Reserved on : 21.03.2025
Pronounced on : 29.04.2025

R

IN THE HIGH COURT OF KARNATAKA AT BENGALURU

DATED THIS THE 29TH DAY OF APRIL, 2025

BEFORE

THE HON'BLE MR. JUSTICE M. NAGAPRASANNA

WRIT PETITION No.2358 OF 2025 (GM – RES)

BETWEEN:

M. MOSER DESIGN ASSOCIATES (INDIA) PVT. LTD.,
A COMPANY INCORPORATED UNDER
THE COMPANIES ACT, 1956
HAVING ITS REGISTERED OFFICE AT:
2ND AND 3RD FLOOR, NO 374,
MSQUARE, 100 FEET ROAD,
HAL 2ND STAGE, INDIRA NAGAR,
BENGALURU, INDIA – 560 038
REPRESENTED BY ITS
AUTHORISED REPRESENTATIVE AND
COMPANY SECRETARY
MR. PANKAJ ARYA,
AGED 46 YEARS.

... PETITIONER

(BY SRI JATIN SEHGAL, ADVOCATE A/W
SRI MADHAV NARAYAN,
SMT.DEVNA SONI
SMT.ELSHEBA SALY RAJU AND
SRI ROHAN KOTHARI, ADVOCATES)

AND:

1 . STATE OF KARNATAKA
HOME DEPARTMENT,
THROUGH THE HOME SECRETARY
SECRETARIAT,
ROOM NO.222, II FLOOR,
VIDHANA SOUDHA,
BENGALURU.

2 . UNION OF INDIA,
MINISTRY OF HOME AFFAIRS
THROUGH THE HOME SECRETARY,
NORTH BLOCK,
NEW DELHI – 110 001.

3 . STATE OF KARNATAKA
THROUGH CEN CRIME PS, EAST DIVISION
SHIVAJI NAGARA, SULTHANGUNTA,
BENGALURU – 560 051
REPRESENTED BY LD. SPP
HIGH COURT BUILDING,
KARNATAKA – 560 001.

4 . UNION OF INDIA
MINISTRY OF ELECTRONICS AND
INFORMATION TECHNOLOGY (MEITY),
GOVERNMENT OF INDIA
THROUGH THE DIRECTOR GENERAL (DIT)
CYBER LAWS AND E-SECURITY,
ELECTRONICS NIKETAN,
6, CGO COMPLEX, LODHI ROAD,
NEW DELHI – 110 003.

5 . DEPARTMENT OF TELECOMMUNICATIONS,
THROUGH ITS SECRETARY,
MINISTRY OF COMMUNICATIONS AND IT

20, SANCHAR BHAWAN, ASHOKA ROAD,
NEW DELHI – 110 001.

6 . DIRECTOR-GENERAL AND
INSPECTOR GENERAL OF POLICE,
KARNATAKA STATE POLICE,
POLICE HEADQUARTERS,
NO.2, NRUPATHUNGA ROAD,
BENGALURU 560-001, KARNATAKA.

7 . PROTON AG
A COMPANY INCORPORATED UNDER
THE LAWS OF SWITZERLAND
ROUTE DE LA GALAISE 32
1228 PLAN-LES-OUATES
GENEVA, SWITZERLAND
REPRESENTED BY ITS CEO
ANDY YEN.

... RESPONDENTS

(BY SRI SHAMANTH NAIK, HCGP FOR R-1, R-3 AND R-6;
SRI K.ARVIND KAMATH, ADDL.SOLICITOR GENERAL OF INDIA
A/W SRI ADITYA SINGH, CGC FOR R-2, R-4 AND R-5)

THIS WRIT PETITION IS FILED UNDER ARTICLES 226 AND 227 OF THE CONSTITUTION OF INDIA PRAYING TO DIRECT R-1 AND 2 TO TAKE ALL SUCH STEPS AS ARE NECESSARY FOR SECURING THROUGH EXTANT MUTUAL LEGAL ASSISTANCE ARRANGEMENTS BETWEEN INDIA AND SWITZERLAND ALL NECESSARY INFORMATION AND DOCUMENTS PERTAINING TO THE SENDER OF THE OFFENDING EMAIL DTD. 27.09.2024 ANNX-A SENT THROUGH THE EMAIL ADDRESS ReemaGaandari @proton.me AND EMAIL DTD. 01.10.2024 ANNX-E AND D SENT THROUGH THE EMAIL ADDRESS reemagr08@proton.me USING R-7'S PLATFORM, PROTON MAIL, IN A TIME-BOUND MANNER AND ETC.,

THIS WRIT PETITION HAVING BEEN HEARD AND RESERVED FOR ORDERS ON 21.03.2025, COMING ON FOR PRONOUNCEMENT THIS DAY, THE COURT MADE THE FOLLOWING:-

CORAM: **THE HON'BLE MR JUSTICE M.NAGAPRASANNA**

CAV ORDER

The petitioner is before this Court seeking the following prayers:

(A) Issue a writ in the nature of mandamus (or any other writ/order/direction) directing Respondent No.1 and 2 to take all such steps as are necessary for securing through extant mutual legal assistance arrangements between India and Switzerland all necessary information and documents pertaining to the sender of the offending email dated 27-09-2024 (Annexure-A) sent through the email address ReemaGaandari@ proton.me and email dated 01-10-2024 annexure E & D sent through the email address reemagr08@proton.me using respondent No.7's platform, Proton Mail, in a time bound manner;

(B) In the alternative to Prayer (A), issue a writ in the nature of mandamus (or any other writ/order/ direction) directing respondent No.3 to forthwith seek issuance of Letters Rogatory/legal request through the jurisdictional Magistrate, i.e., Ld. XLV Addl. Chief Metropolitan Magistrate, at Bangalore to the Federal Office of Justice, Switzerland for supply of all relevant information and documentation pertaining to the sender of the offending email dated 27-09-2024 (Annexure-A) sent through the email address ReemaGaandari@proton.me and email dated 01-10-2024 (Annexures E & D) sent through the email address reemagr08@proton.me sent using respondent No.7's platform Proton Mail, in a time-bound manner;

(C) Issue a writ in the nature of mandamus (or any other writ/order/direction) directing respondent No.1, 2 and 3 to take all such steps as are necessary, through extant mutual legal assistance arrangements between India and Switzerland, to preserve all relevant information and documents pertaining to the sender of the offending email dated 27-09-2024 (Annexure-A) sent through the email address ReemaGaandari@proton.me and email dated 01.10.2024 (Annexures E & D) sent through the email address reemagr08@proton.me, sent using respondent No.7's platform Proton Mail, in a time bound manner.

(D) Issue a writ in the nature of mandamus (or any other writ/order/direction) directing respondent No.4 and 5 to provide to this Hon'ble Court to provide a complete and up-to-date information as to the regulations in place regarding use and access of Respondent No.7's platform Proton Mail, within India;

(E) Issue a writ in the nature of mandamus (or any other writ/order/direction) directing respondents No.4 and 5 to take such steps as are necessary to ban the use of respondent No.7's platform, Proton Mail, in India; and

(F) Pass any other order(s)/direction(s) as this Hon'ble Court deems fit, in the interest of justice and equity."

2. Facts, in brief, germane are as follows:-

The petitioner is a Company incorporated under the Indian Companies Act, 1956. The Company is said to be engaged in the business of architecture, interior design and project management and is said to have Pan Asia representation including the city of Bangalore and is said to have established an impeccable reputation

in the said industry. The other protagonists in the *lis* are the State of Karnataka in the Department of Home, respondent No.1; Ministry of Home Affairs, Government of India, respondent No.2; The Cyber Police, Karnataka, respondent No.3; Ministry of Electronics and Information Technology, Government of India, respondent No.4; Department of Telecommunications, Government of India, respondent No.5; the Head of the Police Force, State of Karnataka, respondent No.6 and Proton AG, respondent No.7 a Swiss-based Company incorporated under the laws of Switzerland, which provided an end-to-end encrypted email services. What has driven the petitioner to this Court is an electronic mail that dropped into the mail box of the petitioner/Company on 27-09-2024; the mail containing obscene, abusive, vulgar, sexually coloured, derogatory and defamatory remarks in respect of one of the female senior personnel of the petitioner. This comes through a mail ID generated from Proton Mail. This caused extreme humiliation and trauma and is said to have tarnished her personal reputation in the society.

3. On 28-09-2024 the next day, notice of legal action and formal abuse complaint was issued to Proton Mail Abuse Team

through email requesting them to investigate the matter and take appropriate action against the sender of the obscene mail. On 30-09-2024, a mail in return comes from Proton Mail Abuse Team that they have disabled the said Proton Mail account of the sender of the aforesaid derogatory mail. On 01-10-2024 the petitioner communicates another mail to Proton Mail Abuse Team requesting them to provide information regarding the action taken on the said sender. On the same day, an email containing obscene, derogatory lascivious and defamatory content along with sexually explicit images including morphed images of the very same employee of the petitioner and all other employees was sent by an unknown user of a newly created Proton Mail ID to the petitioner mail box. The petitioner immediately communicates to provide details of the sender, as it was sent through Proton Mail. No reply comes about.

4. On the same day, cyber crime complaint was registered in the National Cyber Crime Reporting Portal reporting the obscene emails coming through Proton Mails. The complaint is taken on record. It is then forwarded to Indiranagar Police Station of the Cyber Crime Branch. Communications between Proton Mail Abuse

Team and the petitioner go on. On 03-10-2024 again morphed explicit mail comes into the mail box of the same female senior personnel. The petitioner then registers a formal complaint and seeks investigation into the allegation. On 09-11-2024, the crime in Crime No.876 of 2024 comes to be registered for offences punishable under Sections 66, 66C and 67 of the Information Technology Act, 2000 (hereinafter referred to as 'the Act' for short). The learned Magistrate then seeks status report from the hands of the jurisdictional police who are conducting the investigation. The Police file a status report that they could not take any concrete effective steps to identify the accused in terms of the existing mutual legal assistance arrangements between India and Switzerland. Due to non-stopping of said mails coming into the mail box of the petitioner, the petitioner is before this Court seeking the afore-quoted prayers.

5. Heard Sri Jatin Sehgal, learned counsel appearing for the petitioner, Sri Shamanth Naik, learned High Court Government Pleader appearing for respondents 1, 3 and 6 and Sri K.Arvind

Kamath, learned Additional Solicitor General of India appearing for respondents 2, 4 and 5.

6. The learned counsel appearing for the petitioner would take this Court through the documents appended to the petition to demonstrate that it is necessary for this Court to intervene and ban Proton Mail in the country, as Proton Mail does not have a server in India. Therefore, they are utilizing the fact that no crime can be registered against them and indicating all such things through mail boxes. It is not the safety of the individual involved in the case at hand, but the security of the nation as well. He would submit that hoax bomb mails also come from Proton Mail. He would take this Court through several provisions of the Act to buttress his submission, as also to a judgment rendered by the High Court of Delhi in the case of **X v. UNION OF INDIA**[1]. He would seek the prayers to be granted as sought in the petition.

7. Per-contra, the learned Additional Solicitor General of India Sri K. Arvind Kamath would, though not refute the submissions,

---

[1]2021 SCC OnLine Del 1788

puts across legal frame work, taking this Court through the provisions of the Act and BNSS 2023. It is his submission that there is a procedure in place to ban a particular electronic entity. It is not that bans are not happening in this country, but all of them require procedure to be followed and the balance of bilateral relations between the two countries. He would submit that in terms of Rule 10 of the Information Technology (Procedure and Safeguards for Blocking of Access of Information by Public) Rules, 2009 (hereinafter referred to as 'the Rules' for short) if this Court or the competent criminal Court would direct action to be taken against Proton Mail, the same would be taken. He places reliance upon a communication received from the Information Technology of India in support of his submission.

8. The 7th respondent though served, has remained unrepresented. The communication of the petitioner through e-mail to the representative of Proton AG is produced along with a memo. The only response that the 7th respondent renders is as follows:

> "Proton Legal <legal@proton.me>
> To: Elsheba Raju <elsheba.raju@chambersrk.com>

Cc: rohan.kothari@chambersrk.com, Office Administrator <admin@chambersrk.com>

Hello,

Thank you for reaching out.

We acknowledge reception of your request and would gladly assist.

However, under Swiss law, we can only comply with requests duly instructed by law enforcement. We advise you to contact your local law enforcement authority. It will be required from them to act through international police cooperation to request the relevant data. We can also preserve data of an account in anticipation of proceedings, but we require to be contacted by law enforcement (https://proton.me/legal/law-enforcement).

If you would like us to investigate the account for a breach of our Terms & Conditions, please forward the evidence of abuse to our anti-abuse team (abuse@proton.me) so appropriate action can be taken.

We stay at your disposal for any information.

Best regards,

Proton Legal Team"

The response of the 7th respondent is that they would cooperate for any investigation in a crime in terms of laws of Switzerland, but do not represent themselves before this Court. Therefore, the learned counsel for the petitioner and the learned Additional Solicitor General of India are heard.

9. I have given my anxious consideration to the submissions made by the respective learned counsel and have perused the material on record.

10. The afore-narrated facts, dates and the link in the chain of events, are all a matter of record. The sordid narrative unfolds on 27-09-2024 when the petitioner was visited with an electronic mail, that dropped into its mail box with foul language and imagery laced with sexually explicit content and defamatory insinuations. The communication comes from a pseudonymous address - reemagr08@proton.me and ReemaGaandari@proton.me. The pictures in the mail are placed for perusal of the Court. They do contain sexually explicit images. Immediately, the petitioner causes a notice for legal action against Proton Mail's Abuse Team on 28-09-2024 registering a formal abuse complaint. The communication reads as follows:

> "From: ReemaBhandari-M Moser Associates
> Sent: Sat, 28 Sep 2024 05:04:11 +0000
> To: abuse@protonmail.com
> Cc: VikramSingh-M Moser Associates
> Subject: Formal Abuse Complaint and Notice of Legal Action
> Importance: High
>
> Dear ProtonMail Abuse Team,

I am writing to formally report abusive behavior conducted via your platform. We have received a highly offensive and defamatory email sent from the address **ReemaGaandari@proton.me**. The email in question contains explicit, derogatory, and defamatory content targeting an individual and was sent with malicious intent to several recipients in our organization. We have received such emails via Proton platform multiple times now.

The language used in this email is highly offensive, inappropriate, and defamatory. It is clearly a violation of ProtonMail's terms of service, which prohibits abusive or harmful behavior on your platform.

Here are the details of the offending email with below trail email for your reference and action!

Request for Action:

We request that ProtonMail immediately investigate this incident and take appropriate action against the sender for violating your platform's policies. Additionally, we request that you prevent further abusive emails from this account to our organization.

Legal Notice:

Please note that if we continue to receive any further abusive communications from this account or similar ones on your platform, we will be forced to take legal action to address this matter. This includes pursuing any available remedies for defamation, harassment, and cyber abuse under applicable law. We trust that ProtonMail takes these issues seriously and will respond swiftly to prevent further incidents.

Thank you for your attention to this matter. We look forward to your prompt response and action.

Sincerely.

Reema Bhandari
Director

T +91 80 4900 0600
M+91 9611302239

M Moser Associates

2nd & 3rd Floor, No 374, MSquare,
100 Feet Road. HAL, 2nd Stage, Indira Nagar
Bengaluru – 560 038 India
mmoser.com"

Another mail comes about from Proton Mail's Abuse Team from the aforesaid mail ID. The contents of the mail are as follows:

"…. …. ….

Resending to the Gaan

Sent with Proton Mail secure email.

On Friday, September 27th, 2024 at 6:09 PM, Reema Gaan (ass)dari <ReemaGaandari@proton.me>

wrote:

> Hello all,
>
> Via this email I want to formally introduce the biggest prostitute in real estate industry Reema Gaandari. Her gaan has been the recepient of many cocks like how she claims to be recepient of many awards. Many clients have seen and used her big gaan which is on rent
> I will share more information very soon.
>
> Kind wishes
>
> Sent with Proton Mail secure email."

This time, the petitioner registers a formal abuse complaint with Proton Mail requesting legal action. The said communication reads as follows:

> "From: ReemaBhandari - M Moser Associates
> Sent: Mon, 30 Sep 2024 02:36:12 +0000
> To: Vikram Singh-M Moser Associates
> Subject: Fw: Formal Abuse Complaint and Notice of Legal Action
>
> FYI
>
> Reema Bhandari
>
> Director
>
> T+91 80 4900 0600
>
> M+91 9611302239
>
> X M Moser Associates
>
> mmoser.com
>
> See our locations around the globe
>
> From: Proton Abuse <abuse@proton.me>
> Sent: Monday, September 30, 2024 4:29:15 AM
> To: ReemaBhandari-M Moser Associates
> <ReemaB@mmoser.com>
> Subject: Re: Formal Abuse Complaint and Notice of Legal Action
>
> Greetings,
>
> Thank you for the message.
>
> We would like to promptly inform you that adequate action has been taken against the user, meaning that we have just

disabled their account, and it will probably remain in that state until further notice.

Best Regards,
Proton Mail Abuse Team

On Saturday, September 28th, 2024 at 7:04 AM, ReemaBhandari - M Moser Associates <ReemaB@mmoser.com> wrote:

Dear ProtonMail Abuse Team,

I am writing to formally report abusive behavior conducted via your platform. We have received a highly offensive and defamatory email sent from the address **ReemaGaandari@proton.me**. The email in question contains explicit, derogatory, and defamatory content targeting an individual and was sent with malicious intent to several recipients in our organization. We have received such emails via Proton platform multiple times now.

The language used in this email is highly offensive, inappropriate, and defamatory. It is clearly a violation of ProtonMail's terms of service, which prohibits abusive or harmful behavior on your platform.

Here are the details of the offending email with below trail email for your reference and action!

Request for Action:

We request that ProtonMail immediately investigate this incident and take appropriate action against the sender for violating your platform's policies. Additionally, we request that you prevent further abusive emails from this account to our organization.

Legal Notice:

Please note that if we continue to receive any further abusive communications from this account or similar ones on your platform, we will be forced to take legal action to address this matter. This includes pursuing any available remedies for defamation, harassment, and cyber abuse under applicable law.

We trust that ProtonMail takes these issues seriously and will respond swiftly to prevent further incidents.

Thank you for your attention to this matter. We look forward to your prompt response and action.

Sincerely.

Reema Bhandari"

They also register a complaint before the Cyber Crime Police. The complaint so registered reads as follows:

"I am writing to formally report a serious case of abusive behavior occurring through the ProtonMail platform. We have received multiple highly offensive and explicit emails from the address ReemaGaandariproton.me and another account. These emails contain derogatory and defamatory content specifically targeting women in leadership within our organization, sent with malicious intent to several recipients in our industry. The use of explicit language and the misrepresentation of our women leaders images in these emails is not only inappropriate but constitutes harassment and defamation. This behavior is entirely unacceptable and violates ProtonMails terms of service, which strictly prohibits abusive and harmful conduct. Details of the Offending EmailsSenders ReemaGaandariproton.me and ReemaGaandariproton.meNature of Content Explicit, derogatory, and defamatory language, including the misuse of images Frequency Multiple instances of similar abusive emails received Request for Action We urgently request that the cyber crime branch take appropriate action against the sender for violating laws related to harassment and defamation.

Additionally, we ask that you provide us with the senders information so we can initiate legal proceedings. We also request that measures be implemented to prevent any further

abusive communications from these accounts to our organization. This behavior not only undermines our leaders but also reflects poorly on the integrity of your platform. Thank you"

(Emphasis added)

The mails do not stop coming. A complaint is registered before the CEN Crime Police Station, which becomes a crime in Crime No.876 of 2024. The complaint so registered reads as follows:

"…. …. ….

Subject: Request for Registration of FIR and Investigation in respect of Complaint dated 01.10.2024 (Acknowledgement No. 21610240049531)

1. That the present complaint / representation is being filed by M Moser Design Associates India Private Limited, a company duly incorporated and registered under the Indian Companies Act, 1956 having its office at 2nd & 3rd Floor, No. 374, MSquare, 100 Feet Road HAL 2nd Stage, Indira Nagar, Bengaluru, India 560038 (hereinafter "**the Complainant**"), acting through its authorized representative Mr. Pankaj Arya, who is duly authorized vide Board Resolution dated 07.11.2024. The Complainant is a company in the business of architecture, interior design and project management having its offices at several locations in India as well as overseas.

2. I am writing on behalf of the Complainant with a request to register an FIR and carry out investigation in respect of the complaint filed with the National Cybercrime Reporting Portal on 01.10.2024 bearing Acknowledgment Number **21610240049531**, after which the same has been transferred to your good offices for investigation and appropriate action on 02.10.2024. Sir the present complaint is in respect of very serious and grave offences committed by certain unknown persons, wherein by way of e-mail dated 27.09.2024 sent from the e-mail ID

ReemaGaandari@proton.me the accused persons have shared, published and circulated through electric mode obscene, abusive, derogatory, lascivious and defamatory content specifically targeting senior women in leadership within our organization and vide e-mail dated 01.10.2024 sent from the e-mail ID reemagr08@proton.me, the accused persons have shared, published and circulated through electric mode sexually explicit, obscene and vulgar content wherein images of the Company's senior female personnel and other personnel have been morphed on sexually explicit and obscene content through the ProtonMail platform. This e-mail has been circulated by the e-mail address reemagr08@proton.me and has been issued to the e-mail IDs of the personnel of the Petitioner (reemab@mmoser.com, ananthk@mmoser.com. sylvial@mmoser.com saleema@mmoser.com. nadeemr@mmoser.com. madhug@mmoser.com.), as well as to its associates and vendors (amit.shrivastav@savills.in, jaikishan.c@savills.in, deepika @ostraca.in, deepika@ostraca.in, smorris@ea.com, Gaurav.pawar@cbre.com, Narayan.babu@asnr.com) and even its competitors (Nethra.gowda@unispace.com) to sexually harass, intimidate, defame and malign their reputation as well as the reputation of the Complainant company.

3. **These actions of the certain unknown accused persons clearly disclose commission of several cognizable offences inter alia under Sections 75, 79, 356 of the Bhartiya Nyaya Sanhita, 2023 ("BNS") and Sections 67 and 67A of the Information Technology Act, 2000 ("IT Act")**

4. **Therefore, we request your good offices to take swift and appropriate action and register an FIR under Sections 75, 79, 356 of the BNS and Sections 67 and 67A of the IT Act and carry out investigation thereon.**

5. **Additionally, we request that measures be implemented to prevent any further abusive communications from these accounts to our**

organization, as this behaviour not only undermines the dignity of our leaders and personnel but also threatens our professional relationships and reputation.

6. Thank you for your attention and immediate action on this matter. We trust in the police department's commitment to uphold justice and remain available to provide any further information or documentation needed to assist in the investigation."

(Emphasis added)

The learned Magistrate, upon the registration of the crime, orders investigation at the hands of the jurisdictional police, in the case at hand the CEN police station. The investigation conducted by the Police leads to a report that they are not in a position to investigate. The report is as follows:

"ಈ ಮೇಲ್ಕಂಡ ವಿಷಯ ಹಾಗೂ ಉಲ್ಲೇಖನಕ್ಕೆ ಸಂಬಂದಿಸಿದಂತೆ ಮಾನ್ಯ ನ್ಯಾಯಾಲಯಕ್ಕೆ ನಿವೇದಿಸಿಕೊಳ್ಳುವುದೆನೆಂದರೆ, ದಿನಾಂಕ: 09.11.2024 ರಂದು ದೂರುದಾರರಾದ Pankaj Arya S/o D.R Arya Address: M Moser Design Associates (India) Pvt Ltd M Square, 2nd & 3rd Floor 374, 100 Ft Road, Indiranagar, Bengalore. ರವರು ನೀಡಿರುವ ದೂರಿನ ಸಂಕ್ಷಿಪ್ತ ಸಾರಾಂಶವೇನೆಂದರೆ That the present complaint/representation is being filed by M Moser Design Associates India Private Limited, a company duly Incorporated and registered under the Indian Companies Act, 1956 having its office at 2nd & 3rd Floor, No 374, MSquare, 100 Feet Road HAL 2nd Stage, Indira Nagar, Bengaluru, India 560038 (hereinafter "the Complainant"), acting through its authorized representative Mr. Pankaj Arya, who is duly authorized vide Board Resolution dated 07.11.2024. The Complainant is a company in the business of architecture, Interior design and project management having its offices at several locations in India as well as overseas. I am writing on behalf of the Complainant with a request to register an FIR and carry out investigation in

respect of the complaint filed with the National Cybercrime Reporting Portal on 01.10.2024 bearing Acknowledgment Number 21610240049531, after which the same has been transferred to your good offices for investigation and appropriate action on 02.10.2024. Sir the present complaint is in respect of very serious and grave offences committed by certain unknown persons, wherein by way of e-mail dated 27.09.2024 sent from the e-mail ID ReemaGaandari@proton.methe accused persons have shared, published and circulated through electric mode obscene, abusive, derogatory, lascivious, and defamatory content specifically targeting senior women in leadership within our organization and vide e-mail dated 01.10.2024 sent from the e-mail ID reemagr08@proton.me, the accused persons have shared, published and circulated through electric mode sexually explicit, obscene and vulgar content wherein images of the Company's senior female personnel and other personnel have been morphed on sexually explicit and obscene content through the ProtonMail platform. This e-mail has been circulated by the e-mail address reemagr08@eraton.me and has been issued to the e-mail IDs of the personnel of the petitioner (reemab@mmoser.com, ananthk@mmoser.com, sylvival@mmoser.com, saleema@mmoser.com, nadeemr@mmoser.com, madhug@mmoser.com.), as well as to its associates and vendors (amit.shrivastav@savills.in, jaikishan.c@savills.in, deepika@ostraca.in, smorris@ea.com, Gaurav.pawar@cbre.com, Narayan.babu@asnr.com) and even its competitors (Nethra.gowda@unispace.com) to sexually harass, intimidate, defame and malign their reputation as well as the reputation of the Complainant company etc" ದೂರನ್ನು ಪಡೆದುಕೊಂಡು ಠಾಣಾ ಮೊ.ಸಂ. 876/2024 ಕಲಂ 67, 66, 66 (ಸಿ) ಐಟಿಆಕ್ಟ್-2000 ಪ್ರಕರಣವನ್ನು ದಾಖಲಿಸಿಕೊಂಡು ತನಿಖೆಯನ್ನು ಕೈಗೊಂಡಿರುತ್ತದೆ.

• ಸದರಿ ಪ್ರಕರಣದ ತನಿಖಾ ಪ್ರಗತಿ ವರದಿ.

1. ದಿನಾಂಕ:09.11.2024 ರಂದು ಸದರಿ ಪ್ರಕರಣಕ್ಕೆ ಸಂಬಂಧಿಸಿದಂತೆ reemagr08@proton.me & ReemaGaandari@proton.me ಮೇಲ್‌ಗಳ ಬಳಕೆದಾರರ ಮಾಹಿತಿ ನೀಡುವಂತೆ Legal Manager Proton AG Route de la Galaise

32, 1228 Plan-les-Ouates, Geneva Switzerland ಮೇಲ್ ಮೂಲಕ ನೋಟಿಸ್ ನೀಡಿರುತ್ತದೆ.

2. ದಿನಾಂಕ: 11.11.2024 ರಂದು **Proton AG** ರವರಿಂದ ಮೇಲ್ ಮೂಲಕ ಸದರಿಯವರು ಗೌಪ್ಯತೆ ಮತ್ತು ಭದ್ರತಾ ಕಾರಣಗಳಿಗಾಗಿ, ಸ್ವಿಸ್ ಪೊಲೀಸ್ ರವರ ಮೂಲಕ 'ಬರುವ ವಿನಂತಿಗಳನ್ನು ಮಾತ್ರ ಸ್ವೀಕರಿಸುತ್ತದೆ. **INTERPOL Or Europol National Bureau** ರವರ ಮೂಲಕ ಮಾಹಿತಿ ಪಡೆದುಕೊಳ್ಳಬಹುದು ಎಂದು ತಿಳಿಸಿರುತ್ತಾರೆ.

3 ದಿನಾಂಕ:27.11.2024 ರಂದು ಸದರಿ ಪ್ರಕರಣಕ್ಕೆ ಸಂಬಂಧಿಸಿದಂತೆ **reemagr08@proton.me & ReemaGaandari@proton.me** ಮೇಲ್‌ಗಳ ಬಳಕೆದಾರರ ಮಾಹಿತಿ ನೀಡುವಂತೆ **Legal Manager Proton AG Route de la Galaise 32, 1228 Plan-les-Ouates, Geneva Switezerland** ಮೇಲ್ ಮೂಲಕ ನೋಟಿಸ್ ನೀಡಿರುತ್ತದೆ.''

4. ಸದರಿ ಪ್ರಕರಣದಲ್ಲಿ ಆರೋಪಿತನ ಮೇಲ್ ತೆಗೆದು ಹಾಕಲು ಸಂಬಂಧಪಟ್ಟ ಅಧಿಕಾರಿಗಳಿಗೆ ನಿರ್ದೇಶನ ನೀಡುವಂತೆ ಮಾನ್ಯ ನ್ಯಾಯಾಲಯಕ್ಕೆ ಮನವಿ ಸಲ್ಲಿಸಿರುತ್ತದೆ.

5. ದಿನಾಂಕ:27.11.2024 ರಂದು ಸದರಿ ಪ್ರಕರಣಕ್ಕೆ ಸಂಬಂಧಿಸಿದಂತೆ **reemagr08@proton me & ReemaGaandari@proton.me** ಮೇಲ್‌ಗಳ ಬಳಕೆದಾರರ ಮಾಹಿತಿ ನೀಡುವಂತೆ **Marc Alexander Loebekken Legal Director Proton AG Route de la Galaise 32, 1228 Plan-les-Ouates, Geneva Switezerland** ಮೇಲ್ ಮೂಲಕ ನೋಟಿಸ್ ನೀಡಿರುತ್ತದೆ.

6. ದಿನಾಂಕ: 02.12.2024 ರಂದು ಸದರಿ ಪ್ರಕರಣಕ್ಕೆ ಸಂಬಂಧಿಸಿದಂತೆ ಮೇಲ್‌ಗಳನ್ನು ಡಿಲೀಟ್ ಮಾಡುವಂತೆ Proton AG ರವರಿಗೆ ನೋಟಿಸ್ ನೀಡಿರುತ್ತದೆ.

7. ದಿನಾಂಕ: 03.12.2024 ರಂದು **Proton AG (abuse@proton.me)** ರವರು ಮೇಲ್ ಮೂಲಕ ಸದರಿ ಎರಡು ಮೇಲ್‌ಗಳನ್ನು ಕೊನೆಗೊಳಿಸಿದೆ (ಡಿಲೀಟ್) ಮಾಡಿರುತ್ತದೆ. ಇನ್ನು ಮುಂದೆ ಅವುಗಳು ಬಳಕೆಯಲ್ಲಿರುವುದಿಲ್ಲವೆಂದು ತಿಳಿಸಿರುತ್ತಾರೆ.''

(Emphasis added)

The investigation, though earnest, in endeavour, faltered against the bulwark of international jurisdiction, and

encryption. The State machinery hamstrung, by the absence of enforceable cooperation from Proton AG and the lack of a server within its jurisdiction, submitted its helplessness, in the form of a report quoted *supra.* Therefore, the petitioner is before this Court seeking favourable consideration of the prayers that are sought.

11. **This Court is therefore tasked not merely with adjudicating the writ, but with weighing the balance between the technological liberty and digital accountability**. The petitioner pleads for directions invoking mutual legal assistance treaties with Switzerland and if necessary, prohibition of Proton Mail within the bounds of Indian Cyber Space. To consider the same, it is necessary to notice the applicable legal canvass. The canvass spreads to vast and varied enactments - **Information Technology Act, 2000, as amended by Information Technology (Amendment) Act, 2008 ('Act' for short); Information Technology (Procedure and Safeguards for Blocking for Access of Information by Public) Rules, 2009 ('Rules 2009' for short) and Information Technology (Intermediaries**

Guidelines) Rules, 2011 ('Rules 2011' for short). The aforesaid enactments delineate the duties of intermediaries, impose obligations of redress, mandate expeditious removal of objectionable content and empower the Competent Authority to act swiftly in the interests of decency, privacy, national integrity and security of the nation. Provisions germane of the aforesaid enactments are as follows:

Information Technology (Amendment) Act, 2008:

> "1. *Short title, extent, commencement and application*.—
>
> …
>
> (2) It shall extend to the whole of India and, save as otherwise provided in this Act, it applies also to any offence or contravention thereunder committed outside India by any person.
>
> ***
>
> 2. Definitions—
>
> (1) In this Act, unless the context otherwise requires,—
>
> ***
>
> (*o*) 'data' means a representation of information, knowledge, facts, concepts or instructions which are being prepared or have been prepared in a formalised manner, and is intended to be processed, is being processed or has been processed in a computer system or computer network, and may be in any form (including computer printouts magnetic or optical storage media, punched cards, punched tapes) or stored internally in the memory of the computer;
>
> ***
>
> (*v*) 'information' includes data, message, text, images, sound, voice, codes, computer programmes,

software and data bases or micro film or computer generated micro fiche;

(*w*) 'intermediary', with respect to any particular electronic records, means *any person who on behalf of another person receives, stores or transmits that record or provides any service* with respect to that record and *includes telecom service providers*, network service providers, internet service providers, *web hosting service providers, search engines*, online payment sites, online auction sites, online market places and cyber cafes;

***

***67*. Punishment for publishing or transmitting obscene material in electronic form. *Whoever publishes or transmits* or *causes to be published or transmitted* in the electronic form, any material *which is lascivious or appeals to the prurient interest* or if its effect is such as *to tend to deprave and corrupt persons who are likely, having regard to all relevant circumstances, to read, see* or hear the matter contained or embodied in it, shall be punished on first conviction with imprisonment of either description for a term which may extend to three years and with fine which may extend to five lakh rupees and in the event of second or subsequent conviction with imprisonment of either description for a term which may extend to five years and also with fine which may extend to ten lakhs rupees.**

***67-A. Punishment for publishing or transmitting of material containing sexually explicit act, etc., in electronic form*. Whoever publishes or transmits or causes to be published or transmitted in the electronic form any material which contains sexually explicit act or conduct shall be punished on first conviction with imprisonment of either description for a term which may extend to five years and with fine which may extend to ten lakhs rupees and in the event of second or subsequent conviction with imprisonment of either description for a term which may extend to seven years and also with fine which may extend to ten lakhs rupees.**

***

69-A. Power to issue directions for blocking for public access of any information through any computer resource.—(1) Where the Central Government or any of its officers specially authorised by it in this behalf is satisfied that it is necessary or expedient so to do, in the interest of sovereignty and integrity of India, defence of India, security of the State, friendly relations with foreign States or public order or for preventing incitement to the commission of any cognizable offence relating to above, it may subject to the provisions of sub-section (2), for reasons to be recorded in writing, by order, direct any agency of the Government or intermediary to block for access by the public or cause to be blocked for access by the public any information generated, transmitted, received, stored or hosted in any computer resource.

(2) The procedure and safeguards subject to which such blocking for access by the public may be carried out, shall be such as may be prescribed.

(3) The intermediary who fails to comply with the direction issued under sub-section (1) shall be punished with an imprisonment for a term which may extend to seven years and shall also be liable to fine.

***

75. *Act to apply for offences or contravention committed outside India*—(1) Subject to the provisions of sub-section (2), *the provisions of this Act shall apply also to any offence or contravention committed outside India by any person irrespective of his nationality*.

(2) For the purposes of sub-section (1), this Act shall apply to an offence or contravention committed outside India by any person *if the act or conduct constituting the offence or contravention involves a computer, computer system or computer network located in India*.

***

"79. *Exemption from liability of intermediary in certain cases*.—(1) Notwithstanding anything contained in any law for the time being in force but *subject to the provisions of sub-sections (2) and (3)*, an intermediary *shall*

not be liable for any third party information, data, or communication link made available or hosted by him.

(2) The *provisions of sub-section (1) shall apply if—*

(*a*) the *function of the intermediary is limited to providing access* to a communication system over which information made available by third parties is transmitted or temporarily stored or hosted; or

(*b*) the *intermediary does not—*

(*i*) initiate the transmission,
(*ii*) select the receiver of the transmission, and
(*iii*) *select or modify the information* contained in the transmission;

(*c*) *the intermediary observes due diligence while discharging his duties under this Act* and *also observes such other guidelines as the Central Government may prescribe* in this behalf.

(3) The provisions of *sub-section (1) shall not apply if—*

(*a*) the *intermediary has conspired or abetted or aided or induced*, whether by threats or promise *or otherwise* in the commission of the unlawful act;

(*b*) *upon receiving actual knowledge, or on being notified by the appropriate Government or its agency* that any information, data or communication link residing in or connected to *a computer resource controlled by the intermediary is being used to commit the unlawful act*, the *intermediary fails to expeditiously remove or disable access to that material on that resource* without vitiating the evidence in any manner."

***

"81. *Act to have overriding effect*.—The provisions of this Act shall have effect *notwithstanding anything inconsistent therewith contained in any other law* for the time being in force:

> Provided that nothing contained in this Act shall restrict any person from exercising any right conferred under the Copyright Act, 1957 (14 of 1957) or the Patents Act, 1970 (39 of 1970)."

(Emphasis supplied)

Section 69A deals with power to issue directions for blocking for public access any information through any computer source. The reasons for blocking are manifold which are found in the provision itself. Sub-section (2) of Section 69A deals with procedure and safeguards subject to which blocking for access by the public may be carried out as may be prescribed. The prescription is under the Rules. The Government of India in exercise of powers conferred under Section 87 of the Act has framed the Rules of 2009 - **Information Technology (Procedure and Safeguards for Blocking for Access of Information by Public) Rules, 2009.** Rule 10 is germane to be noticed. It runs as follows:

> **"10. *Process of order of court for blocking of information*— In case of an *order from a competent court in India for blocking of any information* or part thereof generated, transmitted, received, stored or hosted in a computer resource, the Designated Officer shall, *immediately on receipt of certified copy of the court order*, submit it to the Secretary, Department of Information Technology and *initiate action as directed by the court*."**

(Emphasis supplied)

Likewise, the Government of India has also framed **Information Technology (Intermediaries Guidelines) Rules, 2011.** Rules that are germane are as follows:

> "3. *Due diligence to be observed by intermediary*.— The intermediary shall observe following due diligence while discharging his duties, namely :
>
> (1) The intermediary shall publish the rules and regulations, privacy policy and user agreement for access or usage of the intermediary's computer resource by any person.
>
> (2) Such rules and regulations, terms and conditions or user agreement *shall inform the users of computer resource not to host, display, upload, modify, publish, transmit, update or share any information that*—
>
> ***
>
> **(*b*) Is grossly harmful, *harassing*, blasphemous defamatory, obscene, pornographic, paedophilic, libellous, *invasive of another's privacy*, hateful, or racially, ethnically objectionable, disparaging, relating or encouraging money laundering or gambling, or otherwise unlawful in any manner whatever.**
>
> ***
>
> (3) The *intermediary shall not knowingly host or publish any information* or shall not initiate the transmission, select the receiver of transmission, and select or modify the information contained in the transmission *as specified in sub-rule (2)*:
>
> Provided that the following actions by an intermediary *shall not amount* to hosting, publishing, editing or storing of any such information as specified in sub-rule (2)—
>
> (*a*) Temporary or transient or intermediate storage of information automatically

within the computer resource as an intrinsic feature of such computer resource, involving no exercise of any human editorial control, for onward transmission or communication to another computer resource.

(*b*) *Removal of access* to any information, data or communication link *by an intermediary after* such information, data or communication link *comes to the actual knowledge* of a person authorised by the intermediary *pursuant to any order or direction* as per the provisions of the Act.

(4) The *intermediary*, on whose computer system the information is stored or hosted or published, *upon obtaining knowledge by itself or been brought to actual knowledge by an affected person in writing or through email* signed with electronic signature about any such information as mentioned in sub-rule (2) above, *shall act within thirty-six hours and where applicable, work with user or owner of such information to disable such information that is in contravention of sub-rule (2)*. Further the intermediary shall preserve such information and associated records for at least ninety days for investigation purposes.

(5) The intermediary shall inform its users that *in case of non-compliance with rules and regulations, user agreement and privacy policy* for access or usage of *intermediary computer resource, the intermediary has the right to immediately terminate the access or usage rights of the users* to the computer resource of intermediary and remove non-compliant information.

(6) The *intermediary shall strictly follow the provisions of the Act or any other laws for the time being in force*.

(7) *When required by lawful order, the intermediary shall provide information or any such assistance to government agencies who are lawfully authorised for investigative, protective, cyber security activity*. The information or any such assistance shall be provided for the purpose of verification of identity, or for prevention, detection, investigation, prosecution, cyber security incidents and punishment of offences under any law for the time being in force, on a request in writing stating clearly

> the purpose of seeking such information or any such assistance.
>
> ***
>
> (11) The intermediary shall *publish on its website the name of the Grievance Officer and his contact details as well as mechanism by which users or any victim who suffers as a result of access or usage of computer resource by any person in violation of Rule 3 can notify their complaints* against such access or usage of computer resource of the intermediary or other matters pertaining to the computer resources made available by it. *The Grievance Officer shall redress the complaints within one month from the date of receipt of complaint*."
>
> (emphasis supplied)

Rule 10 of 2009 Rules quoted *supra* mandates that in case of an order from a competent Court in India for blocking of any information or part thereof, the Department of Information Technology should initiate process as directed by the Court. The learned Additional Solicitor General of India has placed a memo appending to it a document which reads as follows:

> "Sir
>
> Kindly find inputs in the captioned matter in compliance of the Court order dated 13.02.2025 and 03.03.2025 as below:-
>
> The central government (MeitY) or an authorized officer is empowered to issue directions for blocking of any Information to any agency or intermediary to block for access by public. To issue such directions, MeitY follows the due process as provided in concomitant Rules (the Information Technology (Procedure and Safeguards for Blocking for Access of Information by Public) Rules, 2009). **Therefore, MeitY can exercise this power upon receipt of a request from a Nodal Officer and after examination and recommendation by the Committee; if**

> **satisfied that the same is necessary and expedient to do so 'in the interest of sovereignty and integrity of India, defence of India, security of the State, friendly relations with foreign States or public order or for preventing incitement to the commission of any cognizable offence relating to above'. Further, as per the Rule 10 of the aforesaid Rules, action can also be taken under section 69A if so ordered by a competent Court.**
>
> It is submitted that Proton Mail has not been blocked in India under Section 69A of IT Act, 2000 and is operating in India."
>
> (Emphasis added)

The communication is from the Ministry of Electronics and Information Technology, Government of India. It indicates that the Ministry will exercise its power to ban/block on receipt of a request, from the nodal officer or the recommendation by a Committee. This action would be taken if, integrity of India, Defence of India, Security of a State, friendly relations with foreign States or public order is threatened, or any cognizable offence relating to the aforesaid circumstance is registered. It is only then the invocation of Rule 10 could be entertained. It further indicates that action would be taken under Section 69A, if so ordered by a competent Court.

12. It is in public domain that Proton Mail earlier had its server in India. In 2020, when accountability on all intermediaries was brought in, on all those who operate in India, Proton Mail removes its server in India and operates from Switzerland, claiming anonymity. Proton Mail has some policies or terms of service when anyone wants to open a mail ID. The learned counsel for the petitioner submits that when any question is asked, in 30 seconds the mail ID gets generated. It is, therefore, necessary to notice the privacy policy of Proton Mail. It reads as follows:

"…. …. ….

1. Legal framework

The Services are operated by Proton AG (the "Company", "We"), domiciled at Route de la Galaise 32, 1228 Plan-les-Ouates, Geneva, Switzerland. It is therefore governed by the laws and regulations of Switzerland. Additional information about the legal framework can be found in our transparency report.

We are also GDPR compliant. The designated representative of the Company in the European Union (notably for the purpose of art. 27 GDPR) is Proton Europe sàrl, rue de Grünewald 94, L-1912 Luxembourg."

5. Data disclosure

We will only disclose the limited user data we possess if we are legally obligated to do so by a binding request coming from the competent Swiss authorities. We may comply with electronically delivered notices only when they

are delivered in full compliance with the requirements of Swiss law. Proton's general policy is to challenge requests whenever possible and where there are doubts as to the validity of the request or if there is a public interest in doing so. In such situations, we will not comply with the request until all legal or other remedies have been exhausted. Under Swiss law, subjects of judicial procedures have to be notified of such procedures, although such notification has to come from the authorities and not from the Company. Under no circumstances can Proton decrypt end-to-end encrypted content and disclose decrypted copies. Aggregate statistics about data requests from the competent Swiss authorities can be found in the transparency reports listed in our products-specific policies.

***

Transparency report

"From time to time, Proton may be legally compelled to disclose certain user information to Swiss authorities, as detailed in our Privacy Policy. This can happen if Swiss law is broken. As stated in our Privacy Policy, all emails, files and invites are encrypted and we have no means to decrypt them.

Under Article 271 of the Swiss Criminal Code, Proton may not transmit any data to foreign authorities directly, and we therefore reject all requests from foreign authorities. Swiss authorities may from time to time assist foreign authorities with requests, provided that they are valid under international legal assistance procedures and determined to be in compliance with Swiss law. In these cases, the standard of legality is again based on Swiss law. In general, Swiss authorities do not assist foreign authorities from countries with a history of human rights abuses."

(Emphasis added)

The afore-quoted are the legal frame work of Proton Mail, the data disclosure conditions and transparency report. It clearly holds that no matter or no data encrypted would be disclosed. Under Swiss law, subjects of judicial procedures are notified, it is only then they would act. It is in public domain that Switzerland and India have mutual legal assistance in criminal matters. An agreement drawn on 20-02-1989, when conventional crimes were in existence. Certain clauses therein also impose certain obligations of investigation of crime by police or other law enforcement agencies to compel any person to answer questions or to provide information. This is ingrained in the statute i.e., the BNSS 2023 where a chapter is dedicated – CHAPTER VIII viz., Reciprocal arrangements for assistance in certain matters and procedure for attachment and forfeiture of property. Section 112 reads as follows:

> "**112. Letter of request to competent authority for investigation in a country or place outside India**.—(1) If, in the course of an investigation into an offence, an application is made by the investigating officer or any officer superior in rank to the investigating officer that evidence may be available in a country or place outside India, any Criminal Court may issue a letter of request to a Court or an authority in that country or place competent to deal with such request to examine orally any person supposed to be acquainted with the facts and

> circumstances of the case and to record his statement made in the course of such examination and also to require such person or any other person to produce any document or thing which may be in his possession pertaining to the case and to forward all the evidence so taken or collected or the authenticated copies thereof or the thing so collected to the Court issuing such letter.
>
> (2) The letter of request shall be transmitted in such manner as the Central Government may specify in this behalf.
>
> (3) Every statement recorded or document or thing received under sub-section (1) shall be deemed to be the evidence collected during the course of investigation under this Sanhita."

The earlier regime i.e., the Cr.P.C. also had Section 166A which dealt with the Competent Authority permitting investigation in a country or place outside India on mutual agreements. Section 112 *supra* permits a request to be communicated to the Competent Authority of investigation in a country or place outside India. The requisition has been made in the case at hand. There is no response in terms of the report placed by the Investigating Officer before the competent Court. Thus the said exercise, has also been attempted to, by the Law Enforcing Agency of the State. The only answer that the 7th respondent renders to the notice issued by this Court is quoted hereinabove, it is conditional, but at the same time no action is taken to stop the mail dropping into the mail box of the

petitioner, notwithstanding clear evidence furnished by the petitioner to the 7th respondent seeking investigation into the alleged abuse. Therefore, there is failure on the part of the 7th respondent to cooperate with the investigation and immediately take down or block the offensive mails.

The Menace through Proton Mail:

13. The menace of Proton Mail does not stop at indicating sexually explicit images to mail IDs. It has also generated hoax bomb calls. The bomb threat received by the Chief Minister, Government of Karnataka is from Proton Mail. It reads as follows:

> "Days after a suspected improvised explosive device (IED) blast in a cafe in Bengaluru's technology hub, several ministers of the Karnataka government, including chief minister Siddaramaiah and his deputy DK Shivakumar, received a bomb threat on Tuesday via email, warning of an explosion in public places on Saturday, along with a ransom demand of $2.5 m (about ₹21 cr).
>
> The City Crime Branch (CCB) registered a complaint after the CM, deputy CM, home minister G Parameshwara and Bengaluru's police commissioner received identical emails from a person using the email address Shahidkhan10786@protonmail.com.
>
> "If you don't provide us with $2.5 million, we will carry out explosions on buses, trains, temples, hotels and public areas throughout Karnataka," the email said."

Likewise, for every State fake bomb threats are being generated by Proton Mail. It is in public domain that State of Tamil Nadu decides to block Proton Mail after fake bomb threats in Tamil Nadu. The report is as follows:

> "GOVERNMENT
>
> **IT Ministry Decides to Block Proton Mail After Fake Bomb Threats in Tamil Nadu: Report**
>
> The Wire Staff
> 15/Feb/2024. 5 min read
>
> An officer representing the Tamil Nadu police said during a content blocking committee meeting that they were unable to trace the perpetrators behind fake bomb threats sent to schools using Proton Mail."

Noticing this problem of generation of fake mails, the United Arab Emirates has issued a warning over travel fraud on 16-08-2022. The warning is as follows:

> "HOME / UAE
>
> **UAE: Indian Embassy issues warning over travel fraud**
>
> Mission advises residents to cross-check e-mail IDs and social media accounts to avoid getting cheated
>
> Published: Tue 16 Aug 2022, 5:26 PM
> Updated: Thu 18 Aug 2022, 11:06 AM

By Ashwani Kumar"

***

"Using fake Twitter handle @embassy_help, which closely resembles an official government page, and email ID ind_embassy.mea.gov@protonmail.com, the fraudsters allegedly seek anywhere between Rs15,000 (Dh700) to Rs40,000 (Dh1,800) from those in need of an air ticket from the UAE to India or visa application fees. Earlier in the day, the embassy issued a public advisory following which the tweets from the fake Twitter account have been protected.

The embassy has been receiving several complaints from victims and email alerts from vigilant community members who are aware about the embassy's official Twitter handle: @IndembAbuDhabi."

Russia has also banned Proton Mail owing to several fake news generated and to focus on user privacy. Banning of Proton Mail by Moscow is as follows:

"MOSCOW (Reuters) - Russia said on Wednesday it had blocked the Swiss email service ProtonMail, popular among journalists and activists for its focus on user privacy and high level of encryption.

Russian communications watchdog Roskomnadzor said ProtonMall, which uses end-to-end encryption to protect user data, had been used to send fake, anonymous bomb threats.

Such threats have frequently led to mass evacuations of public buildings across Russia.

Roskomnadzor said that ProtonMail had refused to provide Russian authorities with information on the owners of email accounts allegedly associated with fake bomb threats.

> It said these had been sent via ProtonMail since last year and that incidence had increased this month after a similar service, Smartmail.com, was blocked.
>
> Protonmail denied having received any requests for assistance from Russian authorities and said the block would do nothing to stop bomb hoaxes but rather only limit ordinary Russians' access to privacy in communications."

The afore-quoted are a few illustrations of menace of Proton Mail and such instances of menace leading to blocking. The blocking is said to be in several countries. Russia is one of them. If blocking of such mail hubs are not done by the nation, it is likely lead to threatening of the security of the nation by, generating false alarms or sometimes communication of mails which are derogatory, defamatory, touching upon the integrity of the nation. It is therefore, necessary for the Government of India to forthwith take steps in terms of Rule 10 *supra*.

Judicial Canvass:

14. The Constitution Courts in the country have also considered to issue directions to block certain mails, apps *inter alia*,

as the case would be. The High Court of Delhi in the case **X v. UNION OF INDIA[2] ,** has held as follows:

"…. …. ….

86. In the present case, the petitioner's photographs and images, though not in themselves obscene or offensive, were taken from her Facebook and Instagram accounts without her consent and were uploaded on a pornographic website, adding derogatory captions to them. It is an irrefutable proposition that if the name and/or likeness of a person appears on a pornographic website, as in the present case, without the consent or concurrence of such person, such act would by and in itself amount to an offence inter alia under Section 67 of the IT Act. This is so since Section 67 makes it an offence to publish or transmit, or causes to be published or transmitted, in the electronic form, any material which appeals to the prurient interests of those who are likely, having regard to all relevant circumstances, to read, see or hear the matter contained or embodied in it. The only purpose of posting the petitioner's photograph on a pornographic website could be to use it to appeal to the prurient interests of those who are likely to see it. That apart, the inclusion of the name and/or likeness of a person on such website, even if the photograph of the person is not in itself obscene or offensive, without consent or concurrence, would at the very least amount to breach of the person's privacy, which a court may, in appropriate cases, injunct or restrain. It is evident that such publication would likely result in ostracisation and stigmatisation of the person concerned in society; and therefore immediate and efficacious remedy is required in such cases.

87. While appreciating the indisputably anarchic nature of the internet as a medium and accepting that the world wide web is intractable by reason of its global expanse, interconnectedness and the fact that content,

---

[2] 2021 SCC OnLine DEL 1788

including offending content, can be very easily placed on the world wide web by people from the farthest corners of the world, which it is almost impossible to control, it cannot be ignored that the law and judicial opinion in India as also in several other jurisdictions, as gathered from the foregoing discussion, mandates intermediaries to remove and disable access to offending content once they receive "actual knowledge" by way of a court order or upon being notified by the appropriate Government or its agency, failing which the intermediary is liable to lose the exemption from liability available to it under Section 79(1) of the IT Act.

…. …. ….

91. On an overall appreciation of the legal and practical aspects of the matter, and to answer the queries framed in para 11 of this judgment, in the opinion of this Court, a fair balance between the obligations and liabilities of the intermediaries and the rights and interests of the aggrieved user/victim would be struck by issuing directions as detailed below, which would be legal, implementable, effective and would enable meaningful compliance of the orders of a court without putting any impossible or untenable burden on intermediaries.

(*i*) Based on a "grievance" brought before it, as contemplated in Rule 2(1)(*j*) of the 2021 Rules or otherwise, and upon a court being satisfied in any proceedings before it, whether at the interim or final stage, that such grievance requires immediate redressal, the court may issue a direction to the website or online platform on which the offending content is hosted, to remove such content from the website or online platform, forthwith and in any event within 24 hours of receipt of the court order. Since this timeframe is mandated in Rule 3(2)(*b*) of the 2021 Rules read with Rule 10 of the 2009 Rules for other similar kinds of offensive content, in the opinion of this Court, the same timeframe ought to

be applied if the court is satisfied that any offending content requires immediate removal.

(*ii*) A direction should also be issued to the website or online platform on which the offending content is hosted to preserve all information and associated records relating to the offending content, so that evidence in relation to the offending content is not vitiated, at least for a period of 180 days or such longer period as the court may direct, for use in investigation, in line with Rule 3(1)(*g*) of the 2021 Rules.

(*iii*) A direction should also be issued by the court to the search engine(s) as the court may deem appropriate, to make the offending content non-searchable by "deindexing" and "dereferencing" the offending content in their listed search results, including deindexing and dereferencing all concerned web pages, sub-pages or sub-directories on which the offending content is found. For reference, some of the most commonly used search engines in India are Google Search, Yahoo Search, Microsoft Bing and DuckDuckGo. This would be in line with the obligation of search engines to disable access to the offending content under the Second Proviso to Rule 3(1)(*d*) of the 2021 Rules. It is necessary to point out that in the Second Proviso to Rule 3(1)(*d*), which deals with due diligence required by an intermediary, the time-frame set down inter alia for disabling access to offending content is "... as early as possible, but in no case later than thirty-six hours from the receipt of the court order ..."; but under the grievance redressal mechanism engrafted in Rule 3(2)(*b*), the intermediary has been mandated to remove certain specified kinds of offending content within twenty-four hours from receipt of a complaint from any person. In the opinion of this Court, the intermediary must be obliged to comply with a court order directing removal or disabling access to offending content within twenty-four hours from receipt of such order.

(*iv*) The directions issued must also mandate the concerned intermediaries, whether websites/online platforms/search engine(s), to endeavour to employ pro-active monitoring by using automated tools, to identify and remove or disable access to any content which is "*exactly identical*" to the offending content that is subject-matter of the court order, as contemplated in Rule 4(1)(*d*) of the 2021 Rules.

(*v*) Directions should also be issued to the concerned law enforcement agency/ies, such as the jurisdictional police, to obtain from the concerned website or online platform all information and associated records, including all unique identifiers relating to the offending content such as the URL (Uniform Resource Locator), account ID, handle name, Internet Protocol address and hash value of the actual offending content alongwith the metadata, subscriber information, access logs and such other information as the law enforcement agency may require, in line with Rule 3(1)(*j*) of the 2021 Rules, as soon as possible but not later than seventy-two hours of receipt of written intimation in this behalf by the law enforcement agency.

(*vi*) Also, the court must direct the aggrieved party to furnish to the law enforcement agency all available information that the aggrieved party possesses relating to the offending content, such as its file name, Image URL, web URL and other available identifying elements of the offending content, as may be applicable; with a further direction to the law enforcement agency to furnish such information to all other entities such as websites/online platforms/search engines to whom directions are issued by the court in the case.

(*vii*) The aggrieved party should also be permitted, on the strength of the court order passed regarding specific offending content, to notify the law enforcement agency to remove the offending

content from any other website, online platform or search engine(s) on which same or similar offending content is found to be appearing, whether in the same or in a different context. Upon such notification by the aggrieved party, the law enforcement agency shall notify the concerned website, online platform and search engine(s), who (latter) would be obligated to comply with such request; and, if there is any technological difficulty or other objection to so comply, the website, online platform or search engine(s) may approach the concerned court which passed the order, seeking clarification but *only after first complying* with the request made by the aggrieved party. This would adequately address the difficulty expressed by Google LLC in these proceedings that a search engine is unable to appreciate the offending nature of content appearing in a different context. In this regard attention must be paid to Rule 4(8) of the 2021 Rules which contemplates that an intermediary may entertain a "request for the reinstatement" of content that it may have voluntarily removed; whereby the 2021 Rules now specifically provide that offending content may be removed in the first instance, giving to any interested person as specified in Rule 4(8) the liberty to object to such removal and to request for reinstatement of the removed content. This has been provided in the rules since, evidently, it affords a more fair and just balance between the irreparable harm that may be caused by retaining offending content on the world wide web and the right of another person to seek reinstatement of the content by challenging its removal.

(*viii*) The court may also direct the aggrieved party to make a complaint on the National Cybercrime Reporting Portal (if not already done so), to initiate the process provided for grievance redressal on that portal.

(*ix*) Most importantly, the court must refer to the provisions of Sections 79(3)(*a*) and (*b*) read with

Section 85 of the IT Act and Rule 7 of the 2021 Rules, whereby an *intermediary would forfeit the exemption from liability* enjoyed by it under the law if it were to fail to observe its obligations for removal/access disablement of offending content despite a court order to that effect.

92. Lest it be thought that the exercise done by this Court in the present matter was needless, this Court would like to record that what impelled it to undertake this somewhat prolix and painstaking exercise, is that the integrity of the court process has to be protected in the most effective way, the anarchical nature of the internet notwithstanding. It cannot be over-emphasised that even if, given the nature of the internet, offending content cannot be completely "removed" from the world wide web, offending content can be made unavailable and inaccessible by making such content "non-searchable" by deindexing and dereferencing it from the search results of the most widely used search engines, thereby serving the essential purpose of a court order almost completely. In the opinion of this Court, the directions issued by a court seized of a case such as the present one, must be specific, pointed and issued to all necessary parties, so as to ensure that the purpose sought to be achieved by the court is fulfilled and that the directions and orders issued are not merely on paper or purposeless.

Directions in this matter

93. In line with the above suggested template of directions, in the present case this Court is satisfied that the action of the petitioner's photographs and images having been taken from her Facebook and Instagram accounts and having been posted on the website www.xhamster.com; and then having been reposted onto other websites and online platforms, amounts prima facie to an offence under Section 67 of the IT Act in addition to other offences under the IPC; and that appropriate directions are required to be issued directing the State and other respondents to forthwith remove and/or disable access to the offending content from the world wide web to the maximum extent possible. Accordingly the following directions are issued:

(*i*) The petitioner is directed to furnish in writing to the investigating officer of the subject FIR, all available information relating to the offending content, including the Image URL and web URL pertaining to the offending image files, within 24 hours of receipt of a copy of this judgment, if not already done so.

(*ii*) The Delhi Police/CyPAD Cell are directed to remove/disable access to the offending content, the web URL and Image URL of which would be furnished by the petitioner as above, from all websites and online platforms, forthwith and in any event within 24 hours of receipt of information from the petitioner. It may be recorded that the Delhi Police have stated before this Court that the offending content has already been removed from Respondent 5 website www.xhamster.com.

(*iii*) A direction is issued to the search engines Google Search, Yahoo Search, Microsoft Bing and DuckDuckGo, to globally deindex and dereference from their search results the offending content as identified by its Web URL and Image URL, including deindexing and dereferencing all concerned web pages, sub-pages or sub-directories on which the offending content is found, forthwith and in any event within 24 hours of receipt of a copy of this judgment along with requisite information from the Investigating Officer as directed below.

(*iv*) A further direction is issued to the search engines Google Search, Yahoo Search, Microsoft Bing, DuckDuckGo, to endeavour to use automated tools, to proactively identify and globally disable access to any content which is exactly identical to the offending content, that may appear on any other websites/online platforms.

(*v*) The investigating officer is directed to furnish in writing the web URL and Image URL of the offending content to the other entities to whom directions have been issued by this Court in the

present matter, along with a copy of this judgment, within 24 hours of receipt of such copy;

(*vi*) The Delhi Police are directed to obtain from the concerned website, namely, www.xhamster.com and from the search engines Google Search, Yahoo Search, Microsoft Bing, DuckDuckGo (and any other search engines as may be possible) all information and associated records relating to the offending content such as the URL, account ID, handle name, internal protocol address, hash value and other such information as may be necessary, for investigation of case FIR No. 286 of 2020 dated 18-7-2020 registered under Sections 354-AIPC and 66C IT Act at PS : Dwarka South, forthwith and in any event within 72 hours of receipt of a copy of this judgment, if not already done so;

(*vii*) Furthermore, the petitioner is granted liberty to issue written communication to the investigating officer for removal/access disablement of the same or similar offending content appearing on any other website/online platform or search engine(s), whether in the same or in different context; with a corresponding direction to the Investigating Officer to notify such website/online platform or search engine(s) to comply with such request, immediately and in any event within 72 hours of receiving such written communication from the petitioner;

(*viii*) Notwithstanding the disposal of the present petition by this order, if any website, online platform, search engine(s) or law enforcement agency has any doubt or grievance as regards compliance of any request made by petitioner as aforesaid, such entity shall be at liberty to approach this Court to seek clarification in that behalf.

94. It is made clear that non-compliance with the foregoing directions would make the non-compliant party liable to forfeit the exemption, if any, available to it generally under Section 79(1) of the IT Act and as specified by Rule 7 of the 2021 Rules; and shall make

> **such entity and its officers liable for action as mandated by Section 85 of the IT Act."**
>
> (Emphasis supplied)

The aforesaid judgment is challenged before the Division Bench of the High Court of Delhi and there is no interim order of stay of the said judgment. Subsequent to the said judgment, another bench learned Judge of the Delhi High Court in the case of **X v. UNION OF INDIA**[3] notices the aforesaid judgment and observes as follows:

> "The instant writ petition has been filed under Article 226 of the Constitution of India, read with Section 482 of the Code of Criminal Procedure (hereinafter referred to as "CrPC") seeking, in a nutshell, the blocking of certain sites exhibiting intimate images of the petitioner herein, and for registration of a first information report (FIR) arising out of the complaint dated 3-8-2021 made by the petitioner to Lajpat Nagar Police Station, New Delhi.
>
> **3.** Having stated the above, the facts, in brief, leading to the instant petition are stated as under :
>
> 3.1 It is stated that the petitioner is a married woman with a nine-year-old son. In December 2019, she became acquainted with one Mr Richesh Manav Singhal who approached her through social media and introduced himself as a British Chartered Accountant. It is stated that in February 2020, the petitioner shared her personal contact number with Mr Singhal, and over a period of time, the petitioner became close to Mr Singhal.

[3] **2023 SCC OnLine Del 2361**

3.2 In July 2020, it is stated that as the petitioner was living with her son at a rented accommodation in Gurugram on account of her job and financial constraints. Mr Singhal took advantage of the absence of the petitioner's family members, came over to her place and forced himself upon her. He allegedly not only clicked explicit pictures of the petitioner, but also transferred to himself from the mobile phone of the petitioner explicit pictures that the petitioner had taken of herself for the purpose of sharing them with her husband.

3.3 It is stated that Mr Singhal involved the minor son of the petitioner in various sexual acts as well. Consequently, the petitioner lodged a complaint against Mr Singhal at the Lajpat Nagar Police Station, and on the basis of the same, a zero FIR was registered with the investigation thereafter being transferred to Gurugram. It is stated that on multiple occasions, Mr Singhal threatened the petitioner that he would leak her sexually explicit photographs on various pornographic websites and that he would kill her son if she did not pay huge amounts of money to him. Consequently, the petitioner was extorted into paying lakhs of money to Mr Singhal, along with handing him all her jewellery.

3.4 It is stated that as the funds of the petitioner had depleted and she was unable to pay any more money to Mr Singhal, he followed through on his threats and leaked the petitioner's explicit images on various pornographic websites without the consent or permission of the petitioner. This led to the petitioner addressing a complaint dated 3-8-2021 against Mr Singhal to the SHO at Police Station Lajpat Nagar recording the new offences. The said complaint notes that Mr Singhal had made a YouTube channel in the petitioner's name, and has been posting her explicit videos and photographs on a daily basis.

3.5 Despite the petitioner having approached the grievance cells of Respondents 3 to 6 i.e. Google LLC, Microsoft India Pvt. Ltd. (later replaced by Microsoft Ireland Operations Ltd. which is the entity managing its search engine, Bing), YouTube.com and Vimeo.com, as well as having placed multiple complaints on cybercrime.gov.in, the explicit images of the petitioner were not taken down.

3.6 Aggrieved by the failure in the redressal processes available to her, the petitioner herein has approached this Court by way of the instant writ petition for directions to the respondents for removal of all her non-consensual intimate images on the internet.

… … …

57. In a judgment of this Court in *X* v. *Union of India* [*Da Cunha* v. *Yahoo de Argentina SRL*, AR/JUR/40066/2010] , a direction had been given to all intermediaries by the learned Single Judge Bench to engage in proactive monitoring and removal of NCII content that the court had deemed to be illegal. There is currently an appeal pending against the said judgment, however, no stay has been granted, and thus, the order is still in operation. The working paper published by CCG records the risks that overbroad directions may pose, however, the viability of the directions in the said judgment is of no consequence in the instant matter as the directions and suggestions being issued herein are restricted to search engines only. The relevant portion of the working paper is as under :

"*Proactive monitoring for NCII content* : In 2021, a Single Judge of the Delhi High Court attempted to address the problem of reuploading of known NCII by stipulating that all intermediaries must engage in the proactive monitoring and removal of NCII that the court had previously determined to be illegal. 16 such mandatory monitoring obligations create significant free speech and privacy risks as intermediaries must monitor all users to identify those uploading unlawful content. 17 such automated filtering has also been demonstrated to disproportionately restrict lawful expression by individuals from racial and linguistic minorities. 18 imposing a monitoring requirement on all intermediaries could lead to more content removal, but not necessarily better content removal, resulting in the removal of lawful speech. Therefore, curbing the redistribution of NCII requires a more nuanced approach."

… … …

60. The fact that search engines do not host or publish or create content themselves is of no consequence when it comes to the question of removal of the access to the offending content. It is undeniable that they do have the ability, the capacity, and the legal obligation to disable access to the

> offending content; this responsibility of the search engine cannot be brushed under the carpet on the ground that it does not host content.
>
> **61.** This Court painfully notes that there is an abysmal absence of a collaborative effort that should ideally be undertaken by the intermediaries and the State. The focus of such entities and authorities should be on the quick redressal of the complaint brought before them rather than the shirking of blame or making submissions on the onerous nature of their duties. In the process of shirking responsibility, precious time is lost in removal of the offending content and it enables the offender to keep reposting the content. It further encourages other potential offenders to undertake such dissemination of NCII content as they are aware of the lack of consequences. This in turn frustrates the legal redressal mechanism in place and the harm, both emotional and reputational, caused to the victim/user persists and perpetuates. In a conservative country like India where matters of this nature are not a part of dinner table conversations, NCII abuse does indeed lead to harrowing consequences and everlasting stigma for the victim. In light of this, the endeavour of every entity involved should be to expeditiously resolve the issue."

The High Court of Delhi was answering a petition filed under Article 226 of the constitution of India r/w section 482 of the Cr.P.C. seeking blocking of certain sites exhibiting intimate images of the petitioner therein. The facts before the High Court of Delhi is noticed in paragraph 3.2 to 3.4 quoted *supra*. The Delhi High Court holds that the fact that search engines do not publish or create content themselves is of no consequence, when it comes to the question of removal of the access to the offending content. The

Delhi High court was dealing with blocking of URLs which exhibited objectionable content of the petitioner therein.

15. A little earlier to the aforesaid judgment of the High Court of Delhi, the High Court of Madras in the case of **REGISTRAR (JUDICIAL) V. UNION MINISTRY OF COMMUNICATIONS[4],** has held as follows:

"…. …. ….

> **30.** The Blue Whale is not a freely downloadable game but comes in a secret social media group with a curator who "sends you the app" and tracks you with your feedback and the results of the activities undertaken, prompting the participants to send photos of the activities accomplished as per instructions. It would be shocking to know that these activities include getting up at 4 A.M., climbing down flights of hundreds of staircase-steps, watching horror movies at night, walking outside alone at midnight, going to the graveyard alone, spending a whole day in silence etc. Gradually, the intensity or difficulty of the tasks increases, and advanced activities include inflicting self-injuries on the body by cutting the skin. The Game culminates with the final activity of going to a roof-top and jumping off a high-rise to commit suicide. It sounds scary to even read this. It is further shocking to know that there is reportedly an 'Indian curator' for the challenge or some one with Indian victim-participation in mind, since the final task ie Day-50 which was originally with an instruction to "Jump from the top floor and kill yourself" has been reportedly changed for the Indian victims as "Hang yourself" to suit the Indian conditions of not many high rise buildings and yet 'facilitate' killing!. We have been coming across several cases of suicide across the globe by participants in the Blue Whale Challenge, and since the beginning of this year, such cases are being reported almost daily. In India too, in the past few months, the media has been reporting several such cases from down South in Kerala to the West in Mumbai, and other parts of the country too. In many educational institutions, school authorities have noticed increasing interest by the students to explore this scary Challenge. It is curiousity, no doubt. It is reported that some school authorities have noticed unusual and strange behaviour in their students, and on investigation, they have discovered that these

[4] 2017 SCC online MAD 25298

students were participants in the Blue Whale Challenge. Unfortunately, on being questioned, they first feigned ignorance of any such activity or 'Game'. Such confidentiality by the participants is a social, psychological issue typical for an adolescent and is to be handled with care by elders and seniors.

31. Having considered the issue from all perspectives, we issue the following directions:—

A. Directions to the Central Government:—

i. The Central Government is directed to take appropriate steps, as expeditiously as possible to bring all the "Over The Top" services as well as service providers into a legal framework obliging them to comply with the laws of India and to provide the required information to the law enforcing agencies. Methods must to be devised to ensure that those OTTs which could not be brought within such framework are not accessible in India.

ii. CERT-In is directed to collect the digital equipments such as smart mobile phones, tablet computers and laptops used by the victims of Blue Whale challenge game for conducting digital forensic analysis so that the source of the game as well as the administrators of the game could be found out.

iii. The internet service providers must be directed to take due diligence to remove all the links and hash-tags presently being circulated in the social media platforms such as Facebook, Twitter etc. and also in dark net with URLs/links related to Blue Whale game.

iv. The internet service providers in India must be called upon to furnish information regarding downloads/access to suspicious links/URLs of the game, prior to the removal from their platforms.

v. The Central Government must seek co-operation and use its diplomatic relationship with Russia to block the URLS/Links related to Blue Whale game and penal action against the culprits on behalf of India.

vi. The Technology Companies and Websites follow the Laws of their respective jurisdiction and as such, they are not providing the "Data and Information", in spite of making a request for it by the Law Enforcing Agencies in India on account of violation of Indian Laws. This is evident from the communication dated 22 May, 2017, received by the Director, Cyber Laws and Security Group, Ministry of Electronics and Information Technology, Government of India from Google India Private Limited, that Google service, such as Google play are provided by Google Inc, a company incorporated under and governed by the Laws of United States. The Central Government must address this issue seriously and consider amending the relevant Rules and Regulations applicable to the Indian subsidiaries and websites making it compulsorily amenable to Indian Laws.

B. Directions to the State Government:—

i. The Government of Tamil Nadu shall designate forthwith Shri.Dr. S. Murugan, I.P.S., an Expert in Cyber Law, presently functioning as Joint Director, Department of Vigilance and Anti Corruption, Chennai - 16, as the Nodal Officer in terms of Rule 4 of the Information Technology (Procedure and Safeguards for Blocking for Access of Information by Public) Rules, 2009. This would be in addition to his duties as Joint Director, Department of Vigilance and Anti-Corruption.

ii. The Nodal Officer must in coordination with the Designated Officer appointed under Rule 3 of the Information Technology (Procedure and Safeguards for Blocking for Access of Information by Public) Rules, 2009 and other authorities must ensure the implementation of the order blocking the website and removal of links. The State Government is directed to provide necessary manpower and resources to the Nodal Officer for carrying out his functions in larger public interest. It is open to the Nodal Officer to take the assistance of other Experts in the field of Cyber Law and preferably Ms. Lavanya, ADSP, who is presently with the C.B.C.I.D., Chennai.

iii. The Director General of Police is directed to ensure that the instructions given vide circular bearing C. No. 121311/General-1/2017 dated 01.09.2017 are complied with in letter and spirit.

iv. The Principal Secretary to Government, School Education Department, the Principal Secretary to Government, Higher Education Department, the Director of School Education and the Director of College Education shall take active steps to ensure that all Educational Institutions in Tamil Nadu sensitize and warn the students as well as the parents not only about this Blue Whale challenge game but also the lurking dangers in the digital world.

v. The Government must constitute District and Taluk Level Committee comprising members from Non-Governmental Organization, Psychiatrists, Voluntary Organizations, Educationalists and all other stake-holders to chalk out programmes for giving counselling taking the Educational Institutions as a unit. The volunteers appointed by the Committee must take up the work of counselling to students as a mission. They should earmark dedicated telephone numbers, so as to enable those who are in need of counselling and their parents to approach the volunteers for timely help.

vi. The Government must issue advisories periodically to the youth and students in particular underlining the ill effects of this game and the facilities available to come out of this dangerous game.

vii. The Superintendent of Police, Madurai Rural shall forthwith transmit the digital equipments seized in connection with the suicide of Vicky @ Vignesh to CERT-In for forensic analysis.

viii. Those who are providing links and promoting this dangerous game even after its ban must be prosecuted by invoking the relevant provisions of the Information Technology Act, 2000 and Penal Code, 1860.

ix. The Press and Media also owe a duty to the Society by reporting the measures taken by the Government and

other Agencies for counselling and appeal to the youth not to try this game on any account.

CONCLUDING REMARKS:

32. Internet is intended to connect the individual with the world at large. Citizens have become netizens. But even as we connect, we tend to get alienated also. There are negative as well as perverse tendencies inherent in any human being. The online phenomena such as Blue Whale game, bring this out. There are sharks on the prowl ready to prey and pounce upon the innocent and unwary victims. Protecting the Society is the joint responsibility of the service providers, the content providers, the Law makers, the Society, the family and the Community at large, and of course, the users of internet themselves. Courts cannot remain mute spectators when faced with such a social menace. Hence we have issued the aforementioned directions in larger public interest."

(Emphasis supplied)

16. It is not that Government of India has not banned any app or any mail. The Government of India has banned 59 mobile apps which, according to it, were prejudicial to the sovereignty and integrity of India or even security. The banning of 59 mobile apps and the reasons thereon are as follows:

"Government Bans 59 mobile apps which are prejudicial to sovereignty and integrity of India, defence of India, security of state and public order

Posted On: 29 JUN 2020 8:47PM by PIB Del

The Ministry of Information Technology, invoking it's power under section 69A of the Information Technology

Act read with the relevant provisions of the information Technology (Procedure and Safeguards for Blocking of Access of Information by Public) Rules 2009 and in view of the emergent nature of threats has decided to block 59 apps (see Appendix) since in view of information available they are engaged in activities which is prejudicial to sovereignty and integrity of India, defence of India, security of state and public order.

Over the last few years, India has emerged as a leading innovator when it comes to technological advancements and a primary market in the digital space.

At the same time, there have been raging concerns on aspects relating to data security and safeguarding the privacy of 130 crore Indians. It has been noted recently that such concerns also pose a threat to sovereignty and security of our country. The Ministry of Information Technology has received many complaints from various sources including several reports about misuse of some mobile apps available on Android and iOS platforms for stealing and surreptitiously transmitting users' data in an unauthorized manner to servers which have locations outside India. The compilation of these data, its mining and profiling by elements hostile to national security and defence of India, which ultimately impinges upon the sovereignty and integrity of India, is matter of very deep and immediate concern which requires emergency measures.

The Indian Cyber Crime Coordination Centre, Ministry of Home Affairs has also sent an exhaustive recommendation for blocking these malicious apps. This Ministry has also received many representations raising concerns from citizens regarding security of data and risk to privacy relating to operation of certain apps. The Computer Emergency Response Team (CERT-IN) has also received many representations from citizens regarding security of data and breach of privacy impacting upon public order issues. Likewise, there have been similar bipartisan concerns, flagged by various public representatives, both outside and inside the Parliament of India. There has been a strong chorus in the public space to take strict action against Apps that harm India's sovereignty as well as the privacy of our citizens.

> On the basis of these and upon receiving of recent credible inputs that such Apps pose threat to sovereignty and integrity of India, the Government of India has decided to disallow the usage of certain Apps, used in both mobile and non-mobile Internet enabled devices. These apps are listed in the attached appendix.
>
> This move will safeguard the interests of crores of Indian mobile and internet users. This decision is a targeted move to ensure safety and sovereignty of Indian cyberspace."
>
> (Emphasis supplied)

Number of apps that are banned are listed at page 133, which read as follows:

"1. Tik Tok	31. Mi Video Call - Xiaomi
2. Shareit	32. WeSync
3. Kwai	33. ES File Explorer
4. UC Browser	34. Viva Video-QU Video Inc
5. Baidu map	35. Meitu
6. Shein	36. Vigo Video
7. Clash of Kings	37. New Video Status
8. DU battery saver	38. DU Recorder
9. Helo	39. Vault-Hide
10. Likee	40. Cache Cleaner DU App studio
11. YouCam makeup	41. DU Cleaner
12. Mi Community	42. DU Browser

13. CM Browers	43. Hago Play With New Friends
14. Virus Cleaner	44 Cam Scanner
15. APUS Browser	45. Clean Master-Cheetah Mobile
16. ROMWE	46. Wonder Camera
17. Club Factory	47. Photo Wonder
18. Newsdog	48. QQ Player
19. Beutry Plus	49. We Meet
20. WeChat	50. Sweet Selfie
21. UC News	51. Baidu Translate
22 QQ Mail	52. Vmate
23. Weibo	53. QQ International
24. Xender	54. QQ Security Center
25. QQ Music	55. QQ Launcher
25. QQ Newsfeed	56. U Video
27. Bigo Live	57. V fly Status Video
28. SelfieCity	58. Mobile Legends
29. Mail Master	59. DU Privacy”
30. Parallel Space	

The 7th respondent – Proton AG undoubtedly falls short of the duties prescribed under Indian Law. Its inaction and opacity strike at the heart of digital accountability and embolden the malicious. The plea is therefore put for preserving the sanctity of Indian Cyber Space. As observed hereinabove, the Government of India has banned several applications. When the situation of the subject kind has emerged, this Court fails to understand the complacency of the Union of India in not taking action towards blocking the Proton Mail, as the generation of torrent of mails from the mail box of Proton AG including hoax bomb mails threatening the security of the Nation, have not stopped. As noted hereinabove, other Nations have swung into swift action to block either the URLs or the mail generator itself. If what is narrated hereinabove is noticed, it is undoubtedly a serious issue which the Government of India should take immediate action.

17. The submission of the learned Additional Solicitor General of India with regard to procedure had been considered by the High Court of Delhi in its judgment quoted *supra.* The High Court of Delhi

holds that there need not be a recommendation from the Nodal Officer. Action can be taken even without waiting for such recommendation when situations warrant and such action is required to be taken without delay. I am in respectful agreement with what the High Court of Delhi has observed with regard to interpretation of Rule 10 *supra*. Courts cannot remain mute spectators when faced with such menace which undermines privacy and integrity of women in particular. Protecting the society is the joint responsibility of service providers, content providers, law makers. It is the duty of the State to bring such perpetrators of crime to justice, which has become difficult in the case at hand. Hence, in the light of the egregious facts, prevailing legal frame work and owing to the preceding analysis, I deem it appropriate to answer the prayers of the petitioner. Therefore, the Union of India/Competent Authority shall now take steps in terms of Section 69A of the Act read with Rule 10 of the Rules to block Proton Mail.

18. For the aforesaid reasons, the following:

ORDER

(i) Writ Petition is allowed.

(ii) *Mandamus* issues to respondents 2, 4 and 5 to initiate proceedings in terms of Section 69A of the Information Technology (Amendment) Act, 2008 r/w Rule 10 of the Information Technology (Procedure and Safeguards for Blocking of Access of Information by Public) Rules, 2009 to block Proton Mail, bearing in mind the observations made in the course of the order.

(iii) Till such proceedings are taken up by the Government of India, the offending Uniform Resource Locator - URLs that are indicated in the petition shall be blocked forthwith.

Sd/-
(M.NAGAPRASANNA)
JUDGE

bkp
CT:MJ