancang Li, Li Xu & Xinheng Wang, *Compressed Sensing Signal and Data Acquisition in Wireless Sensor Networks and Internet of Things*, 9 Ind. Inform. IEEE Trans. On 2177 (2013).

[59] Deqing Zou et al., *A Multigranularity Forensics and Analysis Method on Privacy Leakage in Cloud Environment*, 6 IEEE Internet Things J. 1484 (2019).

[60] Gulshan Kumar et al., *Internet-of-Forensic (IoF): A Blockchain Based Digital Forensics Framework for IoT Applications*, 120 Future Gener. Comput. Syst. 13 (2021).

[61] Mumin Cebe et al., *Block4Forensic: An Integrated Lightweight Blockchain Framework for Forensics Applications of Connected Vehicles*, 56 IEEE Commun. Mag. 50 (2018).

[62] Forensic-chain: Blockchain based digital forensics chain of custody with PoC in Hyperledger Composer - ScienceDirect, https://www.sciencedirect.com/science/article/abs/pii/S174228761830344X (last visited Sep 10, 2023).

tracing back the sources through which the evidence has been acquired unlike the other blockchain systems currently functioning in the world.[63]

Balkin,a Yale professor[64] suggests a more Adam Smith approach to the whole problem. He suggests there should be economic or a tax incentive for the data fiduciaries in return of abiding by their 'fiduciary obligation'[65]given the obligations are not nonspecific. Though he mentions that it does not tackle the power imbalances that are inherent in our current data feudalist structure, he says that it does not take away the leeway to pay fiduciaries like doctors and lawyers even though they are called as professions which are not created for profit. There is also the creation of data trusts which build on the concept of a bottom-up data governance where the data principles are both settlors and the beneficiaries of a pooled up rights of data under a certain legal framework known as 'Trust'.[66]

CONCLUSION

We can see that the above provisions under the Data Protection Act have been able to tackle the majority of the problems and yet are unable to address issues such as data localisation which was highly protested by the stakeholders. Technology has a way of creating havoc while also making advancements and this is the perfect example. The evidence gathered during an investigation process has a habit of backtracking especially in digital crimes where the data can be hindered or tampered with at any given time without the knowledge of the state or legal authorities. The only bright line here can be seen through the lens blockchain-induced forensic chain system as suggested in the paper if we ever want to keep the scale balanced.

[63]Li, Xu, and Wang, *supra* note 17.

[64] Nathan Heller, *We May Own Our Data, but Facebook Has a Duty to Protect It*, The New Yorker, Apr. 2018,https://www.newyorker.com/tech/annals-of-technology/we-may-own-our-data-but-facebook-has-a-duty-to-protect-it (last visited Sep 10, 2023).

[65] Jack M Balkin, *Information Fiduciaries and the First Amendment*, 49.

[66] Sylvie Delacroix & Neil D Lawrence, *Bottom-up Data Trusts: Disturbing the 'One Size Fits All' Approach to Data Governance*, Int. Data Priv. Law ipz014 (2019).