TC 08

4TH SURANA AND SURANA AND CUSAT SCHOOL OF LEGAL STUDIES

DR. A T MARKOSE MEMORIAL TECHNOLOGY LAW MOOT COURT COMPETITION, 2024

BEFORE

THE HON'BLE SUPREME COURT OF INDICA

—— IN THE MATTER BETWEEN ——

WRIT PETITION (CIVIL) NO. _____ OF 2024

C.G. CAR COMPANY AND OTHERS **…PETITIONERS**

V.

UNION OF INDIA **….RESPONDENT**

CLUBBED WITH

SUO MOTU TRANSFER PETITION NO. _____ OF 2024

MR. IAN **….PETITIONER**

V.

STATE OF ANTARTAKA **…RESPONDENT**

ON SUBMISSION TO THE HON'BLE SC OF INDICA

(UNDER ARTICLE 32 AND 139A OF THE CONSTITUTION OF INDICA)

MEMORANDUM ON BEHALF OF PETITIONERS

—— DRAWN AND FILED ON BEHALF OF PETITIONERS ——

TABLE OF CONTENTS

INDEX OF AUTHORITIES

I. CASES:

22. Suresh Kumar Kaushal v. Naz Foundation, (2014) 6 SCC 433.

23. Directorate of Revenue v. Mohammed Nisar Holia (2007) 12 SCR 906.

24. Hanif Quareshi v. State of Bihar, 1959 SCR 629.

25. Ajay Bhardwaj v. UoI Writ Petition (Criminal) No 231 of 2019.

26. State of West Bengal v. B.K. Mondal & Sons, AIR 1962 SC 779.

27. M.H. Hoskot v. State of Maharashtra, (1978) 3 SCC 544.

28. Boyd v. United States, 116 U.S. 616 (1886).

29. State of Gujarat v. Shyamlal Mohanlal 1962 SCC OnLine Guj 40.

30. Hunter v. Southam [1984] 2 SCR 145 At 159, 11 DLR (4th) 641 [Hunter].

31. R v Dyment [1988] 2 SCR 417 at 426, 73 Nfld & Peir 13 [Dyment].

32. Additional District Magistrate, Jabalpur v. Shivkant Shukla, AIR 1976 SC 1207.

33. R v Spencer (2014) 2 SCR 212 [38]-[47].

34. Bimolangshu Roy v. State of Assam, (2018) 14 SCC 408.

35. S and Marper v United Kingdom [2008] ECHR Applications nos. 30562/04 and 30566/04.

36. Catt v United Kingdom [2019] ECHR Application no. 43514/15.

37. Big Brother Watch and others v. United Kingdom (Grand Chamber) Applications nos. 58170/13, 62322/14 and 24960/15

38. R. v. Mills, [1999] 3 S.C.R. 668

39. Ram Jethmalani & Others v. Union Of India (2011) 8 SCC 1

40. Olmstead v U.S 277 [1928] U. S. 438, 478

41. Suchita Srivastava v. Chandigarh Administration, AIR 2010 SC 235

42. Aruna Ramachandra Shanbaug v. Union of India, (2011) 4 SCC

43. Jamiruddin Ahmed v. State of West Bengal, AIR 2009 SC 2685.

44. Justice Sriram v. Union of India, (2019) 10 SCC 578

45. Shankari Prasad Singh Deo v. Union of India, AIR 1951 SC 458

46. Sajjan Singh v. State of Rajasthan, AIR 1965 SC 845.

47. L. Chandra Kumar V Union of India, (1997) 3 SCC 261

48. Lucknow Development Authority v. M.K. Gupta (1993) III CPJ 7 (SC)

II. STATUTES:

1. The Constitution of Indica, 1950.

2. The Indican Penal Code, 1860.

3. The Information Technology Act, 2000.

4. The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021.

5. The Central Goods and Services Act, 2017.

6. The Consumer Protection Act, 2019.

7. The Indican Telegraphs Act, 1885.

8. The Credit Information Companies Regulation Act, 2005.

III. BOOKS:

1. Ruma Pal, 'Indian Constitutional Law' (2010).

2. Bhimrao Ramji Ambedkar, 'The Constitution of India' (2019).

3. Granville Austin, 'The Indian Constitution' (1966).

4. Shikher Deep Aggarwal & Kush Kalra, 'Commentary on the Information Technology Act'.

IV. LEGAL DATABASES:

1. www.scconline.com

2. www.manupatra.com

3. www.lexisnexis.com

STATEMENT OF JURISDICTION

The Petitioners submit to the inherent jurisdiction of the Hon'ble SC of Indica arising by virtue of Article 32 along with 139A of the Constitution of Indica to hear and adjudicate over the present Writ Petition clubbed with the Suo Motu Transfer Petition in the case of ***C.G. Car Company and others v. UOI***.

The present memorial puts forth the facts, arguments, and laws in the present case.

STATEMENT OF FACTS

BACKGROUND

- **Location and Demographics**: The Republic of Indica, a democratic country in Southern Asia, is the world's most populous democracy, characterized by its pluralistic, multilingual, and multi-ethnic society.
- **Legislative Developments**: Indica enacted the Information Technology Act in 2000, amended in 2008, and introduced the National Information and Technology Policy in 2015, reflecting its commitment to regulating technological advancements.
- **State of Antartaka**: A leading state in Indica, particularly noted for its IT sector in Singaluru, which is likened to the Silicon Valley of Indica.

INCIDENT AND INVESTIGATION

- **Discovery of a Crime Scene**: On August 13, 2022, a family traveling to Sundarpur National Park discovered a body next to a Trudi car on State Highway No. 106. The victim was identified as Mr. Anand, a Vice President at MATT Private Limited.
- **Preliminary Findings**: Anand's death was suspected to be a homicide with a bullet wound to the head. No forceful entry was detected in or around his car. Simultaneous to the incident, Indica enforced rules under the IT Act, mandating approval and key sharing for cryptographic tools usage.
- **Primary Suspect**: Mr. Ian, an individual who frequented the same café as Anand and drove through the incident area at an unusual time, became the primary suspect. Ian's car, equipped with blockchain and encrypted data, became a focus for potential evidence.

LEGAL PROCEEDINGS

- **High Court**: Mr. Ian's legal challenge in the High Court of Antartaka addressed the alleged infringement of privacy and self-incrimination rights under the Constitution of Indica.
- **SC**: The SC consolidated Ian's case with a writ petition by CG Car Company, questioning the constitutional validity of mandatory cryptographic key sharing under the IT Act.

STATEMENT OF ISSUES

I. Whether Section 69 of the Information Technology Act, 2000 is constitutionally valid?

II. Whether Governmental control over the use of cryptographic techniques is too restrictive in nature?

SUMMARY OF ARGUMENTS

Issue I: Whether the Section 69 of the Information Technology Act, 2000 is constitutionally valid?

The Counsel for Petitioners contends that Section 69 of the IT Act, 2000, violates fundamental rights by compelling decryption and infringing on privacy. Mr. Ian argues that providing his private key constitutes self-incrimination, protected by Article 20(3) of the Constitution. This contention is supported by legal precedents highlighting the testimonial nature of cryptographic keys. Additionally, the constitutionality of Section 69 is challenged, asserting that it lacks proportionality and violates the right to privacy, as established in the K.S. Puttaswamy case. The section fails the four-prong test of proportionality, and the Government's overreach is deemed arbitrary, exceeding the necessary limits for national security. Furthermore, the forced disclosure of cryptographic keys infringes on CG Car Company's right to privacy, compromising its trade secrets and impacting its business operations. The Counsel argues that Section 69 imposes undue restrictions on business, violating Article 19(1)(g) of the Constitution. The provision lacks reasonable safeguards and adaptability, potentially hindering modern business operations. The compelled decryption is seen as an overreach with inadequate safeguards, impacting both individual rights and business interests.

Issue II: Whether Governmental control over the use of cryptographic techniques is too restrictive in nature?

The Counsel argues that decryption keys' demand from CG Car Company violates constitutional privacy rights, encroaching upon Article 21's protection of confidentiality and autonomy. Mandatory disclosure infringes on fundamental rights, posing security risks and contradicting manufacturers' duty to safeguard customer rights. The obligation to protect consumer privacy in the car purchase agreement emphasizes the commitment breached by Government traceability authority, impacting freedom of expression under Article 19(1)(a). Compelled decryption is deemed arbitrary and an abuse of power, violating international conventions and protection against unreasonable searches. The Counsel urges the SC to regulate cryptographic security protocols, ensuring a balanced approach that upholds legal imperatives while preserving individual rights and privacy.

ARGUMENTS ADVANCED

ISSUE I: WHETHER SECTION 69 OF THE INFORMATION TECHNOLOGY ACT IS CONSTITUTIONALLY VALID?

¶ 1. The Counsel for Petitioners humbly submits before the SC of Indica that Section 69 of the IT Act, 2000[1] violates the basic principles of law and[2] the exercise of Government power to decrypt personal data and compel companies to provide access to customer information[3] violates the constitutional rights and principles guaranteed to citizens of Indica.

¶ 2. The Petitioners argue that the actions, mandated by the IT Act, 2000,[4] subject them to unconstitutional norms, overturning the safeguards, freedoms, and rights granted and this unconstitutionality of Section 69[5] of the IT Act would be elucidated through the core arguments of the Petitioners by: **[1.1]** *the Right against Self-Incrimination and Privacy Concerns of Mr. Ian*, **[1.2]** *Determining the Constitutional Validity of Section 69,*[6] and **[1.3]** *the Business Impact and Economic Rights of CG Car Company.*

1.1. The Right against Self-Incrimination and Privacy Concerns of Mr. Ian.

¶ 3. Mr. Ian contends that Section 69[7] compels him to do act in a manner that defeats his fundamental right against self-incrimination under Article 20(3).[8] Testimonial evidence typically involves oral or written statements that reveal the contents of an individual's mind, providing a password or private key for decryption is akin to making a statement – revealing knowledge that exists in the mind of the accused.[9]

1.1.1. The Act of giving the Encryption of Private Key is Testimonial in Nature:

¶ 4. The Counsel humbly submits that the private key or password required for decryption is unique to Mr. Ian's knowledge.[10] It is not a physical object like a fingerprint or a blood sample but a mental parameter known only to him. When compelled to provide this key, Mr. Ian is essentially testifying about his own knowledge and possession of the key.

---

[1] Information Technology Act 2000, s 69.
[2] Additional District Magistrate, Jabalpur v. Shivkant Shukla AIR 1976 SC 1207.
[3] Moot Proposition ¶ 20.
[4] ibid.
[5] ibid s 69.
[6] ibid.
[7] ibid.
[8] Constitution of Indica 1950, art 20(3).
[9] R v Spencer (2014) 2 SCR 212 [38]-[47].
[10] Moot Proposition ¶ 17.

¶ 5. Recently, the SC of Indica in ***Ajay Bhardawaj v. Union of India***[11] (GainBitcoin scam case) asked the accused to provide the username and password of his crypto wallet and make full disclosures to the investigating agency. The Indican courts are encountering a growing number of cases where individuals accused of crimes are compelled by investigating agencies or court directives to decrypt or unlock content stored on digital devices, [12] in analogous fashion, in the present instance, Mr. Ian was obligated to divulge his personal information.

¶ 6. In the American case of ***United States v. Doe (In re Grand Jury Subpoena Duces Tecum),*** [13] the Court of Appeal held that refusal to decrypt to be justified on when the decryption would require the use of the contents of a person's mind and could not be fairly characterized as a physical act that would be non-testimonial in nature.

1.1.2. Compelled Decryption in the present case amounts to Self-Incrimination:

¶ 7. Compelling Mr. Ian to provide information (private key)[14] under Section 69[15] of the Information Technology Act, 2000, incriminates him. He is compelled to be a witness against himself to the authorities to investigate the death of Mr. Anand. Article 20(3)[16] of the Indican Constitution, protects individuals from being compelled to be a witness against themselves. This principle was emphasized in the landmark case of ***State of Bombay v. Kathi Kalu Oghad***,[17] where the SC held that the protection against self-incrimination is a fundamental right.

¶ 8. In the ***M.P. Sharma case***,[18] the SC delineated the protection under Article 20(3) against the *"compulsory production of documents of a testimonial character."* This implies that if the act of producing documents is of a testimonial character, it falls within the protective ambit of Article 20(3).[19] Applying this precedent to Mr. Ian's situation, the cryptographic keys can be equated with testimonial evidence. The keys are not merely physical objects; they represent Mr. Ian's knowledge and control over his encrypted data, making them inherently testimonial in nature. Mr. Ian's act of producing the cryptographic keys involves mental processes, constituting a testimonial act that attracts the protection of Article 20(3).[20]

---

[11] Ajay Bhardawaj v. Union of India, Writ Petition (Criminal) No 231 of 2019.
[12] ibid.
[13] United States v. Doe (In re Grand Jury Subpoena Duces Tecum), 670 F.3d 1335 (11th Cir. 2012).
[14] Information Technology Act 2000, s 2(1)(zc).
[15] Information Technology Act 2000, s 69.
[16] Constitution of Indica 1950, art 20(3).
[17] State of Bombay v. Kathi Kalu Oghad, 1961 SCC OnLine SC 74.
[18] M.P. Sharma v. Satish Chandra, (1954) 1 SCR 1077.
[19] Constitution of Indica 1950, art 20(3).
[20] ibid.

¶ 9. The cryptographic keys, being unique to Mr. Ian and representing his inherent knowledge and control over encrypted data, can be likened to the act of producing documents that have a testimonial character.[21] The compelled disclosure of these keys would force Mr. Ian to communicate his knowledge and control over potentially incriminating data, akin to making a statement against his will.

¶ 10. In the ***Selvi v. State of Karnataka***,[22] the SC explicitly recognized the privilege against self-incrimination as a constitutional right. This constitutional protection extends not only to oral testimony but also to any communication that might have testimonial significance. Mr. Ian's case involves the compulsion to disclose cryptographic keys, which can be argued to have testimonial significance, falling within the ambit of this constitutional protection.

¶ 11. The ***Selvi case***[23] recognized the need for a broad interpretation of the privilege against self-incrimination to adapt to evolving forms of evidence and testimonial significance. In the digital age, where information is often encrypted, the act of compelling the disclosure of cryptographic keys is a modern manifestation of the testimonial nature of evidence. ***Selvi case***[24] highlighted the importance of judicial scrutiny in Mr. Ian's case, the compelled disclosure of cryptographic keys should be subject to rigorous judicial scrutiny to ensure that it does not violate his fundamental right against self-incrimination.

¶ 12. Mr. Ian can exercise his *Right to Silence* that was established in the ***Nandini Sathpathy v. P.L. Dani,*** [25] the SC emphasized the broad interpretation of the right against self-incrimination under Article 20(3)[26] of the Indican Constitution. A cryptographic key, being an essential component for decrypting digital data, has testimonial significance. Mr. Ian's private key is not a mere physical object but a crucial piece of information that, when disclosed, can be used against him in the investigation. This communication, though not verbal, is a form of expression that falls within the purview of Article 20(3).[27]

1.2. Section 69 of the IT Act, 2000 is Unconstitutional in Nature:

¶ 13. The Constitutionality of Section 69[28] of the IT Act is brought into question, and the crux of the matter lies in the interpretation of the term "*unconstitutional,"*[29] the court asserted that

---

[21] National Research Council, *Cryptography's Role in Securing the Information Society* (1996).
[22] Selvi v. State of Karnataka, (2010) 7 SCC 263.
[23] ibid.
[24] Selvi v. State of Karnataka, (2010) 7 SCC 263.
[25] Nandini Satpathy v. P.L. Dani, (1978) 2 SCC 424.
[26] Constitution of Indica 1950, art 20(3).
[27] ibid.
[28] Information Technology Act 2000, s 69.
[29] Bimolangshu Roy v. State of Assam, (2018) 14 SCC 408.

even if a law is initially non-discriminatory, the passage of time without justification can render it discriminatory and challengeable under Article 14[30] of the Indican Constitution.[31]

¶ 14. The court established a principle that the mere passage of time from the enactment of a provision, that violates Article 14[32] of the Constitution, without justification, constitutes grounds for challenge. Applying this rationale to Section 69 of the IT Act,[33] continued discrimination without a rational basis for a prolonged period is unjustifiable.

¶ 15. The Counsel humbly submits that the unconstitutionality of Section 69 of the IT Act, 2000[34] can be identified in several aspects, primarily related to the violation of constitutional rights.

¶ 16. There is a need to list down the specific conditions to be fulfilled for selecting targets for interception without compromising the Fundamental Rights of Citizens.[35] Default of this could result in discriminatory application. If certain groups or individuals such as Mr. Ian are disproportionately targeted to compelled decryption without a rational basis raises concerns under Article 14[36] which prohibits discrimination.

¶ 17. It is further submitted that Section 69[37] grants sweeping powers to the Central or State Government to intercept, monitor, or decrypt information from any computer resource. A notable case that addresses the issue of laws granting sweeping powers to the Government and the potential unconstitutionality of such provisions is ***K.S. Puttaswamy v. Union of India***.[38]

¶ 18. While the case primarily focused on the Right to Privacy, the SC, in its judgment, expressed concerns about expansive powers granted to the Government under the Aadhaar Act. Mr. Ian's Right to Privacy is violated by compelled decryption of his private key.[39]

1.2.1. Section 69 of the IT Act, 2000 does not pass the Four Prong Test of Proportionality:

¶ 19. In the context of the Right to Privacy, the court asserted that any limitation on this right must satisfy the three-fold test of legality, necessity, and proportionality.[40] Section 69[41] fails to

---

[30] Constitution of Indica 1950, art 14.
[31] Motor General Traders v. State of A.P, (1984) 1 SCC 222.
[32] Constitution of Indica 1950, art 14.
[33] Information Technology Act 2000, s 69.
[34] ibid.
[35] Constitution of Indica 1950, part III art 12-35.
[36] Constitution of Indica 1950, art 14.
[37] Information Technology Act 2000, s 69.
[38] K.S. Puttaswamy v. Union of India, (2017) 10 SCC 1.
[39] Moot Proposition ¶ 18.
[40] K.S. Puttaswamy v. Union of India, (2017) 10 SCC 1.
[41] Information Technology Act 2000, s 69.

meet the proportionality standard laid down in the ***Puttaswamy case***,[42] as compelled disclosure of cryptographic keys is not a proportionate response to the objective of national security.

¶ 20. The presence of a less intrusive alternative renders the original decryption as arbitrary and unreasonable. The Section lacks a mandate to explore less invasive alternatives may lead to unnecessary intrusions into individuals' private communications and data. Mr. Ian's activities can be tracked through CCTV footage from public spaces around the time of the incident, and digital forensics experts can be engaged to analyze Mr. Ian's devices for any evidence of involvement in the crime without decrypting the entire system.

¶ 21. Additionally, in the ***Modern Dental College & Research Centre***,[43] four subcomponents of proportionality that need to be satisfied were taken note of. These are: (*a*) A measure restricting a right must have a legitimate goal, (*b*) It must be a suitable means of furthering this goal, (*c*) There must not be any less restrictive but equally effective alternative, and (*d*) The measure must not have a disproportionate impact on the right holder.

¶ 22. The Counsel humbly submits that the goal of addressing cyber threats and criminal activities is legitimate, but the extent of authority granted to compel decryption raises concerns about overreach. The grounds on which the Government can block public access to information, such as the "interest of sovereignty and integrity of Indica, defense of Indica, security of the State, friendly relations with foreign States, or public order," are broad and open to interpretation. This broad language provides the Government with significant discretion, which leads to overreach.

¶ 23. The provision may be deemed suitable for achieving its goal, but questions arise regarding other alternative measures that can be used instead of compelled decryption of Mr. Ian's data.[44] The indiscriminative use of decryption powers without clear criteria, mandatory nature of this requirement and applicability of sections which would result in violation of fundamental rights are reasons for Section 69 to be declared unconstitutional.

1.2.2. The Government's Overreach is Excess and Arbitrary in Nature:

¶ 24. The Counsel humbly submits that interference with confidential communications affect both right to privacy and freedom of expression.[45] Adopting encryption measures aligns

---

[42] K.S. Puttaswamy v. Union of India, (2017) 10 SCC 1.
[43] Modern Dental College & Research Centre v. State of M.P., (2016) 7 SCC 353.
[44] Moot Proposition ¶ 18.
[45] O.L. van Daalen, 'The right to encryption: Privacy as preventing unlawful access' (2023) 49 Computer Law & Security Review < https://www.sciencedirect.com/science/article/pii/S0267364923000146#cit_68> accessed 05 January 2024.

Indica's data protection practices with international standards, as seen in the GDPR.[46] This alignment fosters trust among global stakeholders, encourages data flows, and promotes Indica as a responsible participant in the global digital ecosystem.

¶ 25. The Counsel humbly submits that though the investigating officers proceeded to decrypt data after an assent was passed from *"The Authority on Control and Regulation of Cryptography,"*[47] it is not sufficient to protect Mr. Ian's privacy. It is the inherent duty of the Government to establish legal frameworks that facilitate cooperation between law enforcement agencies and technology companies.[48] The lack of sufficient safeguards and judicial oversight amplifies the imbalance, as it allows executive authorities to use significant power without adequate checks. *Storage of personal data* is an interference, because of what might be done with the data in the future.[49] It has also repeatedly underlined that the continuously advancing sophistication of surveillance technologies increases the risk of arbitrariness.[50]

¶ 26. The Basic Structure Doctrine[51] aims to prevent the concentration of unchecked power in any one branch of the Government. Compelling decryption without judicial oversight infringes upon the right to privacy. Mr. Ian and C.G Car Company shows the situations where there is arbitrary exercise of power in the interest of public.

1.2.3. There has Been no "Consent" Expressly Given By Mr. Ian To Disclose Information to the Third Parties:

¶ 27. The Counsel respectfully asserts that in the case of ***R. Rajagopal v. State of T.N,***[52] which held that no *"personal information"* can be disseminated without the individual's consent, irrespective of its veracity, commendatory or critical nature.

¶ 28. The Counsel humbly submits that the SC mandated WhatsApp to furnish a duly executed undertaking, sworn under oath, asserting that it refrains from divulging users' private data without their explicit consent.[53] When soliciting user consent for data processing, companies are obligated to furnish explicit consent. Importantly, in cases where a user has granted consent for data processing prior to the enactment of the law, the company is required to provide a notice stating the explicit consent at the earliest opportunity that is deemed "reasonably

---

[46] European Union General Data Protection Regulation (2016) Regulation (EU) 2016/679.
[47] Moot Proposition ¶ 11.
[48] O.L. van Daalen, 'The right to encryption: Privacy as preventing unlawful access' (2023) 49 Computer Law & Security Review January 2024.
[49] S and Marper v United Kingdom [2008] ECHR Applications nos. 30562/04 and 30566/04.
[50] Cattv the United Kingdom [2019] ECHR Application no. 43514/15 114; Big Brother Watch and others v. United Kingdom (Grand Chamber) 322.
[51] Kesavananda Bharathi v. UOI (1973) 4 SCC 225.
[52] R. Rajagopal v. State of T.N., (1994) 6 SCC 632.
[53] ibid.

practicable." It is to be humbly examined that the notice sent did not involve the explicit consent of the customer.

1.3. Restriction on Business of CG Car Company.

¶ 29. The writ petition filed by CG Car Company argues that Section 69[54] is too restrictive and substantially affects their business in Indica. It is to be interpreted as a violation of the right to carry on business, which is protected under Article 19(1)(g)[55] of the Constitution. Right to Carry on Business.

1.3.1. Violation of Article 19(1)(g) of the Indican Constitution:

¶ 30. The imposition of obligations under Section 69 of the IT Act[56], requiring the submission of cryptographic keys, interferes with the fundamental right of CGCC to carry on its business without reasonable restrictions. The test of reasonableness as laid down in ***Madras v. V.G. Row***[57] states that "*it is important to bear in mind that the test of reasonableness, wherever prescribed should be applied to each individual statute impugned, and no general pattern can be laid down as applicable to all cases*." In the present circumstance, Section 69[58] grants wide-ranging powers to intercept and decrypt information without clearly defined safeguards. Section 69,[59] when applied without adequate safeguards is restrictive, especially in the context of modern business operations of CGCC.

¶ 31. The company's ability to attract clients is closely tied to the security features it provides in its autonomous cars. Any additional regulatory burdens affecting these features could substantially impact its business operations, facing the imposition of stringent requirements under Section 69[60] of the IT Act.

¶ 32. In the ***Mohammed Hanif Quareshi case***, the SC recognized the fundamental right to carry on trade or business as a part of Article 19(1)(g).[61] The provisions of Section 69[62] amounts to an unreasonable restriction on trade and commerce. While the purpose is to address concerns related to national security, it results in undue intrusion of personal data and private keys issued by CGCC and its right to carry on business.

1.3.2. Business and Economic Rights of CGCC:

---

[54] Information Technology Act 2000, s 69.
[55] Constitution of Indica 1950, art 19(1)(g).
[56] Information Technology Act 2000, s 69.
[57] State of Madras v. V.G. Row, (1952) 1 SCC 410.
[58] Information Technology Act 2000, s 69.
[59] ibid.
[60] ibid.
[61] Constitution of Indica 1950, art 19(1)(g).
[62] Information Technology Act 2000, s 69.

¶ 33. In the ***I.T.C. Ltd. case***,[63] the SC recognized that the right to carry on business includes the right to protect sensitive business information. Any infringement on this right is set by Section 69,[64] by imposing mandatory requirements that are not justifiable in the interest of the general public.

¶ 34. In the case of ***Bayer Corporation v. Union of India***,[65] the Delhi High Court emphasized the importance of protecting intellectual property rights, acknowledging them as valuable assets that contribute to a company's business operations. The Court recognized that intellectual property rights, being an integral part of a company's business, should be safeguarded. The cryptographic tools used by CGCC are crucial for the security features of their vehicles, contributing to their business reputation and consumer trust.[66] CGCC's proprietary information, particularly the cryptographic techniques embedded in their vehicles, constitutes valuable intellectual property. The forced disclosure of such information would infringe on their privacy and jeopardize their market competitive edge.[67]

¶ 35. The Right to Privacy encompasses not only protection from unwarranted intrusions into personal data but also extends to the privacy of business operations and sensitive information. CGCC, in safeguarding its cryptographic keys, seeks to maintain the privacy of its proprietary information. When compelled to disclose these keys under Section 69[68] it undermines the company's ability to protect its confidential data, including security measures embedded in its products.

¶ 36. ***Vodafone International Holdings BV v. Union of India***[69] underscores the importance of a stable and non-hostile business environment for maintaining trust and attracting investments. Applying this principle, CGCC can argue that Section 69[70] creates a hostile environment by compromising the perceived security of its products. Section 69[71] infringes upon CGCC's right to privacy and compromises its trade secrets by compelling the disclosure of cryptographic keys. The right to keep proprietary information confidential is crucial for businesses, especially in the technology sector.

1.3.3. Violation of Right to Privacy of CGCC:

---

[63] ITC Ltd. v. Britannia Industries Ltd., 2016 SCC Online Del 500.
[64] Information Technology Act 2000, s 69.
[65] Bayer Corporation v. Union of India, 2014 SCC Online SC 1709.
[66] Moot Proposition ¶ 16.
[67] Moot Proposition ¶ 20.
[68] Information Technology Act 2000, s 69.
[69] Vodafone International Holdings Bv v. Union of India, (2012) 6 SCC 613.
[70] Information Technology Act 2000, s 69.
[71] ibid.

¶ 37. Section 69[72] infringes upon CGCC's right to privacy and compromises its trade secrets by compelling the disclosure of cryptographic keys. The Right to Keep proprietary information confidential is crucial for businesses, especially in the technology sector. In ***Mr. X v. Hospital Z***,[73] the court held, *"Right of privacy may, apart from contract, also arise out of a particular specific relationship which may be commercial, matrimonial, or even political."* The court, in the case, recognized that the right to privacy may arise from specific relationships, including commercial relationships. CGCC's proprietary information, especially cryptographic keys, is a vital aspect of its commercial relationship, and compelling disclosure without adequate safeguards infringes upon its right to privacy.

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

¶ 38. The Counsel for the Petitioners humbly submits that encryption[74] plays a crucial role in safeguarding the confidentiality of personal records,[75] including medical information,[76] financial data, and electronic mail.[77] Consequently, the Government's regulation of cryptographic security techniques *(hereinafter, to be denoted as **"CST")*** is excessively restrictive in its nature,[78] given that **[2.1]** *strict Governmental Control (hereinafter, to be denoted as "**GC**") infringes on individuals' Right to Privacy vested by the Indican Constitution,* **[2.2]** *GC over cryptographic techniques infringes the Right of Freedom of Expression,* and **[2.3]** *compelled decryption is incongruous to jurisprudence and results in the arbitrary use of power.*

2.1. The Strict GC Infringes on Individuals' Right To Privacy Vested by The Constitution.

¶ 39. The Counsel humbly submits that encryption and the study of cryptography afford individuals a legitimate exercise of their Rights to Freedom of Speech and Expression, as well as the Right to Engage in conversations free from intrusion, by enabling communication that remains unintelligible to third parties without explicit permission from the communicators.[79]

---

[72] Information Technology Act 2000, s 69.
[73] Mr.'X' v. Hospital 'Z', (1998) 8 SCC 296.
[74] Information Technology (Certifying Authorities) Rules 2000, Schedule V.
[75] Theodore F. Claypoole, "Privacy Regulations A Concern With Internet", [2004] Lexis Nexis.
[76] Digital Information Security Health Care Act (DISHA) 2018.
[77] Indusind Media & Communications Ltd. v. Commr. of Customs, (2019) 17 SCC 108.
[78] K.S. Puttaswamy v. Union of India, (2017) 10 SCC 1.
[79] Banarasi Das v. Teeku Dutta, 2005 (4) SCC 449

¶ 40. The Petitioners' Counsel respectfully argues that the requirement imposed on the Head office of CGCC to submit copies of decryption keys to the Authority on Control and Regulation of Cryptography constitutes a violation of the constitutional rights to privacy enshrined in the Indican Constitution, specifically under the privacy provisions.[80]

¶ 41. The Counsel humbly submits that an individual possesses the right to life and personal liberty, subject to deprivation solely through a legal procedure duly established by law.[81]

¶ 42. The concept of *"personal liberty"* as articulated in **Article 21**[82] encompasses a broad spectrum of rights, including but not limited to confidentiality, autonomy, human dignity, human rights, self-determination, restricted and safeguarded communication, and the mitigation of unwarranted public exposure.[83]

¶ 43. In the case of ***District Registrar and Collector v. Canara Bank***,[84] the SC held that the revelation of the content of private documents or reproductions constitutes a breach of confidentiality and such disclosure is deemed to be in violation of the privacy rights.[85]

¶ 44. The constitutional acknowledgment of the right to privacy serves as a safeguard against unauthorized Government intrusion into personal privacy and was affirmed in the case of ***Khushwant Singh v. Maneka G***.[86]

¶ 45. The Counsel respectfully submits that, in the specific instance of CGCC and other automotive manufacturers, the obligation to safeguard the security features inherent to their customers imposes constraints[87] Mandatory directive to disclose cryptographic techniques employed in vehicles to the Government is unduly restrictive in nature as customers are obliged to be protected and is a direct breach of fundamental rights.

2.1.1. Every Individual is Entitled to the Privilege of Maintaining their Own Personal Space under the Indican Constitution:

¶ 46. The Counsel humbly submits that the Right to Privacy was affirmed as safeguarding an individual's *"private space in which man may become and remain himself"* in the context of Section 377 IPC, with scrutiny conducted under Articles 14, 19, and 21.[88]

---

[80] Ram Jethmalani & Others vs Union of Indica(2011) 8 SCC 1
[81] Olmstead v U.S 277 [1928] U. S. 438, 478; Maneka Gandhi v. Union of India, AIR 1978 SC 597.
[82] Constitution of Indica 1950, art 21.
[83] Kharak Singh v. State of U.P., AIR 1963 SC 1295; Govind v. State of M.P., AIR 1975 SC 1378.
[84] District Registrar and Collector v. Canara Bank, AIR 2005 SC 186.
[85] Girish Ramchandra Deshpande v. Central Information Commr., (2013) 1 SCC 212.
[86] Khushwant Singh v. Maneka Gandhi, 2001 SCC OnLine Del 1030.
[87] Moot Proposition ¶ 20.
[88] Suresh Kumar Kaushal v. Naz Foundation, (2014) 6 SCC 433.

¶ 47. The Counsel humbly submits that in the case of ***Directorate of Revenue v. Mohammed Nisar Holia***[89] the SC established that, an advanced technology capable of revealing details of a person's personal information, infringes upon privacy rights.[90]

¶ 48. In the case of ***Boota Singh v. State of Haryana***, the SC ultimately determined that a car not being subject to access by the general public, and the Court affirmed the characterization of a personal car as constituting a private space.[91]

¶ 49. In 1994, the SC, in the ***R. Rajagopal v. State of T.N.***,[92] decreed that every citizen retains the right to safeguard their privacy, emphasizing that no information, whether accurate or not, shall be disseminated, which in this instance the Government pressurizes the CGCC to disclose all the *"personal information"* of the consumer which violates the freedom vested to him by the Indican Constitution.[93]

2.1.2. The Duty of the Manufacturers to Protect the Rights of Its Customers:

¶ 50. The Counsel humbly submits that the CGCC cooperation would contravene the security measures extended to their customers and the data owner, specifically Mr. Ian in this instance.[94]

¶ 51. The Counsel for Petitioners would humbly submit that safeguarding information provided to organisations is imperative and should be preserved in accordance with the protocols established by the justice system of the country.[95]

¶ 52. The primary rationale for this lies in the fact that the conclusive recognition of the right to privacy as a fundamental right was only conclusively established in the ***K.S. Puttaswamy case***, marking a recent development in legal precedent.[96]

¶ 53. The Counsel respectfully asserts that consumers possess the entitlement to seek remedy in cases of unfair trade practices, restrictive trade practices, or unscrupulous exploitation.[97] The unfair practice, in this context, encompass the disclosure of any personal information provided in confidence by the consumer to a third party. Thus, the car manufacturers are obliged to protect the customers accordingly.[98]

---

[89] Directorate of Revenue v. Mohammed Nisar Holia, (2007) 12 SCR 906.
[90] Suchita Srivastava v. Chandigarh Administration, AIR 2010 SC 235
[91] Aruna Ramachandra Shanbaug v. Union of India, (2011) 4 SCC
[92] R. Rajagopal v. State of T.N., AIR 1995 SC 264.
[93] Diwan Singh v. Inderjeet, AIR 1981 All. 342.
[94] MOOT PROPOSITION ¶19.
[95] Gian Kaur v. State of Punjab, AIR 1996
[96] K.S. Puttaswamy v. Union of India, (2017) 10 SCC 1.
[97] Jamiruddin Ahmed v. State of West Bengal, AIR 2009 SC 2685.
[98] Moot Proposition ¶ 20.

¶ 54. Sections 43-A[99] and 72-A[100] of the Information Technology Act, 2000 constituted explicit provisions aimed at safeguarding an individual's personal data, distinct from the provisions of the TA Act, 1885,[101] which regulated communication interception. The recently promulgated Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021,[102] impose obligations on entities that collect information for the protection of private data.[103]

¶ 55. Thus, it is humbly submitted that the automated system, operable through Mr. Ian's linked smartphone, records detailed driving and vehicle conditions, emphasizing CG-Metron's commitment to safeguarding customer information.[104]

2.2. The GC on Cryptographic Techniques Infringes the Right to Freedom Of Expression.

¶ 56. The Counsel humbly submits that in the case of ***M.P. Sharma v. Satish Chandra***,***[105]*** the SC ruled that Indican Constitution does not explicitly guarantee the right to privacy.

¶ 57. The Court has established three criteria, namely "law," a "legitimate State interest," and the requirement of "proportionality," to assess whether any State activity infringes upon the fundamental right to privacy, and the Court has reiterated the four sub-tests for determining the proportionality of a state action, as articulated in the 2016 decision in ***Modern Dental College and Research Centre v. State of Madhya Pradesh***.[106]

¶ 58. The authority granted to the Government for traceability infringes upon Article 19(1)(a)[107] of the Indican Constitution, as it poses a deterrent impact on the freedom of expression.

2.2.1. The Purchase of the Car Between the Car Manufacturers and Customers Protects the Freedom of Expression Vested to them:

¶ 59. The Counsel representing the Petitioners respectfully submit that upon the purchase of a car, consumers select and acquire the specified features based on their suitability[108], and the company is duty-bound to ensure the provision of said features.

---

[99] Information Technology Act 2000, s 43(a).
[100] ibid s 72(a).
[101] Telegraph Act 1885.
[102] Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules 2021.
[103] Justice Sriram v. Union of India, (2019) 10 SCC 578
[104] MOOT PROPOSITION ¶ 20.
[105] M.P. Sharma v. Satish Chandra, (1954) 1 SCR 1077.
[106] Modern Dental College & Research Centre v. State of M.P., (2016) 7 SCC 353.
[107] Constitution of Indica 1950, art 19(1)(a).
[108] Spring Meadows Hospital v. Harjot Ahluwalia JT 1998(2) SC 620.

¶ 60. Section 72-A of the IT Act[109] stipulates penalties for the divulgence of "*personal information"* by any service provider without the explicit consent of the data and prescribes criminal consequences, for intentional disclosure of an individual's personal information acquired.

¶ 61. The Counsel respectfully submits that the act of purchase entails an obligation for customers to receive the specified features, and any deviation from this commitment may result in potential business losses with the breach of trust of its customers.[110]

2.2.2. The Defence of State Emergency or to Protect National Security cannot be Invoked to Violate the Fundamental Rights Vested by the Constitution:

¶ 62. The Counsel humbly states that the SC declared Section 66A of IT Act[111] unconstitutional, emphasizing its potential for misuse beyond constitutionally sanctioned limits and aligning with Court's precedent on safeguarding against unconstitutional restrictions.[112]

¶ 63. In the case of ***Maneka Gandhi v. Union of India***,[113] SC ruled that measures regulating or curtailing a Fundamental Right must be fair, sensible, and meticulously devised to uphold the underlying substantive right and to ensure fairness, justice, and reasonableness in justifying any invasion of privacy.

¶ 64. The Counsel respectfully submits that, as established in ***Hanif Quareshi v. State of Bihar***,[114] the SC maintains ultimate authority to determine the acceptability of a restriction in the public's interest, notwithstanding the initial acknowledgment that the legislature is presumed to be the best judge of what benefits the community it represents through suffrage.[115]

¶ 65. Hon'ble Justice Nariman disagreed with the state's suggestion to use the "reasonable expectation of privacy test" in defining the right to privacy, stating that it is vested and infringing them leads to the violation of plausible foundation under Articles 14[116], 19[117], 20[118] and 21[119] of the Indican Constitution.

2.3. Compelled Decryption is Congruous to Jurisprudence and Results in Arbitrary use of Power.

---

[109] Information Technology Act 2000, s 72(a).
[110] Lucknow Development Authority v. M.K. Gupta, (1993) III CPJ 7 (SC)
[111] Information Technology Act 2000, s 66.
[112] K.A. Abbas v. Union of India, (1970) 2 SCC 780.
[113] Maneka Gandhi v. Union of India, (1978) 1 SCC 248.
[114] Mohd. Hanif Quareshi v. State of Bihar, 1959 SCR 629.
[115] I.R. Coelho v. the State of Tamil Nadu, (1999) 7 SCC 580
[116] Constitution of Indica 1950, art 14.
[117] ibid art 19.
[118] ibid art 20.
[119] ibid art 21.

¶ 66. In the case of ***State of West Bengal v. B.K. Mondal and Sons***[120], it was affirmed that reliance on such precedents is contingent upon the caveat that paramount consideration should always be accorded to the language pertinent to Indica's Statute, the context and circumstances in which it is enacted, and notably, the prevailing conditions in Indican.[121] The "self-incrimination" doctrine constitutes an integral facet of the criminal law jurisprudence in a civilized nation. Both Article 20(3) of the Indican Constitution[122] and the Fifth Amendment of the United States Constitution afford safeguards against self-incrimination.

¶ 67. In ***Boyd v. United States***,[123] established that Fifth Amendment prohibits Government from coercing an individual suspected of a crime into surrendering self-incriminating documents.

2.3.1. Compelled decryption can also be invoked in this Instance of Cryptographic Securities as it is against Article 20(3) of the Indican Constitution:

¶ 68. It is humbly submitted that in the case of ***M.P. Sharma v. Satish Chandra***[124], the interpretation and scope of Article 20(3)[125] were elucidated and expressing the unanimous view as, *"to be a witness is nothing more than to furnish evidence … indeed, every positive volitional act which furnishes evidence is testimony, thereby emphasizing that both oral and documentary evidence fall within the purview of Article 20(3)."*

¶ 69. In the case of ***Selvi v. State of Karnataka***, the SC noted that Article 20(3) [126]establishes a sphere of mental privacy, preventing the State from intruding to procure personal information related to a significant fact and the Court determined that if statements have the potential to incriminate directly or "contribute a link in the chain of evidence," the protections under Article 20(3)[127] of the Constitution would be applicable.

¶ 70. The question of whether this authority could be applied to accused individuals was addressed by a Constitution Bench in ***Shyamlal Mohanlal v. State of Gujarat***[128] and court ruled that such power could not be employed concerning accused persons, as it would contravene the provisions of Article 20(3).[129]

---

[120] State of West Bengal v. B.K. Mondal & Sons, AIR 1962 SC 779.
[121] M.H. Hoskot v. State of Maharashtra, (1978) 3 SCC 544.
[122] Constitution of Indica 1950, art 20(3).
[123] Boyd v. United States, 116 U.S. 616 (1886).
[124] M.P. Sharma v. Satish Chandra, (1954) 1 SCR 1077.
[125] Constitution of Indica 1950, art 20(3).
[126] ibid art 20(3).
[127] ibid.
[128] State of Gujarat v. Shyamlal Mohanlal, 1962 SCC OnLine Guj 40.
[129] Constitution of Indica 1950, art 20(3).

2.3.2. Compelled decryption is Arbitrary and involves the Abuse of Power From the Centre:

¶ 71. The encroachment upon the privacy and liberty of individuals not only infringes upon a fundamental right but also violates the stipulations of the International Convention on Civil and Political Rights (ICCPR).[130] The ICCPR safeguards against arbitrary or unlawful encroachments on an individual's privacy and home.[131]

¶ 72. Section 8[132] affirms that *"[e]veryone possesses the right to be protected against unreasonable search or seizure." The determination of whether a search or seizure has taken place hinges on whether the state has encroached upon the claimant's "reasonable expectation of privacy."*[133] The objections underscore the delicate balance required between legal imperatives and the protection of individual rights,[134] particularly in contexts where disclosure may implicate personal privacy or potentially lead to self-incrimination. As per the SC, the principle against self-incrimination is founded on two legal principles: firstly, to safeguard against compelled decryption, and secondly, to guard against abuses of power by the state.[135]

¶ 73. Therefore, it is respectfully submitted to the SC of Indica that the protocols instituted by the Government concerning cryptographic security techniques display inherent bias and warrant regulation[136], as articulated in the aforementioned arguments.

---

[130] International Covenant on Civil and Political Rights (1966) Treaty Series, 999, 171.
[131] K.S. Puttaswamy v. Union of India, (2017) 10 SCC 1.
[132] Canadian Charter of Rights and Freedoms, s 8; Constitution Act, 1982, part 1; R. v. Mills, [1999] 3 S.C.R. 668, p. 77-89, 94, 99 and 108.
[133] Hunter v Southam Inc, [1984] 2 SCR 159, 11 DLR (4th) 641 [Hunter]; R v Dyment, [1988] 2 SCR 426, 73 Nfld & Peir 13 [Dyment].
[134] Shankari Prasad Singh Deo v. Union of India, AIR 1951 SC 458, Sajjan Singh v. State of Rajasthan, AIR 1965 SC 845.
[135] L. Chandra Kumar V Union of India, (1997) 3 SCC 261.
[136] Moot Proposition ¶ 20.

PRAYER

Wherefore, considering the facts stated, questions presented, pleadings advanced, and authorities cited, counsels for the Petitioners pray that this Hon'ble Court may be pleased to adjudge and declare that:

1. Section 69 of the Information Technology Act, 2000 is unconstitutional.
2. The Governmental control over the use of cryptographic techniques is too restrictive in nature.

The Hon'ble Court, being satisfied, may also make any such order as it may deem fit in the light of Justice, Equity, and Good conscience.

All of which is most humbly prayed.

ON BEHALF OF THE PETITIONERS.

PLACE: _____ Sd/

DATE: _____ Counsel for the Petitioners