TL-09

4TH SURANA & SURANA AND CUSAT SCHOOL OF LEGAL STUDIES,

DR. AT MARKOSE MEMORIAL TECHNOLOGY LAW

MOOT COURT COMPETITION, 2024

19TH JANUARY – 21ST JANUARY 2024

BEFORE THE HON'BLE SUPREME COURT OF INDICA

In the clubbed matter of:

CG CAR COMPANY AND OTHERS — **PETITIONERS**

V.

UNION OF INDICA — **RESPONDENT**

PETITION UNDER ARTICLE 32 OF THE CONSTITUTION OF INDICA

UPON SUBMISSION TO THE HON'BLE CHIEF JUSTICE AND HIS LORDSHIP'S COMPANION JUSTICES OF THE HON'BLE SUPREME COURT OF INDICA

Written Submission on behalf of the Petitioners

Counsel for the Petitioners

TABLE OF CONTENTS

INDEX OF AUTHORITIES

STATUES

CASES

BOOKS

OTHER SOURCES

STATEMENT OF JURISDICTION

The petitioners approach the Hon'ble Supreme Court of Indica under Article 32 of the constitution against Section 69 Information Technology Act, 2000, and the government control rules mention in the Rule of 13 August 2022 and "The Authority on Control and Regulation of Cryptography".

Article 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

STATEMENT OF FACTS

In the Southern part of Asian Sub Continent, the Republic of Indica has State of Antartaka as the most developed state of the country. It is famous for its growth of the Information Technology sector and the city of Singaluru is often referred to as Silicon Valley of Indica. The body of Mr. Parth was found lying in a pool of blood beside his car, on the side of State Highway No. 106 by a family around 7:00 am on 13th August 2022. The investigative officers sent the body to Government Hospital after the necessary formalities and inquest were fulfilled.

After preliminary investigation the suspicion was on Mr. Ian as the time estimated of the death of Mr. Anand was same as the time when the SUV, CG-Metron of Mr. Ian passed through the State Highway. The suspicion on Mr. Ian is bolstered as his vehicle took longer time for covering the distance, compared to the other vehicles. It was found that Mr. Ian and Mr. Anand used to frequent the same eatery. During investigation, Mr. Ian answered all the question posed without any dispelling doubt but couldn't give a satisfactory reason for his travel during the specified time. His car was confiscated by police to check the movement and other details of the vehicle as it had ICT facilities.

The investigative officers found that the data was secured by password and needed private key to decrypt it. By exercising the power given by "The Authority on Control and Regulation of Cryptography" asked for the private key to which he declined stating that it is an self-incriminating evidence under Art.20(3). Police officers after following the procedure contacted Headquarters of CG Metron for the copy of key to which they denied stating that the security of the data is their trade secret. Police tried to hack into the system off the records to investigate and failed. They proceeded against CG Metron and Mr. Ian under S. 69 of IT Act, 2000. Mr. Ian challenged it in 482 CrPC before HC for infringement of privacy and CG Metron filed a writ in SC contending S. 69 and rules of "The Authority" to be unconstitutional. SC Clubbed the matters.

STATEMENT OF ISSUES

-ISSUE 1-

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

-ISSUE 2-

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

SUMMARY OF ARGUMENTS

1. WHETHER S.69 OF THE INFORMATION TECHNOLOGY ACT, 2000 IS CONSTITUTIONALLY VALID?

The Section 69 of the Information and Technology Act, 2000 is constitutionally invalid as it stands in contravention to the fundamental rights Article 14, Article 19 (1)(g), Article 21 and Article 20(3) protected under Part III of the constitution. The impugned Section 69 is detrimental for the citizen using encrypted data, as this is opening a door for unregulated breach of privacy of the customer data, which would create a fear in their mind of not opting for such technology and ultimately affecting the businesses such as C G Metron.

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

The Governmental Rule in question here, is the rule of 13 August 2022. The rule mandated that the cryptographic algorithms that are used by anyone for any purpose were to be submitted to "The Authority on Control and Regulation of Cryptographic" and the prior approval of the Authority was necessary for using the same. The Authority is to be provided with a copy of keys that could be used for decrypting and they were bound to share the keys with the government on demand. Mr. Ian's phone is confiscated by police and he is being forced by them to tell his private key to which he has denied. Police tried to illegally hack into his system which exhibits arbitrary and unhinged power exercised by the police.

ARGUMENTS ADVANCED

1. WHETHER S.69 OF THE INFORMATION TECHNOLOGY ACT, 2000 IS CONSTITUTIONALLY VALID?

The counsel would like to most humbly submit before this hon'ble court that S.69 stands constitutionally invalid and the apex court has attained the role as that of a "sentinel on the qui vive."[1] The above stated issue shall be dealt under three limbs- **[1.1]** *S.69 stands in contravention to Art 14, 19 and 21*, **[1.2]** *S.69 stands in contravention to Art 20(3)* **&** **[1.3]** *The very essence of the Constitution is being tarnished by the impugned legislation.*

1.1 *The impugned S.69[2] stands in contravention to Art 14[3], 19[4], 21[5]*

A statute can be struck down when it is arbitrary or unreasonable[6], in relation to the constitutional provision such as, Art 14, 19 or 21.[7] *In casu,* S.69 infringes the freedom of trade, occupation, profession and the privacy of the data stored, protected under fundamental rights. It was stated in ***State of West Bengal v. Committee for protection of Democratic Rights, West Bengal***[8] that Art. 13[9] prohibits a state from making a law which either takes away totally or abrogates in part a fundamental right. In ***Renu v. District and Sessions Judge***[10] it is stated that legislature must exercise power within the framework of Constitution and the judicial review is to be exercised to see that the fundamental rights are not contravened [11]. Thus, the legislature cannot enact law inconsistent with the fundamental rights of the citizen[12]**.** *In casu,* S.69 stands in contravention to the fundamental rights protected under Part III of the constitution affecting the human dignity.

---

[1] *State of Madras v VG Row* (1952) SCR 597.
[2] The Information Technology Act 2000, s 69.
[3] The Constitution of India 1949, art 14.
[4] The Constitution of India 1949, art 19.
[5] The Constitution of India 1949, art 21.
[6] *The Collector of Customs, Madras v Nathalla Sampathu Chetty & Anr* (1962) 3 SCR 786.
[7] *District Registrar and Collector v Canara Bank* (2005) 1 SCC 496.
[8] *State of West Bengal v Committee for protection of Democratic Rights, West Bengal* (2010) 3 SCC 571.
[9] The Constitution of India 1949, art 13.
[10] *Renu v District and Sessions Judge* (2014) 14 SCC 50.
[11] *Kesavananda v State of Kerala* (1973) 4 SCC 225.
[12] *Brij Mohan Lal v UOI* (2012) 6 SCC 502.

Reflections of dignity are found in the guarantee against arbitrariness under Art 14, the lamps of freedom under Art 19 and in the right to life and personal liberty under Art 21.

1.1.1. S.69 being arbitrary in nature infringes the Article 14

In ***E.P. Royappa v. State of Tamil Nadu***[13] arbitrariness was developed as a distinct doctrine on which state action could be struck down as being violative of rule of law contained in Art 14. It has been stated in ***Bachan Singh v. State of Punjab***[14]**,** "rule of law which permeates the entire fabric of the Constitution excludes arbitrariness". The test provided in ***UOI v. International Trade Corporation***[15] is whether there is reasonableness to the discernible principle, emerging from the impugned action. *In casu* S.69, provides a limitless authority to the extent of arbitrariness in the hands of the government. As per reading S.69, it appears to be an instrument of monitoring stored data, such as that of SUV CG Metron[16], on the preface of investigation of *any offence*. It provides for monitoring and interception of data for investigation of offences, have an undefined threshold which renders no possible safeguard or essence of reasonableness, proving it to be arbitrary in nature.

The S.69 gives absolute discretion in the hands of the authority, as the authorities may decrypt the data of any individual even *merely* on the basis of suspicion and their unfettered discretion, resulting in a state where arbitrariness equates the innocent and the guilty on the same standards. As per the Hon'ble Supreme Court in ***Sudhir Chandra v. Tata Iron & Steel Corp. Ltd.***[17] "equality before law and absolute discretion cannot fall together".

The Hon'ble SC in ***Gauri Shankar v. UOI***[18] stated that equals should not be treated unlike and unlike shouldn't be treated equally. *In casu*, Mr. Ian, the suspect in the murder case of Mr.

[13] *E.P. Royappa v. State of Tamil Nadu* (1974) SCR (2) 348.
[14] *Bachan Singh v State of Punjab* (1982) AIR 1982 SC 1336.
[15] *UOI v International Trade Corporation* (2003) 5 SCC 437.
[16] Moot Proposition [16].
[17] *Sudhir Chandra v Tata Iron & Steel Corp. Ltd* (1984) 3 SCC 369.
[18] *Gauri Shankar v UOI* (1994) 6 SCC 349.

Anand[19], dispelled all the doubts against himself[20] but then also he was placed behind the bars merely on the basis of suspicion[21]. *"There should be genuineness of complaint and reasonable belief as to a person's complicity for placing a person under arrest and not just suspicion."*[22] Mr. Ian's arrest is majorly on the ground that he was not ready to provide password which would provide the access to his car data[23], states the arbitrary usage of Section 69 to compel him without any reasonable belief to his complicity.

1.1.2. S.69 unreasonably infringes the right protected under Article 19(1)(a)[24]

As per ***Krishnan Kakkanth v. State of Kerala[25]*** while adjudging "reasonableness of restriction"[26], factors such as, duration, extent of the restriction, circumstances under which that imposition has been authorised, need to be looked into. S.69 provides for undefined grounds for encroaching upon the encrypted data and bringing it under the surveillance, which may extend up to the term of 6 months as per the 2009 rules, which clearly establishes unreasonableness, contravening the Fundamental Rights including different facets as found under Art. 19(1)(a) of Indian Constitution. S.69 provides a wider ambit to hold surveillance also upon such person who may not be leading the life of a criminal. It is stated in ***Govind v. State of Madhya Pradesh[27],*** that surveillance should be restricted to *only* the individuals showing 'a determination to lead a life of criminal'.

In reference to international perspective in ***Roman Zakharov v. Russia[28],*** ECtHR while examining violation of Art 8[29] stated that surveillance upon mobile without any remedies, didn't meet the quality of law requirement and was not necessary for the democracy. *In casu,* S.69 by its broad

[19] Moot Proposition [9].
[20] Moot Proposition [17].
[21] Moot Proposition [15].
[22] M P Jain, *Indian Constitutional Law* (8th edn, LexisNexis 2023) 1178.
[23] Moot Proposition [17].
[24] The Constitution of India 1949, art 19 cl 1 sub cl a.
[25] Krishnan Kakkanth v State of Kerala (1997) 9 SCC 495.
[26] *A.K. Gopalan v The State of Madras*
[27] *Govind v State of Madhya Pradesh* (1975) 2 SCC 148.
[28] *Roman Zakharov v Russia* 2015 app no. 47143/06
[29] European Convention to Human Rights, art 8.

terminology provides excess power in the hands of the Government and without justifiable safeguards, provides a safe haven for intrusive surveillance violating Art. 19(1)(a).

1.1.3. S.69 stands in contravention to Article 19(1)(d)[30]

Intrusive surveillance on a citizen's privacy is not permissible under Art 19, as stated in ***Malak Singh v. State of Punjab***[31]. In a minority view in ***Kharak Singh v. State of U.P.***[32]**,** it was stated that shadowed movement would induce a psychological restraint. *In casu,* S.69 provides undefined ambit for the Government to bring the owner of such car[33], using cryptography technique, under intrusive surveillance, which to the extent of reasonableness can't be proved. Therefore, such intrusive surveillance on the means of movement, may tantamount to restraint including psychological restraint on the freedom of movement without any reasonable justification.

1.1.4. S.69 stands in contravention to the right protected under Article 19(1)(g)[34]

S.69 in its process of application, unreasonably affects the right protected under Art 19(1)(g) of the individuals such as shareholders[35], and the occupation of other employees. *'A regulation directly interfering with the exercise of freedom of trade stands challengeable'*[36]as to the reasonableness. Unreasonable means 'unrestricted and unguided discretion' which renders the provision "unfair"[37]. Hon'ble ***Sreenivasa General Traders v. State of Andhra Pradesh***[38] it was held that to determine the reasonableness of restriction, nature and prevailing conditions of the trade must be taken into consideration. *In casu,* the impugned S.69 is detrimental for the citizen dealing in encrypted data, which provides for unregulated breach of privacy of the customer data, which would create an assertion in their mind of not opting for such technology and ultimately affecting the market presence of such businesses, unreasonably.

---

[30] The Constitution of India 1949, art 19 cl 1 sub cl d.
[31] *Malak Singh v State of Punjab* (1981) 1 SCC 420.
[32] *Kharak Singh v State of U.P* (1964) 1 SCR 285.
[33] Moot Proposition [16].
[34] The Constitution of India 1949, art 19 cl 1 sub cl g.
[35] *D.C.G.M. v UOI* (1983) AIR 1983 SC 937.
[36] M P Jain, *Indian Constitutional Law* (8th edn, LexisNexis 2023) 1114.
[37] *AN Parasuraman v State of Tamil Nadu* (1989) 4 SCC 683.
[38] *Sreenivasa General Traders v State of Andhra Pradesh* (1984) 4 SCC 353.

1.1.5. S.69 results in an unreasonable breach of data privacy protected under Article 21

As per, ***Dist. Registrar and Collector v. Canara Bank***[39], w.r.t interference in personal liberty of a person there must be a procedure and it should be tested w.r.t Art 19 and 14. *In casu,* the unreasonable breach of privacy providing no established procedure is resulting in infringement of Art 21. The apex court upheld in ***Justice KS Puttaswamy v. UOI***[40] that invasion in privacy must satisfy the triple test of *legality*, *legitimate aim* and *proportionality*, establishing a rational nexus. In the present case, the impugned clauses provide enormous and arbitrary power to the government and rather than bridging the nexus to achieve a welfare state, it is resulting in the creation of a surveillance state.

The *S.69 doesn't hold the needed legality* as it unreasonably results in the breach of data and privacy of an individual. Right to privacy is protected as an intrinsic part of the right to life and personal liberty under Art 21 and as a part of the freedoms guaranteed under Art 19[41].

The impugned S.69 doesn't have a legitimate aim for it foreseeably leads to depriving an individual's livelihood. As established in ***Dr. Haniraj L Chulani v. Bar Council of Maharashtra and Goa***[42] The easiest way of depriving a person's life would be by depriving his livelihood and *"as a broad interpretation the right to life would also include the right to livelihood and right to work"*[43]. S.69 gives enormous power in the hands of the government, *in casu,* providing the algorithm to the authority[44] and also the copy of keys for decryption of encrypted data[45], which is detrimental for the businesses dealing in Encryption and Decryption technology in Indica[46] and for individuals dependent on those businesses for livelihood.

---

[39] *Dist. Registrar and Collector v Canara Bank* (2005) 1 SCC 496.
[40] *Justice KS Puttaswamy v UOI* (2017) 10 SCC 1.
[41] *Justice KS Puttaswamy v UOI* (2017) 10 SCC 1.
[42] *Dr. Haniraj L Chulani v Bar Council of Maharashtra and Goa* (1996) 3 SCC 345.
[43] *Delhi Development Horticulture Employees' Union v Delhi Administration* (1992) 4 SCC 99.
[44] Moot Proposition [11].
[45] Moot Proposition [11].
[46] Moot Proposition [20].

The S.69 doesn't provide proportionate assertion of being fair, just, and for the welfare of the people. As stated in ***Maneka Gandhi v. UOI,***[47] Art.21 signifies that the procedure established by law to deprive a person of his personal liberty must be "reasonable, fair and just". In the present case, S.69 will lead into the creation of such surveillance state where even a minimal offence will result in the reveal of data of each individual, who comes under suspicion, providing a back door entry into the privacy without any provided safeguard and procedure as in S.69(2)[48].

1.2. S.69 stands in contravention to Article 20(3)[49], i.e., Self-incrimination

The S.69 proves to be self-incriminatory when it seeks data from the accused, which could be used to incriminate oneself. Art 20(3) covers evidence given by accused in any form including digital records and personal data.[50] For invoking Art 20(3), a formal accusation must have been placed upon an individual as— making him as an Accused in an FIR[51] — provided under ***Raja Narayan Bansilal v. Manek Firoz Mistry.***[52] *In casu,* S.69 proves to be in contravention of Art 20(3), as Mr. Ian has been compelled to submit the password for revealing the data which may be used as evidence incriminating himself.

The US courts have already recognised that the sharing of password to access the stored data would amount to a testimony. In the ***U.S.A. v. Kirschner***[53]*court* decided that asking the defendant to give the password key is a testimony from him that would be used to incriminate him. Further also stated ***in re Grand Jury Subpoena Duces Tecum***[54]**,** negated the government's statement that applicant's production of unencrypted files would be non-testimonial transfer. Imperatively the

[47] *Maneka Gandhi v UOI* (1978) 1 SCC 248.
[48] The Information Technology Act 2000, s 69 cl 2.
[49] The Constitution of India 1949, art 20 cl 3.
[50] *MP Sharma v Satish Chandra* (1954) AIR 1954 SC 300.
[51] *RB Shah v DK Guha* (1973) 1 SCC 696.
[52] *Raja Narayan Bansilal v Manek Firoz Mistry* (1961) 1 SCR 417.
[53] *U.S.A. v Kirschner,* 823 F. Supp. 2d 665 (E.D. Mich. 2010).
[54] *In re Grand Jury Subpoena Duces Tecum,* 846 F. Supp. 11 (S.D.N.Y. 1994).

data needed to be accessed through S.69 will ultimately lead to evidence being established by the accused himself, as in case of Mr. Ian[55] contravening Art 20(3).

1.3. The Part III of the Constitution is being violated by S.69

In ***Chiranjit Lal v. UOI[56],*** it was stated that the court is not concerned with the legislative judgement, or to hold the impugned statute to be ill-advised or unjustified or not justified by the prevailing facts, but rather it is to see whether the law transgresses any constitutional restrictions. *In casu,* the impugned S.69 transgresses upon the protected constitutional framework beyond the restricted zone and as such acts as a double-edged knife through the constitutional essence.

1.3.1. The "effect and consequence" of the legislation not aligned with the Constitution

The Express Newspaper v. UOI[57] held that a legislation can be struck down if the disadvantages were the direct and inevitable consequence of the legislation. In ***Maneka Gandhi v. UOI[58],*** the test of "direct and indirect effect" was used to determine whether there was violation of freedom of occupation. In present case, the direct effect of S.69 is the *creation of surveillance state, and the decrease in such technological advancement* by the excessive degree of encroachment of encrypted data.[59]

1.3.2. The "pith and substance" test proves invalid nature of S. 69

The Hon'ble SC laid down in ***State of Bombay v. Balsara[60]*** the test of *pith and substance*, where the main object, scope and effect of any legislation's provisions establishes "*true nature and character*"[61]. *In casu*, the inevitable government actions to keep a blanket monitoring and easy access to the encrypted data for an undefined time, without any safeguards, being arbitrary and affecting the liberties of citizens, establishes the true and despotic nature of S.69.

---

[55] Moot Proposition [19].
[56] *Chiranjit Lal v UOI* (1951) AIR 1951 SC 41.
[57] *Express Newspaper v UOI* (1985) SCR (2) 287.
[58] *Maneka Gandhi v UOI* (1978) 1 SCC 248.
[59] *Man Singh v State of Punjab* (1985) 4 SCC 146.
[60] *State of Bombay v Balsara* (1951) SCR 682 (708).
[61] *EV Chinnaiah v State of AP* (2005) 1 SCC 394.

1.3.3. <u>The impugned legislation falls in ambit of the doctrine of "colourable legislation"</u>

The SC in ***KC Gajapati Narayan Deo v. State of Orissa***[62] held that a legislature cannot violate the constitutional prohibition by employing an indirect method. *What cannot be done directly also cannot be done indirectly.*[63] *In casu,* the impugned S.69 provides for an indirect pathway for unreasonable breach of privacy and obstructive to freedoms under Art 19 which is not permitted by the constitution. As stated in ***RS Joshi v. Ajit Mills, Ahmedabad***[64] that sometimes the legislature is incompetent to enact a particular law, although a sticker of competency is attached to it. S.69 empowers the state for the arbitrary breach of privacy and the same doesn't make the state competent to exercise such legislation in the shadow of working for welfare state.

Therefore, in the light of the above made arguments the counsel would like to most humbly submit before the Hon'ble court that the impugned S.69 stands unconstitutional as it stands in contravention to the fundamental rights and other safeguards protecting the constitutional framework.

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

The counsel would like to most humbly submit before the Hon'ble SC that the rules, notified on 13th August 2022, mandated by the "Authority" in the regulations, regarding the restrictions on cryptographic algorithm stands disproportionately restrictive. The counsel would test the regulation for disproportionately invading the rights of the users and companies using the triple test[65] by establishing the **[2.1]** No established relevance of rule[66] in the society, **[2.2]** The Authority does not serve the legitimate state aim & **[2.3.]** Test of Proportionality is not met by the rules in "Authority"

[62] *KC Gajapati Narayan Deo v State of Orissa* (1953) AIR 1953 SC 375.
[63] M P Jain, *Indian Constitutional Law* (8th edn, LexisNexis 2023) 594.
[64] *RS Joshi v Ajit Mills, Ahmedabad* (1977) 4 SCC 98.
[65] *Justice KS Puttaswamy v UOI* (2017) 10 SCC 1.
[66] Moot Proposition [11].

2.1. No established relevance of the rule in the society

The S.16[67] contains security procedures and practices to secure electronic records and S.69 provides, power to issue directions for interception[68] or monitoring[69] or decryption[70] of any information through any computer resource. However, impugned "The Authority on Control and Regulation of Cryptography"[71] entails the restriction imposed upon cryptographic technique used for any purpose by forcing anyone to submit a copy of key for decryption.[72] The present rule, 2022 does not suffice in the role of being reasonable and non-restrictive, along with pre-existing rule of 2009[73]. The Authority unreasonably is restrictive in nature as the 2022 rule provides for undefined restrictions upon cryptographic technique users *without any safeguards and due procedures.*

2.1.1. S.69 is not in harmonious construction with other Sections of the IT ACT, 2000

While reading S.16 of the IT Act r/w S.69, proviso of former provides for taking into consideration the commercial circumstances, nature of transactions and such other related factors. *In casu*, the rule is likely to affect the business of car companies using the cryptography techniques including CG Metron Car company. As per CG Metron Car company, the security feature using the cryptography techniques provided, is what mostly attract their client and deals with personal data of individuals.

As stated in S.42[74], that a subscriber should exercise reasonable care to retain the control of the private key and take all steps to prevent its disclosure. *In casu*, the impugned legislation is being used to procure copy of private key of an individual which is to be stated against S.42 where the disclosure of same is to be prevented by the individual.

---

[67] The Information Technology Act 2000, s 67.
[68] *Amar Singh v Union of India* (2011) 7 SCC 90.
[69] Jaideep Reddy, ' Central Monitoring System and Privacy: Analysing what we know So Far', 10 IJLT (2014) 41.
[70] *Facebook Inc v Union of India* (2019) SCC Online SC 1264.
[71] Moot Proposition [11].
[72] Moot Proposition [11].
[73] The information Technology (Procedure and safeguards for interception, monitoring and decryption of information) rules, 2009.
[74] The Information Technology Act 2000, s 69.

2.1.2. <u>The rule of 2022 renders indefinite meaning</u>

The invalidity of any rule arises from the probability of the misuse of law to detriment of the individual.[75] It requires that ordinarily legislative[76] definition must be meaningfully precise-or at least that it should not be meaninglessly indefinite. *In casu*, the terminology used for the construction of the rule of 2022, is undetermined as the ambit of power exercised as "used for any purposes", "by anyone" and key holders are "bound to share the keys", exhibits undescribed power of the rule and is therefore lacks fairness[77], is also violating the right to privacy of the citizens and right to trade of the companies like C G Metron. Thus, a fuller statement of the legality ideal would be that it stands for the desirability in principle of advance legislative specification of criminal misconduct.[78] It is an established rule as per ***K.A. Abbas***[79]***,*** that if the persons applying constructions of the legislation, are in a boundless sea of uncertainty and the construction takes away a guaranteed freedom, the law must be held to offend the constitution.

2.1.3. <u>the duration of access of data to the investigative officer is not reasonable</u>

The time limit for *access* is nowhere defined or mentioned in impugned rule. Any restriction on the rule or such similar rule is passed that determines for how long will the authority hold the access of the data. The safeguards regarding the same are non-existent hence makes it ambiguous in nature therefore is restrictive. There is what is described as "'surveillant panoptic assemblage"[80], where data gathered through the ordinary citizen's surveillance practices finds its way to state surveillance mechanisms, through the corporations that hold that data.[81]

---

[75] *Committee Amritsar and Anr v The Sate of Rajasthan* (1960) A.I.R. 1960 S.C. 1100.
[76] In the increasingly unusual case of prosecution for a non-statutory crime, the vagueness inquiry is directed at the degree of precision achieved by prior judicial formulations of the offense charged. See W. LaFave & A. Scott, Handbook on Criminal Law 84 & nn.10-11 (1972).
[77] *Indra Gandhi v. Raj Narain* (1975) SCC (2) 159.
[78] Notes on the Principle of Legality in P. Low, J. Jeffries & R. Bonnie, Criminal Law: Cases and Materials 36-45 (1982).
[79] *K.A. Abbas v. The Union of India & Anr* [1971] 2 S.C.R. 446.
[80] Vian Bakir, 'Veillant Panoptic Assemblage": Mutual Watching and Resistance to Mass Surveillance after Snowden' (2015) Volume 3 (1) COGITATIO 32.
[81] Anna Jonsson Cornell, "Right to Privacy", Max Planck Encyclopaedia of Comparative Constitutional Law (20I5).

2.2. The rule of 2022 does not serve the legitimate state aim

The objective of the rule, 2022 is to procure the cryptographic algorithms for "any purposes".[82] However, in the present generation almost everyone uses encrypted and secure technologies such as passwords, private keys, biometric data etc. Forcing an individual to decrypt a device requires forcing them to part with a parameter known only to them. Once decrypted, the device is not only a storehouse of incriminatory evidence[83], but also serves as an inroad to the most private aspects of the individual's identity, and is therefore diverging from the legislative intent and as a consequence is not fulfilling the legitimate state aim.

2.2.1. The impugned rule is Self-incriminatory

Article 20(3) of the Indian Constitution and the Fifth Amendment of the constitution of USA, both in almost similar terms, provide constitutional protection against self-incrimination. "*No person accused of any offence shall be compelled to be a witness against himself*"[84], is the exact phraseology in the Indian Constitution and adequately represents the thrust of its American counterpart. In both the jurisdictions, the term 'witness against self[85]' corroborates protection against both testimonial evidences and non-testimonial evidences.[86] *In casu,* the 2022 rules of "Authority" can be declared to be in contravention of Article 20(3) on the grounds of classification created by it being based on unintelligible differentia[87] having no nexus with object sought to be achieved and thus being discriminatory.[88]

---

[82] Moot Proposition [11].
[83] Forced decryption of digital devices and accounts: A glimpse at Indian and American perspectives. Forced decryption of digital devices and accounts: A glimpse at Indian and American perspectives (barandbench.com)
[84] *State of Bombay v Kathi Kalu Oghad* (1961) AIR 1808.
[85] Carl B. Swisher, *The Growth of Constitutional Power in the Unites States,* at p. 107; See also 1 *Indian Law Review pp. 16-33, (1950).*
[86] J. U.C. Srivastav, 'Immunity from Self-Incrimination under Article 20(3) of the Constitution of India' (1996) Issue-4&5 J.T.R.I. Journal.
[87] *Karimbil Kunhikoman v State of Kerala* (1962) SCR 829.
[88] *Rajbala v State of Haryana* (2016) 2 SCC 445

2.2.2 The rule is providing ground for arbitrary state action

In the case of ***R.M. Malkani***[89]**,** Hon'ble SC observed that the court will not tolerate safeguards for the protection of the citizens to be imperilled by permitting the police to proceed by unlawful or irregular methods. The same is an established fact in Fourth Amendment, USA wherein ***Riley v. California***[90], the court condemned the warrantless search and seizures of digital contents on a cell phone during an arrest, and declared it unconstitutional. Furthermore, ***R v Plant***[91] is a leading decision of the Supreme Court of Canada on the protection of personal information under the Charter. The issue was whether the warrantless perimeter search of his home and the seizure of electricity consumption records violated his right against unreasonable search and seizure under section 8[92] of the Charter. However, in the present case, police proceeded to go against Mr. Ian to procure his private key by irregular means to hack into his system without any warrant or permissions. This action infringed his privacy without any probable reason hence, violated his minimal expectation of privacy[93] that is acknowledged to be reasonable.

2.3. Test of Proportionality is not met by the rules of 2022

The government and other public authorities must act reasonably and fairly and that each action of such authorities must pass the test of reasonableness.[94] Set of rules determining the necessary and sufficient conditions for test of proportionality-

2.3.1. The test shows the rule doesn't qualify the legitimate goal stage

The Rule should have a designated proper purpose for restricting a right and must have a legitimate goal. The said rule must not be against "legitimate state interest".[95] As per the Constitution of India the Right to privacy is a majoritarian concept[96], held in ***K.S, Puttasawamy***[97]

---

[89] *Ramana Dayaram Shetty v. The Internatrional Airport* (1975) 2 SCR 674.
[90] *Riley v. California*,573 US (2014).
[91] *R. v Plant* [1993] 3 S.C.R. 281.
[92] Canadian Charter of Rights and Freedom of 1982.
[93] *Kangan J., Florida v Jardines*, 569 US (2013).
[94] *Hansraj H Jain v. State of Maharashtra* (1993) 3 SCC 634.
[95] *Justice KS Puttaswamy v UOI* (2017) 10 SCC 1.
[96] *Mosley v News Group Paper Ltd.* (2008) EWHS 1777 (QB).

as such the right of privacy cannot be denied, even if there is a miniscule fraction of the population which is affected. In the words of **Sanjay Kishan Kaul J**.- "*This concept is not applied to Constitutional rights and the Courts are often called up on to take a non-majoritarian view, under the check and balance of power envisaged under the Constitution of India.*" *In casu* the rationale to bring this rule to life is to have access to data of everyone using cryptographic algorithms regardless of citizens or company infringing their fundamental rights and have no nexus needed to sought assertiveness to be achieved by the rule is not established.

2.3.2. The rule doesn't have qualifications to clear sustainability or rational connection stage

The measures undertaken to effectuate such a limitation are rationally connected to the fulfilment of that purpose, it must be suitable measure for furthering the goal. The concerns expressed are arising from the possibility of the State infringing the right to privacy, can be met by the test suggested for limiting the discretion of the State.[98] It is an age of "big data" or the collection of data sets. These data sets are capable of being searched; they have linkages with other data sets; and are marked by their exhaustive scope[99] and the permanency of collection.[100] *In casu,* "The Authority" had succumbed to indeterminate, open-ended power to process every device that has a cryptographic algorithm[101] and in the case of Mr. Ian, police took the action to seize and search Mr. Ian's phone, deeming it as an illegal and unreasonable act.

2.3.3. The impugned rule is intervening with the Right to Privacy of the citizens

Safeguarding one's privacy is a very vital issue and proponents of privacy rights adopting legal and technical measures to safeguard one's privacy.[102] This aspect of the right to privacy has assumed particular significances in this information age and in view of technological

---

[97] *Justice KS Puttaswamy v UOI* (2017) 10 SCC 1.
[98] *Keshavananda Bharti v State of Kerala* (1973) 4 SCC 225.
[99] Yvonne McDermott, 'Conceptualizing the right to data protection in an era of Big Data' (2017) 4 (1) Big Data and Society (4) (PDF) Conceptualising the right to data protection in an era of Big Data (researchgate.net)
[100] Yvonne McDermott, 'Conceptualizing the right to data protection in an era of Big Data' (2017) (4) (1) Big Data and Society (1) (PDF) Conceptualising the right to data protection in an era of Big Data (researchgate.net)
[101] Moot Proposition [11].
[102] Privacy and Human Rights: 2003 Threats to Privacy, see at: http://epic.org./privacy/threat/pr.html

improvements. A personhood would be a protection of one's personality, individuality and dignity.[103] It has been established in ***Maharashtra v. Bahrat Shanti Lai Shah***[104]*,*by the Hon'ble SC, the interception of data constitutes an invasion of an individual's right to privacy it can be curtailed in accordance with procedure validly established by law. The court has to see that the procedure itself must be fair, just and reasonable and not arbitrary, fanciful or oppressive. An authority cannot be given an unsustainable, untrammelled power to infringe the right to privacy of any person and companies in consequence berefting them of their trade by undermining their trade secrets and contracts with their customers therefore, the 2022 Rule is not sustainable in nature.

2.3.4. Qualifications required by rule to clear necessity stage are absent

The contemporary age has been aptly regarded as "an era of ubiquitous dataveillance, or the systematic monitoring of citizen's communications or actions through the use of information technology"[105]It is a European approach which examines whether the measures undertaken are necessary in that there are no alternative measures that may similarly achieve that same purpose with a lesser degree of limitation i.e., less restrictive and equally effective alternative. An individual has a right to protect his reputation from being unfairly harmed and such protection of reputation needs to exist not only against falsehood but also certain truths.[106] *In casu,* although the times need strict regulation of the encrypted data technology but the rule rather adds for a backdoor to infringe data privacy of an individual by the production of a copy of a key[107].

2.3.5. There is no checks and balances regarding the impugned rule

The balance between data regulation, encryption and decryption and individual privacy raises complex issues requiring delicate balances to be drawn between the legitimate concerns of the

[103] Daniel Solove,'10 Reasons Why Privacy Matters' published on January 20, 2014 https://www.teachprivacy.com/10-reasons-privacy-matters/
[104] *Maharashtra v. Bahrat Shanti Lai Shah* (2008) 13 SCC 5.
[105] Yvonne McDermott, 'Conceptualizing the right to data protection in an era of Big Data' (2017) 4 (1) Big Data and Society (1) (PDF) Conceptualising the right to data protection in an era of Big Data (researchgate.net)
[106] *The Second Circuit's decision in Haelam Laboratories v. Topps Chewing Gum*, 202 F.2d 866(2d Cir. 1953).
[107] Moot Proposition [11].

State on one hand and individual interest in the protection of privacy on the other.[108] The rule needs proper relation between achieving the purpose and social importance of preventing the limitation of the constitutional right i.e., the measure must not have a disproportionate impact on the right holder. Hence, it is duty of the courts should strike balance between the changing needs of society and the protection of the rights of the citizens as and when the issue relating to the infringement of the rights of the citizen comes up for consideration. Such a balance can be achieved only through securing and protecting liberty, equality and fraternity with social and political justice to all the citizens under rule of law.[109] Nevertheless, in the present case the impugned rule is hampering various fundamental rights therefore, is arbitrary in nature. In consequence, "The Authority" is not striking the balance between the legislative intent behind its implementation to the action done.

Therefore, in the light of the above-mentioned submissions the counsel humbly submits before the Hon'ble Court that rule laid down in "The Authority on Control and Regulation of Cryptography", 2023 is too restrictive in nature as it failed the triple test to prove its validity.

[108] Christina P. Moniodis, 'Moving from Nixon to NASA: Privacy 's Second Strand- A Right to Informational Privacy', (2012), Vol. 15 (1) Yale Journal of Law and Technology 159.
[109] *S.S, Bola & Ors. v B.D. Sardana & Ors.* (1997) (8) SCC 522.

PRAYER

Wherefore, may it please the Hon'ble Supreme Court of Indica, in the light of facts and circumstances, the issue presented, arguments advanced, and authorities cited, the Petitioners prays that this Hon'ble Court may be pleased to adjudge, rule upon and declare the following-:

1. That Section 69 of the Information Technology Act, 2000 is constitutionally invalid.
2. That governmental control over the use of cryptographic techniques is too restrictive in nature.

And pass any such order that this Hon'ble Court deems fit in the interest of justice, equity and good conscience.

Rest is left to this Hon'ble Court's wisdom and fine sense of judgment.

All of which is respectfully affirmed and submitted

(Counsels on behalf of Petitioners)