



Case Comment: The Israeli Supreme Court's Decision in the Cyber Unit Case

HCJ 7846/18 Adalah v. The Cyber Unit

By: Rabea Eghbariah, Adalah Attorney and SJD Candidate, Harvard Law School

On 12 April 2021, the Israeli Supreme Court gave a green light to the informal cooperation of the Cyber Unit, which operates within the Israeli State Attorney's Office, with social media platforms (e.g. Facebook, YouTube, Twitter). In a ruling spanning 52 pages, delivered as a landmark retirement case of Justice Hanan Melcer, the court rejected a petition filed by Adalah and the Association for Civil Rights in Israel (ACRI) challenging the Cyber Unit's "alternative enforcement" mechanism. Within this capacity, the Cyber Unit submits thousands of referrals each year, based on alleged violations of the private platforms' terms of service, asking the platforms to "voluntarily" remove users' content that the Cyber Unit deems to be "terrorist" or otherwise unlawful. The court found that this activity does not violate constitutional rights, falls under the government's authority, and is "crucial to the national security and social order" (para. 72).

The practice of referring users' content to online intermediaries for their "voluntary" takedown started with the establishment of the Cyber Unit in 2015. Since then, the volume of content referred to the social media platforms saw a dramatic increase: from 2,241 referrals in 2016 to more than 19,600 referrals in 2019 (the last year with data available). The growing number of referrals has been accompanied by a growing rate of compliance by the private platforms: whereas in 2016 the overall compliance rate stood at 76.5%, in 2019 this rate stood at 90%. Although the Cyber Unit's activity is diverse, the overwhelming majority of referrals target what the Cyber Unit classifies as "terrorist" or inciteful content. Neither the Cyber Unit nor the private platforms provide any substantive information about this mechanism of referrals and removals.

Challenging this practice, Adalah and ACRI filed a petition to the Israeli Supreme Court in 2019 and argued that the Cyber Unit's referral activity violates the constitutional rights of freedom of expression and opinion and the user's rights of due process without any authorization by law. The petition emphasized the structural relations between the state and corporate powers and the state's leverage to push private companies to cooperate with its requests. The petitioners argued that the state's ability to impose regulation and taxation on these companies, many of whom are incorporated in Israel (e.g. Facebook, Google), substantially decreases the degree of voluntariness that these companies enjoy when considering state requests.

While the state responded by claiming that the Cyber Unit's referrals do not constitute state action since the removal of content is ultimately done by private third-parties (i.e. the private platforms such as Facebook), the court rejected this argument. The court ruled that the Cyber Unit's referrals constitute state action that requires adequate authorization by law. The court, however, dismissed the petitioners' argument that the activity violates constitutional rights, and ruled that it is sufficiently grounded in the government's discretionary powers and is "crucial to the national security and social order" (para. 72). This finding stands, despite the court's conclusion that state referrals may "influence the discretion of the content intermediaries" (para. 53). Furthermore, the court concluded that "as long as a violation [of rights] exists, it is carried out by the operators of the online platforms, and not by a state actor" (para. 67). The court went further to assume that a bulk of the content removed is generated by bots and stated that "robots do not have human rights" (para. 31).

Implications of the decision and general concerns

The court's decision in the Cyber Unit case grants a blank check for the state to continue to engage in these practices of voluntary cooperation with private third-parties. As such, it raises the specter of abuse of power, as it allows censorship of arguably legitimate content without any adequate authorization by law, transparency, or ability to challenge the referrals or the takedown of users' content.

Authorization by law: While the court found that the Cyber Unit's referrals constitute state action that requires adequate legal authorization, it still concluded that such authorization is sufficiently grounded in the government's discretionary powers and the state prosecutor's

general policing powers. This conclusion stands at odds with long-established judicial precedents that require explicit authorization for governmental conduct or action that either violates human rights or constitutes a substantial use of state authority. The court bypassed this analysis by concluding that the petitioners did not prove a concrete violation of constitutional rights, as elaborated below, and opened the door for legalizing unauthorized activity that clearly threatens freedom of expression and opinion, due process and constitutional norms.

Violation of rights: The court’s conclusion that the petitioners failed to prove a violation of constitutional rights (mis) places the burden on the petitioners to prove a concrete violation of rights even when it is impossible by design. The court ignored the fact that the “alternative enforcement” mechanism employed by the Cyber Unit lacks any substantive transparency that allows the petitioners, or the public more generally, to scrutinize the referral and removal decisions. In fact, since the removals are based on the platforms’ terms of service, users who are affected by the Cyber Unit’s activity are not aware that the state might have triggered the removal of their content. Furthermore, the court assumed in this context that a substantial part of the Cyber Unit’s activity pertains to content published by bots (and therefore does not fall under constitutional protection). This conclusion, however, is not based on information disclosed by the state during the proceedings, and it remains unclear to what extent it is precise.

Censorship of content written by Palestinian users: Although the Cyber Unit’s remit is diverse and expanding (e.g., most recently, the Cyber Unit was involved in removing misinformation and disinformation pertaining to COVID-19 vaccinations), the vast majority of content removed falls under what the Cyber Unit classifies as “terrorist” or inciteful content. These broad and often ill-defined categories may be easily interpreted to capture legitimate speech and lead to a “censorship creep.” Palestinians may not be the only ones harmed by the “alternative enforcement” mechanism, but long experience shows that they are often the first and most affected by censorship under the pretext of national security.

Worldwide removal of content and potential conflict of laws: The court’s conclusion that the Cyber Unit’s activity is legal allows the state to use its leverage to censor online content not only within its jurisdiction but also beyond it. Since the removals are based on the

companies' terms of service, rather than on a court order for example, the content removed becomes unavailable worldwide. This situation, where the Cyber Unit is interpreting and relying on the companies' terms of service to takedown content, allows the Israeli Cyber Unit to be involved, through the platforms' content regulation apparatus, in removing content that is published and protected in other jurisdictions. Although the removals are ultimately based on the universally unified corpus of terms of service, this framework is prone, as many scholars have pointed out, to many indeterminacies and overbroad interpretation.

Links to Court Decision and Documents (in Hebrew)

Decision: bit.ly/3gSosCB

Petition: bit.ly/39P8SDt

Amicus: bit.ly/2R9TI54

State response: bit.ly/2Q2BXUS

Court interim decision: bit.ly/3t2ibYg

State supplemental written argument: bit.ly/3dKyPVU

Petitioners' response: bit.ly/3dP7kKG