

\$~22

\* **IN THE HIGH COURT OF DELHI AT NEW DELHI**  
+ **W.P.(CRL) 1062/2021**

**JUBILANT FOOD WORKS LIMITED** ..... Petitioner

Through : Mr. Dayan Krishnan, Senior Advocate  
with Mr. Shankh Sengupta, Mr.  
Pallav Shukla, Mr. Aayush Chandra,  
Mr. Sukrit, Mr. Sanjeev Seshadri and  
Mr. Ashish Kumar Advocates.

versus

**UNION OF INDIA THROUGH THE SECRETARY**  
**MINISTRY OF ELECTRONICS AND INFORMATION**  
**TECHNOLOGY GOVERNMENT OF INDIA & ORS. ..Respondents**

Through : Mr. Kirtiman Singh, CGSC, Mr. Waize  
Ali Noor and Taha Yasin Advocates  
for R-1, 2 & 4.  
Mr. Piyush Singhal, Advocate for  
Mr. Ashish Aggarwal, ASC for the  
State.

**CORAM:**  
**HON'BLE MR. JUSTICE YOGESH KHANNA**

**ORDER**

% **02.06.2021**

1. The hearing has been conducted through Video Conferencing.

**CRL.M.A. 8638/2021**

2. Exemption allowed, subject to all just exceptions.

3. The application stands disposed of.

**W.P.(CRL) 1062/2021 & CRL.M.A. 8637/2021**

4. The Jubilant FoodWorks Limited/petitioner herein has preferred the instant Writ petition seeking Writ of Mandamus or any other appropriate Writ/direction to the Ministry of Electronics and Information Technology respondent No. 1 herein and the Department of Communications, Ministry of Communications/respondent No. 2 to direct and notify the intermediaries

such as telecom service providers, internet service providers, search engines, etc. to immediately remove or disable access to the uniform resource locator(s) (URLs) created by one or more unknown persons/hackers to illegally share the data of thousands of customers of the petitioner on the internet. The petitioner operates Dominos Pizza stores in India.

5. The data hosted on the URLs by the hackers is part of the computer resource owned by the petitioner. The hackers have illegally and unauthorizedly accessed such data from the petitioner's secure computer resource and hosted it on the URLs without consent, thus invading the privacy of the petitioner's customers. It is alleged the hackers had also attempted to intimidate and extort ransom from the petitioner and that such action of the hackers is an offence under sub-clause (a) access data without permission and sub-clause (b) download, copy or extract data without permission of section 43; and section 66 computer related offences of the Information Technology Act, 2000 and sections 384/506/34 IPC. The respondent Nos. 1 and 2 being the appropriate government under IT Act for internet based communication are under a duty to immediately notify the intermediaries and issue directions to remove or disable access to the URLs as part of their statutory obligation under clause (b) of sub-section (3) of section 79 of the IT Act read with Rule 3 (1) (d) of the 2021 Rules.

6. It is further argued that in view of the judgment passed by this Court titled as *X vs Union of India* in W.P. (Crl) 1082/2020 decided on 20 April 2021, petitioner is seeking issuance of directions to the DCP Cyber Crime Cell and the SHO, Cyber Crimes Cell, South East District – Delhi, Police Station – Chittaranjan Park/respondent No. 3, to take steps (a) immediately remove/disable access to the URLs; and (b) obtain from the concerned

intermediaries all information and associated records, including all unique identifiers relating to the URLs, under Rule 3 (1) (j) of the 2021 Rules, for the purposes of prevention, detection, investigation and prosecution of offences committed by the hackers under the IT Act.

7. It is argued by reason of inaction of the respondents, the hackers merrily continue to re-post, re-direct and re-publish the data of the petitioner's customers from one URL to another resulting in severe reputational risk and harm to the petitioner and, more importantly, a compromise of the personal data of thousands of petitioner's customers. Recently, the petitioner has become aware that the hackers have posted an advertisement on one of the URLs with an offer to sell the illegally obtained data of the petitioner's customers. If the URLs are not immediately removed or disabled, the hackers would continue to further compromise the data of the petitioner's customers on the internet, thus invading their privacy and causing irreparable harm to the petitioner's customers. Hence, the petitioner seeks the indulgence of this Court to pass immediate directions to remove and disable access to the URLs since any delay in the present circumstances can render the same ineffective and futile, hence, the present Petition.

8. It is submitted by the learned senior counsel for the petitioner they have written to the respondents and have also received the response thereof which notes they need a Court order so that the needful may be done. The learned senior counsel refers to *X vs. Union of India* in W.P. (Crl) 1082/2020 decided on 20 April 2021 more specifically the template suggestions in para 90 of such order which is as under:

*“90. 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 'de indexing' and 'dereferencing' the offending content in their listed search results, including de-indexing and de-referencing all concerned webpages, 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 Cyber-Crime 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 section 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.”*

9. The learned counsel for UOI is present and he submits the URLs supplied to them have already been blocked and they shall continue to take proactive steps as and when the complaints shall be filed by the petitioner before them. Besides this there are other respondents who are also directed to act as per law, including those of the observations/directions laid down in X (supra).

10. The petitioner is hereby granted liberty to make written communication to the investigating officer for removal/access disablement of the same or similar offending content appearing including URLs on any other website/online platform or search engine(s), whether in the same or in different context; and the investigating officer is 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.

11. The petition stands disposed of in view of the above. Pending application(s), if any also stands disposed of.

**YOGESH KHANNA, J.**

**JUNE 02, 2021/ᵀᵀ**