2024:DHC:4987

* **IN THE HIGH COURT OF DELHI AT NEW DELHI**

Date of decision: 02nd JULY, 2024

IN THE MATTER OF:

\+ **W.P.(C) 7789/2023**

SUBLIME SOFTWARE LTD. ..... Petitioner

Through: Mr. Bhuvan Mishra, Mr. Arjun Adarian Dsouza, Mr. Yash Maheshwari, Mr. Krishna Kanhaiya Kumar and Mr. Tanmay Mishra, Advocates.

versus

UNION OF INDIA ..... Respondent

Through: Mr. Vaibhav Gaggar, SPC with Mr. Utkarsh Tiwari and Ms. Shefali Munde, Advocates.
Mr. Vedansh Anand, GP.

CORAM:
HON'BLE MR. JUSTICE SUBRAMONIUM PRASAD

JUDGMENT

1. The Petitioner has approached this Court seeking a direction to the Respondent to produce and publish the Order passed by the Respondent under Section 69A of the Information Technology Act, 2000 blocking the open-source messaging application of the Petitioner called '*Briar*'. The Petitioner has also prayed for setting aside the said order.

2. The facts of the case reveal that the Petitioner is a software development company, having its registered office at Brighton, United Kingdom. It is stated that the Petitioner developed an app called '*Briar*', which is a Free and Open Source Software (FOSS). It is pertinent to mention

here that FOSS is a term used to denote software which is freely licensed to be used and anyone can copy, study and change the software in any way and the source code is openly shared so that people are encouraged to voluntarily improve the design of the software. It is stated in the Writ Petition that FOSS promotes interoperability and obviates occurrences of single load failure. It is stated that Briar operates on a technology in which a person can directly send a message to another person even when there is no internet connectivity. It is stated that the technology is crucial in times of emergency, natural calamities & catastrophic disasters in providing emergency healthcare and disaster management as it enables smooth communication between persons and authorities during times of distress. It is also stated in the Writ Petition that *Briar* was widely used by the authorities and residents to coordinate and provide relief in the absence of internet connectivity during the floods that hit the state of Tamil Nadu in the year 2017. It is stated that the access to the applications like '*Briar*' is regulated by the provisions of the Information Technology Act, 2000 (*hereinafter referred to as 'the IT Act'*). Section 69A of the IT Act empowers the Central Government to issue directions for blocking access of any information through any computer resources for reasons contained in Section 69A of the IT Act. It is stated that in exercise of powers conferred under the IT Act read with Information and Technology (Procedure and Safeguards for Blocking of Access of Information by Public) Rules 2009 (*hereinafter referred to as 'the Blocking Rules'*) the Respondent has blocked the software of the Petitioner in India.

3. Petitioner has approached this Court stating that it has not been

informed about the blocking and that the Order of blocking has been passed without following the procedure given in the Blocking Rules. It is also stated that the Petitioner is not in a position to access the software throughout the country because of the blocking.

4. Learned Counsel for the Petitioner relies on Rules 8 & 9 of the Blocking Rules. It is stated that Rule 8 of the Blocking Rules postulates that in case a request is received for blocking any application/software then the designated officer shall make all efforts to identify the persons or intermediary who has hosted the information or part thereof as well as the computer resource on which such information or part thereof is being hosted and where he is able to identify such person or intermediary and the computer resource hosting the information or part thereof which have been requested to be blocked for public access, he shall issue a notice by way of letters or fax or e-mail signed with electronic signatures to such persons or intermediary in control of such computer resource to appear and submit their reply and clarification, if any, before the Committee referred to in Rule 7 of the Blocking Rules. It is the case of the Petitioner that the said procedure has not been followed by the Respondents. Learned Counsel for the Petitioner also draws the attention of this Court to Rule 8(3) of the Blocking Rules which states that in case intermediary who has been served with the notice under Rule 8(1) of the Blocking Rules is a foreign entity or body corporate as identified by the Designated Officer then the notice shall be sent by way of letters or fax or e-mail signed with electronic signatures to such foreign entity or body corporate and the foreign entity has to respond to such a notice within the time specified and only then can an Order of blockage be

passed. It is also stated that Rule 9 of the Blocking Rules deals with blocking of information in cases of emergency and the same can be done only as an interim measure. It is the case of the Petitioner that since the Blocking Rules have not been followed, the Blocking Order must be revoked immediately or at least the Petitioner must be made aware of the said blocking order so that the Petitioner can take adequate legal remedy in accordance with law.

5. *Per contra*, it is stated by the learned Counsel for the Respondents that the application of the Petitioner has been blocked only in Jammu and Kashmir for the reason that it poses threat to national security and sovereignty. It is stated that 14 mobile messaging applications (Apps), including the application of the Petitioner herein, have been blocked in the region of Jammu Kashmir under Section 69A of the IT Act as they contain material that is prejudicial to the Sovereignty and Integrity of India, Defence of India, Security of the State and Public order. It is further submitted by the learned Counsel for the Respondent that since the Petitioner do not have any representative in India, they could not be informed about the blocking. He further states that Rule 16 of the Blocking Rules provides that strict confidentiality should be maintained regarding all the requests and complaints received and actions taken on them and, therefore, the Order of blocking cannot be shared.

6. Heard the learned Counsels for the parties and perused the material on record.

7. At the outset it is to be stated that in matters of national security, principles of natural justice can be given a go-by. It is well settled that the

right to a fair hearing may have to yield to overriding considerations of national security. According to Sir William Wade [H.W.R. William Wade and C.F. Forsyth, Administrative Law (10th Edn., Oxford University Press Inc., 2009) 468-470] , any restriction, limitation or exception on principles of natural justice is "only an arbitrary boundary". To quote further:

> "*The right to a fair hearing may have to yield to overriding considerations of national security. The House of Lords recognised this necessity where civil servants at the government communications headquarters, who had to handle secret information vital to national security, were abruptly put under new conditions of service which prohibited membership of national trade unions. Neither they nor their unions were consulted, in disregard of an established practice, and their complaint to the courts would have been upheld on ground of natural justice, had there not been a threat to national security. The factor which ultimately prevailed was the danger that the process of consultation itself would have precipitated further strikes, walkouts, overtime bans and disruption generally of a kind which had plagued the communications headquarters shortly beforehand and which were a threat to national security. Since national security must be paramount, natural justice must then give way.*
>
> ***The Crown must, however, satisfy the court that national security is at risk. Despite the constantly repeated dictum that 'those who are responsible for the national security must be the sole Judges of what the national security requires', the court will insist upon evidence that an issue of national security arises, and only then will it accept the opinion of the Crown that it should prevail over some legal right.***"
>
> *(emphasis supplied)*

8. The Apex Court in Ex-Armymen's Protection Services (P) Ltd. v. Union of India, **(2014) 5 SCC 409,** while dealing with a challenge regarding grant of security clearance to a ground handling agency in different airports has observed as under:

> *"15. It is difficult to define in exact terms as to what is "national security". However, the same would generally include socio-political stability, territorial integrity, economic solidarity and strength, ecological balance, cultural cohesiveness, external peace, etc.*
>
> *16. What is in the interest of national security is not a question of law. It is a matter of policy. It is not for the court to decide whether something is in the interest of the State or not. It should be left to the executive. To quote Lord Hoffman in Secy. of State for Home Deptt. v. Rehman [(2003) 1 AC 153 : (2001) 3 WLR 877 : (2002) 1 All ER 122 (HL)] : (AC p. 192C)*
>
> > *"... [in the matter] of national security is not a question of law. It is a matter of judgment and policy. Under the Constitution of the United Kingdom and most other countries, decisions as to whether something is or is not in the interests of national security are not a matter for judicial decision. They are entrusted to the executive."*
>
> ***17. Thus, in a situation of national security, a party cannot insist for the strict observance of the principles of natural justice. In such cases, it is the duty of the court to read into and provide for statutory exclusion, if not expressly provided in the rules governing the field. Depending on the facts of the particular case, it will however be open to the court to satisfy itself whether there were justifiable facts, and***

in that regard, the court is entitled to call for the files and see whether it is a case where the interest of national security is involved. Once the State is of the stand that the issue involves national security, the court shall not disclose the reasons to the affected party."

(emphasis supplied)

9. Similarly, the High Court of Karnataka in its judgment dated 30.06.2023 in **Writ Petition No. 13710/2022** titled as X Corp v. Union Of India & Anr., has held as under:

"*(c) This court is convinced of the contention of learned ASG that the Blocking Orders are reasoned decisions and they are founded on stronger footings of law, facts & evidentiary material. The objectionable content comprises of tweets, pictures & audios/videos (screenshots). Many of them have outrageous content; many are treacherous & anti-national; many have abundant propensity to incite commission of cognizable offences relating to sovereignty & integrity of India, security of the State and public order. No reasonable person in the trade would agree with the contention of petitioner that, reasons for the impugned orders are lacking. Sufficiency of evidence or reasons again belongs to the domain of the authority. The reasons have a thick nexus with the statutory grounds.* ***It is not that one single official functionary of the government in the fit of anger or anxiety has made these orders. The statutory committee comprises of high functionaries of the government and there is no allegation of malafide or the like leveled against them. True it is legalistically speaking, in the language of Rules 8 & 9, it is one single officer of the high rank, who considers recommendations of the Committee and passes orders either agreeing or disagreeing with such recommendations. When the***

> ***Designated Officer agrees with the recommendation, his decision partakes the character of an institutional decision. When he does not agree, it can be his individual decision, and that is not the case here. The impugned orders are a product of institutional deliberation in which the representatives of petitioner with prior notice had participated,. The decision whether certain information is objectionable in the teeth of provisions of the Act and the Website Blocking Rules, does essentially belong to the domain of Executive. In matters like this, Writ Court cannot run a race of opinions with the statutory functionaries."***
>
> *(emphasis supplied)*

10. The Respondent states that the software/application developed by the Petitioner can work even when there is no internet connection, and is suspected to be used by terrorists in State like Jammu and Kashmir. The application can be misused and can definitely be a potential threat to the national security, sovereignty and integrity of India.

11. The process for blocking a website/software/application has been provided under Section 69A of the IT Act read with the Blocking Rules. Under Rule 3 of the Blocking Rules, the Central Government designates an officer not below the rank of Joint Secretary as the 'Designated Officer' for the purpose of issuing directions for blocking for access by the public any information generated, transmitted, received, stored or hosted in any computer resource. It is further stated that a request was received from the Indian Cyber Crime Coordination Center (I4C), Ministry of Home Affairs *vide* letter dated 26.04.2023 to block 14 applications, including *Briar,* in the Union Territory of Jammu and Kashmir as the said applications were used

by terrorists and their supporters. Under Rule 6 of the Blocking Rules, the request/complaints are sent to the concerned Nodal Officer of the Organisation for blocking of access by the public any information generated, transmitted, received, stored or hosted in any computer resource and after being satisfied, the Nodal Officer sent a request to the Designated Officer in the format specified under the Rules. Rule 7 of the Blocking Rules provides that the request of the alleged offending information shall be examined by a Committee consisting of the Designated Officer as its Chairperson and representatives not below the rank of Joint Secretary in Ministries of Law and Justice, Home Affairs, Information and Broadcasting and the Indian Computer Emergency Response Team appointed under the IT Act. The request is examined under Rule 8 and directions are issued. Rule 9 of the Blocking Rules provides for blocking of information in cases of emergency and the same reads as under:

> "*9. Blocking of information in cases of emergency.- (1) Notwithstanding anything contained in rules 7 and 8, the Designated Officer, in any case of emergency nature, for which no delay is acceptable, shall examine the request and printed sample information and consider whether the request is within the scope of sub-section(1) of section 69A of the Act and it is necessary or expedient and justifiable to block such information or part thereof and submit the request with specific recommendations in writing to Secretary. Department of Information Technology.*
>
> *(2) In a case of emergency nature, the Secretary, Department of Information Technology may, if he is satisfied that it is necessary or expedient and justifiable for blocking for public access of any information or*

part thereof through any computer resource and after recording reasons in writing, as an interim measure issue such directions as he may consider necessary to such identified or identifiable persons or intermediary in control of such computer resource hosting such information or part thereof without giving him an opportunity of hearring.

(3) The Designated Officer, at the earliest but not later than forty-eight hours of issue of direction under sub-rule (2), shall bring the request before the committee referred to in rule 7 for its consideration and recommendation.

(4) On receipt of recommendations of committee, Secretary. Department of Information Technology, shall pass the final order as regard to approval of such request and in case the request for blocking is not approved by the Secretary, Department of Information Technology in his final order, the interim direction issued under sub-rule (2) shall be revoked and the person or intermediary in control of such information shall be accordingly directed to unblock the information for public access."

12. In the present case, it is stated by the learned Counsel for the Respondent that since the Petitioner does not have any representative in the country, the Petitioner could not be contacted. Rule 16 of the Blocking Rules provides that strict confidentiality shall be maintained regarding all the requests and complaints received and actions taken thereof. This Court can take judicial notice of the fact that decisions taken at the highest level and for the benefit of the security & sovereignty of the country can be kept confidential. As held by the Apex Court in Ex-Armymen's Protection

Services (supra) the principles of natural justice can be given a go-by in the matters related to security and sovereignty of the country. The interim Order has been reviewed by the Committees constituted under Section 7 of the Blocking Rules and as stated earlier, the Committee consists of top officials of the Government of India. The blocking orders have been passed for 14 applications/softwares, including the software/application of the Petitioner herein as it was being used by the Terrorists and their supporters to disturb the security and sovereignty of the country. The application of the Petitioner has been blocked only in the State of Jammu and Kashmir and the same can be used in all other parts of the country.

13. In view of the above, this Court is not inclined to entertain the present Writ Petition.

14. Accordingly, the Writ Petition is dismissed along with the pending applications, if any.

SUBRAMONIUM PRASAD, J

JULY 02, 2024
Rahul