TEAM CODE: TL - 18

4TH SURANA & SURANA AND CUSAT SCHOOL OF LEGAL STUDIES, DR. A T MARKOSE MEMORIAL TECHNOLOGY LAW MOOT COURT COMPETITION, 2024

IN THE HON'BLE SUPREME COURT OF INDICA

UNDER ARTICLE 32 AND 139-A OF THE CONSTITUTION OF INDICA

WP NO._ OF 2023

CG CAR COMPANY AND OTHERS

(PETITIONER)

V.

UNION OF INDICA

(RESPONDENT)

MEMORIAL ON BEHALF OF THE RESPONDENT

TABLE OF CONTENTS

LIST OF ABBREVIATIONS

Anr	Another
v.	Versus
Hon'ble	Honourable
Ors.	Others
AIR	All India Report
SC	Supreme Court
SCC	Supreme Court Cases
SCR	Supreme Court Report
Art.	Article
Const.	Constitution
HC	High Court
Sec.	Section
No.	Number
Edn.	Edition
cd.	Code
cl.	Clause
&	And
IT Act	Information Technology Act, 2000
DPDP Act	The Digital Personal Data Protection Act, 2023
Anr	Another
v.	Versus
Hon'ble	Honourable
Ors.	Others
Anr	Another

INDEX OF AUTHORITIES

BOOKS

1. M P Jain, *Indian Constitutional Law* (7th edition, LexisNexis 2018) 533-549
2. Mahendra P. Singh, *V. N. Shukla's Constitution of India*, (11th edition, Eastern Book Company 2008) 160
3. H. M. Seervai, *Constitutional Law of India: A Critical Commentary* (Volume 1, 4th edition, Universal Law Publishing Co. Pvt. Ltd 1991) 435-440
4. Dr. L. M. Singhvi & Jagadish Swarup, *Constitution of India* (Volume 1, 3rd edition, Thomson Reuters 2013) 986
6. Dr. Durga Das Basu, *Commentary on the Constitution of India* (Volume 2, 8th Edition, LexisNexis 2007) 1464-1475
7. H. K. Saharay, *The Constitution of India An Analytical Approach* (4th Edition, Eastern Law House 2012) 274-281
8. Mamta Rao, *Constitutional Law* (Eastern Book Company pvt. ltd. 2021) 35
9. C.K. Takwani, *Textbook on Constitutional Law of India* (Whytes & co. 2021) 599

CASES

1. K.S. Puttaswamy v Union of India [2017] 10 SCC 1.
2. Ram Krishna Dalmia v Justice Tendolkar AIR 1958 SC 538 [547]
3. Maneka Gandhi v UOI [1978] AIR 597.
4. International Tourist Corporation v. The State of Haryana [1981] 2 SCC 318.
5. Supreme Court of India v Subhash Chandra Agarwal [2020] 5 SCC 481.
6. Modern Dental College and Research Centre v State of Madhya Pradesh (2016) 7 SCC 353.
7. Anuradha Bhasin v Union of India [2020] 3 SCC 637 [102].
8. Johnson Controls Technology Company v Schwöbel 2011 SCC OnLine BAEPO 399
9. Ukha Kolhe v State of Maharashtra AIR 1963 SC 1531.
10. State of Maharashtra v Natwarlal Damodardas Soni [1980] 4 SCC 669; State of H.P. v Pawan Kumar [2005] 4 SCC 350.

11. R.M. Malkani v State of Maharashtra AIR 1973 S.C. 157.
12. Ganga Ram v Habib-Ullah 1935 SCCOnline All 310; Matter of Great Public Importance Touching Upon the Independence of Judiciary, In re, [2019] 19 SCC 405.
13. State of Maharashtra v Natwarlal Damodardas Soni AIR 1980 S.C. 593; Radhkishan v. State of U.P. [1963] Supp. 1 S.C.R. 408.
14. Umesh Kumar v State of A.P. [2013] 10 SCC 591 [35].
15. Bharati Tamang v Union of India [2013] 15 SCC 578 [30].
16. Manoharan v. State [2020] 5 SCC 782.
17. P.N. Krishna Lal v Govt. of Kerala 1995 Supp (2) SCC 187.
18. Maneka Gandhi v Union of India [1978] 1 SCC 248.
19. Tofan Singh v State of T.N. [2021] 4 SCC 1 [398].
20. Bachan Singh v State of Punjab [1980] 2 SCC 684 [41].
21. State of Maharashtra v Bharat Shanti Lal Shah [2008] 13 SCC 5.
22. Raja Narayanlal Bansilal v Maneck Phiroz Mistry [1961] 1 SCR 417.
23. M.P. Sharma v Satish Chandra, 1954 SCR 1077 : AIR 1954 SC 300.
24. Kharak Singh v State of U.P. 1962 SCC OnLine SC 10.
25. State of Bombay v Kathi Kalu Oghad AIR 1961 SC 1808.
26. Ram Jethmalani v Union of India [2011] 8 SCC 1.
27. V.S. Kuttan Pillai v Ramakrishnan [1980] 1 SCC 264.
28. Selvi v State of Karnataka [2010] 7 SCC 263.
29. Nandini Satpathy v P.L. Dani [1978] 2 SCC 424.
30. Raja Narayanlal Bansilal v Maneck Phiroz Mistry AIR 1961 SC 29.
31. People's Union for Civil Liberties (PUCL) v. Union of India [1997] 1 SCC 301.
32. Vijay Madanlal Choudhary v Union of India 2022 SCC OnLine SC 929.
33. Krishnan Kakkanath v Govt. of Kerala [1997] 9 SCC 495.
34. Viklad Coal Merchant v Union of India [1984] 1 SCC 619 .
35. Nazeria Motor Service v State of A.P. [1969] 2 SCC 576.
36. Laxmi Khandsari v State of U.P. [1981] 2 SCC 600.
37. Federation of Hotel & Restaurant Association of India v Union of India [1989] 3 SCC 634.
38. Express Hotels Pvt. Ltd. v State of Gujarat [1989] 3 SCC 677.
39. Saghir Ahmad v State of U.P. [1955] 1 SCR 707.
40. Ramji Lal Modi v State of U.P. [1957] SCR 860.

41. Virendra v State of Punjab [1958] SCR 308.
42. Debi Saron v State of Bihar [1953] SCC OnLine Pat 100.
43. Om Prakash Sharma v CBI [2020] 5 SCC 679.
44. CBI v Vijay Sai Reddy [2013] 7 SCC 452.
45. Arjun Panditrao Khotkar v Kailash Kushanrao Gorantyal [2020] 7 SCC 1.
46. Paramjit Kaur v State of Haryana [2023] SCC OnLine P&H 3534.
47. People's Union for Civic Liberties v Union of India & Ors [1997] 1 SCC 301.
48. Maneka Gandhi v Union of India [1978] SCR (2) 621.
49. Ram Jethmalani v Union of India [2011] 8 SCC 1.
50. Malak Singh v State of Punjab [1981] 1 SCC 420.
51. Supdt., Central Prison v Dr. Ram Manohar Lohia [1960] SCC OnLine SC 43.
52. Franklin Templeton Trustee Services (P) Ltd. v Amruta Garg [2021] 9 SCC 606.
53. Municipal Corporation v. Indian Oil Corporation 1991 Supp (2) SCC 18.

STATUTES

1. The Constitution of India.
2. The Digital Personal Data Protection Act, 2023.
3. Information Technology Act, 2000.
4. The Evidence Act, 1872.
5. The Criminal Procedure Code, 1973.
6. Information Technology (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules 2009.
7. Telegraph Act, 1855.

ARTICLES

1. Aditya Sarmah, 'Privacy and the Right Against Self-Incrimination: Theorising a Criminal Process in the Context of Personal Gadgets' 3.2 CALQ [2017] 28.

2. Alekhya Sattigeri, 'Gauging the Constitutionality of S. 69 of the IT Act Vis-à-Vis Test of Proportionality Laid Down in KS Puttaswamy', (*Live Law,* 10 Apr 201)

<https://www.livelaw.in/columns/information-technology-act-2000-ks-puttaswamy-fundamental-rights-172407?infinitescroll=1> accessed on 27 Dec 2023.

3. Bedavyasa Mohanty, 'The Constitutionality of Indian Surveillance Law: Public Emergency as a Condition Precedent for Intercepting Communications' (*The Centre for Internet & Society*) <https://cis-india.org/internet-governance/blog/the-constitutionality-of-indian-surveillance-law> accessed on 27 December 2023.
4. Monica Shaurya Gohil and Chetna Bujad, 'Data Privacy Implications of Contact Tracing Apps in India' (2021) 11.1 NULJ 1.
5. Vinod Joseph & Protiti Basu, 'Right of Erasure - Under the Personal Data Protection Bill, 2019' (*MONDAQ*) <https://www.mondaq.com/india/data/protection/877732/right-of-erasure---under-the-personal-data-protection-bill-2019> accessed on 27 December 2023.
6. Supratim Chakraborty, 'Data Protection in India: Overview' (Khaitan & Co. LLP) <https://www.khaitanco.com/sites/default/files/2021-04/Data%20Protection%20in%20India%20Overview.pdf> accessed on 3 January 2024.

INTERNATIONAL LEGISLATION

1. The General Data Protection Regulation, 2016.
2. European Data Protection Board's Guidelines 01/2020 on processing personal data in the context of connected vehicles and mobility related applications.

OTHER SOURCES

1. Justice B.N. Srikrishna Committee, A Free and Fair Digital Economy [2018].
2. Chapter 8, Committee of Experts under the Chairmanship of Justice B.N. Srikrishna
3. EU General Data Protection Regulation (GDPR): Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), OJ 2016 L 119/1.
4. Department of Telecommunication, Ministry of Communications & Government of India, Licensing Agreement for Unified License [2014].

5. Reserve Bank of India (RBI), Report on Internet Banking [2001].
6. SEBI, Securities and Exchange Board of India (SEBI) Guidelines on Internet based Trading and Services [2000].

STATEMENT OF JURISDICTION

The Hon'ble Court has Jurisdiction to hear the instant matter under Art. 32 and Article 139-A of the Constitution of Indica. Art. 32 of the Constitution of Indica reads as:

"32. Remedies for enforcement of rights conferred by this Part
(1) The right to move the Supreme Court by appropriate proceedings for the enforcement of the rights conferred by this Part is guaranteed
(2) The Supreme Court shall have power to issue directions or orders or writs, including writs in the nature of habeas corpus, mandamus, prohibition, quo warranto and certiorari, whichever may be appropriate, for the enforcement of any of the rights conferred by this Part
(3) Without prejudice to the powers conferred on the Supreme Court by clause (1) and
(2), Parliament may by law empower any other court to exercise within the local limits of its jurisdiction all or any of the powers exercisable by the Supreme Court under clause (2)
(4) The right guaranteed by this article shall not be suspended except as otherwise provided for by this Constitution"

Article 139-A grants power to the Supreme Court to Transfer certain cases

"139A. Transfer of certain cases-
(1) Where cases involving the same or substantially the same
questions of law are pending before the Supreme Court and one or more High Courts or before two or more High Courts and the Supreme Court is satisfied on its own motion or on an application made by the Attorney-General of India or by a party to any such case that such questions are substantial questions of general importance, the Supreme Court may withdraw the case or cases pending before the High Court or the High Courts and dispose of all the cases itself:
Provided that the Supreme Court may after determining the said questions of law return any case so withdrawn together with a copy of its judgment on such questions to the High Court from which the case has been withdrawn, and the High Court shall on receipt thereof, proceed to dispose of the case in conformity with such judgment.
(2) The Supreme Court may, if it deems it expedient so to do for the ends of justice, transfer any case,

appeal or other proceedings pending before any High Court to any other High Court."

The Respondent shall humbly accept the Court's decision as final and binding and execute it in good faith and with due diligence.

STATEMENT OF FACTS

INDICA

The Republic of Indica is a democratic country and has become a fast-growing major economy. The Parliament of Indica enacted various legislations to regulate the advancements that have occurred. One such prominent legislation was the Information Technology Act in the year 2000 which was extensively amended in 2008.

THE ACCIDENT

On 13th of August 2022, at about 7:00 am, a family, on vacation, saw a body lying in a pool of blood on the road next to the car (with registration number SK 47 BH 1234). The police arrived and after searching, understood that the body was of Mr. Anand.

UNDISPUTED FACTS

The police took note of the vehicles passed through State Highway No. 106 and decided to investigate more into Mr. Ian. Police confiscated Mr. Ian's car, and identified that the said vehicle had onboard ICT facilities which could show details of the vehicle.

AUTOMATED SYSTEM

The automated system used in CG-Metron used blockchain technology for storing data and the access to the same was using the private key with the owner. The electronic modules used in the vehicle recorded information about driving, vehicle conditions and features.

THE DISPUTE

This proceeding was challenged by Mr. Ian the High Court of Antartaka. The Head office of CG Car Company in India filed a writ petition in the Hon'ble Supreme Court of Indica. The Supreme Court of Indica ordered the transfer of the connected case and decided to hear both the matters.

STATEMENT OF ISSUES

ISSUE 1

WHETHER SECTION 69 OF THE INFORMATION TECHNOLOGY ACT, 2000 IS CONSTITUTIONALLY VALID?

ISSUE 2

WHETHER GOVERNMENTAL CONTROL OVER THE USE OF CRYPTOGRAPHIC TECHNIQUES IS TOO RESTRICTIVE IN NATURE?

SUMMARY OF ARGUMENTS

ISSUE 1

The Counsel on behalf of the Respondents humbly submit, before this Hon'ble Court, that section 69 of the Information Technology Act, 2000, appears constitutionally valid under a three-pronged assessment. It passes the tests of Legality, Necessity, and Proportionality, aligning with privacy principles in the Digital Personal Data Protection Act (DPDP Act). Vehicular information, not classified as personal data, falls within legal bounds. Illegally obtained evidence is generally admissible, subject to scrutiny. The provision doesn't violate the right against self-incrimination, as no formal accusation exists. Safeguards and compliance with interception rules further support the constitutionality of Section 69. The arguments collectively affirm its validity, addressing constitutional concerns.

ISSUE 2

The Counsel on behalf of the Respondents humbly submit, before this Hon'ble Court, that the control over the use of cryptographic techniques is not too restrictive in nature. Firstly, the mandatory requirement to submit the usage of cryptographic requirements is not too restrictive as it is in line with the parent legislation. Secondly, the control over cryptographic techniques is backed by adequacy of procedural safeguards. Thirdly, the restrictions imposed by the government does not infringe the rights of the Petitioners as it amounts to reasonable restrictions imposed under Article 19. Additionally, governmental control over cryptographic techniques is also in consonance with the Code of Criminal Procedure, Digital Personal Data Protection Act, 2023 and the Non-Personal Data governance framework. Therefore, it is submitted that the governmental control over cryptographic techniques is not too restrictive.

ARGUMENTS ADVANCED

ISSUE 1

WHETHER SECTION 69 OF THE INFORMATION TECHNOLOGY ACT, 2000 IS CONSTITUTIONALLY VALID?

1. The Respondents' Counsel respectfully asserts that Section 69 of the Information Technology Act, 2000, stands constitutionally sound through a comprehensive evaluation based on legality, necessity, and proportionality. It successfully aligns with privacy principles outlined in the Digital Personal Data Protection Act (DPDP Act). Vehicular data, not considered personal information, remains within legal parameters. Admissibility of illegally obtained evidence is generally acceptable, pending careful examination. The provision doesn't infringe upon the right against self-incrimination due to the absence of a formal accusation. Furthermore, adherence to safeguards and interception rules strengthens the constitutional validity of Section 69, addressing pertinent concerns.

I. FALLS UNDER REASONABLE RESTRICTION

2. It is submitted that Section 69 of the IT Act[1] is a reasonable restriction on the Right to Privacy provided under the Constitution of Indica. It satisfies the three-pronged test of Legality, Necessity and Proportionality laid down in K.S. Puttuswamy v. Union of India,[2] for it to qualify as a reasonable restriction. The premise of the present submission is threefold: (i) Section 69 of the IT Act satisfies the condition of **Legality;** (ii.) Section 69 of the IT Act satisfies the test of **Necessity**; and (iii.) Section 69 of the IT Act satisfies the test of **Proportionality**.

(i) SECTION 69 QUALIFIES THE TEST OF LEGALITY

3. It is submitted that Section 69 of the IT Act satisfies the condition of legality as Article 21 of the Constitution of Indica is not absolute and falls under the reasonable

[1] Information Technology Act 2000, s 69.
[2] *K.S. Puttaswamy v Union of India* [2017] 10 SCC 1.

restrictions. The condition of legality requires that there must be the existence of Law.[3] The provisions of the Act are constitutional. There is a presumption in favor of the constitutionality of an enactment and the burden to prove the contrary is upon the person who challenges it.[4]

4. Section 69 of the IT Act inherently fulfils the criterion of legality,[5] as it was enacted by the Parliament, and the Parliament possesses the authority to pass such laws. Examining Article 248 in conjunction with Entry 97 of List 1 in the 7th schedule, it becomes evident that Parliament holds exclusive authority to legislate on residuary subjects.[6] For a state legislature to assert legislative competence, the subject in question must not be enumerated in the State list or Concurrent list.[7]
5. Section 69 of the IT Act includes for preventing incitement to the commission of any cognizable offence relating to above or for investigation of any offence, which falls well within the ambit of the current investigation against Mr. Ian.

(ii) SECTION 69 QUALIFIES THE TEST OF NECESSITY

6. It is submitted that Section 69 of the IT Act satisfies the test of Necessity. The requirement of a need, in terms of legitimate State aim, ensures that the law which imposes restrictions is reasonable and does not suffer from manifest arbitrariness.[8]
7. The information acquired from unlocking with the private key is necessary for the investigation against Mr. Ian and this requirement does not suffer from manifest arbitrariness as the Petitioner was required to submit a public key.
8. In the case of *Facebook Inc. v. UOI*,[9] the court highlighted that de-encryption, if available easily, could defeat the fundamental right of privacy and de-encryption of messages may be done under special circumstances but it must be ensured that the privacy of an individual is not invaded. However, at the same time, the sovereignty of the State and the dignity and reputation of an individual are required to be protected. For purposes of detection, prevention and **investigation of certain criminal activities it may be necessary** to obtain such information. De-encryption and revelation of the

[3] *K.S. Puttaswamy v Union of India* [2017] 10 SCC 1 [310].
[4] *Ram Krishna Dalmia v Justice Tendolkar* AIR 1958 SC 538 [547].
[5] *Maneka Gandhi v UOI* [1978] AIR 597.
[6] The Constitution of India, art. 248.
[7] *International Tourist Corporation v. The State of Haryana* [1981] 2 SCC 318.
[8] *K.S. Puttaswamy v. Union of India* [2017] 10 SCC 1 [310].
[9] Facebook Inc v Union of India, 2019 SCCOnline SC 1264.

identity of the originator may also be necessary in certain other cases, some of which have been highlighted hereinabove.

(iii) SECTION 69 QUALIFIES THE TEST OF PROPORTIONALITY

9. It is submitted that Section 69 of the IT Act satisfies the test of Proportionality.[10] The proportionality test laid down[11] states that a measure must serve a legitimate goal; be a suitable means of furthering this goal; there must not be any less restrictive but equally effective alternative; and the measure must not have a disproportionate impact on the right-holder.
10. In the current case the investigation to understand the death of Mr. Anand and his family is the legitimate goal and acquiring the private key to decrypt the data is a suitable means of furthering the goal. It is not restrictive and does not have any disproportionate impact on Mr. Ian as the data collected does not amount to "personal information".
11. Therefore, as Section 69 satisfies the 3-pronged test it also satisfies the interception rules laid down in *Anuradha Bhasin*,[12] in which the interception rule under the section 5(2) of Telegraph Act provides for lawful interception in the interests of the sovereignty, and integrity of India, the security of the State, friendly relations with Foreign States or public order or for preventing incitement to the commission of an offence.

II. SECTION 69 IS IN CONSONANCE WITH THE FUNDAMENTAL PRINCIPLES OF PRIVACY

12. The Digital Personal Data Protection Act (DPDP Act) emerged from the landmark Puttaswamy judgement, which recognized privacy as a fundamental right in India. Inspired by the Puttaswamy Court's reliance on international principles and foreign precedents, the DPDP Act embodies these principles, including purpose limitation, data minimization, transparency, and individual rights. It builds upon the Puttaswamy foundation, translating its ideals into a comprehensive framework for protecting personal data in the digital age.

[10] *Supreme Court of India v Subhash Chandra Agarwal* [2020] 5 SCC 481.
[11] *Modern Dental College and Research Centre v State of Madhya Pradesh* (2016) 7 SCC 353.
[12] *Anuradha Bhasin v Union of India* [2020] 3 SCC 637 [102].

13. Section 69 of the IT Act aligns with the Data Protection Act's Sections 17(1)(c)[13] and 17(2)(a).[14] Section 69 empowers government agencies to intercept or decrypt data for reasons of national interest, public order, or preventing offenses. Section 69 of the IT Act, in alignment with the Data Protection Act's Sections 17(1)(c) and 17(2)(a), is particularly relevant in the context of **investigations**. It empowers authorized government agencies to intercept, monitor, or decrypt information stored in computer resources when necessary for investigation purposes. This aligns with Section 17(1)(c) of the Data Protection Act, which exempts the application of certain provisions such as consent,[15] notice,[16] and processing of personal data,[17] when personal data processing is essential for the investigation or prosecution of offenses.
14. In the committee report under the Chairmanship of Justice B.N. Srikrishna,[18] it determined the circumstances under which the consent is either not appropriate, necessary, or relevant for processing. To understand the nature of the interests owing to which non-consensual processing will be permitted, a useful starting point would be the Puttaswamy judgment. Chandrachud, J., identified four legitimate state interests 'to be considered in the context of privacy'. He listed 'national security', 'prevention and investigation of crime', 'protection of revenue' and 'allocation of resources for human development'.[19]
15. Therefore, the CG-Metron data stored in the blockchain technology can be accessed in the course of an investigation as it falls well within the exemptions mentioned under the DPDP Act, 2023 and its preceding committee report.

III. VEHICULAR INFORMATION DOES NOT CLASSIFY AS "PERSONAL INFORMATION"

16. According to the DPDP Act, 2023 it defines "personal data"[20] as any data about an individual who is identifiable by or in relation to such data. Vehicular information such

[13] Digital Personal Data Protection Act, 2023 s 17(1)(c).
[14] Digital Personal Data Protection Act, 2023 s 17(2)(a).
[15] Digital Personal Data Protection Act, 2023 s 6.
[16] Digital Personal Data Protection Act, 2023 s 5.
[17] Digital Personal Data Protection Act, 2023 s 4.
[18] Justice B.N. Srikrishna Committee, *A Free and Fair Digital Economy* [2018].
[19] Chapter 8, Committee of Experts under the Chairmanship of Justice B.N. Srikrishna.
[20] Digital Personal Data Protection Act, 2023 s 2(t).

as charging events and status, the enabling/disabling of various systems, diagnostic trouble codes, speed, direction, etc cannot be used to identify any person.

17. The European Guidelines on processing data in the context of connected vehicles and mobility related applications[21] categorizes vehicle related data into "offense related" data which in order to process data that relate to potential criminal offences within the meaning of art. 10 GDPR which states that "*Processing of personal data relating to criminal convictions and offences or related security measures based on Article 6(1) shall be carried out only under the control of official authority or when the processing is authorised by Union or Member State law providing for appropriate safeguards for the rights and freedoms of data subjects. 2Any comprehensive register of criminal convictions shall be kept only under the control of official authority.*" This is similar to Section 69 of the IT Act, 2000 and Section 17(1)(c) of the DPDP Act, 2023.
18. Therefore, since the vehicle information system doesn't classify as personal data and falls within the ambit of **"offense related" data**, it does not violate the Right to Privacy laid down by K.S. Puttaswamy v. UOI and enshrined in Article 21 of the Constitution of Indica.
19. In the *Johnson Controls Technology case*,[22] the court declared that vehicular information system which was required as evidence did not classify as "personal data".

IV. ADMISSIBILITY OF ILLEGALY OBTAINED EVIDENCE

20. The overwhelming judicial view is thus that illegally obtained evidence is admissible except where a prejudice is caused to the accused. Further, such evidence is to be viewed with care and caution.[23] It was held, assuming that the search was illegal,[24] it **did not affect the validity of the seizure** and its admissibility in evidence.[25] At the most the court may be inclined to examine carefully[26] the evidence relating to the

[21] EU General Data Protection Regulation (GDPR)*:* Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), OJ 2016 L 119/1.
[22] *Johnson Controls Technology Company v Schwöbel* 2011 SCC OnLine BAEPO 399.
[23] *Ukha Kolhe v State of Maharashtra* AIR 1963 SC 1531.
[24] *State of Maharashtra v Natwarlal Damodardas Soni* [1980] 4 SCC 669; *State of H.P. v Pawan Kumar* [2005] 4 SCC 350.
[25] *R.M. Malkani v State of Maharashtra* AIR 1973 S.C. 157.
[26] *Ganga Ram v Habib-Ullah* 1935 SCCOnline All 310; *Matter of Great Public Importance Touching Upon the Independence of Judiciary*, In re, [2019] 19 SCC 405.

seizure.[27] It is a settled legal proposition that even if a document is procured by improper or illegal means, there is no bar to its admissibility if it is relevant and its genuineness is proved. If the evidence is admissible, it does not matter how it has been obtained.[28]

21. The K.S. Puttaswamy Judgement laid down that the state has a duty to protect an individual's reasonable expectation of privacy but the same must be balanced against a "reasonable" search in public interest.[29]
22. Therefore, the police trying to hack into the blockchain technology to obtain the private key constitutes as reasonable search in public interest and was necessary for furthering the means of the investigation as laid down in the test of necessity. The evidence obtained through the private key would be admissible as the petitioners were required to submit a public key.
23. The *Bharati Tamang*[30] case rejects the argument that intercepted materials violate constitutional rights. The investigation is ongoing, and the intercepted materials have been sent for forensic analysis.[31] The court holds that it's premature to exclude such evidence, allowing the accused to challenge the forensic report during the trial court proceedings. Similarly, the court cannot reject the admission of the data as it does not violate any constitutional rights such as the right against self-incrimination under article 20(3) of the Constitution of Indica.[32]

V. NOT VIOLATIVE OF RIGHT AGAINST SELF INCRIMINATION

24. The automated system used in CG-Metron used blockchain technology for storing data. The same was encrypted using an **asymmetric cryptographic** technique and the access to the same was using the private key with the owner.[33] Therefore, CG Car Company was required to submit a **public key**[34] because the blockchain technology was stored using an asymmetric key and they haven't complied with the **procedure laid down by**

[27] *State of Maharashtra v Natwarlal Damodardas Soni* AIR 1980 S.C. 593; R*adhkishan v. State of U.P*. [1963] Supp. 1 S.C.R. 408.
[28] *Umesh Kumar v State of A.P*. [2013] 10 SCC 591 [35].
[29] P. 99, *Hunter v Southam Inc*. [1984] 2 SCR 145.
[30] *Bharati Tamang v Union of India* [2013] 15 SCC 578, p. 30.
[31] *Manoharan v. State* [2020] 5 SCC 782.
[32] P.*N. Krishna Lal v Govt. of Kerala* 1995 Supp (2) SCC 187.
[33] Moot Proposition [16].
[34] Information Technology Act 2000, s 2(f).

law.[35] For, no person can be deprived of his life or personal liberty except in accordance with the procedure established by law.[36] Laws that prevent organised crime or if it is intended to collect the evidence to the commission of such an organised crime through interception, shall be upheld.[37] The investigating officers issued notice through proper channels to the manufacturers of the car to provide assistance to decrypt the said protection.[38]

25. The essential conditions for invoking the constitutional guarantee enshrined in Article 20(3) is that a formal accusation relating to the commission of an offence.[39] In *M.P. Sharma*,[40] the court lays down that the constitutional right against self-incrimination can be invoked only when there is a **formal accusation** filed against them. In the current case, there is no such formal accusation filed against Mr. Ian which violates his right to privacy[41] and right against self-incrimination.[42]
26. In the case of *Ram Jethmalani v. UOI,*[43] the court stated that disclosure[44] of information which is relevant to the investigation[45] is necessary when there is no formal accusation against a person. Withholding of information by the petitioners can be permissible on when it's done under the exceptions laid down in Article 19(2) of the Constitution.
27. The second requirement for invoking Article 20(3) is that the person is **required to give evidence against herself**. [46] As proved in the above argument, submitting vehicular information **doesn't classify as "personal information".** The third requirement is there should be compulsion,[47] there was **no act of "compulsion"** conducted on the behalf of police to acquire any evidence. [48]

---

[35] *Maneka Gandhi v Union of India* [1978] 1 SCC 248; *Tofan Singh v State of T.N*. [2021] 4 SCC 1 [398].
[36] *Bachan Singh v State of Punjab* [1980] 2 SCC 684 [41].
[37] *State of Maharashtra v Bharat Shanti Lal Shah* [2008] 13 SCC 5.
[38] Moot Proposition [17].
[39] *Raja Narayanlal Bansilal v Maneck Phiroz Mistry* [1961] 1 SCR 417.
[40] *M.P. Sharma v Satish Chandra*, 1954 SCR 1077 : AIR 1954 SC 300; *Kharak Singh v State of U.P*. 1962 SCC OnLine SC 10.
[41] Aditya Sarmah, 'Privacy and the Right Against Self-Incrimination: Theorising a Criminal Process in the Context of Personal Gadgets' 3.2 CALQ [2017] 28.
[42] *State of Bombay v Kathi Kalu Oghad* AIR 1961 SC 1808.
[43] *Ram Jethmalani v Union of India* [2011] 8 SCC 1.
[44] Information Technology (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules, 2009, Rule 17.
[45] V.*S. Kuttan Pillai v Ramakrishnan* [1980] 1 SCC 264.
[46] *Selvi v State of Karnataka* [2010] 7 SCC 263.
[47] *Nandini Satpathy v P.L. Dani* [1978] 2 SCC 424.
[48] Proposition [18].

28. The private key needs to be submitted by the petitioner to comply with Section 65B(2)(c)[49] and 85B[50] of the Evidence Act to **prevent alteration** such as to affect the electronic record or the accuracy of its contents of the data necessary for the completion of the investigation.
29. Therefore, as the current case does not satisfy the grounds to invoke of Article 20(3), it upholds Article 14 of the Constitution of Indica.[51]

VI. COMPLIED WITH SAFEGUARDS FOR SECTION 69

30. For interception or decryption of communication on grounds such as national security, the Supreme Court (1996) had mandated various safeguards including: (i) establishing necessity, (ii) purpose limitation,[52] and (iii) storage limitation.[53] This was laid down in *PUCL v. UOI,* which allowed the interception of data under section 5(2) of the Telegraph Act when it is in the in the interests of the sovereignty, and integrity of India, the security of the State, friendly relations with Foreign States or public order or for preventing incitement to the commission of an offence.
31. The Srikrishna Committee (2018)[54] had recommended that in case of processing on grounds such as national security and prevention and prosecution of offences, obligations other than fair and reasonable processing and security safeguards should not apply. The Information Technology (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules, 2009 [hereinafter referred to as "**Interception Rules**"], in **Rule 4**[55] clearly lays down procedure for purpose limitation and storage limitation.
32. Therefore, Section 69 complies with the purposes laid down in **Section 65B**[56] of the Evidence Act. It also satisfies the purpose limitation mentioned in **Section 39** of the Evidence Act by taking only the part of the evidence required for the investigation under the Rule 4 of the Interception Rules.

---

[49] Digital Personal Data Protection Act 2023, s 65B(2)(c).
[50] Digital Personal Data Protection Act 2023, s 85B.
[51] *Raja Narayanlal Bansilal v Maneck Phiroz Mistry* AIR 1961 SC 29.
[52] Digital Personal Data Protection Act 2023, s 6(1).
[53] *People's Union for Civil Liberties (PUCL) v. Union of India* [1997] 1 SCC 301.
[54] Justice B.N. Srikrishna Committee, *A Free and Fair Digital Economy* [2018].
[55] Information Technology (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules, 2009, S.I. 2009/1234.
[56] Indian Evidence Act 1872, s 65B(5)(b).

33. The above line of arguments prove that Section 69 of the IT Act, 2000 is constitutionally valid and does not violate Article 14, Art. 19, Art. 20(3), Art. 21 of the Constitution of Indica.[57]

[57] *Vijay Madanlal Choudhary v Union of India* 2022 SCC OnLine SC 929.

ISSUE 2

WHETHER GOVERNEMNT RESTRICTIONS ON CRYPTOGRAPHIC TECHNIQUES ARE TOO RESTRICTIVE OR NOT

34. The Respondents' Counsel suggests that the regulation of cryptographic techniques is not excessively restrictive. Firstly, the mandatory submission of cryptographic usage aligns with the relevant existing legislation. Secondly, the oversight of cryptographic techniques is supported by robust procedural safeguards. Thirdly, these government-imposed restrictions do not violate the Petitioners' rights, constituting reasonable constraints under Article 19. Furthermore, governmental control over cryptographic techniques is consistent with the Code of Criminal Procedure, Digital Personal Data Protection Act, 2023, and the Non-Personal Data governance framework. Thus, it is contended that the governmental regulation of cryptographic techniques is appropriately balanced and not unduly restrictive.
35. The Respondents humbly submit before this Hon'ble Court that the government control over cryptographic techniques is not too restrictive for the following reasons:

I. MANDATORY REQUIREMENT TO SHARE CRYPTOGRAPHIC TECHNIQUES NOT TOO RESTRICTIVE

36. The Rules with respect to the use of cryptographic tools requires cryptographic algorithms that were proposed to be used by anyone for any purpose to be submitted to 'The Authority on Control and Regulation of Cryptography'[58].
37. The above stated requirement is not far too restrictive, as the **IT Act, 2000 empowers the government to prescribe modes and methods for encryption**[59]. Examples of this can be seen in the DoT & ISP Licensing agreement,[60] RBI guidelines[61] and SEBI guidelines.[62]
38. The IT Act, 2000 also empowers the government to prescribe security procedures and practices with regards to securing electronic records and securing electronic

[58] Moot proposition [20].
[59] Information Technology Act 2000, s 84-A.
[60] Department of Telecommunication, Ministry of Communications & Government of India, Licensing Agreement for Unified License [2014].
[61] Reserve Bank of India (RBI), Report on Internet Banking [2001].
[62] SEBI, Securities and Exchange Board of India (SEBI) Guidelines on Internet based Trading and Services [2000].

signatures[63]. The power to make rules in prescribing security procedures and practices is also given in the IT Act.[64]

39. Thus, it is abundantly clear that the rules made that establish governmental control over cryptographic techniques, are in line with the provisions of the parent act. In the case of *Municipal Corporation v. Indian Oil Corporation*[65], the Supreme Court upheld the validity of delegated legislation, when it is in line with the provisions of the parent act.

II. ADEQUACY OF PROCEDURAL SAFEGUARDS

40. Sec. 69 of the Information Technology Act, 2000 confers upon the government to issue directions for the decryption of information from computer sources. The Rules made thereunder provide for a **just and fair procedure** for regulating the exercise of powers conferred under Sec. 69 of the IT Act.
41. The cases of *PUCL v. Union of India*[66] & *Maneka Gandhi v. Union of India*[67], both of which dealt with the validity of powers conferred under Sec. 5(2) of Telegraph Act, 2005, held that the powers conferred by the Telegraph Act must have procedural backing so that the exercise of power is just, fair and reasonable in order to safeguard the rights[68] of the citizens guaranteed by the Constitution of India.
42. Since Sec. 69 of the IT Act, 2000 has procedural backing[69] that ensure the exercise of power is just, fair and reasonable, the impugned provision must be held valid as it has adequate procedural safeguards.

III. DOES NOT AMOUNT TO AN INFRINGEMENT ON THE FREEDOM TO PRACTICE ANY BUSINESS[70]

43. Sec. 69 of the Information Technology Act, 2000 and the rules made thereunder, confer upon the government the power to issue directions for decryption of information from computer sources. This provision and the rules also impose an obligation upon

[63] Information Technology Act 2000, s 16.
[64] Information Technology Act 2000, s 87(2)(ea).
[65] *Municipal Corporation v. Indian Oil* Corporation 1991 Supp (2) SCC 18.
[66] *People's Union for Civic Liberties v Union of India & Ors* [1997] 1 SCC 301.
[67] *Maneka Gandhi v Union of India* [1978] SCR (2) 621.
[68] Constitution of India, art 19; Constitution of India, art 21.
[69] Information Technology (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules, 2009.
[70] Constitution of India, art 19(1)(g).

intermediaries to extend all facilities and technical assistance in the decryption of said information. In the present case, CG Car Company, along with other car manufacturers, have felt that this is likely to affect their business in Indica substantially.

44. However, this is no way impacts their freedom to practice any business and does not infringe on their rights guaranteed under Art. 19(1)(g). It has been held by the Supreme Court that an infringement of the freedom guaranteed under Art. 19(1)(g) must have a direct impact on the restriction on such freedom, and not ancillary or incidental effects on such freedom[71].

45. It was held in the case of *Nazeria Motor Service v. State of A.P.* [72] that any measure that would result in the diminution of profits cannot be held to be violative of Art. 19(1)(g), even if the profits would be greatly reduced. A similar position has also been held in a number of judgements given by the Apex Court[73].

IV. AMOUNTS TO REASONABLE RESTRICTIONS IMPOSED UNDER ARTICLE 19

(i) THE RESTRICTION IMPOSED IS IN THE INTEREST OF GENERAL PUBLIC[74]

46. The restriction imposed by the impugned provision can be held to be a reasonable restriction. The reasonableness of a restriction must be determined in an objective manner and from the standpoint of the interests of the general public, and not from the standpoint of the persons upon whom the restrictions are imposed[75]. A restriction imposed cannot be held to be unreasonable merely for the reasons that it operates harshly[76]. In the present case, the restriction imposed on CG Car Company can most certainly held to be reasonable even though it is likely to affect their business substantially, as long as the restriction imposed is in the interest of the general public.

47. The term **'in the interest of general public'** has been interpreted in a manner that gives a very **wide ambit** with regards to the protection that the restriction imposed aims to

[71] *Krishnan Kakkanath v Govt. of Kerala* [1997] 9 SCC 495; *Viklad Coal Merchant v Union of India* [1984] 1 SCC 619.
[72] *Nazeria Motor Service v State of A.P.* [1969] 2 SCC 576.
[73] *Laxmi Khandsari v State of U.P.* [1981] 2 SCC 600; *Federation of Hotel & Restaurant Association of India v Union of India* [1989] 3 SCC 634; *Express Hotels Pvt. Ltd. v State of Gujarat* [1989] 3 SCC 677.
[74] Constitution of India, art 19(6).
[75] *Krishnan Kakkanath v Govt. of Kerala* [1997] 9 SCC 495; *Saghir Ahmad v State of U.P.* [1955] 1 SCR 707.
[76] *Krishnan Kakkanath v Govt. of Kerala* [1997] 9 SCC 495; *Saghir Ahmad v State of U.P.* [1955] 1 SCR 707.

achieve, and a restriction imposed under Article 19 can be to provide for the protection of the general public against any particular evil[77]. Thus, the restriction imposed by the Sec. 69 of the Information Technology Act, 2000 and the Rules made thereunder would be reasonable if the power to issue directions for decryption are done so for any of the grounds[78] as mentioned in the said provision.

V. IN CONSONANCE WITH THE CODE OF CRIMINAL PROCEDURE

48. Sec. 69 of the Information Technology Act, 2000 confers upon the government similar powers to ones given by the Code of Criminal Procedure[79]. Sec. 91 of the CrPC gives a police officer or a court, the power to issue an order or summons for the production of a document or a thing, if such production is deemed necessary or desirable for the purpose of any investigation, inquiry, trial or other proceedings. This power of the government can be exercised over any person, who has possession or power over such document or thing.
49. The Apex Court has held that the only requirement for the exercise of the powers under Sec. 91 of the CrPC would be necessity or desirability of such document or thing for the purposes of the investigation, inquiry, trial or other proceedings[80]. The Supreme Court has also held that when an investigating officer is in need of certain documents/information, the same must be provided as per **Sec. 91 of the CrPC**, and that there is no requirement of a court order for such instances[81]. It has also been held that Sec. 91 of the CrPC gives power to a police officer or court to issue an order or summons for the production of electronic records as well[82].
50. It is very evident that Sec. 69 of the IT Act and Sec. 91 of the CrPC confers upon public authorities very analogous powers. Since the Courts have upheld the validity of the powers conferred by Sec. 91 of the CrPC, the powers conferred by Sec. 69 of the IT Act, 2000 must also be similarly upheld.

---

[77] *Ramji Lal Modi v State of U.P.* [1957] SCR 860; *Virendra v State of Punjab* [1958] SCR 308; *Debi Saron v State of Bihar* [1953] SCC OnLine Pat 100.
[78] Information Technology Act 2000, s 69.
[79] The Code of Criminal Procedure 1973, s 91.
[80] *Om Prakash Sharma v CBI* [2020] 5 SCC 679.
[81] *CBI v Vijay Sai Reddy* [2013] 7 SCC 452.
[82] *Arjun Panditrao Khotkar v Kailash Kushanrao Gorantyal* [2020] 7 SCC 1; *Paramjit Kaur v State of Haryana [2023] SCC OnLine P&H 3534.*

VI. IN CONSONANCE WITH THE DIGITAL PERSONAL DATA PROTECTION ACT, 2023

51. The Digital Personal Data Protection Act, 2023 confers upon the government to power to call for any information from a Data Fiduciary or an Intermediary[83]. The Act also states that no suit or legal proceedings can be instituted against the government or a public authority, for any action taken in good faith[84]. Additionally, the DPDP Act also exempts a data fiduciary from their duties when the data is processed in the interest of prevention, detection, **investigation or prosecution of any offence** or contravention of any law[85]. This Act also permits the processing of personal data by the government or an instrumentality[86] for the grounds as set out in Sec. 17(2)(a) of the Act.
52. Thus, Sec. 69 of the IT Act and the rules made thereunder[87] are in conformity with the provisions of the DPDP Act, and therefore must be upheld.

VII. IN CONSONANCE WITH THE EXPERT COMMITTEE REPORT ON NON-PERSONAL DATA[88]

53. The Expert Committee Report on Non-Personal Data enables the government the right to request non-personal data by the government or a public entity for **sovereign purposes**, which includes investigations and law enforcement.
54. Thus, Sec. 69 of the IT Act, and the rules made thereunder, are also in conformity with the Expert Committee Report on Non-Personal Data, and therefore, cannot be held to be too restrictive.

[83] Digital Personal Data Protection Act, 2023, s 36.
[84] Digital Personal Data Protection Act, 2023, s 35.
[85] Digital Personal Data Protection Act, 2023, s 17(1)(c).
[86] Digital Personal Data Protection Act, 2023, s 17(2)(a).
[87] Information Technology (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules, 2009.
[88] Report by the Committee of Experts on Non-Personal Data Governance Framework.

PRAYER

Wherefore, in light of the issues raised, arguments advanced, and authorities cited, it is most humbly by the counsel of respondents and respectfully prayed before this Hon'ble Court to:

1) Section 69 of the Information Technology Act, 2000 is constitutionally **valid.**

2) Governmental control over the use of cryptographic techniques is **not excessively restrictive** in nature.

AND/OR

Pass any other order it may deem fit, in the interest of Justice, Equity and Good Conscience.

All of which is most humbly and respectfully submitted.