HCJ 7846/19

Petitioners:	1.	**Adalah Legal Center for Arab Minority Rights in Israel**
	2.	**Association for Civil Rights in Israel**
		v.
Respondents:	1.	**State Attorney's Office – Cyber Department**
	2.	**Attorney General**
Requests to Join:	1.	**Lori Shem Tov**
	2.	**Movement for Freedom of Information**

Petition for order nisi

Israeli Supreme Court cases cited:

[1] EA 8/21 *Shachar Ben Meir, Adv., v. Likud*, (Feb. 27, 2019)

[2] EA 27/21 *Yisrael Beiteinu Faction v. Shamir Systems and Operators Ltd*., (Feb. 26, 2019)

[3] AAA 3782/12 *Tel Aviv-Jaffa District Commander v. Israel Internet Association*, (March 24, 2013) [https://versa.cardozo.yu.edu/opinions/tel-aviv-jaffa-district-commander-v-israel-internet-association]

[4] LCA 4447/07 *Mor v. Barak I.T.T. [1995] International Telecommunications Services Corporation*, IsrSC 63(3) 664 (2009)

[5] HCJ 8600/04 *Shimoni v. Prime Minister*, IsrSC 59(5) 673 (2005)

[6] HCJ 6824/07 *Manaa v. Israel Tax Authority*, IsrSC 64(2) 479 (2010)

[7] HCJ 399/85 *Kahana v. Broadcasting Authority Management Board*, IsrSC 41(3) 255 (1987)

[8] HCJ 5185/13 *A. v. Great Rabbinical Court*, (Feb. 28, 2017)

[9] MApp 2065/13 *A. v. State of Israel*, (March 22,2013)

[10] HCJ 6972/07 *Akiva Laxer, Adv. v. Minister of Finance*, (March 22, 2009)

[11] HCJ 84/82 *Histadrut Po'alei Agudat Yisrael v. Minister of Religious Affairs*, IsrSC 37(1) 813 (1984)

[12] HCJ 828/90 *Likud Faction of the Haifa Municipal Council v. Haifa Municipal Council*, IsrSC 45(1) 506 (1991)

[13] HCJ/149 *Bejarano v. Police Minister*, IsrSC 2 80 (1949) [https://versa.cardozo.yu.edu/opinions/bejerano-v-police-minister]

[14] LCrimA 10141/09 *Ben Haim v. State of Israel*, (March 6, 2012)

[15] HCJ 2918/93 *Kiryat Gat Municipality v. State of Israel*, IsrSC 47(5) 832 (1993)

[16] HCJ 5128/94 *Federman v. Minister of Police*, IsrSC 48(5) 647 (1995)

[17] HCJ 8600/04 *Chair of the Hof Azza Regional Council v. Prime Minister*, IsrSC 59(5) 673 (2005)

[18] HCJ 11163/03 *Supreme Monitoring Committee for Arab Affairs in Israel and others v. Prime Minister of Israel*, (Feb. 27, 2006) [https://versa.cardozo.yu.edu/opinions/supreme-monitoring-committee-arab-affairs-israel-and-others-v-prime-minister-israel]

[19] HCJ 144/50 *Dr. Israel Sheib v. Minister of Defence*, IsrSC 5 399 (1951) [https://versa.cardozo.yu.edu/opinions/sheib-v-minister-defence]

[20] HCJ 4374/15 *Movement for Quality Government v. Prime Minister*, (March 27, 2016) [https://versa.cardozo.yu.edu/opinions/movement-quality-government-v-prime-minister]

[21] CA 9183/09 *Football Association Premier League Ltd. v. Anon.*, IsrSC 65(3) 521 (2012)

[22] HCJ 7721/96 *Israeli Insurance Adjusters Association v. Supervisor of Insurance*, IsrSC 55(3) 625 (2001)

[23] HCJ 6579/99 *Filber v. State of Israel*, (Nov. 1, 1999)

[24] HCJ 551/99 *Shekem Ltd. v. Director of Customs and VAT*, IsrSc 54(1) 112 (1999)

[25] 5860/16 *Facebook Inc. v. Ben Hamu*, (May 31, 2018)

[26] LCA 1239/19 *Shaul v. Nayadli Communications Ltd*., (Jan. 8, 2020)

[27] HCJ 11163/03 *Supreme Monitoring Committee for Arab Affairs in Israel and others v. Prime Minister of Israel*, IsrSC 61(1) 1 (2006) [https://versa.cardozo.yu.edu/opinions/supreme-monitoring-committee-arab-affairs-israel-and-others-v-prime-minister-israel]

[28] HCJ 5100/94 *Public Committee against Torture v. State of Israel*, IsrSC 53(4) 817 (1999) [https://versa.cardozo.yu.edu/opinions/public-committee-against-torture-v-israel]

[29] LCA 3145/99 *Bank Leumi v. Hazzan*, IsrSC 57(5) 385 (2003)

[30] CA 6821/93 *United Mizrahi Bank v. Migdal Cooperative Village*, IsrSC 49(4) 221 (1995); IsrLR 1995 (2) [https://versa.cardozo.yu.edu/opinions/united-mizrahi-bank-v-migdal-cooperative-village]

[31] HCJ 10203/03 *Hamifkad Haleumi v. Attorney General*, IsrSC 62(4) 715 [https://versa.cardozo.yu.edu/opinions/hamifkad-haleumi-v-attorney-general]

[32] HCJ 2442/11 *Haim Shtanger, Adv. v. Speaker of the Knesset*, IsrSC 66(2) 640 (2013) [https://versa.cardozo.yu.edu/opinions/shtanger-v-speaker-knesset]

[33] HCJFH 9411/00 *Arco Electric Industries Ltd. v. Mayor of Rishon LeZion*, IsrSC 63(3) 41 (2009)

[34] MApp 1190/18 *Ethics Committee of the Tel Aviv District of the Bar Association v. David Yedid, Adv.*, (March 28, 2019)

[35] HCJ 442/71 *Lansky v. Minister of the Interior*, IsrSC 26(2) 337 (1972)

[36] CA 5739/18 *Operators of the Website www.oligarchescorts.com v. State of Israel*, (Oct. 15, 2018)

[37] CrimFH 7383/08 *Ungerfeld v. State of Israel*, (July, 11, 2011)

[38] LCrimA 5991/13 *Segal v. State of Israel*, (Nov. 2, 2017)

[39] LCrimA 7052/18 *State of Israel v. Rotem*, (May 5, 2020)

[40] HCJ 4455/19 *Tebeka Advocacy for Equality and Justice for Ethiopian Israelis v. Israel Police*, (Jan. 25, 2021)

[41] HCJ 1901/94 *MK Landau v. Jerusalem Municipality*, IsrSC 48(4) 403 (1994)

[42] HCJ 151/11 *Ruth and Emanuel Rackman Center for the Advancement of the Status of Women v. Minister of Justice*, (Dec. 27, 2011)

[43] HCJ 384/82 *Pachmas Metal & Plastic, Registered Partnership from Ein Horesh v. Minister of Finance*, IsrSC 37(4) 297 (1982)

The Supreme Court sitting as Hugh Court of Justice

Before: President E. Hayut, Deputy President H. Melcer, Justice A. Stein

Judgment

(April 12, 2021)

Deputy President H. Melcer:

1. The petition before the Court concerns the constitutionality of the activity of the Cyber Department of the State Attorney's office (hereinafter: the Cyber Department, or the Department) in regard to online network operators, content providers and other online platforms (hereinafter: online platform operators or operators) with whom the Department maintains contact in order to prevent publications that may violate Israeli criminal law.

2. In the framework of the petition, The Petitioners requested that an order nisi be issued against the Respondents, ordering them to show why the Cyber Department should not immediately desist from requesting that operators "voluntarily" remove content from the network.

I will now present the facts relevant to deciding the matter.

Background and summary of relevant facts

3. In September 2015, a cyber-enforcement unit was created in the Ministry of Justice (in the framework of the State Attorney's Office). It's creation "derived from the need for a focused effort to confront crime and terror in cyberspace, after identifying a sharply rising trend in cybercrime" (from the 2015-2016 Summary of the State Attorney's Office – Appendix P/1 of the petition; hereinafter: the 2015 Summary). As arises from the preliminary response of the Respondents listed in the heading, the tasks assigned to the unit, which became a department, focused upon activity intended to reduce the harms and dangers caused by crimes perpetrated online, in two separate enforcement tracks that will be described below.

The statutory enforcement track

4. The first enforcement track, which is not central to the present petition, concerns proceedings conducted by the Cyber Department by virtue of the Authorities for the Prevention of Committing Crimes through use of an Internet Site Law, 5777-2017 (hereinafter: Authorities for the Prevention of Crimes Law, or the Law), whose purpose is to prevent the commission of certain offenses, or the exposure of internet users to certain offenses committed by means of internet sites, by means of judicial orders (above and hereinafter: *the statutory enforcement track*). The Cyber Department's activity conducted pursuant to the Law is consistent with the classic view of criminal enforcement in which the a *prosecutor*, as defined by the Law (who is one of the attorneys in the Department who, in accordance with sec. 1 of the Authorities for the Prevention of Crimes Law, has been so authorized by the Attorney General) applies to a District Court judge (so authorized by the President of the District Court) for an order instructing providers of access, searches and storage of content on the internet to remove or restrict access to content appearing on various internet sites, pursuant to the authority established therefor in the Prevention of Crimes Law (sec. 2 – 4 of the Law). This authority is specific to a number of criminal offenses perpetrated on the internet, such as: organizing or conducting illegal gaming, lotteries or betting (sec. 222 of the Penal Law, 5737-1977 (hereinafter: the Penal Law)), publishing pedophilic content (sec. 214(b) of the Penal Law), publishing prostitution services (secs. 202, 205A, 205C(a), 205D of the Penal Law), trafficking in dangerous drugs (secs. 13-14 of the Dangerous Drugs Ordinance [New Version], 5773-1973), an offence under sec. 7 of the Fight Against the Phenomenon of the Use of Dangerous Substances Law, 5773-2013, and internet activity by a terrorist organization (under the Counter Terrorism Law, 5776-2016).

In accordance with the Law, these restraining orders are contingent upon various constraints, including that a restriction of access will not be issued if the means for executing the order constitute eavesdropping under the Eavesdropping Law, 5739-1979, whose provisions apply to the matter.

5. In addition to the aforesaid, there are additional statutory provisions that grant the courts authority to order the removal of an advertisement, or restrict the publication of certain information, which are not specifically found in the Prevention of Crimes Law (e.g., publication

of the name of a complainant in regard to sex offenses (sec. 352 of the Penal Law), or a publication in contravention of the provisions of sec. 34 of the Adoption of Children Law, 5741-1981 (which prohibits publishing the identity of various actors related to the adoption procedure)). In regard to these provisions, the Cyber Department noted in its preliminary response that it only "informs" (the providers) of the fact that the offending content does not meet the restrictions under the relevant law or a judicial order issued thereunder.

6. In their preliminary response, the Respondents emphasized that the *statutory enforcement track* is not comprehensive, inasmuch as there is currently no coercive enforcement track that would allow the Cyber Department to act on the internet (subject to a court order) for the removal of additional publications that constitute other criminal offences, among them: content that incites violence, terror, or racism, or content that amounts to sexual harassment and threats. In this regard, it should be noted that the Respondents and others tried to advance legislation that would have granted the courts broader authority to remove harmful content published on the net, but for various reasons, those legislative initiatives did not come to fruition (see: Prevention of Committing Crimes by Means of the Internet (Removal of Content) Bill, 5778-2018; and Removal of Content from the Internet whose Publication Constitutes an Offense Bill, 5777-2016).

This need, and other reasons that will be presented below, led to the creation of an *additional, voluntary enforcement track*, which is the focus of the petition before the Court.

The voluntary enforcement track

7. The absence of general, explicit legal provisions granting authority to a judicial instance to order the removal of a publication that amounts to a prima facie criminal offense (beyond the Law, which was itself enacted only on July 26, 2017) led the State Attorney's office to formulate *another, additional* conception for criminal enforcement that *focuses upon the offense rather than its perpetrator*. In this framework, it concentrates its efforts upon *network platform operators*. This activity is the focus of the petition. The term *network platform* is a codeword for a variety of civil bodies, mostly very powerful multinational corporations that operate a variety of frameworks for net activity, including:

A. Online social networks that allow users to communicate with and be visible to other users, and inter alia, also share information, positions, and opinions (e.g., *Facebook*).

B. Online search engines that facilitate searching for and retrieving information available on the internet (e.g., *Google*).

C. Providers of hosting services for building and storing various internet sites. (In accordance with a work procedure appended to the Respondents' preliminary response, titled: "Treatment of unlawful contents published in cyberspace" (hereinafter: the Work Procedure)).

8. There would not appear to be any need to discuss the centrality of the above *online platforms*, which in our current digital age are a center for transmitting and exchanging views, and operate the space in which that discourse occurs. In the absence of regulatory legislation in the area, they also have the power to define the boundaries of the discourse and establish, inter alia, the rules for what is permitted and prohibited in all that concerns expression and the sharing of content on the net. Accordingly, each such *platform operator* establishes conditions for use or service, and "community rules" that apply to and obligate those seeking to use the social network or the search engine it operates. (See Prof. Balkin's article: Jack M. Balkin, *Free Speech is a Triangle*, 118 COLUM. L. REV. 2011 (2018) (hereinafter: Balkin, *Triangle*)).

In the framework of the preliminary response, the Respondents presented such rules, which were brought to its attention, that prohibit publication of content, including statements of intentions to commit violent acts, or support for terrorist organizations, as well as incitement and hate speech, or information likely to infringe the privacy of others. It further arises from the material presented to us that various *operators* also established a general prohibition in their "community rules" upon activity that violates local law. Common to all these conditions for use (or, at least, to all the *operators* whose community rules were presented to us) is that every user of the online platform, or any person exposed to the publication (whether a person, a corporation or a governmental authority) is afforded the possibility of reporting that a publication violates the platform's rules, and that the decision as to how to act after the *online platform operator* is informed of a publication that appears to be harmful is, apparently, given to the exclusive discretion of the platform operator.

Thus, for example, as the Respondents present it in their preliminary response, the community standards of the Facebook social network establish that a user cannot use the end-user services for a purpose "that is unlawful, misleading, discriminatory or fraudulent". The said company also has the power to deny or restrict access to content that constitutes a violation of the rules. In addition, the community standards of that company-operator establish various restrictions on content published on *Facebook*, and in regard to activity on that platform, inter alia, provisions in regard to publications that will not be permitted. Thus, for example, they establish a prohibition upon publishing threats that are likely to lead to "high-severity" violence, and declarations of intentions to commit violent acts.

These rules generally create a "Notice and Take Down" mechanism (and see: EA 8/21 *Shachar Ben Meir, Adv., v. Likud* [1], para. 86 (Feb. 27, 2019); and compare: EA 27/21 *Yisrael Beiteinu Faction v. Shamir Systems and Operators Ltd*. [2], paras 28-29 (Feb. 26, 2019)). By virtue of this mechanism, if the *network platform operators* receive notice of an alleged violation, they decide whether to leave the publication or remove it. Of late, it is possible to challenge a "take down decision", at least on *Facebook*, before a kind of "appeals committee" that has the authority to conclusively decide upon complaints concerning decisions to remove contents from the platform. In early 2020, the board of directors published the said appeals committees, and the rules and procedures that govern such "appeals" (see: OVERSIGHT BOARD BYLAWS (2021); and see: Evelyn Douek, *What Kind of Oversight Board Have You Given Us?*, U. CHICAGO L. REV. ONLINE 1 (2020)).

9. The *Cyber Department* thus operates on the above track of a "notice and take down mechanism". In the context of the matter before us, this is carried out in a manner agreed upon between the *Department* and the *relevant internet platform operators*, according to which, when the *Department* takes notice of information concerning a publication that, prima facie, violates Israeli law (whether included in the Prevention of Crimes Law, or not included in that Law), the staff of the Department refers the matter to the attention of the internet platform operators, by means of a structured mechanism for reporting harmful publications, that a prima facie offense is being committed on the infrastructure that it operates. The internet platform operators, in turn, address the report and decide, at their independent discretion, how to act and what to do in regard to the said report – whether to restrict access to that publication, remove it, block the user who

violated their "user rules" in regard to publication, or not to take any action. Occasionally, according to the 2015 Summary, the report leads the internet platform operators to suspend or remove the user who published the prohibited expression that was the subject of the report.

10. The present petition concerns the initiating of the said referrals by the Cyber Department to the internet platform operators in regard to alleged offenses of the aforesaid types that are perpetrated on the net. As noted in the Respondents' preliminary response and detailed in the Work Procedure that regulate its activities, the Cyber Department periodically receives various requests regarding publications disseminated on the internet from various governmental sources (most of the requests come from security agencies). In accordance with he Work Procedure, upon receiving the request, a preliminary examination is conducted in regard to the existence of a prima facie offence in the publication. The examiner sends its recommendation for further action, and the matter is re-examined by a designated attorney in the Department. Pursuant to the Work Procedure, in appropriate cases, the decision on the request is sent for the personal approval of the Department's director when the request concerns a publication that relates to senior civil servants, including employees of the Ministry of Justice and judges, or when there are doubts as to the lawfulness of the publication, or where the publication raises some other material question. Additionally, when the matter falls within a departmental area of responsibility and raises a question of interpretation, the Cyber Department consults with that department. In addition to the above, prior approval by the State Attorney is required on the following matters: taking action in regard to a publication concerning an elected official, requests in regard to content that relates to or is directed at particularly senior public servants, or in precedent setting cases or case that would involve the expansion of the activities of the Cyber Department.

The above enforcement mechanism is referred to above and hereinafter as the *voluntary enforcement mechanism.* It is additional to the *statutory enforcement mechanism,* and in general (in the appropriate cases established in the Law) precedes it and renders it superfluous when results are achieved.

11. In accordance with the Work Procedure, the Cyber Department considers a request to the internet platform operators only when three cumulative conditions are met:

A. The content constitutes a prima facie offense under Israeli law;

B. The content violates the internet platform's term of use and there are additional considerations for reporting or referring it to the internet platform, such as: the actual circulation of the publication, its severity, the date of publication, the "viral" potential of the publication, or how the publication is likely to be interpreted by those who receive it.

C. The balancing conducted by the Cyber Department between the values of freedom of expression and access to information on the net as opposed to the values of the constitutional right to privacy, dignity and the reputation of the subject of the publication, as well as the public interest, justifies issuing the report so that the online platform operators will consider whether to remove the publication rather than leave it on the net.

12. It would be appropriate to note at this juncture that, as arises from the arguments of the parties before us, the Work Procedures (some of which also concern enforcement actions under the Prevention of Crimes Law) have not yet been published. I, therefore, find it appropriate to note, already at this stage, that I believe it would be proper that the Work Procedures be brought to light in the manner that, for example, the Attorney General's Guidelines are published (with the exception of those parts of the Procedures that concern state security or contacts between the Department and security agencies). See: Dalit Ken-Dror Feldman & Niva Elkin-Koren, *Transparency in the Digital Environment: Governmental Removal of Illegal Speech via Online Platforms*, 25 HAMISHPAT 25, 42-43 (2020) (Hebrew) (hereinafter: *Ken-Dror Fedman & Elkin-Koren*).

13. In their preliminary response, the Respondents stated that the Cyber Department's activity in the framework of the *voluntary enforcement mechanism* primarily focuses on reports and requests in regard to publications concerning the activities of terrorist organizations and incitement to violence and terrorism (according to the statement, this represents some 99% of the reports referred to the internet platform operators in 2018). The reports to the internet platform operators in regard to such contents point out that such publications appearing on those platforms amount, prima facie, to offenses of incitement and terror, identification with a terrorist organization, and so forth, and would appear to violate the "community rules" of the platform. The Respondents

further note in their preliminary response that it is the estimation of the security agencies that a significant part of the terrorist activity perpetrated in the course of the "knife intifada" beginning in October 2015 was influenced by increasing consumption of social-network contents that incited violence and terror. This led to a need to act to reduce exposure to those publications on internet platforms by reporting to the internet platform operators that they amounted to prima facie criminal offences and deviated from the platform's Terms of Use.

14. In addition, it was explained that the Department also operates in the area of harm to minors, in cooperation with the National Child Online Protection Bureau, when it reports instances of violence and crime against children and youths (that amount to prima facie offenses of threats, sexual harassment, and infringement of privacy) on the internet to the internet platform operators. According to what was submitted, the Cyber Department also sends reports in regard to sexual images and videos that constitute prima facie offenses under the Prevention of Sexual Harassment Law, 5758-1988.

15. Another area in which the Cyber Department operates is the prevention and restriction of harmful advertising that amounts to prima facie offenses of threats, infringement of privacy, or harassment of "certain types" of civil servants, where the advertisements can potentially deter the civil servants from exercising their authority and perform their duties, as part of the defensive shield that the state affords its employees, and when required for the proper functioning of the civil service. The Respondents noted that the Cyber Department acts with "great restraint" in this area, in view of the importance of public accountability of civil servants and the civil service in general. Thus, reports in this area are sent only in "the most extreme cases", and at times, only after obtaining the consent of the State Attorney and given the existence of a real threat of harm to the public interest and the proper functioning of the civil service (we should note here that in all that relates to harmful publications against judges, the Courts Administration established Procedure 12-2019 of the Administrator of the Courts in the matter of "Work Procedures and Supervision for Treating Harmful Publications on the Internet" (2019), which is intended to promote, in cooperation with the Cyber Department, the removal or restriction of content that amounts to danger, humiliation, debasement, or harm to holders of judicial appointments (contempt of court constitutes an offense under sec. 255 of the Penal Law).

16. Lastly, the Respondents' preliminary response noted that the Cyber Department also acts to protect the integrity of Knesset elections. Thus, for example, in the last elections (for the 21st and 22nd Knessets), which took place after the Department was established, it was agreed – with the joint consent of the Central Elections Committee and the Attorney General – that reports would be sent to internet platform operators in regard to accounts of computer-generated fictitious users ("bots"), particularly when the identity of the person operating them (if there is one) is unknown, and in regard to fraudulent user accounts or human impersonators. All of the above was carried out in special circumstances and under restrictive conditions established "with great caution". It is important to note in this regard that in all that concerns *voluntary enforcement* actions connected to the election process, the Department's referrals concern *technological actions prohibited* by the criminal law, and not publications that, by virtue of their content, amount to prima facie offenses, and for the enforcement of restraining orders by virtue of sec. 17B of the Election (Means of Propaganda) Law, 5719-1959.

17. There would not appear to be any disagreement among the parties as to the dimensions and effectiveness of the activities of the Cyber Department. As noted in the Cyber Department's reports, upon which the parties rely: in 2016, the Department sent 2,241 reports, regarding which 76.5% of the publications were removed (in whole or in part); in 2017, reports were sent concerning 12,351 publications, regarding which 88% of the publications were removed; in 2018, reports were sent concerning 14,283 publications, of which some 92% of the reported publications were removed; in 2019, 19,606 reports were sent, regarding which some 90% of the reported publications were removed. It should be noted, as the Petitioners argue in their response, that it cannot be inferred from this that the data reflects the number of reports or requests for removal of content, inasmuch as it is possible that each said report comprised more than one link to harmful content (in fact, the 2015 Summary Report notes that, at times, each such report includes tens and even hundreds of links).

The above data also demonstrate the widening of the phenomenon of prohibited content on the networks.

As for the identity of the internet platform operators to whom the Respondents send requests – the Cyber Department's reports show that in 2018, 87% of the reports were sent to

Facebook, 8% to Twitter, and the remainder were sent to other internet platform operators (e.g., YouTube, Instagram, and Google).

Arguments of the parties in the petition before the Court

18. This petition was filed after the requests sent by the Petitioners over the course of the last few years to bring about the cessation of the Respondents' *voluntary enforcement mechanism* did not succeed. In the framework of the petition, the Petitioners argue that the manner in which the mechanism is employed can potentially infringe the constitutional rights to due process and freedom of expression, while not meeting the conditions of the "Limitations Clause" established in sec. 8 of Basic Law: Human Dignity and Liberty. Their main argument in this regard concerns the lack of express statutory authorization to act in this manner, such that the *voluntary enforcement mechanism* operates, in their opinion, in breach of fundamental principles of constitutional and administrative law. In this regard, it is further argued that we are concerned with a mechanism that grants the prosecution (the State Attorney's Office) broad authority to delineate the bounds of freedom of expression, in that it is the Department that decides that certain content is unlawful, without turning to the courts and without granting a right to be heard.

In the Petitioners' view, it is uncontestable that a referral initiated by the Respondents to the internet platform operators for the purpose of removing content is, in fact, governmental activity that requires express statutory authorization, inasmuch as even if the Cyber Department's action does not amount to a coercive order, every action by the Department constitutes a governmental action that requires authorization. In the absence of such authorization, the Court must order the cessation of the Cyber Department's activity, even without a showing of the extent of the violation of the protected rights and the activity's conformance to the other conditions of the Limitations Clause established in sec. 8 of Basic Law: Human Dignity and Liberty.

In the support of their arguments, the Petitioners referred to two petitions that, in their view, treated of related subjects, as follows:

The *first* is AAA 3782/12 *Tel Aviv-Jaffa District Commander v. Israel Internet Association* [3] (hereinafter: the *Israel Internet Association* case), which held (*per* Justice U. Vogelman, President A. Grunis concurring, Justice N. Sohlberg dissenting) that the authority of a police

district commissioner to order the closure of a gambling site does not extend to internet providers in regard to an online gambling website that violated sec. 229(a)(1) of the Penal Law (as it then stood), inasmuch as the provision of the said law does not expressly grant statutory authority to the District Commissioner to order third parties (providers of access who are not the website operators) to block an online gambling website.

The *second* is LCA 4447/07 *Mor v. Barak I.T.T. [1995] International Telecommunications Services Corporation* [4] (hereinafter: the *Mor* case), which held that in the absence of a legislative framework that creates a possibility for ordering a provider of internet access to expose the identity of an anonymous user, it should not be pursued by "judicial legislation" (see, *ibid*., at p. 688).

19. As for the possibility that the Cyber Departments authority to act in a "voluntary" manner is granted by virtue of the government's residual power under sec. 32 of Basic Law: The Government, the Petitioners' take the view that such authority does not apply to cases in which the exercise of the authority results in a violation of basic rights. In this regard, they referred to HCJ 8600/04 *Shimoni v. Prime Minister* [5], 687, and HCJ 6824/07 *Manaa v. Tax Authority* [6] (hereinafter: the *Manaa* case) (regarding the enforcement authority). In addition, the Petitioners also rejected the possibility that the Cyber Department's authority is granted by virtue of the auxiliary powers set out in sec. 17(b) of the Interpretation Law, 5741-1981 (hereinafter: the Interpretation Law), which provides: "Any empowerment to do or enforce the doing of something implies the conferment of auxiliary powers reasonably required therefor". In the opinion of the Petitioners, that provision cannot support the Respondents, inasmuch as in the framework of the reports that the Department sends, it, in practice, trespasses the boundaries of the courts, which alone, according to the Petitioners, hold the authority to decide, after hearing the parties, whether or not a particular publication constitutes a crime.

20. In addition to the above, the Petitioners also argue extensively in regard to the manner in which, in their opinion, the voluntary enforcement mechanism violates constitutional basic rights, first and foremost, the right to freedom of expression, which they believe, under the case law of this Court, is broad enough to encompass even harmful expression that rises to the level of incitement to violence or racism. In this regard, they cited HCJ 399/85 *Kahana v. Broadcasting Authority Management Board* [7]. In this regard, it is argued that removing and restricting the said publications not only prevents the publisher from expressing his opinion freely, but also harms the

other users of the internet online platforms due to restricting their access to the information that has been restricted or removed. They also argue that the voluntary enforcement mechanism is also indicative of a violation of the separation of powers inasmuch as it represents a situation in which the "last word" in all that regards the lawfulness of any publication rests in the hands of an administrative agency or the internet platform operators, and not the court, which is normally supposed to decide such matters. It is further argued that removal of the publication by the internet platform operators (pursuant to a request by the Cyber Department) constitutes a violation of the right of users to due process. Moreover, the Petitioners argue that there are additional defects in the Respondents' activities, such as: not maintaining an appropriate record in regard to publications for which reports were sent by the Department to internet platform operators.

21. As opposed to what is argued in the petition, the Respondents are of the opinion that the enforcement procedure that is the subject of the petition is *a completely voluntary procedure* that should not be seen as a governmental act, *per se*, and that the discretion in regard to removal or other steps pursuant to the report is entirely in the hands of *the internet platform operators alone* (inter alia, the Respondents rely in this regard upon HCJ 5185/13 *A. v. Great Rabbinical Court* [8], which treats of the "Rabbeinu Tam sanctions"[1] (hereinafter: the *Rabbeinu Tam Sanctions Affair*)). This argument was expanded upon elsewhere by the founder and head of the Cyber Department, Dr. Haim Vismonski, who said as follows:

> In practice, an act on the voluntary-consensual level is not an exercise of authority in the sense of an order or an obligatory demand. In practice, it is a request based upon the understanding that the service provider will examine it in accordance with its own terms of use and criteria. (Haim Vismonski, *Alternative Enforcement of Expression Offenses in Cyberspace*, LAW, SOCIETY & CULTURE 691, 725 (2018) (Hebrew).

The Respondents further point to the unique advantages of the Cyber Department over persons (harmed individuals) or other bodies that might serve as reporters of offenses of the type under discussion in cybernetic space, and the great benefit of the Department's actions for the public interest. It is argued in this regard that in view of the fact that the Department is a "repeating player" that is proficient in the terms of use of the online platforms, and keeps abreast of changes

[1] Sanctions established in the 12th century by Rabbi Jacob ben Meir "Tam", which may be imposed upon a "recalcitrant husband" who refuses to grant a divorce.

to those terms from time to time, it enjoys an inherent advantage and reliability in operating the voluntary track. It is, therefore, appropriate that it speak on behalf of other governmental bodies, as well as for plain citizens, who cannot contend on their own with internet platform operators and with those who abuse the platforms or access to them. It is thus argued that the Department serves the public in general. In this regard, the Respondents emphasize that the referrals to internet platform operators are made only when the publications meet the criteria set out in para. 11 above, and when it is appears that the publications conspicuously violate the Terms of Use of the online platforms.

22. Moreover, the Respondents point out that the Cyber Department has been granted the status of "reliable reporter" by several of those internet platform operators, which gives examination of the Department's reports precedence over others, and the speed of the response results in reducing the harm (however, according to the Respondents, that does not influence the manner of examining the report submitted to the internet platform). In addition, the Respondents note that due to its nature, in view of the resources and significant knowledge at the disposal of the various governmental organs, it is important to maintain the voluntary enforcement mechanism as a means for which there is currently no alternative for reporting and acting against acts of impersonation, fraud or other criminal offenses perpetrated on the internet. Moreover, due to the location of such criminal acts – generally beyond the borders of the state – and given the limited international judicial authority, in the absence of the voluntary enforcement track, "bad actors" in cyberspace would continue to succeed and their acts would not be subject to enforcement.

23. Parenthetically, but not of marginal importance, the Respondents argue that the petition should be dismissed for not meeting the threshold requirements for filing a petition due to a substantial factual deficiency and for not joining relevant respondents – the internet platform operators. The Respondents argue that joining those parties could shed light on the independent discretion that they exercise in regard to the Department's referrals, as well as other subjects comprised by the petition, which will be explained below.

Additional developments

24. Following the hearing of the parties to the petition on Aug. 3, 2020, we ordered the Respondents to supplement their arguments, inter alia, in regard to parallel arrangements in other countries.

25. The Respondents did so, and in that context, presenting examples from comparative law, they reiterated their arguments that internet platform operators have broad discretion in deciding whether or not to remove publications, and that the Respondents' authority to act in the framework of the voluntary mechanism is grounded in their power to enforce the rule of law and to protect the public interest. Therefore, in their view, they are permitted to act to bring about the removal of harmful internet publications that appear to violate criminal law, and that this is in accordance with the auxiliary power granted to them as an administrative agency (in our case, in reliance upon sec. 17(b) of the Interpretation Law). The Respondents also repeated their arguments that the reporting of publications overwhelmingly concerns instances of expression that can harm state security, and that the referrals are made subject to the fulfilment of a number of cumulative criteria, demonstrating that the governmental agencies and the State Attorney's Office will only act in this area in exceptional, extreme circumstances.

26. Turning to comparative law, it is argued that a number of democratic states and international bodies also address this subject through *voluntary enforcement*, without any specific, express authority in primary legislation, and that the world now agrees that this is the only effective means for the removal of violating publications from the internet, and that otherwise a situation of total anarchy would emerge, in which everyone would do as he sees fit, while violating local criminal law. In this regard, it is further argued that international arrangements and regulatory guidelines applicable under European law serve as the source of authority for voluntary enforcement by states and various bodies in the European Union in the matter of removing harmful publications from the internet. Examples of this were provided from France, Belgium, Spain, Germany, and Great Britain.

Thus, for example, in 2016, the European Union signed an arrangement with Facebook, Microsoft, Twitter, and YouTube that outlines the treatment of hate publications by means of the internal reporting mechanisms of the internet platforms. These arrangements were later joined by such companies as Instagram, Snapchat, and TikTok. Pursuant to the arrangement, various bodies

in the European Union were recognized as "reliable reporters" – mostly third-sector organizations, and some state agencies. According to the Respondents, this arrangement constitutes a framework for the activity of European states on the voluntary track, although some of them have specific, internal arrangements.

The Respondents also noted the existence of coercive arrangements in some European states, which do not refer to the possibility of voluntary action *even though it takes place*, such as the activity of the Swiss Federal Office of Police, for example (in Belgium, there is a governmental agency whose authorities are defined in a cooperation agreement between the federal government and the districts and communities. This agreement grants the governmental agency general authority "to take legal action").

As opposed to this, it was noted that the law enforcement agency of the European Union, Europol, acts on the voluntary level by virtue of express authorization in reg. 4(1)(m) of Europol Regulation 2016/794. In France, the Central Office for the Fight against Crime linked to Information Technology and Communication (OCLCTIC) is authorized by sec. 1 of an order pursuant to the counter-terrorism law (loi n° 2004-575 du 21 juin 2004, amended in 2014) to request that search engines or hosting service providers remove content that amounts to certain criminal offenses, such as encouraging terror or pedophilia, without need for a judicial order.

27. At this point we should note that, prior to the hearing, requests to join the proceedings were filed by Lori Shem Tov and the Movement for Freedom of Information (hereinafter: the Movement), as noted in the heading.

The request of the Movement (which sought to join as an amicus curiae) is primarily based upon the argument that the question of authority at the focus of the petition should also be examined in light of the fact that, according to the Movement, the Cyber Department operates without transparency, and this is expressed by a lack of *documentation* of the content of the publications that the Cyber Department seeks to remove (according to the Movement, this can be inferred from the reply it received to its freedom of information request of Nov. 1, 2019). It is argued that this, inter alia, raises a fear that the Respondents' referrals are "slanted and tainted by discrimination", or arise, in part, from imprecise translation of the publications concerned. In addition, it is argued that there is a lack of clear guidelines for structuring the Cyber Department's

discretion prior to submitting a report to the internet platform operators. Moreover, the Movement argues that the transparency reports published by the Department are insufficient, and that they should include much more data, such as: the characteristics of the report sent to the operators and the demands therein (whether the agency requests the blocking of content, or, for example, also blocking the user); noting the relationship of the publications to the residents of the state, insofar as possible; clarification of whether the Department acts when the policy rules of the platform are violated, even if the publication does not constitute an offence, and so on.

Lori Shem Tov (who did not attend the hearing before the Court, although she was invited), noted in her request to join that she wished to join as a petitioner because she claims to have been harmed by the conduct of the Cyber Department, and that she believes that the Department's actions led to the removal of publications from the website she operates, on the claim that they constituted prima facie offenses against public servants.

28. After examining the said requests to join, we decided to suffice with examining them without granting the requests to join, inasmuch as, inter alia, we have in any case decided to deny the petition for the reasons that will be set forth below. Moreover, in regard to the said requests to join, including the operators as respondents is *absolutely necessary*, and the fact that they chose not to do so is a *fundamental defect* under the circumstances.

Discussion and Decision

29. After examining the parties' briefs and appended documents, including the Cyber Department's Work Procedure, and after hearing the arguments of the parties' attorneys in the hearing and reading the supplementary briefs, I am of the opinion that the petition should be denied, subject to a number of comments for the future that the Respondents should consider, and so I recommend to the President and my colleague.

30. Before delving into the various aspects that must be decided, I will note fundamental principles, which are no longer very new, in regard to the arena addressed by the petition, in which the Cyber Department operates – the *internet*. I will not elaborate upon the great blessing bestowed by technology in general, and upon the fundamental changes to the world and humanity following

the arrival of online platforms – the narrowing of gaps, the availability of various services to individuals and society, the empowerment of marginalized populations, the enhancement of freedom of information, communication, expression, the press and association by connecting the close to the far, etc. (see the groundbreaking article by Prof. Niva Elkin-Koren, *The New Intermediaries in the Virtual Public Forum*, 6 MISHPAT UMIMSHAL pp. 381-420 (2003) (Hebrew)).

As opposed to this, the petition before the Court treats of the manner in which the virtual space provided by the internet can serve as fertile ground for poisonous plants, weeds, and rotten fruit (compare: MApp 2065/13 *A. v. State of Israel* [9]). In this regard, the internet provides malicious actors with a platform for perpetrating crimes by "remote control", in far wider dissemination than was available in the "old" world prior to the internet revolution, while the possible ill effects of their acts may embrace sectors and communities that were not previously exposed to the harmful activity.

It would appear that this new sphere of activity therefore also requires means of enforcement that differ from the previously accepted methods, which hold the potential for quick, effective frustration of criminal activity on the internet. However, we should emphasize that this petition does not primarily concern adapting the means to the objective and examining the possibility that granting court orders in appropriate cases (pursuant to the statutory enforcement track) constitutes a less harmful means than the voluntary enforcement mechanism.

The petition before us concerns the question of the *authority* to conduct the voluntary activity in the manner and form employed by the Cyber Department. I will, therefore, address these arguments in their order, below, but I will first examine the *preliminary arguments* raised against the petitioners, which claimed that the petition lacks a sufficient factual foundation, and that the fact that the Petitioners did not join the internet platform operators as respondents requires the dismissal of the petition.

Insufficient Factual Grounds

31. In my opinion, it was possible to dismiss the petition on the basis of the *absence of sufficient factual grounds* for the argument that the Department acts without authority.

In practice, the data submitted with the petition do not testify to the scope of the harm to the values of freedom of speech and access to information (to the extent that they do not amount to a crime). Of course, no one denies that the Cyber Department's activity may ultimately cause the removal of various criminal publications from the internet. However, even if that is so, it is not at all clear to what extent the Cyber Department's voluntary enforcement activity leads to a violation of protected rights, including the freedom of speech of the holders of the rights, in regard to publications that are not unlawful. There is no need to elaborate upon the fact that a fundamental condition of the protection granted under Basic Law: Human Dignity and Liberty is that the *object of the claimed harm* to the constitutional right be a "person" (see sec. 1 of the Basic Law, which speaks of the fundamental rights of *the human being* in Israel, and the end of sec. 2, which establishes: "There shall be no violation of the life, body or dignity of any *person as such*. (emphasis added – H.M.)). The reality provided by the internet shows that, at times, in order to prove that a fundamental right was *violated* (which is at the heart of the Petitioners' arguments, along with the claim of lack of authority), the petitioner must show that the object of the harm is, indeed, a "person" (and in my view, impersonators of people, like avatars and bots, are excluded).

In other words, avatars and robots do not enjoy human rights, not to mention that some of those robots are not even operated by humans but by artificial intelligence. In this regard, see: RYAN ABBOT, THE REASONABLE ROBOT: ARTIFICIAL INTELLIGENCE AND THE LAW (2020); Harry Surden, *Artificial Intelligence and Law: An Overview*, 35 GA. ST. U. L. REV. 1305 (2019); Ryan Calo, *Artificial Intelligence Policy: A Primer and Roadmap*, 51 U.C.D. L. REV. 399 (2017).

32. In the matter before us, concerning the area of the internet in which varied and various entities, organized in different configurations, operate (among them, foreign governmental actors, "bot" networks, forged accounts, and impersonators), a *minimal* evidentiary basis for a claimed violation of freedom of expression is required, particularly in regard to a publication that does not constitute a crime. Note that I do not think that the voluntary enforcement actions of the Cyber Department are incapable of potentially violating the activity of certain individuals, whether in Israel or abroad. However, in the absence of a specific example by the Petitioners that such voluntary enforcement activities, as such, affected any of them (assuming that no prima facie offense was committed), it is difficult to accept the Petitioners' argument that the entirety of the Cyber Department's voluntary enforcement activities harm the Petitioners as such, and it is

difficult to identify which aspects of the Department's many activities require express statutory authority (compare: HCJ 6972/07 *Akiva Laxer,Adv. v. Minister of Finance* [10]). In this sense, the petition is not ripe.

33. As described above, it appears from the Cyber Department's data that the overwhelming majority of referrals by the Department to online platform operators concerns publications related to *terrorist acts and extreme violence*. In my view, the fear expressed in the Petitioners' arguments that under the cover of this enforcement activity – which almost entirely concerns the protection of national security – the government also contends with political messages protected within the bounds of freedom of expression *was not proven*. If such were the case, it is clear that express, concrete authorization would be required for the agency's actions in such circumstances. The problem is that other than the Petitioners' general arguments of principle, no trace of evidence was brought for the conjecture that publications that pose a challenge to freedom of speech were blocked under the excuse of preventing offenses of incitement to violence or terror. Moreover, in the absence of contradictory evidence, it may well be the case that a large part of the Cyber Department's activity concerns publications that are not produced by any human subject, but rather a *computerized object* (robot), or a widespread system of hostile users who seek to promote various unlawful messages.

34. Another uncertainty, which also cannot be examined in the framework of the present petition due to a lack of adequate data and the fact that the point was not argued by the parties, is the scope of the applicability of Basic Law: Human Dignity and Liberty to expression concerning Israel by users who *are not* citizens or residents of Israel, or who live in the country or have some other territorial connection to it. In my view, it is highly doubtful if, for example, a publication by a person outside of Israel that calls for violent action against the Israeli embassy in his country, or against another Israeli target there, is indeed a publication that must be examined in accordance with the constitutional balancing required under of Basic Law: Human Dignity and Liberty. This issue was not developed by the parties, although it may be that the reason for the failure to address this issue also derives from the lack of data held by the parties, or the difficulty of identifying the locale and name of a person publishing on the internet.

35. The above notwithstanding, I did not find that the petition should be dismissed *in limine* for an insufficiency of factual foundation, but it did make it difficult to issue an order nisi over the entire matter, and contributed to the dismissal of the petition for other reasons that will be presented below.

Failure to join relevant respondents

36. Another reason for why it may have been correct to dismiss the petition *in limine* concerns the failure to join relevant respondents. As noted above, the Petitioners (and those requesting to join) refrained from naming the online platform operators as respondents, and it would seem that this is to their detriment. As will be explained, the question of the exercise of discretion by those bodies is of no minor consequence for the questions at the focus of these proceedings. The issue of whether reporting harmful publications is a governmental act is significantly contingent upon how and to what extent the multi-national operators are independent, and whether their discretion relies upon their own local law or upon Israeli law, or only upon their own Terms of Use.

37. In the course of the hearing, the Petitioners were asked to explain the failure to name the online platform operators as respondents, but they provided no adequate explanation. In my opinion, that was sufficient for dismissing the petition *in limine*, inasmuch as had the online platform operators been joined as respondents, their arguments could have shed light on some of the Petitioners' central arguments.

Adding Respondents at a later stage, after the Petitioners knowingly chose not to do so, is unacceptable (and compare: HCJ 84/82 *Histadrut Po'alei Agudat Yisrael v. Minister of Religious Affairs* [11]; HCJ 828/90 *Likud Faction of the Haifa Municipal Council v. Haifa Municipal Council* [12]; and see: RAANAN HAR-ZAHAV, PROCEDURE IN THE HIGH COURT OF JUSTICE, 34-35 (1991)).

38. The preliminary defects in the petition are, indeed, severe. However, due to the *substantive arguments* raised in regard to the activity of the Cyber Department, the importance of the matters raised in the petition, their consequences, and their raising a matter of first impression, I will address the Petitioners' arguments on the merits so as not to leave the constitutional and administrative law issues hanging in midair.

I will, therefore, address the issues from first to last.

The question of authority

39. The main argument raised by this petition concerns the constitutionality of the voluntary enforcement policy in the absence of express statutory authority, in the opinion of the Petitioners. This argument derives from the principle of rule of law, which establishes (inter alia) that a governmental agency must act on the basis of statutory norms (see: HCJ 1/49 *Bejarano v. Police Minister* [13]; LCrimA 10141/09 *Ben Haim v. State of Israel* [14]). It is argued that the Cyber Department's actions to remove what it deems unlawful forms of expression by means of reporting them to the online platform operators constitute governmental enforcement that is prohibited in the absence of express statutory authorization, in view of the rule-of-law principle and the principle of administrative legality.

The Petitioners also argued that this situation at least appears to contravene the normal criminal-procedure distinction between the investigative authority and the prosecution. Thus, for example, sec. 59 of the Criminal Procedure Law [New Version], 5742-1982, authorizes the police to conduct investigations, while sec. 60 of the said law instructs the police to deliver the investigative material to the duly authorized prosecutor. In the present case, it is argued that the examination is conducted by the Cyber Department (in a manner somewhat akin to the police authority to initiate an investigation if it becomes aware of a crime, pursuant to the said sec. 59), and argued that it is also the "prosecutor", i.e., the body that applies to the relevant private body (the online platform operators) to exercise its discretion whether or not to remove the publication.

40. As described above, the Government Respondents countered in this regard that it is difficult to view the Cyber Department's actions as constituting an exercise of governmental power, inasmuch as the online platform operators exercise exclusive discretion in the matter, whereas its actions are limited to a *voluntary* application to the online platform operators, which therefore lacks the force of an administrative act of consequence.

41. On the face of it, the Respondents would appear to be correct that in the absence of a coercive governmental act, the question of authority does not generally arise. However, it seems to me that the Respondents erred in categorizing the Cyber Department's activity and its initiation

of referrals as acts that lack any governmental force, and their opinion that, as such, they do not fall within the purview of the principle of administrative legality, and do not require any statutory authorization. In my opinion, the Respondents were imprecise in sufficing with laconically citing the fact that we are concerned with a voluntary act for which the discretion on enforcement is entirely left to an external (private) body. Nevertheless, I am of the opinion that the Cyber Department's activity does, at present, have adequate authorization.

I will clarify this point.

42. To identify what constitutes a "governmental act" that is subject to the principles of administrative law, it not enough that the act in question is seemingly performed "voluntarily", or that it, itself, lacks any operative force. Indeed, as I will explain, an examination of the very many functions fulfilled by the public administration reveals that many of them are not addressed in specific legislation, yet there is no question that they are, nevertheless, at the heart of the role that a properly functioning state is required to fulfil, and therefore have a statutory basis.

In his book ADMINISTRATIVE AUTHORITY, vol. I, 419 (2nd expanded ed., 2010) (Hebrew) (hereinafter: ZAMIR), Prof. Zamir describes this as follows:

> In practice, the scope of authority granted to the government is far broader than the scope of the specific authorities that the statutes expressly grant it. Many of the functions imposed upon the government, among them basic functions of any government, and the authority required to carry them out, are not mentioned at all in the law. This is dictated by reality. The legislature cannot, and is therefore not asked, to arrange all of the all-embracing areas of governmental activity, and expressly establish the necessary authority for each individual area. The result is that the government conducts a wide-ranging variety activity that lacks an express foothold in the law. Such are, for example, almost all of the activities of the Ministry of Foreign Affairs, the Ministry of Construction and Housing, the Ministry of Immigrant Absorption, and the Ministry of Culture. Other ministries largely act on the basis of laws, but even among those, you hardly find a ministry whose functions are not partly – whether to a small or large extent – performed without express support in the law. Here are but a few of the many examples: The Government Press Office, professional training institutions, tourist information offices, research institutes, importing essential food items, The Institute of Advanced

> Judicial Studies. Sometimes, such activity is ancillary, so to speak, to some other activity, as if it were an auxiliary function of an activity authorized by law, but not infrequently, it stands alone, apparently without any supporting law. *How does this situation conform with the principle of administrative legality? The answer is provided by sec. 32 of Basic Law: The Government. This section establishes: "The Government is authorized to perform in the name of the State, subject to all laws, any act, which is not assigned by law to another authority"* (*ibid*., pp. 418-419; emphasis added – H.M.).

And see: HCJ 2918/93 *Kiryat Gat Municipality v. State of Israel* [15], 841; HCJ 5128/94 *Federman v. Minister of Police* [16], 651, *per* President Shamgar, before an expanded panel (hereinafter: the *Federman* case); HCJ 8600/04 *Chair of the Hof Azza Regional Council v. Prime Minister* [17], 682-683; HCJ 11163/03 *Supreme Monitoring Committee v. Prime Minister* [18], para. 6 of the opinion of Deputy President M. Cheshin; and also see: MARGIT COHN, GENERAL POWERS OF THE EXECUTIVE BRANCH, (2002) (Hebrew) (hereinafter: COHN).

We thus see that in order to evaluate the character and nature of the administrative activity before us, we must review some of the case law that constitutes the foundation of our constitutional and administrative system.

43. In categorizing the various administrative authorities, Prof. Hans Klinghoffer included the existence of a "disguised administrative act". Such activity can be defined as a governmental act performed under the cloak of a non-coercive governmental act, where in fact, the substance of the act – or at least the way it is understood by those to whom it is addressed – is a governmental act of coercive significance, or as Klinghoffer expresses it:

> A unique type of unclear act is the disguised act. When an agency does not see a legal path for achieving its desired objective, it will, at times, try to present the action in a disguised manner in order to increase the chances for it to be interpreted as a lawful act. Our judicature is unwilling to accept such trickery (see: HANS KLINGHOFFER, ADMINISTRATIVE LAW, pp. 109-111 (1957) (Hebrew), and in general on the theory of administrative acts, pp. 82-117).

An example of this can be found in HCJ 144/50 *Sheib v. Minister of Defence* [19] (hereinafter: the *Sheib* case). In that famous case, the Director of the Department of Education in

the Ministry of Education demanded that the administration of a school not employ the petitioner due to the opposition of the (then) Prime Minister and Minister of Defense (David Ben Gurion) (due to his position in regard to the petitioner's political activity). What is relevant to the matter before us is one of the arguments made by the respondents in that case, who admitted that the order not to employ the petitioner was not based upon express legislation, while pointing out that this act was not obligatory, but rather only a ("voluntary") request that the school to which it was sent could have declined.

The Court refused to accept the position of the respondents, stating:

> As I have said, the respondent admitted that his action was not based upon law, and he therefore emphasised the nature of his approach to the principals of private schools, stating that he only "requested" them not to employ teachers in their schools save with the consent of the Inspector. *It is not necessary to say that a "request" such as this is tantamount to an order at least in so far as the petitioner before us is concerned, because for reasons which are self-evident, schools would tend to yield to a "request" of this kind, as the present case proves. It is possible that had the respondent approached the principals of schools in a form that was less compelling, and had emphasised that his request had no binding force, it would have been difficult to find any fault with his approach*. It is clear to me, however, from the evidence of the respondent in his affidavit, that he in fact did not employ language which gave the principals any choice – that if they so wished they could follow his opinion, and if not they could disregard it and employ a teacher against his will. In this case the respondent did not set out in the circular that the principals of schools had a choice in the matter. I have no doubt, therefore, that the respondent exceeded his authority in approaching the principals of schools (*ibid*., p. 419 [para. 9 of the opinion of Justice Witkon] (emphasis added – H.M.)).

It would appear from the above that had it concerned a non-obligatory request, "it would have been difficult to find any fault with his approach". However, it is clear from the justice's statement (in the section in italics) that even if it were a "voluntary" request, as long as the addressee will "tend" to "yield" and comply with the request, such a request can be viewed as a governmental act (compare: the *Rabbeinu Tam Sanctions Affair* in para. 1 of the opinion of President M. Naor, and para. 5 of the opinion of Justice I. Amit).

44. However, it is important to make it clear that the case before us is *different* for several reasons:

First, since not even initial evidentiary grounds were presented to rebut the presumption of administrative regularity, it can be assumed that the Cyber Department's referrals to online platform operators are, indeed, conducted in accordance with the Department's understanding that this only constitutes reporting that does not involve any element of coercion of the online platform operators (in this regard, see: DAPHNE BARAK-EREZ, CITIZEN, SUBJECT, CONSUMER – LAW AND GOVERNMENT IN A CHANGING STATE (2012) (Hebrew)).

I would also note in this regard what is stated in sec. 6 of the Cyber Department's Work Procedure, which instructs as follows:

> In all that regards referrals on the voluntary level, no *demand* should be presented to the online platform for the removal of content, restriction of access to it, and so forth (emphasis added – H.M.).

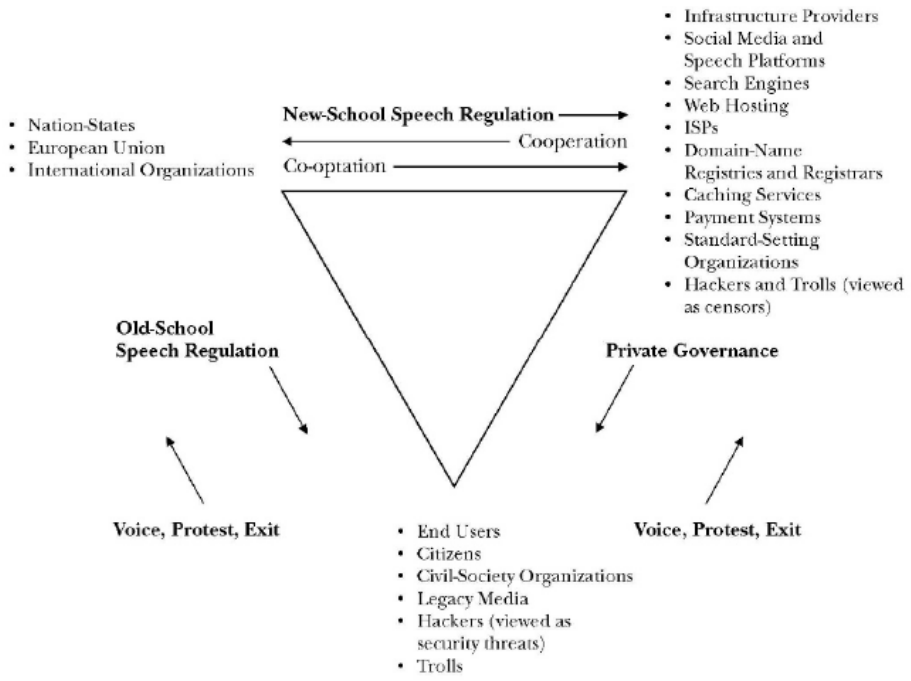
Second, the "relationship" before us is, indeed, distinguishable to no small degree from the example presented above (the *Sheib* case). In the present case, the online platform operators are *very powerful* multi-national entities that appear to act independently, that exercise their own independent discretion, and that decide how to act under the circumstances of the matter. Therefore, the voluntariness involved in the Department's referral, and the manner of the exercise of independent discretion of those entities is *qualitatively different* from what occurred in the *Sheib* case.

45. Nevertheless, I cannot accept the Respondents' position on this point in its entirety. In my view, the referrals to the online platform operators should be seen as a type of *governmental act*. My position, which I will explain below, is that the interaction among the state, the online platform operators, and the end users can be categorized as a unique relationship in which the "geometric place" of the state is *on one of the sides of a triangle* connecting the above three entities, and in this framework, the state has no inconsiderable influence (see: Balkin, *Triangle*).

For convenience, I have attached Chart 1 – the diagram that Prof. Balkin presented in his article, and Chart 2, which simplifies it for our needs. The diagrams map the relationship triangle

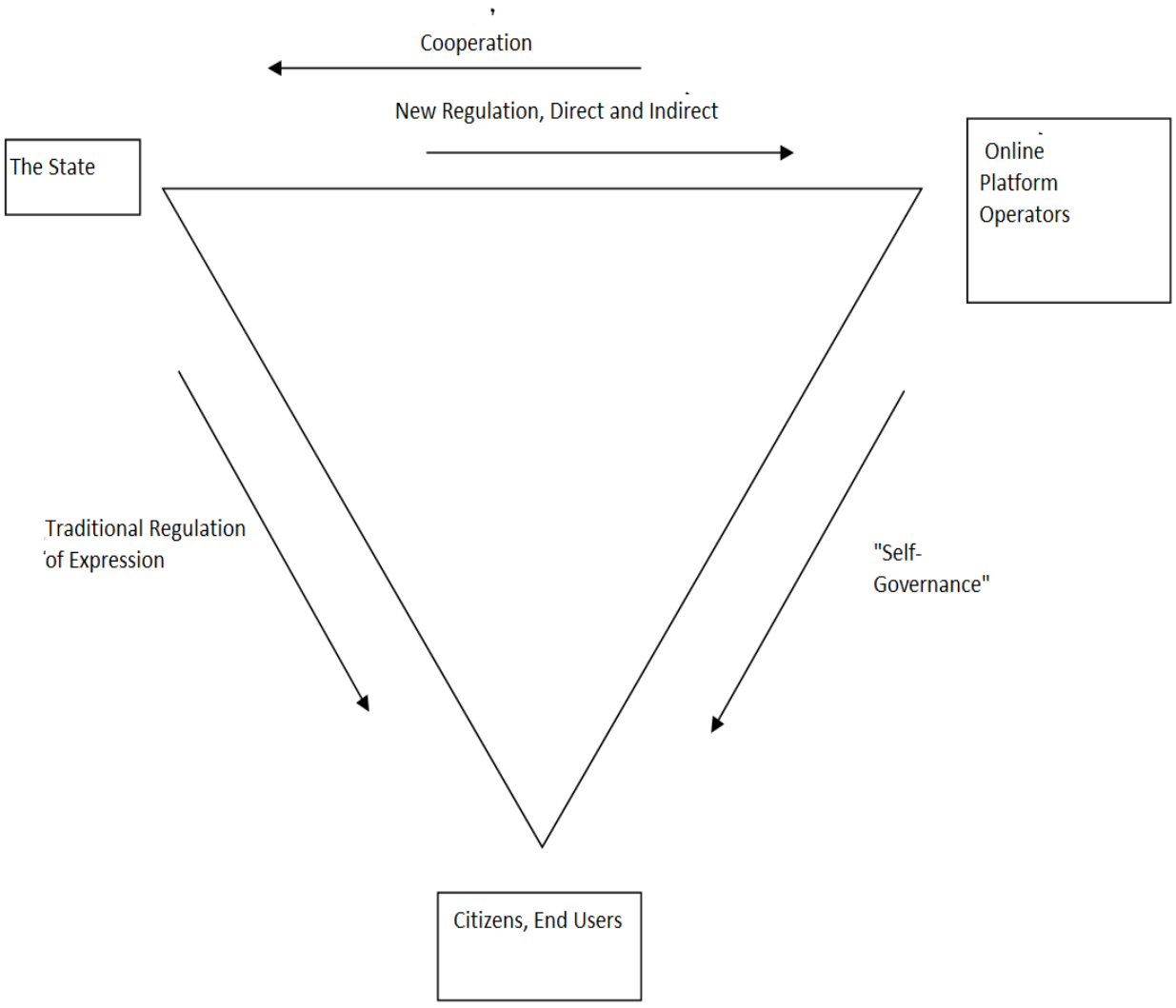
among the end user, the platform operators, and the governmental authorities, and describe the relationship and power structure among these entities in regard to "classic" regulation in which the state acts directly opposite the individual in matters of freedom of expression, and the "new" regulation that shapes the relationship between the state and the online networks, where the state seeks to encourage the platforms to conduct their own supervision of unlawful expression by private governance. This has developed over the years, and shapes the relationship between the users of the platform and the supervision of expression and information by the former (what I noted as the Terms of Use and the "community rules").

Diagram 1:



(See: Balkin, *Triangle*, p. 2014).

Diagram 2:


Cooperation
New Regulation, Direct and Indirect
The State
Online Platform Operators
Traditional Regulation of Expression
"Self-Governance"
Citizens, End Users

In my opinion, in this situation in which there is a *possibility* that the voluntary referrals of the Cyber Department are a trigger for the "enforcement" actions of the online platform operators (as noted, we do not have any data in this regard), and that the Department's referrals may influence the discretion of the online platform operators, *there is a need for some statutory authorization* for the said cooperation.

I will explain this in detail below.

"Inverse Regulation" and the Activity of the Cyber Department

46. Normally, it is the state that regulates and directs the conduct of the individuals and entities that exist within it. The accepted means for this are legally operative norms (like primary and secondary legislation). Frequently, the state also chooses to regulate markets and various spheres of activity of "private players" by establishing rules that apply only to those markets, direct the activity of the parties that operate within them, and even conducts supervision and enforcement over such activity. However, at times, the state permits an organizing body to police itself, subject to the permission of the governmental authority (as is the case, for example, in regard to the Tel Aviv Stock Exchange). This practice, in its various aspects, is one of the meanings of the concept "regulation", which has significantly developed over the last years (on regulation as a separate conceptual framework in Israeli law, see recently: Neta Ziv, *Judicial Review meets Regulation: A Preliminary Conceptual Mapping*, ELYAKIM RUBINSTEIN VOLUME, 1125, 1130-1136 (2021) (Hebrew) (hereinafter: Neta Ziv, *Regulation*), and also see: CASS R. SUNSTEIN, AFTER THE RIGHTS REVOLUTION – RECONCEIVING THE REGULATORY STATE (1990); Ayelet Hochman, Alon Jasper & Dan Largman, *Talking about Regulation: The Term "Regulation" and its Role in Israeli Law*, THE GOVERNANCE OF REGULATION: LAW AND POLICY LAW, SOCIETY AND CULTURE, Yishai Blank, Roy Kreitner & David Levi-Faur (eds.), 47, 48 (2016) Hebrew); SHARON YADIN, REGULATION: ADMINISTRATIVE LAW IN THE AGE OF REGULATORY CONTRACTS, 21-28 (2016) (Hebrew) (hereinafter: YADIN).

By creating rules that are designed ad hoc for a sphere of activity, regulation that sought to direct the players in a market sphere by means of a system of rules intended to direct the parties subject to it in a "vertical manner" gained prominence. In this manner, rules were created for directing such markets as health, commerce, savings, insurance, banking, and energy. These rules,

which include primary legislation, and at times, directives and orders issued by the regulatory authority in the framework of regulations, are often accompanied by various mechanisms for supervision and *post facto* enforcement of the applicable arrangements. As Prof. Neta Ziv points out, the move to regulation reflects a change in the role of the executive branch, primarily in distributing new functions and powers between the state and the non-state arena, where, in general, the regulatory rules define the means for the government's exercise of power in regard to the supervised body (individual or corporate), and employ language, terminology and internal logic that can be identified as a distinct field of knowledge (see: Neta Ziv, *Regulation*, p. 1128).

The regulatory model described above reflects regulation in its primary sense, known as "command and control", which is the classic model in which the moderator is positioned "above" the players in a particular sector, directing their actions, and enforcing *post facto* the rules that it or the legislature established (for definitions of the accepted model of "command and control", see: Neta Ziv, *Regulation*, p. 1142).

However, over the years, a variety of more sophisticated models of regulation developed, which apply "softer" methods of enforcement. This is the "new regulation". Thus, for example, beginning in the last century, we see the development of self-regulation in which the regulator "recommends" that the "market players" adopt a general policy as a (non-obligatory) condition for the proper administration of the particular market (on "the new regulation", see: YADIN, pp. 21-32; Sharon Yadin, *Miscommunication: Between Public Interest and Private Interest in the Regulation of Channel 10*, 8 HAIFA LAW REVIEW (DIN UDVARIM) 391, 409-410 (2015); Neta Ziv, *Regulation*, pp. 1142-1145).

47. Another development is expressed in the ascension of the *regulatory contract*, which grounds the element of governmental direction upon an *agreement* between the regulator and the supervised entity. The framework of the regulatory contract represents a move from the "vertical" model to a "horizontal" model in which the state and the supervised entity *negotiate* the conditions that will apply between the parties, and the parties form a contractual, or quasi-contractual relationship, as expressed by my colleague President E. Hayut in para. 2 of her opinion in HCJ 4374/15 *Movement for Quality Government v. Prime Minister* [20], (hereinafter: the *Gas Outline* case):

> This combination of regulatory provisions and obligations of commercial corporations in the area addressed by those provisions bears clear characteristics of a "regulatory contract", which is a relatively new legal phenomenon, first found in the United States in the nineteen-nineties, as a tool that bases regulatory provisions in various fields on contractual relations. One of the salient characteristics of the regulatory contract, as opposed to other governmental contracts, is the identity of the parties to the contract. "A regulatory contract is made between an administrative agency, in its role as regulator, and a private corporation. [..] The legal framework of the regulatory contract is largely the result of the challenges faced by the authorities in the modern age due to the complexity of the regulation required in various fields, including, and perhaps primarily, in developed, free markets that intensify the need for supervisory regulation. Against this background, new models of administrative regulation have developed, *among them regulation based upon cooperation with private entities that is grounded in contracts*. One of the advantages inherent to such a regulatory model is the achieving of voluntary cooperation by the supervised entities which, on their part, may derive benefit from activity that is coordinated with the supervising body, as opposed to coercive provisions that are drafted and established unilaterally by it. However, the regulatory contract model raises many questions from both the legal and public aspects that may have consequences, inter alia, on the scope of judicial review applicable to such a regulatory model… (and see: YADIN, p. 38; emphasis added – H.M.).

48. The case before us is characterized by relationships between the state and private entities (primarily multi-national corporate giants) that do not match any of the distinct cases listed above and do not fall within the scope of those regulatory schemes. It is therefore clear that the agency's referrals to the online platform operators do not reflect a "command and control" relationship. The online platform operators are not subject to rigid regulation, and the Terms of Use and their "community rules" are, it would appear, *independently* established by those operators.

The legal literature recognizes a regulatory phenomenon known as "voluntary regulation", in which the market actor establishes its own manner of operation (see: Yair Amichai-Hamburger & Oren Perez, *Environmental Self-Management: Effectiveness, Organizational Change, and Lessons for the Environmental Regulation System*, 25 BAR ILAN LAW REV. 633 (2009) (Hebrew);

and see Vismonski, who categorizes the relationship between the state and the operators as "contractual", Vismonski, *Alternative Enforcement*, pp. 716-717). Nevertheless, in my opinion, what we have here is not a "voluntary regulation" model in the full sense. Although the online platform operators act independently in defining the rules that govern the relationship between them and the users, when the Respondents draw their attention to breaches of local law, their Terms of Use and "community rules", it would seem that in the specific area of activity that concerns us (social networks and the area of network content), we cannot yet rule out the possible influence of such a referral on the online platform operators and their fear of the authority, which can act to limit their actions, whether by primary legislation or by administrative means (see and compare: Hannah Bloch-Wehba, *Global Platform Governance: Private Power in the Shadow of the Global State*, 72 SMU L. REV. 27, 79 (2019) (hereinafter: Bloch-Wehba); Ken-Dror Fedman & Elkin-Koren, pp. 31-32; Balkin, *Triangle*, p. 2020).

49. As we see, the case before us represents a new model in which law enforcement and regulation of the relationship among the various market players – the state, the social network participants (the authors of the various publications and the web surfers), and the online platform operators themselves – are carried out with the state acting as a reporter that refers the apparent breach for the examination and decision of the online platform operators. This framework, which might be called "inverse regulation" – inasmuch as the final decision rests in the hands of the online platform operators – neither increases nor lessens the problems that frequently arise in other regulatory models (such as violating personal freedom and the autonomy of the individuals subject to "command and control" regulation, and the problem of restricting the discretion of the authority in the framework of a regulatory contract). However, the "inverse regulation" model raises a fundamental question that derives from the aforementioned question of authority – given that we are concerned with non-obligatory, "voluntary" referrals by the government, can it be said that we are concerned with regulation? In other words, is the Cyber Department actually acting under a "soft" regulatory model when it initiates referrals to the online platform operators, and should such referrals be deemed governmental actions that justify the conferral of express legislative authority, or not?

The theoretical position as to the nature of the "regulation" (to the extent that it exists under the circumstances) can be of consequence for the legal analysis of the legality of the administration's actions.

50. As described above, in situations that do not concern a "disguised governmental act" that is *actually* coercive, which must be voided for a lack of legal authority, it is entirely possible that a completely voluntary act whose result entirely depends upon the independent exercise of discretion by the body referred to does *not* require *specific, express* authorization by law, and thus, for example, the residual authority granted to the government under sec. 32 of Basic Law: The Government would therefore be sufficient. For example, under this approach the Cyber Department's referrals to the online platform operators are not essentially different from requests sent by Israeli security and diplomatic actors to their foreign counterparts asking, for example, that they thwart plans by hostile foreign actors seeking to harm the State of Israel abroad or at home (on the subject of acting by virtue of the general authority granted under sec. 32 of Basic Law: The Government, or sec. 17 of the Interpretation Law, see SHIMON SHETREET, THE GOVERNMENT: THE EXECUTIVE BRANCH – COMMENTARY ON SECTION 18 OF BASIC LAW: THE GOVERNMENT, (2018) (Hebrew) (hereinafter: SHETREET).

As opposed to this, where we are concerned with a regulatory act that can interfere with the freedom of action of players in the marketplace or restrict it, it may be assumed that, in this regard, the state must act in accordance with the principles of administrative law (see: Neta Ziv, *Regulation*, p. 1139).

51. To my understanding, as long as it has not been proven otherwise (and as noted, this petition lacks respondents essential to examining the issues in dispute), the framework in which the Cyber Department operates does have a some potential for influencing and directing the actions of players in the marketplace and for creating an "inverse regulation" environment. This is so because, in my view, as opposed to the way that the Government Respondents seek to present themselves, a referral by a private individual to those online platform operators cannot be compared to a referral by a governmental agency that appears before the online platform operators as a "repeating player" who may also act against them in other ways. My position is, therefore, that the *very possibility* that the "sword of coercive regulation", which the government, or someone

on its behalf can draw against the online platforms if their operators frequently fail to accede to the referrals is sufficient to show that we are concerned with a *governmental act* that requires some legislative authorization. Indeed, there is the possibility that the state will seek to establish rigid normative rules to require the online platform operators to comply with the Respondent's referrals or be exposed to various steps and sanctions, and that constitutes a lever for applying pressure that raises the fear that – at least potentially – we are not concerned with cooperation between the state and the private commercial entities that is completely voluntary (for examples of attempts at regulation to restrict publications on online platforms, see: Defamation (Prohibition) (Amendment – Disclosing the Name of a Tortfeasor) Bill, 5770-2010; Defamation (Prohibition) (Amendment – Prohibiting Defamation on the Internet) Bill, 5775-2015; Defamation (Prohibition) (Amendment – Correcting Defamation on the Internet) Bill, 5781-2020). As opposed to this, see the Copyright (Amendment No. 5) Law, 5779-2019 (which was enacted pursuant to comments by the Court in CA 9183/09 *Football Association Premier League Ltd. v. Anon.* [21] (hereinafter: the *Premier League* case)).

In this regard, I will quote Dalit Ken-Dror Feldman & Niva Elkin-Koren:

> The platforms that are commercial companies exposed to the exercise of governmental power are subject to a threat that if they do not cooperate with the alternative enforcement arrangement, they may be required to perform enforcement actions due to changes in the law, which would leave them less flexibility and discretion (Ken-Dror Feldman & Elkin-Koren, p. 38).

In this regard, also see the statement of the Commission for Establishing Means for protecting the Public and Officeholders in the Civil Service against Harmful Activity and Publications as well as Bullying on the Internet – Report (2020) (hereinafter: the Arbel Commission Report), which established as follows:

> It should be borne in mind that the expression "voluntary" regulation, which is sometimes employed to describe referrals by the authority to request the removal of content, is not entirely appropriate to the situation it purports to describe. Indeed, the various platforms reserve the right to refuse the state's request to remove content, *however, there is no doubt that a state request bears significant weight, much greater than that of a referral by a citizen. This being so, use of this tool should be reserved for*

> *exceptional cases*. The threshold requirement of the existence of a criminal offense appears to be an appropriate balance point [emphasis added – H.M.].

Also see the statement by the head of the Cyber Department, Dr. Haim Vismonski, who is of the opinion that:

> The distinction between voluntarily agreed defensive actions and actions pursuant to a coercive provision is not a dichotomy […] The service providers, on their part, fear legislative changes that would broaden the state's authority to impose coercive provisions upon them that would intervene in the manner they regulate the content that they publish. The said fear encourages the providers to increase their agreed, voluntary cooperation with the states […] This somewhat undermines the voluntary basis, and it is possible to present the move as a coercive one by the state, even if somewhat covert (Vismonski, *Alternative Enforcement*, pp. 722-723).

52. This is the place to explain that, in the framework of this petition, since the online platform operators were not named as respondents, this possibility is *but a theoretical fear* that we cannot properly examine. It is indeed possible that in examining referrals regarding breaches of the "community rules" and the Terms of Use, those powerful multinational corporations that operate the said platforms act without fear of the individual who may be harmed or of the *administrative agency* (for a view of online platform operators as acting independently in regard to governmental referrals, see: Alan Z. Rozenshtein, *Surveillance Intermediaries*, 70 STAN L. REV. 99, 154 (2018).

53. The conclusion to be drawn from the above is that although not even preliminary evidence was presented to show any defect in the discretion exercised by the Cyber Department, the fact that it transfers – if only temporarily – the decision in the matter to the online platform operators, which are civil bodies that seek to maintain good relations with the *authority*, raises the fear that, *in practice*, the Department's referrals influence the discretion of those operators. Therefore, in my opinion, the Cyber Departments actions are of a governmental nature that requires authority, even if of a general sort.

If we add to all the above the apparently uncontested fact that restricting or removing publications by the online platform operators may ultimately lead to limiting the fundamental

rights of the publisher (insofar as a human entity is concerned), primary among them the right to freedom of expression, it is clear that the Department's activities, even in the framework of "inverse" regulation, can influence, even if indirectly, the restriction of those protected fundamental rights.

54. *In conclusion*, in their preliminary response, the Respondents discussed at length the view that it should be recognized that: "The activity of the Cyber Department in the voluntary track of referring reports of prima facie offenses that breach the Terms of Use established by the companies themselves *does not involve the exercise of governmental authority*" [emphasis added – H.M.]. It would seem that the Respondents' intention was to say that if, indeed, the exercise of governmental authority is not concerned, then there is no need for specific legislative authority and the publication of the rules under which the agency operates.

As stated, *I hold a different view*, and I therefore expanded upon identifying the Department's conduct in the voluntary enforcement track as an exercise of some power in the regulatory field.

There is an additional reason for this. The current scholarship on regulatory theory sees "the change in the power paradigm", which we pointed out, as one of the primary *adjustments* to which administrative law must adapt in the modern age. If we take the case before us as an example, the rise of online platforms that provide convenient, available and effective infrastructure for disseminating messages and content of every type, creates a change in the balance of power, in which a limited number of private, multinational actors hold tremendous power to administer the "marketplace" in all that regards the exchange of opinions and messages, while any person with a keyboard (or touchscreen) can disseminate harmful, inciting and violent messages, as well as terror, while using a fabricated or fictional identity, and thus create a "market failure" and significant problems of enforcement (see and compare: Terry Flew, Fiona Martin & Nicolas Suzor, *Internet Regulation as Media Policy: Rethinking the Question of Digital Communication Platform Governance* 10 J. DIGITAL MEDIA POL. 33 (2019); Bloch-Wehba, pp. 71-78).

55. In view of the rise of various factors operating in the markets in previously non-existent forms and methods, Dr. Yuval Roitman is of the opinion that it would be appropriate "to distinguish between circumstances in which there is a need for restraining governmental power

that is abused, and circumstances in which judicial review should *encourage* the exercise of governmental power, inasmuch as it is the state's omission that is the flaw," Yuval Roitman, *Administrative Law in the Regulatory State*, Mishpat Umimshal 219, 234 (2017) (Hebrew) (hereinafter: Roitman) [emphasis added – H.M.].

In this regard, attention must also be paid to the consequences of the actions of entities operating in the marketplace (in our case, the online platform operators) as they relate to the general public. Prof. Neta Ziv gives the example of the view of Justice I. Zamir in HCJ 7721/96 *Israeli Insurance Adjusters Association v. Supervisor of Insurance* [22], who was of the opinion that in view of the excess power of insurance companies at the time, a "supra-arrangement" should be established to better protect the insured public. Therefore, in addition to the fact that we are faced with a special case of "inverse" regulation in which the regulatory authority (apparently) subjugates itself to the decisions of the market players, there is no doubt that there is a need for an *agreed arrangement* in regard to the behavior of the main players and the users of the social networks, and therefore, the activity of the Department on the voluntary enforcement track fulfils its obligation to act for the prevention of criminal offenses in a speedy and effective manner.

56. What has been said so far shows, however, that the principle of administrative legality also requires that there be formal authorization in the case before us to facilitate the activity of the Cyber Department. As we see, its activity in the voluntary enforcement track may constitute a form of administrative act of operative effect. Therefore, in accordance with the fundamental principles of administrative law, in order to establish that the activities of the Cyber Department are lawful, authority, *even if only general*, must be found in the law.

I will address this immediately, below.

The activity of the Cyber Department by virtue of the government's residual authority

57. The courts are not infrequently called upon to respond to situations in which it is claimed that an administrative authority is not performing its duty *in accordance with the law*. The touchstone established in the case law concerns the complete "shirking" of this duty by the authority, or its unreasonable refraining to carry out its duty (see: HCJ 6579/99 *Filber v. State of*

Israel [23]; Roitman, pp. 265-266). This is another exceptional aspect of the present petition. In the matter before us, we are asked to address arguments of alleged "over-enforcement" by the Respondents. If the general position of the Court is that it is not its role to "take the place of the authorized agency and establish a law-enforcement plan for it" (HCJ 551/99 *Shekem. v. Director of Customs* [24]), then in the present petition, we are asked to examine whether the activity framework of the Department conforms to the authorities it has been granted.

Before entering main hall, we should present some additional background data while still in the corridor, as I shall now do below.

58. The internet, for all its advantages and disadvantages, as noted above, created a space in which access to the net and the activity there is, as my colleague Justice Sohlberg stated in the *Israel Internet Association* case:

> … all over the world, but its existence is "nowhere" (para. 22 of his opinion).

Moreover, in this situation, again quoting my colleague:

> Offenders against the law adapt to progress more rapidly than its enforcers […] The former have no restraints; the latter do.

In this situation, criminal and civil law do not, at present, provide a sufficient response to the offenses and torts perpetrated by means of the internet, and there are, therefore, those who are of the opinion that in view of the virtual nature of the said space, the laws of space, time and state should not be applied to the internet (see: Yuval Karniel and Haim Vismonski, *Freedom of Expression, Pornography, and Community in the Internet*, 23 (1) BAR ILAN STUDIES IN LAW 259 (2006) (Hebrew); Michal Agmon-Gonen, *The Internet as a City of Refuge?! Legal Regulation in Light of the Possibilities of the Technological Bypass Technologies and Globalism of the Net*, LEGAL NETWORK: LAW AND INFORMATION TECHNOLOGY, Michael Birnhack and Niva Elkin-Koren, eds., 207 (2011) (Hebrew); and see: Vismonski, *Alternative Enforcement*, pp. 692-704).

Some solutions for these problems have recently been offered in the literature by means of using *cloud technology* (see: Yochai Benkler, *Degrees of Freedom, Dimensions of Power*, 145 DAEDALUS 18 (2016)), and in our case law.

In a judgment handed down three years ago by my colleague President E. Hayut (Justice A. Baron concurring) and myself in LCA 5860/16 *Facebook Inc. v. Ben Hamu* [25] (hereinafter: the *Facebook* case), the Court held that Facebook's community rules constituted an *adhesion contract* between Facebook and the network users, which opened many possibilities for enforcement (and see and compare: LCA 1239/19 *Shaul v. Nayadli Communications* [26]).

However, the advancement of case law, which by its very nature is "bottom up" (from the trial court to the Supreme Court), cannot suffice to stop the "bad actors" operating on the net.

In addition, the *decentralized* nature of the production and virtual distribution on the internet makes it very difficult to carry out enforcement by the traditional means of bringing the offender to trial, not to mention that anonymity on the internet makes it difficult to identify offenders and tortfeasors (see, e.g., the *Mor* case). Another challenge for enforcement is the *global* nature of the network. Thus, for example, various legal issues arise concerning the application of local law to alleged offenders where it is unclear whether they are citizens or residents, or operate within the territory of the state. Moreover, due to the global character of the internet, it is possible that expression that is deemed potentially criminal in one legal system does not constitute prohibited speech in another (see: Ken-Dror Fedman & Elkin-Koren, p. 35). In addition, in the United States, for example, certain online platform operators enjoy *immunity* (see: Madeline Byrd and Katherine J. Strandburg, *CDA 230 for a Smart Internet*, 88 FORDHAM L. REV. 405 (2019)), which may apply extraterritorially.

Thus, the voluntary enforcement mechanism was created to provide answers to most of these problems.

What, then, is the source of authority for the Cyber Department's activity in the framework of this enforcement mechanism?

59. The primary source of authority is to be found in the residual authority granted to the government pursuant to sec. 32 of Basic Law: The Government.

As intimated above, the scope of authority granted to the government is far wider than the individual authorities that the legislature granted expressly, such that by its nature, the government is daily involved in "all embracing" activities that lack any express, specific foothold in the law

(see: ZAMIR, p. 419). This range of activities is conducted, as noted, by virtue of the doctrine of residual power entrenched in sec. 32 of Basic Law: The Government. The direct meaning of this provision is that, in the absence of another provision granting authority to some other agency, the government is authorized to act in the name of the state.

The substance of the doctrine of governmental residual power derives from the tremendous scope of administrative activity, the surprising nature of developments in daily life, as well as the recognition of the fact that legislation cannot keep up with the pace of technological advances (see: DAPHNE BARAK-EREZ, ADMINISTRATIVE LAW, vol. 1, 139 (2010) (hereinafter: BARAK-EREZ); SHETREET, pp. 561-562). I addressed this in the *Premier League* case, where I stated as follows:

> It is well known that technology generally precedes the law. In such cases, the legislature and the courts are called upon to pour the essence of the existing, good and grounded principles into new legal vessels (as though they were aged wine that improves with time and only needs a more modern container. Compare: STEPHEN BREYER, ACTIVE LIBERTY 64 (2009).

My colleague Justice N. Sohlberg added to this in the *Israel Internet Association* case in stating:

> As we know, the law slowly staggers behind the world's innovations, and legislation cannot keep up with the pace of scientific progress and its applications.

60. The force and incidence of the residual power have been addressed in a number of judgments by this Court. Thus, for example, in the *Gas Outline* case, the Court held that:

> The term "residual power" is not a magic word and is not a key to every gate. It is examined after examining the direct powers and should not be ambiguous (para. 142 of the opinion of Justice E. Rubinstein).

In that case, there was a disagreement among the members of the panel, inter alia, on the question whether establishing an outline for treating an essential natural resource found in large quantities on the state's coast exceeds the government's residual power and requires that the outline be established in specific primary legislation, inter alia, because it constitutes a primary arrangement. The majority held that the arrangement did not require express primary legislation

(see: the *Gas Outline* case, para. 11 of the opinion of my colleague Justice E. Hayut; paras. 10-14 of the opinion of Justice U. Vogelman; paras. 50-62 of the opinion of Justice N. Sohlberg. On the dissenting opinion, which was of the view that the outline required particular primary legislation, see: paras. 127-143 of the opinion of Justice E. Rubinstein; and paras. 3-13 of the opinion of Justice S. Joubran. And see: HCJ 11163/03 *Supreme Monitoring Committee v. Prime Minister* [27], para. 10 of the opinion of Deputy President M. Cheshin).

It has further been held that the government cannot act by virtue of its residual power in order to violate entrenched or implied basic rights granted to individuals by Basic Laws. Thus, for example, in HCJ 5100/94 *Public Committee against Torture v. State of Israel* [28], which treated of the authority of the General Security Service[2] to conduct interrogations in general, and particularly the use of special interrogation methods that included employing physical means, President Barak held: "The 'residual' power of the government is not a source of authority that infringes the liberty of the individual. The residual powers of the government authorize it to act whenever there is an 'administrative vacuum' […] There is no such 'administrative vacuum' in this case, as it is 'filled' by the principle of individual freedom. Infringing this principle requires a specific provision".

However, it is important to note that until the enactment of the General Security Service Law, 5762-2002, it appeared that the general authority of the General Security Service to act in its sphere of activity derived from the residual power doctrine (see: *Report of the Commission of Inquiry into the Methods of Investigation of the General Security Service regarding Hostile Terrorist Activity*, p. 41 (1987)), *and the authorities of the Institute for Intelligence and Special Operations* [the "Mossad" – ed.] *rely upon that source of authority to this day*).

61. Specifically, in the matter of infringing freedom of expression, it was previously held in the *Federman* case that this vested right cannot be infringed by virtue of the general authority under the residual principle:

> There are actions that are not within the scope and power of the government because exercising them without legal authority is contrary to fundamental normative concepts that derive from the nature of our regime. So it is in regard to basic rights that are part of our positive law, whether

[2] Now referred to in English as the Israel Security Agency – ed.

> it has or has not yet been included in a Basic Law. Thus, for example, the government does not have the authority to close a newspaper on the basis of an administrative order if there is no express legal provision that addresses such a matter, and even were there not a Basic Law that defines freedom of speech. Such an act would be contrary to our fundamental concepts regarding human liberty inherent to our regime, which can only be limited by statute […] *therefore, the basic right to freedom of speech, which is part of our positive law, creates a restriction that ties the executive's hands and does not permit it to deviate, without legal authority, from the prohibition upon infringing a freedom it grants*. (*ibid*., p. 652; emphasis added – H.M.; and see Zamir, pp. 421-423).

Indeed, these restrictions upon the residual power of the government were intended to ensure that the broad general authority granted under this provision of Basic Law: The Government will not completely erode the principle of administrative legality, and does not replace the constitutional values grounding the system (see: BARAK-EREZ, pp. 139-143).

62. The answer that should be given to this question is *negative in the circumstances*. At present, and in accordance with the evidentiary foundation presented in the petition, there are no grounds for finding that the Cyber Department's activity is unconstitutional. In my opinion, while we cannot deny the possibility that the Cyber Department's activity has operative force, in that it initiates a process that may result in a real act of removing publications or preventing access, I do not believe that there is a *violation* of basic rights, in the usual sense, in most of the areas in which the department acts (as for the exceptional cases, see my comments in para 73(b), below).

I will now explain in detail.

63. What is an infringement of a constitutional right? A review of the case law of this Court reveals that the question of the infringement of the constitutional right has not raised any real problems to date. For example, in LCA 3145/99 *Bank Leumi v. Hazzan* [29], 398, it was held that *infringement* concerns the absence of ability to realize the full scope of the constitutional right (and see: Aharon Barak, *The Constitutional Right and its Violation: The Three-Step Theory*, 19 MISHPAT UMIMSHAL 119 (2018) (Hebrew) (hereinafter: Barak, *The Constitutional Right*)). According to Prof. Barak, examining an infringement of a constitutional right is almost independent of the circumstances, stating:

> An infringement occurs in every situation in which the authority forbids the holder of a right to realize it fully or prevents him from doing so. An infringement is any detraction from full realization of the right. There is no significance to the question whether the infringement was the result of fault (intention, recklessness, willful blindness, negligence) or without fault, whether it was serious or minor, at the heart of the right or its periphery, by an omission or by an act, or whether it was certain or that there was but a possibility – that is not *de minimis* – for its realization. Every infringement, regardless of its scope, moves the constitutional review from the first step to the second, unless the infringement is *de minimis*. (Barak, *The Constitutional Right*, p. 148).

64. However, some resonances of a view that disagrees with the broad scope of the concept of infringement of right, as defined above, can be found in the case law. Thus, for example, in CA 6821/93 *United Mizrahi Bank v. Migdal Cooperative Village* [30], President Shamgar noted in regard to the right to property: "Violation of the right to property, for our purpose, was illustrated by reference to constitutional acts possessing substantive personal repercussions, for example, those by virtue of which the property of a person is confiscated without proper compensation, in an arbitrary or other substantive breach of his rights." (*ibid*., p. 332 [para. 38]; and see the opinion of Justice A. Procaccia in HCJ 10203/03 *Hamifkad Haleumi v. Attorney General* [31], 852-854; and see the opinion of President A. Grunis in HCJ 2442/11 *Shtanger v. Speaker of the Knesset* [32]).

Another possible criticism if the broad view proposed by Prof. Aharon Barak was mentioned by Prof. Barak Medina. In accordance with the deontological-necessity approach presented in his book, an infringement of a constitutional right does not refer to the consequences of the act, alone (that is, the restriction of the full realization of the right), but also concerns evaluating the nature of the act and the reasons for diminishing the protected interest. In the context of the matter before us, Prof. Medina explains that in order for an act by a governmental agency to rise to the level of an infringement of a vested right, the infringement must be "a violation by virtue of an intentional act, *whose consequences are certain*, and under the circumstances of the matter, comprise some breach of a moral constraint concerning the proper relationship between the government and the individual" (BARAK MEDINA, HUMAN RIGHTS LAW IN ISRAEL, 88 (2016) (emphasis added – H.M.).

65. Of course, the above debate might be relevant to the sufficiency of the government's residual power as a source of authority for the activity of the Cyber Department, however, we have no need to decide among the various approaches for a number of reasons:

A) In the present case, it would appear that there is no disagreement that, as earlier noted in para. 21, robots and avatars do not enjoy human rights, and therefore infringement of their right to freedom of expression is not relevant, and some of the harmful publications derive from such bots and avatars. Nevertheless, in my opinion, where there is doubt as to whether the act is likely to lead to a real violation of fundamental rights, extreme caution must be exercised, as stated in para 73(b), below.

The situation of enforcement in regard to social networks is unique and differs in its very nature from the constitutional or classic administrative paradigms in which the individual stands in opposition to the government (see and compare: Michael D. Birnhack & Niva Elkin-Koren, *The Invisible Handshake: The Reemergence of the State in the Digital Environment*, 8 VA. J.L. & TECH, 48-54 (2003)). As Prof. Balkin describes it, on questions of freedom of expression and other issues in the scientific age, there is a *triangular relationship*: The state is at one vertex, the private internet companies and various platforms are at another vertex, while the speaking individual (or organization) is at the third (see: Balkin, p. 2014). In my opinion, in such a unique power *triangle*, where the state does not demand or impose removing or restricting expression, and *the online platform operator* is the one who removes the publication at its discretion, it cannot be said that it is the state that infringes the right, and in any case, those harmed have other remedies, including against the online platform operators.

B) In the present case, the state's involvement in protecting or restricting political expression is slight, as it plays no role in providing the infrastructure for political expression (which is provided, as noted, by the online platform operators).

66. As for the lack of authorization – the Petitioners brought the example of the *Israel Internet Association* case, which held, as noted, that a police officer lacks authority to order the closure of a "gambling site" operating on the internet, inter alia, in view of the possibility that it might lead to a violation of the right to occupation and freedom of expression of the website operator and its

users. However, in my opinion, the said case is entirely different from the one before us for several reasons:

First, because that matter concerned a closure actively imposed by an administrative organ where it, and it alone, had discretion as to how to act, and to order the provider of access to the gambling site not to permit access to that site. In the case before us, there is no disagreement that the authority to exercise discretion is given to the civil organ to whom the matter is referred – the online platform operators (on the possibility that this is a prohibited delegation of authority, compare: the *Israel Internet Association* case, para. 15 of the opinion of Justice U. Vogelman).

Second, and pursuant to our discussion of the infringement of freedom of expression as a fundamental constitutional right, even in the *Israel Internet Association*, Justice Vogelman held: "With respect to gambling websites, and only to them, my opinion, as mentioned above, is that the infringement of free expression that resulted from blocking lawful content on the gambling websites, is of a limited degree, if at all" (*ibid*., para. 10).

Parenthetically, I would note that even the *Mor* case (which held that authority to issue an order for revealing the identity of an anonymous internet user should not be established by "judicial legislation") cannot be of aid to the Petitioners as a source for establishing that the absence of legislative authorization for the restricting activity nullifies the conduct. That affair addressed the limits of interpretation, and in particular, the limits of "judicial legislation", exercised by the *court*, and not the authority of the executive branch.

67. Similarly, we should distinguish the other cases referenced by the Petitioners, as follows:

A) The *Kahane* case concerned prior restraint, whereas in the case before us, the alleged offenses have already been committed, and the purpose is to frustrate their continued perpetration and their harm (on this distinction, see: Avigdor Klagsbald, *Criminal Offense and Prior Restraint*, 2 PLILIM 93 (1991) (Hebrew)).

B) The *Manaa* case concerned activities that restricted freedom of movement (placing roadblocks) by the police. Here, the infringement, to the extent that there is one, is performed by the internet platform operators and not by a governmental organ, not to mention that the potential victims are deemed to have agreed to the "community rules" (assuming that they are a type of adhesion contract, as held in the *Facebook* case).

C) The *Hof Azza Regional Council* case interpreted sec. 32 of Basic Law: The Government, and approved the payment of advances to those seeking to evacuate the Gaza Strip and Northern Samaria voluntarily, as it concerned an executive authority for which there is no legislative arrangement and the government's residual authority therefore applied. This is also the case in the matter before us in regard to the Department's voluntary referrals to the internet platform operators (and compare: HCJFH 9411/00 *Arco Electric Industries Ltd. v. Mayor of Rishon LeZion* [33], 64-65). Even the Prevention of Crimes Law *is not a negative arrangement in this regard, as it does not in any way address the subject of voluntary referrals*.

68. Moreover, in those cases in which residual power cannot be of help, the auxiliary authority under sec. 17(b) of the Interpretation Law comes into play. In such cases, and in the circumstances appropriate to the case before us, primary authority for performing voluntary enforcement derives from the general enforcement authority of the Attorney General by virtue of the criminal procedure laws, the Penal Law, and sec. 13 of the Interpretation Law (as argued by the Respondents), or by virtue of the general authority of the Minister of Justice under the Prevention of Crimes Law, including sec 16 therein (and compare: MApp 1190/18 *Ethics Committee v. David Yedid, Adv.* [34]).

There are also no grounds for the claim that the executive is trespassing, so to speak, the boundaries of the judiciary in finding that a prima facie offense has been committed by the publisher. The State Attorney's Office holds such authority and exercises it as a matter of course, as for example, in filing an information when there is a reasonable expectation of a conviction. Moreover – ever since the judgment in HCJ 442/71 *Lansky v. Minister of the Interior* [35], the accepted view is that a "criminal past" can be established on the basis of the administrative evidence test, even in the absence of a conviction (for a comprehensive survey of the subject, see: RON SHAPIRA, FROM CRIMINAL TO ADMINISTRATIVE ENFORCEMENT: ADMINISTRATIVE EVIDENCE OF THE COMMISSION OF A CRIMINAL OFFENSE – THE NEED FOR A FAIR ADMINISTRATIVE PROCESS (2019) (Hebrew)), and indeed, at times it is not possible to find the offender or bring him to justice, and yet it would appear that a crime has been committed, consequences can be attributed to it, and it is certainly possible to attempt to prevent the harm or its continuation.

This is the appropriate place to add that in most of the above cases, the granting of a right to be heard prior to taking administrative action is irrelevant, as the victim (whether because anonymous or unreachable) is not available (see and compare: CA 5739/18 *Operators of the Website www.oligarchescorts.com v. State of Israel* [36]; BARAK-EREZ, p. 499).

69. And now to return to the matter before us.

In my opinion, as long as it has not been proven that it is the activities of the Cyber Department that directly and certainly lead to a violation of fundamental rights, and as long as no evidentiary foundation has been laid showing that the discretion of the online platform operators is not *actually* independent, a voluntary referral from the Department to the online platform operators is not prohibited. In these cases, it is difficult to view the authority's actions as a form of intentional infringement of fundamental rights in a manner that would negate the authority of the Cyber Department to act to frustrate publications that amount to a prima facie criminal offense.

This is the place to reiterate that a very high percentage of the publications whose removal or restriction was requested by the Cyber Department concerned offenses of violence and terrorism, and it was not argued that those who committed the offenses are subject to Israeli law. The offenses that the Cyber Department seeks to frustrate by restricting publications that incite violence or terrorist acts are therefore at the heart of the residual powers granted to the government in the areas of security and foreign relations (see: SHETREET, pp. 567-597; COHN, p. 164).

In all that concerns offenses of incitement to violence or terrorist acts, this conclusion derives *a fortiori* from the conclusions of the Arbel Commission Report, in which the majority recommended *expanding* the voluntary enforcement mechanism even beyond its present state, so that voluntary referrals by the government would be permitted even when a criminal offense is not concerned. As opposed to this, the minority was of the view that the provisions of the Work Procedure are appropriate to the desirable situation. We are treating of the Work Procedure as it is, and we were not asked for any expansion. That is sufficient in the present matter.

70. Moreover, although the "principle of legality" in administrative law takes on different forms from state to state (and certainly between a state and a supra-national body), the citations and examples appended to the Respondents' supplementary brief show that at least in a number of western democracies, the authority to initiate the "voluntary" removal of harmful publications *is*

not conferred upon the administrative agencies *by virtue of express authorization to act in the said manner*.

71. In addition, I cannot accept the argument that residual power is displaced in the matter before us due to the express legislative provision treating of the authority to investigate and bring charges as detailed above, or by virtue of sec. 17(b) of the Interpretation Law. As noted above, enforcement of the type before us is entirely different from the criminal process – its purpose is not penal, but rather it attempts to prevent publication of material whose affect is immediate and requires speedy action for its removal in order to minimize ongoing harm (respectively): to public safety, public order, protection of the vulnerable, or the proper, fair conduct of elections.

A View to the Future

72. To summarize what has been stated thus far – in my opinion, the Respondents stand, although at times just barely, within the bounds of the law. It cannot be denied that the Cyber Department's activity, as presented in the preliminary response to the petition, is vital to the protection of national security and social order. The voluntary method by which the Cyber Department acts in this regard is not, however, problem free, primarily in regard to the absence of specific authority for its activity in primary legislation. However, until the enactment of detailed legislation on the matter (as has been done in some countries), the current situation can continue by virtue of residual power or auxiliary authority.

73. Beyond that, a number of overall problems have been uncovered that the Respondents should consider and correct, as set out below:

A) The Cyber Department should consider what was stated in the Movement's request to join, which described a series of defects in the Department's work, among them: a lack of documentation of the content of the publications that the Cyber Department seeks to remove, inadequate details in the transparency reports produced by the Department, and the non-publication of the Work Procedure (for example: the type of criminal offense grounding the voluntary act; a more detailed account of the alleged offenses related to the publication; the identity of the publisher and its relationship to the State of Israel, to the extent known to the Department). In addition, there is a problem in clarifying the role of

the online platform operators (which might have been clarified had those operators been joined as respondents to the petition), and the agreements between them and the Department.

In view of the fact that most of the Cyber Department's activity concerns security offenses, exposing the full extent of the Department's activity certainly presents a problem. However, I believe that the Cyber Department should present paraphrases and examples of the character of the referrals it sends and its discussions with the online platform operators in its transparency reports.

B) In making its referrals to the online platform operators, the Department should guide itself in accordance with the case law of this Court, which constitutes law that supersedes residual authority in this regard, including the judgments given in CrimFH 7383/08 *Ungerfeld v. State of Israel* [37]; LCrimA 5991/13 *Segal v. State of Israel* [38]; LCrimA 7052/18 *State of Israel v. Rotem* [39] (further hearing pending)).

C) A legislative initiative should be weighed to provide a detailed arrangement for the voluntary enforcement mechanism, as has been done in some other countries.

74. Another argument, which was not addressed in the framework of this petition, is the need for establishing a *post facto* oversight and supervision mechanism for the Department's activities, and it is recommended that this be considered (on the need for regulating the sphere of activity of actors on the internet in terms of procedure and proper constitutional balances, see my opinion in the *Premier League* case).

The above problems are not insignificant, but they do not, in themselves, justify issuing an order nisi in this petition in its present state. Nevertheless, the Respondents must draw conclusions for ameliorating the system in regard to all the aspects set out above.

Conclusion

75. In view of all the above, if my opinion be accepted, we will order the dismissal of the petition in all its parts, subject to my comments in paras. 73 and 74, without an order for costs.

Justice A. Stein:

I concur.

President E. Hayut:

1. In his comprehensive, in-depth opinion, my colleague Deputy President H. Melcer well described the uniqueness and complexity of the questions raised by this petition, among them the question of defining a governmental act; the question of the incidence of Basic Law: Human Dignity and Liberty beyond the borders of the state; the question of the rights of computer-generated fictitious users ("bots"), where it is unclear whether and to what to extent a human agent stands behind them; as well as questions related to the area of the regulatory relationship between the state and private bodies operating online. They are unprecedented to a large extent, and even according to the Respondents, the activity that is the focus of the petition "is of a character unlike the usual activity of the State Attorney's Office" (see the letter of the Ministry of Justice of Jan. 10, 2019, Appendix R/9 of the Respondents' response to the petition).

I will, therefore, begin by saying that in my opinion, it is very difficult to examine these substantive questions of first impression given the partial picture presented to us. Therefore, if my opinion were accepted, the petition would be dismissed *in limine*.

2. The activity that is the subject of the petition is that of the Cyber Department of the State Attorney's Office (hereinafter: the Cyber Department or the Department) in the "voluntary" enforcement track. As my colleague the Deputy President explained, in accordance with a Work Procedure that it established, the Department initiates referrals to online platform operators (social networks, search engines, and website hosting providers) to report publications that, in the opinion of the State Attorney's Office, constitute an offense under Israeli law and *also* breach the Terms of Use of the platform itself. According to the Department's preliminary response, such referrals are sent to the online platform operators only when there are additional considerations that justify the referral, among them the severity of the publication, the scope of its distribution and its "viral" potential. In practice, the Department focuses primarily upon publications related to the operations of terrorist organizations and in the matter of inciting violence and terror. Referrals are also sent

in regard to publications that may harm minors, certain public servants, or the integrity of Knesset elections.

My colleague the Deputy President noted that the petition suffers from two defects that are sufficient for its dismissal *in limine*. They are *the failure to join the online platform operators* as respondents to the petition, and an *insufficient factual foundation* for the argument that the Cyber Department acts without authority. This, inter alia, in view of the uncertainty as to the questions of whether the publishers that are the subjects of the referrals are people or "bots"; whether they are located in the country or abroad; and whether the online platform operators decide to remove publications independently or are perhaps influenced by the fact that the referring body is the State Attorney's Office. However, my colleague was of the opinion that in view of the fundamental constitutional questions raised by the petition, they should be addressed on the merits. In his opinion, the activity of the Cyber Department constitutes a governmental act, and where there is a possibility that the Department's referrals may influence the decisions of the online platform operators whether to remove the publications, there is a need for some form of authorization for the Department's activity. Therefore, my colleague addressed the question whether it is possible to discover a source that authorizes the Cyber Department to act in this manner, and concluded that it can be premised upon the residual power granted to the government under sec. 32 of Basic Law: The Government, as long as the Cyber Department's activity does not infringe fundamental rights, inasmuch as residual power cannot serve as the basis for such infringement.

3. On the basis of the foundation laid out before us in regard to the manner of the Cyber Department's activity and its consequences for the online platform operators, and in view of the significant deficiencies in that foundation, my colleague is of the opinion that it cannot be said that the state is the entity that infringes a constitutional right. In this regard, he emphasizes the significant difficulty inherent in recognizing the possibility of the infringement of freedom of expression of a non-human entity (e.g., "bots" and "avatars"). He further emphasizes that the entity that holds the power to decide whether or not to remove the publication is the platform operator and not the state. Therefore, my colleague holds that "as long as it has not been proven that it is the activities of the Cyber Department that directly and certainly lead to a violation of fundamental rights, and as long as no evidentiary foundation has been laid showing that the discretion of the

online platform operators is not *actually* independent, a voluntary referral from the Department to the online platform operators is not prohibited" (para. 69 of his opinion).

4. I concur with the conclusion of my colleague the Deputy President that the activity of the Cyber Department that is the subject of the petition constitutes a governmental act. In this context, the words of Justice I. Zamir in regard to the definition of "administrative authority" are apt:

> When an administrative agency exercises its authority, […] it fulfils a public function under law. That being so, it is subject to the special system of laws that is the system of administrative law […] It is possible that this is the simple and appropriate way to define administrative authority: *Administrative authority is a public function in accordance with law* (IZHAK ZAMIR, ADMINISTRATIVE AUTHORITY, vol. I, *The Public Administration*, 205 (2nd expanded edition, 2010) (Hebrew) (emphasis added).

In the matter before us, as my colleague the Deputy President noted in his opinion, the Cyber Department's referral activity is systematic, focused, broad, and organized: Attorneys of the State Attorney's Office send referrals to the online platforms in regard to publications that are prima facie criminal offences, regarding which there is a public interest in their removal, and that prima facie breach the Terms of Use of the platform. This is part of a declared plan of the State Attorney's Office, and in in accordance with a dedicated procedure established for the purpose (see para. 15 of the Respondents' supplementary brief). In these circumstances, it is clear that the Cyber Department's activity constitutes a "public function", and thus is a form of decision or exercise of authority on behalf of the state.

5. The center of gravity of the petition, in its present form, is the question of infringement of a fundamental right. According to the Respondents, even if the Cyber Department's activity constitutes a governmental act, and therefore requires a conferral of authority, it is possible to suffice in this regard with the government's residual power (sec. 32 of Basic Law: The Government, which my colleague the Deputy President discussed at length), or the authority of the State Attorney's Office as the representative of the Attorney General, who holds the auxiliary authorities required for the performance of his role (based upon secs. 3 and 17 of the Interpretation Law, 5741-1981). Auxiliary authority and residual power cannot form the basis of an infringement of a fundamental right (see HCJ 5128/94 *Federman v. Minister of Police* [16], 652; sec. 8 of Basic Law: Human Dignity and Liberty, according to which any violation of rights under that law

requires express authorization by a law or by virtue thereof; and see DAPHNE BARAK-EREZ, ADMINISTRATIVE LAW, vol. 1, 146 (2010) (Hebrew); HCJ 4455/19 *Tebeka Advocacy for Equality and Justice for Ethiopian Israelis v. Israel Police* [40], paras. 14 and 34)). Deciding whether there is sufficient authorization for the activity of the Cyber Department is, therefore, largely contingent upon whether that activity infringes fundamental rights. According to the Respondents, the "informing" and recommending referrals by the Cyber Department to the online platform operators do not amount to a violation of rights. That is so because the platform operators exercise independent discretion in all that concerns the removal of the content that is the subject of the referrals, whereas the Cyber Department only makes recommendations.

The petition before us suffers from two material defects that my colleague the Deputy President addressed, each of which – and *a fortiori* cumulatively – frustrate the possibility of deciding this fundamental question on the merits. Therefore, in my opinion, there is no recourse but to dismiss the petition *in limine*. These defects are, as noted, *the failure to join relevant respondents*, and *a lack of a factual foundation*. I will address these respectively.

6. *Failure to join relevant respondents* – as has been held on more than one occasion, refraining from joining those who may be affected by the decision upon the petition constitutes a material defect that can justify dismissing the petition *in limine*. This, inter alia, because the respondents who were not joined can shed essential light on the issues to be addressed: "In order for the court to ground its decision upon a full, reliable picture of the situation, there is no one better to present the opposing view than one who is related to the matter and may be harmed by a court order" (HCJ 1901/94 *MK Landau v. Jerusalem Municipality* [41], 415 (hereinafter: the *Landau* case); and also see IZHAK ZAMIR, ADMINISTRATIVE AUTHORITY, vol. III, *Judicial Review – Threshold Rules*, 1747 (2014) (Hebrew)). This defect is particularly salient when the petitioner has been granted the opportunity to correct the omission and chose not to do so (HCJ 151/11 *Ruth and Emanuel Rackman Center v. Minister of Justice* [42], para. 17; and compare: HCJ 384/82 *Pachmas Metal & Plastic v. Minister of Finance* [43], 300-301)).

In their preliminary response to the petition, the Respondents raised several arguments in regard to this threshold requirement, and the Petitioners' attorney was even asked about this in the course of the hearing on Aug., 8, 2020, responding:

> We considered whether to join, we considered before whom to petition. We are not arguing against Facebook or any other company. We are arguing that we have here a governmental act by the state that refers to the content providers in this entire sphere of removal of content without connection; the governmental act here is that of initiated referral by the Cyber Department – that is an act that requires authorization. […] We do not believe that there is harm [to the operators] (p. 4, lines 29-32 of the transcript).

7. I am unable to accept this argument. The Cyber Department's Work Procedure lists a "mixed multitude" of "online platforms", and the differences outnumber what they share in common in no few aspects (see sec. 1 of the Procedure). The online social networks (Facebook, etc.) are unlike online search engines (like Google) or website "hosting" providers (like WordPress). And an online social network, in which mostly text and pictures are shared (like Facebook and Twitter) is unlike a social network for sharing only videos (like YouTube). These platform operators are differentiated by a number of criteria that have consequences for the questions at the heart of this petition, among them: the type of contents regarding which the Cyber Department sends notifications; the policy for treating those referrals; and the importance that each operator assigns to the identity of the party requesting the removal of content. The question whether and to what extent these operators are expected (all or some) to be harmed by the granting of the petition was also not sufficiently examined, and I am not convinced that the Petitioners succeeded in showing that those operators *cannot be expected to be harmed at all* by a decision on the merits in this petition. As my colleague the Deputy President noted, we have before us a "triangular relationship" or a "power triangle" with three vertices: the state, the publishers (in whose names the Petitioners argue), and the online platform operators. Without representation for one of the vertices of the triangle, it is impossible to decide material questions that affect the entire triangle.

Indeed, at times the Court is willing to address a petition on the merits despite the defect of not joining relevant respondents, for example, "if the harm to the third party is negligible, if there are grounds for assuming that he is not interested in arguing before the Court, or if it is clear that one of the Respondents will fully and adequately present the arguments in regard to that party" (the *Landau* case, p. 415). Without expressing an opinion on the question of the scope of the harm that would be caused to the platform operators if the petition were granted, it is clear that there are

no grounds for assuming that *all* of these operators are not interested in voicing their position on the matter at the heart of this petition, or for assuming that the parties to the petition can present the full picture in regard to those operators.

8. Thus, we find that this petition suffers from a material defect of not joining respondents who may be harmed by the decision rendered, and the information they have may even materially affect the decision on the merits of the Petitioners' arguments. This is particularly so in regard to the question whether the Cyber Department's activity infringes constitutional rights, and the question of the scope of the alleged infringement. The Petitioners were confronted with the said defect at the preliminary stage and chose not to remedy it.

Even if one were to argue that this defect can be remedied by alternative means, such as joining the respondents at the Court's initiative, that would be to no avail as the petition, in its current state, suffers from an additional, no less material defect in regard to the insuffciency of the factual foundation necessary for deciding upon it.

9. As my colleague the Deputy President emphasized in his opinion, we were not presented with data on the scope of the infringement of fundamental rights caused as a result of the operators' acceding to the Cyber Departments referrals. In particular, it was not made clear what part of the referrals concern publications that originate beyond the borders of the state, anonymous publications, or publications that were not uploaded by human beings – in which case, as my colleague noted, material questions arise in regard to the applicability of Basic Law: Human Dignity and Liberty to those publications. In addition, although the Respondents presented data in regard to the total number of referrals issued by the Cyber Department over the last few years (see para. 17 of the opinion of my colleague the Deputy President) and asked to present *ex parte* "a number of concrete examples of the Cyber Department's reports to the online platforms in various areas" (para. 26 of the preliminary response), it appears from the Movement for Freedom of Information's request to join that the Cyber Department does not maintain a database of all the publications regarding which it sends referrals. The activity reports published by the Cyber Department present only laconic information about the publications regarding which referrals are sent, the identity of the publishers and the reasons for sending the referrals (see para, 73(a) of the opinion of my colleague the Deputy President).

10. The absence of a factual foundation in regard to the activity of the Cyber Department does not fall upon the Petitioners but rather upon the Department itself, and the relevant data is in its possession or can be obtained by it. However, the Petitioners did not focus their arguments upon the transparency of the Cyber Department's activity, did not request an operative remedy in this regard, did not exhaust the procedures with the Respondents in this regard, and it is not clear whether they submitted requests in this matter under the Freedom of Information Law, 5758-1998. In these circumstances, and given the factual gaps addressed in the opinion of my colleague the Deputy President, I do not believe that it is possible to continue to examine the petition on the merits in its current state.

11. The primary question raised by the petition before us is, as stated, whether the referral activity of the Cyber Department – as expressed in the Work Procedure that it established – leads to a violation of fundamental rights. To the extent that the answer is in the negative, it is possible to suffice with the sources of authority cited by the Respondents, and hold that this activity does not constitute a deviation from authority, while to the extent that the answer is positive, the Respondents will be required to find some alternative source of authority, in the absence of which there will be no recourse but to hold that the Cyber Department acts *ultra vires*. A significant component of the Petitioners' argument thus treats of the alleged infringement of freedom of expression. The Petitioners further argue that the Cyber Department's activity also involves an infringement of the right to due process and the right to be heard, because it does not afford the publishers the right to be heard prior to sending the referral, which includes the Department's position that the publication constitutes a prima facie criminal offense.

My colleague the Deputy President is of the opinion that there is no violation of a constitutional right in this case, without seeing a need to decide the question of the criteria for the existence of an infringement of a constitutional right (paras. 63-65 of his opinion). To my mind, the accepted approach, long established in the case law of this Court, is that when there is an infringement of a constitutional right that is not *de minimis*, the constitutional review moves from the first step – that of the violation – to the second, i.e., examining the justification for the violation in the framework of the tests of the Limitation Clause. In any event, under the circumstances of the matter before us, the insufficient factual foundation in regard to the manner in which the Cyber Department operates, together with the insufficient factual foundation in regard to the conduct of

the online platform operators, which largely derives from their not being joined to the petition (particularly the question of the importance they assign to the fact that the referrals are sent by the Cyber Department of the State Attorney's Office of the State of Israel), all lead, in my opinion, to the conclusion that, at this point in time, *it is not possible to decide* the question whether the Cyber Department's activity leads to an infringement of freedom of expression or of the right to be heard and the right to due process. In other words, in view of the partial picture of the necessary facts presented to us, and in view of the absence of the online platform operators as parties to the petition, it is not possible, in my opinion, to examine the material questions raised by the petition, and there is no alternative but to dismiss it *in limine*. I would also join the comments in para. 73 of the opinion of my colleague the Deputy President in regard to the difficulties presented by the activities of the Cyber Department, and his call for the publication of the details of the Work Procedure of the Cyber Department (para. 12 of his opinion). Therefore, were my opinion accepted, we would order the dismissal of the petition *in limine*, without an order for costs.

The petition is denied.

Given this day, the 30th of Nissan 5781 (April 12, 2021).