

Sumit Kumar Singh vs Union of India

Sumit Kumar Singh vs Union of India

SooperKanoon Citation : sooperkanoon.com/1550352

Court : Kerala

Decided On : Jun-17-2022

Judge : Honourable Mr.Justice K.Vinod Chandran,Honourable Mr.Justice C. Jayachandran

Appeal No. : CRL.A/865/2021

Appellant : Sumit Kumar Singh

Respondent : Union of India

Judgement :

IN THE HIGH COURT OF KERALA AT ERNAKULAM

PRESENT THE HONOURABLE MR.JUSTICE K.VINOD CHANDRAN & THE HONOURABLE MR.JUSTICE C. JAYACHANDRAN FRIDAY, THE 17TH DAY OF JUNE 2022 / 27TH JYAISHTA, 1944 CRL.A NO. 865 OF 2021 AGAINST THE COMMON ORDER IN CRL.MP NOS.179/2021 AND 180/2021 IN SC 1/2020/NIA DATED 1.11.2021 OF SPECIAL COURT FOR TRIAL OF NIA CASES,ERNAKULAM APPELLANTS/A1 & A2: 1 SUMIT KUMAR SINGH, AGED 22 YEARS S/O.PRAMOD KUMAR SINGH, WARD NO.13, MILKI, BANAHARA, GANGTA, MUNGER DISTRICT, BIHAR, PIN-811213. 2 DAYA RAM, AGED 23 YEARS S/O.BHANWAR LAL, WARD NO.17, JOGIASAN, BOHAR,

HANUMANGARH DISTRICT, RAJASTHAN, PIN-335 523. BY ADVS. V.JOHN SEBASTIAN RALPH VISHNU CHANDRAN RALPH RETI JOHN APPU BABU SHIFNA MUHAMMED SHUKKUR MAMATHA S. ANILKUMAR ANILA T.THOMAS RESPONDENT/COMPLAINANT: UNION OF INDIA REPRESENTED BY NATIONAL INVESTIGATION AGENCY, KOCHI, REPRESENTED BY THE SPECIAL PUBLIC PROSECUTOR, HIGH COURT OF KERALA, ERNAKULAM, PIN-682031. BY ADVS. MANU S., ASG OF INDIA SMT.MINI GOPINATH, CGC(CG-375) THIS CRIMINAL APPEAL HAVING COME UP FOR ADMISSION ON 30.5.2022, THE COURT ON 17.06.2022 DELIVERED THE FOLLOWING: K.VINOD CHANDRAN & C.JAYACHANDRAN, JJ.
----- Crl.Appeal.No.865 of 2021
----- Dated this the 17th day of June, 2022

J U D G M E N T

Jayachandran, J.

1. Accused nos.1 and 2 in S.C.No.1/2020/NIA on the files

of the Special Court for trial of NIA Cases, Ernakulam, are the appellants herein. The offences alleged against them are punishable under Ss.120B, 201, 380, 454, 461, read with 34 of the Penal Code, as also, under S.66F(1)

(B) of the Information Technology Act, 2000. Two separate Criminal Miscellaneous Petitions bearing nos.179/2021 and respectively, before the Special Court seeking discharge.

In Cr.M.P.No.180/2021, A1 contented that the offence under S.66F(1)(B) of the Information Technology Act, 2000 ('I.T Act', for short) will not lie. In Cr.M.P.No.179/2021, A2 sought discharge on the premise that he was merely a roommate of A1, that he did not stand guard when the theft was committed, that nothing was recovered from him and that his mobile phone was misused to operate the social media account. By virtue of a common order dated

1.11.2021, those applications were dismissed, which order

is impugned in the instant Criminal Appeal.

2. The prosecution allegations are as follows: Indigenous Aircraft Carrier (I.A.C) is a warship being constructed by M/s.Cochin Shipyard Limited for the Indian Navy. Numerous Multi-Function Consoles (M.F.Cs) are critical components to the warship, forming part of the Integrated Platform Management System, which controls several functionalities, including Battle Damage Control

System of the warship. The appellants/accused were contract workers engaged in painting aboard the I.A.C. After undergoing induction training on safety and briefed on the sensitive nature of the project, the accused persons started working as painting assistants at the W-Ring during the period from May, 2019 to September,

2019. A1 being self-trained in handling computer hardware, conspired with A2 and committed theft of the following items, as detailed in the tabular form shown here under:-

Sl.No. Month & Location of theft Components stolen Year 1 May, 2019 CPU of MFC in 5Q 256 GB Solid State Ring Drives (SSDs), Processors & 4GB Random Access Memory (RAM)

2	Second Week	CPU of MFC-29	2 RAMs	
data				
3	Last	week MFC-22 in 4R Ring	2 RAMs	of
data				
4	First	Week MFC-28 in 5N Ring	2 RAMs	of
data from the CPU				
5	Last	week MFC-25 in 7P Ring	2 RAMs	of
data & 2 USB cables from the CPU				

data

3. The prosecution would further allege that on 29.8.2019, in furtherance of the conspiracy between A1 and A2, A1 went to a shop at Ravipuram and purchased an

SSB case and an OTG connector and using the same, accessed the SSDs, formatted it and deleted the critical data from the four stolen SSDs, while the critical data in respect of the remaining SSD was retained. Thereafter, A2 pursuant to the conspiracy with A1, posted an advertisement in his account in the on-line portal, OLX, offering the stolen processor for sale citing his mobile number. One processor was sold on 11.9.2019. The accused persons, who came to know about registration of the crime, left Ernakulam for Surat with the remaining stolen computer hardware components. A1 concealed the stolen articles in the house of his brother at Surat. A2 proceeded to his house at Rajasthan. In November, 2019, A1 left Surat for his native place at Bihar with one RAM, one processor and one SSD, which were seized from his possession during search of his house. A1, while at Surat, installed one SSD and one RAM on the personal computer of his brother, which along with the remaining 3 stolen SSDs, 3 processors, 8 RAMs and one heat sink were

recovered from the house of his brother

caused total damage of Rs.25,77,823.50, besides causing delay in timeline of the defence project, thus affecting the security of the Nation. The accused persons have thus committed the offences punishable under Ss.120B, 201, 380, 454, 461, read with 34 of the IPC, besides under S.66F(1)(B) of the I.T Act.

4. Heard Adv.John S.Ralph, learned counsel for the appellants, and Sri.S.Manu, learned Assistant Solicitor General of India for the respondent. Perused the records.

5. Learned counsel for the appellants contended that the charge for offence punishable under S.66F(1)(B) of the I.T Act will not lie against the appellants.

Relying upon the maxim *actus non facit reum nisi mens sit rea*, learned counsel submitted that the *actus reus*, by itself, would not constitute the crime, unless done with the necessary *mens rea*. Learned counsel propounded the following ingredients for the offence under S.66F(1)(B) of the I.T Act:-

- i. Knowingly or intentionally penetrating or accessing a computer resource.
- ii. Without authorization or exceeding authorization.
- iii. Obtaining access to information, data or computer database that is restricted for reasons of the security of the state or foreign relations.
- iv. With reasons to believe that such information, data or computer database obtained may be used to cause or likely to cause injury to the interest of the sovereignty and integrity of India.

6. By no stretch of imagination, it could be discerned

that the accused persons had 'reasons to believe' that data contained in the stolen components may be used to cause, or likely to cause, injury to the interests of the sovereignty and integrity of India or security of the State or to the advantage of any foreign nation or the like, so as to attract the offence of cyber terrorism as defined. Learned counsel invited our attention to the

definition of reason to believe under S.26 of the Indian Penal Code to point out that the given facts admit of no such satisfaction as regards reasons to believe the user of the data. A mere suspicion or doubt cannot be raised to the required level of 'reason to believe' is the appellants' contention. To drive home the absence of

mens rea, learned counsel relied upon the subsequent conduct of the appellants/accused in erasing the data and selling the stolen articles through the platform, OLX. A processor was sold to CW47, which was later recovered from his house, which conduct would only indicate that the intention of the appellants/accused was monetary

gain, *simpliciter*, for which they resorted to theft. Learned counsel pointed out that erasure of the data in the components stolen before effecting its sale, is a sure pointer that the accused persons did not want to make use of the contents of the

persons, who were engaged on contract basis to effect painting work to the warship, were permitted entry only

through the gate by name, Sannidhi, with fingerprint based bio-metric authentication, besides issuing separate entry pass. They were given induction training on the safety, besides being briefed about the sensitive nature of the project. Thus the accused persons had specific knowledge that the indigenous aircraft carrier is a naval warship of seminal importance to the defence of India.

Theft of various equipments was committed on numerous occasions on various dates between the period from July to September, 2019. The second appellant/A1 is a person self-trained in computer hardware. Learned A.S.G.I submitted that there exist clear materials to show the complicity of the accused persons, pursuant to a common design by and between them.

8. Learned A.S.G.I. Went on to submit that the specific argument with respect to offence under S.66F(1)(B) is bereft of any merits or bona fides. The attendant circumstances above referred would clearly indicate that the appellants/accused persons had every reason to

believe that the information/data contained in the components, dismantled from critical equipments installed in a warship, can be used to cause, or likely to cause, injury to the interests of the sovereignty and integrity of India, security of the State and the like. The act committed is nothing short of cyber terrorism as

defined in S.66F(1)(B) of the I.T Act. Alternatively, learned A.S.G.I submitted that the question as to whether there existed adequate reason for the accused persons to believe that the data will be used or likely to be used to the detriment of the nation is a matter to be unfurled during the course of trial, wherefore, the proceedings cannot be prematurely aborted, presuming absence of mens rea. Learned A.S.G.I discounted the claim based on the polygraph test by pointing out that the same is only an

aid in the hands of the investigators, the results whereof would not have any effect of exoneration/exculpation. As regards erasure of the data, learned A.S.G.I

submitted that with the present technological advance, such data can be retrieved at any point of time by an expert. On such premise, learned A.S.G.I would submit that the instant appeal be dismissed, confirming the order impugned of the learned Special Judge.

9. S.66F(1)(B) of the I.T Act is extracted herein below: 66F. Punishment for cyber terrorism.-(1) Whoever,-

(A) xxx xxx xxx

(B) knowingly or intentionally penetrates

or accesses a computer resource without authorisation or exceeding authorised access, and by means of such conduct obtains access to information, data or computer data base that is restricted for reasons for the security of the State or foreign relations; or any restricted information, data or computer data base, with reasons to believe that such information, data or computer data base so obtained may be used to cause or likely to cause injury to the interests of the sovereignty and integrity of India, the security of the State, friendly relations with foreign States, public order, decency

or morality, or in relation to contempt of court, defamation or incitement to an offence, or to the advantage of any foreign nation, group of individuals or otherwise, commits the offence of cyber terrorism. A dissection of the Section unfolds the following ingredients:

(1) Knowingly or intentionally penetrates or accesses a computer resource without authorisation or by exceeding authorised access.

(2) Obtains by the above conduct access to:

i).information, data or computer data base that is restricted for reasons of the security of the State or foreign relations; or ii).any restricted information, data or computer database.

(3) There exist reasons to believe that such

information, data or computer database so obtained may be used to cause, or likely to cause, injury to the interests of the sovereignty and integrity of India, the security of the State, friendly relations of the foreign states, public order, decency or morality or in relation to contempt of court, defamation or incitement to an offence, or to the advantage of

any foreign nation, group of individuals or otherwise.

10. The first aspect to be ascertained is whether the

data/information contained in the stolen articles is restricted for reasons of security of the state or the like as envisaged in S.66F(1)(B). In the attendant facts, it is indisputed that the theft alleged is committed in respect of electronic equipments installed in a warship, which was being constructed for the Indian Navy by the

Cochin Shipyard Limited, a prestigious project of the Cochin Shipyard Limited as claimed. For that very reason, it is only reasonable to conclude that the information/ data attached to the M.F.Cs is certainly a restricted data/information for reasons of the security of the State, thereby prima facie satisfying the first limb of S.66 F(1)(B).

11. Now, coming to the legal requirement of 'reasons to believe'- the sheet anchor of appellant's arguments - we straight away refer to S.26 of the Penal Code, which is extracted herein below: 26. Reason to believe.- A person is said to have reason to believe a thing, if he has sufficient cause to believe that thing but not otherwise.

12. In the context of S.411 of the Penal Code, which

employs the expression 'reason to believe', it was held

in Abdul Karim v. State of Mysore [1972 CrLJ 217] that if the circumstances are such that a reasonable man would be led by a chain of probable reasoning to conclude or infer that the articles found were stolen, then even though the circumstances may fall short of carrying

absolute conviction on the point, a person must be held

to have reason to believe so. In *Joti Parshad v. State of Haryana* [AIR 1993 SC 1167], the Hon'ble Supreme Court

held that 'reason to believe' is a facet of the state of

mind and mere seeing cannot be equated to believing. After referring to the definition of 'reason to believe' in S.26 of the Penal Code, the Hon'ble Supreme Court observed thus : In substance what it means is that a person must have reason to believe if the circumstances are such that a reasonable man would, by probable reasoning, conclude or infer regarding the nature of the thing concerned. The requirement of reason to believe has to be deduced from the various circumstances of the case, opined the Hon'ble supreme Court.

13. On the following counts, we find that there existed

adequate reasons for the appellants to believe that the data/information/computer database stolen may be put to the use of the character defined in the Section:

(1) The appellants were contract workers engaged for the purpose of performing the painting works in a warship being constructed by the Cochin Shipyard Limited for the Indian Navy.

(2) The appellants were given induction training detailing the safety and sensitive nature of the project.

(3) On account of the sensitive nature of the project,

the employees, including the appellants, were permitted to enter the premise only through restricted entry, with finger print based bio-metric authentication, besides issuance of separate entry pass for entry to the indigenous aircraft carrier.

(4) The Second appellant/A1 is computer savvy person, self trained in computer hardware, as is decipherable from the allegation that he could dismantle the electronic gadgets installed in a warship.

14. The cohort of A2 is all along projected in the prosecution case, as could be seen from the facts that he stood as guard while A1 was dismantling the electronic gadgets; it was his phone number that was given for the purpose of sale in the OLX platform; that he was identified by the buyer of the gadgets (CW47); that stolen articles were kept in his room for a period of one

month without any demur/objection; and that A2 accompanied A1 to Surat for the purpose of hiding the stolen articles at the residence of A1's brother. All the above referred allegations, if proved, would establish the ad idem by and between A1 and A2.

15. The above referred facts, which were in fact perceived by the accused persons by their senses and about which they had clear and unmistakable knowledge,

would, in our considered opinion, prima facie satisfy that the accused persons had all reasons to believe that the data may be used to cause, or likely to cause, injury to the interests of the sovereignty and integrity of India, security of the State and the like, as contemplated in S.66F(1)(B). They cannot claim to have been mere ordinary thieves, since they were thoroughly briefed on the work and were aware of the sensitive nature of the objects thieved. They also erased the SDS before they were sold; which, thieves ignorant of the value of the data contained therein would never attempt to do. As it is well settled, what is to be looked into for the purpose of discharge is the prosecution allegations, supported by the materials produced in support thereof.

16. As regards mens rea, canvassed by the learned counsel

for the appellants, we are of the opinion that the same reflects a state of mind; a positive intention to do or refrain from doing something, wherefore it is too early for us, at this stage, to conclude on the presence, or for that matter the absence, of mens rea in a given conduct. The same is a matter to be assessed after adducing evidence. Therefore, once, actus reus is alleged to have been committed and in the absence of any clinching extenuating/exculpating circumstance, a court of law cannot discharge an accused assuming that he had no mens rea in performing the actus reus. We are not

impressed by the contention that the

injury/damage that could be caused to the security of the nation on such critical data being accessed by others, Secondly, there is an allegation that the data was copied before erasure and thirdly such data is always possible to be retrieved with the aid of an expert. Theoretically, such misuse of the data can be made even at the hands of the purchaser.

17. In the facts and circumstances, we conclude that there exists adequate parameters and circumstances to prima facie infer that the appellants/accused had reasons

to believe that the information/data/computer database may be used to cause or likely to cause injury to the the security of the State. We, therefore, confirm the common

order impugned, of the learned Special Judge and reject

this appeal. We, however, caution the learned Special Judge to proceed with the trial, independent of the observations made in this Order, which are purely prima facie impressions. The Criminal Appeal is dismissed. Sd/- K.VINOD CHANDRAN JUDGE Sd/- C.JAYACHANDRAN JUDGE jg APPENDIX OF CRL.A 865/2021 PETITIONER ANNEXURES Annexure 1 CERTIFIED COPY OF THE POLYGRAPH TEST RESULTS OF THE APPELLANTS DATED 03.08.2020 ISSUED FROM REGIONAL FORENSIC SCIENCE LABORATORY, THRISSUR TO THE HON'BLE JUDGE, SPECIAL COURT FOR NIA CASES, ERNAKULAM.

SooperKanoon - India's Premier Online Legal Search - sooperkanoon.com