COMBINING MULTIPLE DISINFORMATION COUNTERMEASURES TO REGULATE ELECTION DISRUPTIONS: THE SOUTH KOREAN CASE

Soyun Ahn
Annenberg School for Communication and Journalism, University of Southern California

Overview and Framework

Researchers, the press, and the public alike have expressed strong concerns about disinformation influencing public discourse and elections, perceiving it as a direct threat to democracy. Disinformation often involve malicious use of social media to sway public opinion for certain political outcomes, in the form of intentionally fabricated information (Marwick & Lewis, 2017). A recent scrutiny of organized social media manipulation campaigns around the globe detected evidence of such in 70 countries in the year of 2017 and 2018 (Bradshaw & Howard, 2019).

As a reaction, democratic countries once reluctant to restrict freedom of speech are now actively examining countermeasures to disinformation. Bradshaw, Neudert, and Howard (2018) investigated 43 countries which implemented or proposed regulations to combat disruptive online communication since 2016, and provided a typology of measures based on four target actors. The first set of measures go after social media platforms and require them to cooperate with the state through content takedown, enhanced advertising transparency, and user data protection. Second, targeting individual offenders, countries tried to criminalize disinformation and automation through a new legislation, or tried to build on existing legal frames by expanding the definition of illegal content. Third, as a more civil society and citizen centric approach, media watchdog and media literacy education has been funded by multiple states. Lastly, measures targeting governments included disinformation monitoring by government agencies, or an operation of cybersecurity units by the military to address foreign intervention.

Often times, the biggest challenge in making policy decisions to regulate disinformation is the delicate negotiation of the two competing values: protection of the public sphere from malicious actors and the protection of freedom of speech (Fried & Polyakova, 2018).
The existing literature so far has focused more on examining the pros and cons of individual policy directions rather than providing an overview of the entire dynamics when multiples measures are combined in practice (for instance, Haciyakupoglu, Hui, Suguna, Leong, & Rahma, 2018). That is due to the novelty of the problem of disinformation itself and the lack of regulation implementation cases, with most countries being still at their infancy discussing or inventing such measures.

The South Korean Case

South Korea is unique in that it has operated a system dealing with disinformation for over a decade now, and in that it has a system specifically dedicated for election protection. It’s Public Official Election Act specifies a system that combines three of the four measures mentioned above, regulating online platforms, criminalizing offenders, and pervasive governmental monitoring system (Kee, 2018). At the same time, this system has been criticized as largely discounting the freedom of speech in South Korea (Haggard & You, 2015). Through scrutinizing both the legal framework and execution practices of the multiple disinformation regulatory measures in South Korea, this research expands the existing literature by providing an overview of the dynamics how multiple measures cooperate, based on a real-world case analysis.

<table>
<thead>
<tr>
<th>No.</th>
<th>Provision Name</th>
<th>Type</th>
<th>Content</th>
</tr>
</thead>
<tbody>
<tr>
<td>10-3</td>
<td>Cyber Fair Election Support Group</td>
<td>Governmental Monitoring</td>
<td>National Election Commission’s Responsibility to establish and operate a Cyber Election Support Group which monitors online Election Act violation</td>
</tr>
<tr>
<td>82-4</td>
<td>Election Campaigns by Utilizing Information and Communications Networks</td>
<td>Criminalizing Offenders, Regulating Platforms, Governmental Monitoring</td>
<td>Prohibition of disinformation spread, responsibility of providers of internet and communication services to follow the Election Commission’s request to delete or restriction of content that disseminate untrue facts of candidates or their families</td>
</tr>
<tr>
<td>82-6</td>
<td>Identification of Real Names on Bulletin Boards or Chatting Pages, etc. of Internet Press Agencies</td>
<td>Criminalizing Offenders, Regulating Platforms, Governmental Monitoring</td>
<td>Requires internet service providers to collect personal identification information, such as their real name on official documents, for users to post election-related</td>
</tr>
</tbody>
</table>
The existing legal framework regulating disinformation in South Korea is based on a system of the government tightly monitoring online activities, platforms complying to the governmental supervision, and offenders being criminalized and sentenced for their malpractices. Both the government of the candidate could file a case of violation, and then platforms are required to promptly take down content and offenders are arrested.

In practice, for every election, the National Election Commission of South Korea organizes an oversight board that consist of 8 institutions (Korea Communication Commission, Supreme Prosecutor’s Office, National Police Agency, National Forensic Service, Press Arbitration Commission, Korea Internet Self-Governance Organization, Journalists Association of South Korea) and 5 online platforms (Naver, Kakao, Twitter, Facebook, Google), who meet to discuss how to react to cyberspace election disruptions. For the 2020 General Election, they agreed for the followings: a) to form a collaborative board to monitor and stop the spread of misinformation or hate speech, b) to share the personal information of the individuals who spread misinformation and hate speech, c) to create a system where platforms instantly deletes posts and submit relevant information upon requests, and d) to timely collaborate to arrest offenders.

To sum, this paper demonstrates how the legal framework of South Korea’s disinformation regulation combines governmental monitoring, regulating platforms, and criminalizing offenders. Moreover, by looking into the practice, it shows how freedom of speech is discounted not only by individual measures, but also by the institutional settings of multiple measures combinedly operating.

References


