Forum Ilmu Sosial 47 (2), December 2020, pp. 55-63
ISSN 1412-971X (print), ISSN 2549-0745 (online)
DOI: https://doi.org/10.15294/fis.v47i2.27057

The Impact of Surveillance on Journalist Activism

Bonifasius Santiko Parikesit Universitas Paramadina, Indonesia

Abstract
This study explored how alleged surveillance by the authorities was presented, responded to, and impacted journalists' activism. Employing the Panopticon framework, it is expected that those who become the object of surveillance change their behavior to become more submissive to authority. By means of a series of in-depth interviews with two print media journalists and one media researcher, it was found that journalists were threatened by the "disturbance" that befell them. However, this would not change them in conveying the public interest. They also adapted to the threats that came about. Many interview subjects refused to participate in this study because of the sensitivity and potential risks they received from the discussion.

Keywords
Surveillance; Journalist; Panopticism

INTRODUCTION

Since Edward Snowden exposed the National Security Agency (NSA)'s digital surveillance program in the United States in 2013, the controversy has continued to spread widely and has led to speculation about who is being targeted and what impact the act might have. This is because the program coded PRISM is capable of storing and documenting thoroughly digital traces in the form of electronic mail, audio conversations, videos, documents, and other data were taken from 9 digital companies including Google, Apple, Microsoft, and Facebook (Waters, 2018).

The program, which was initially designed to be limited to gathering information related to national security, has also inadvertently collected some data on US citizens (Gellman & Poitras, 2013). James Clapper, Director of the NSA said that although it had involved a number of lengthy procedures and received court approval that only non-US and non-US persons would be targeted, it did not rule out that US citizens could be affected (Stein, 2013).

Even though the information disclosed is not something entirely new, Snowden has made the world aware of the extent to which government surveillance has been exercised without considering human rights values. There have even been repeated acts of harassment and prosecution for those taking critical positions of authority.

Assisted by the rapid development of artificial intelligence and the lowering cost of surveillance technology, actions that are generally carried out in the "label" of this national security program are no longer limited to regimes that have lots of resources, but also by "poor" countries led by the authoritarian (Woodhams, 2019). There are at least 13 countries in Asia that have openly introduced advanced programs to monitor the social media activities of citizens between June 2018-May 2019 (Shahbaz & Funk, 2019).

As a result, as happened in Kazakhstan, Pakistan, and the Philippines, there was a decrease in the index of freedom of expression on the internet. In Kazakhstan, for example, due to the use of monitoring instruments, the government has succeeded in mapping the parties that have been aggressively criticizing. For those who are considered too "harsh", there are consequences in the form of arrest

Email correspondence: bonifasius.parikesit@gmail.com
Received: November 9, 2020; Accepted: December 7, 2020; Published: December 18, 2020.

and prosecution as experienced by Ardak Ashim. In his case, he was interrogated by law enforcement officials before being forcibly placed in a mental hospital (RSF, 2018).

Using the same method with different approaches, the authorities in the Philippines and Pakistan have also done similar actions. In the Philippines, the government combined surveillance equipment purchased by the government from the UK with the Cybercrime Prevention Act. As a result, there was an action to silence a group of parties who were critical of the government, as experienced by Maria Ressa, a journalist for *Rappler*. On the same side, authorities in Pakistan, through a number of robotic accounts, sent messages of hatred and cornered them to intimidate a number of critical journalists (DRM, 2019). This can be seen in the emergence of hashtag *#ArrestAntiPakJournalist* which echoed on Twitter on the fourth and fifth of July 2019.

In Indonesia itself, the state has never acknowledged the existence of surveillance measures carried out by the public. However, in a condition where the state is not serious about revealing the perpetrators of surveillance actions that often lead to hacking, the state is considered to be responsible for the events that occur (Asfinawati, 2020). According to records compiled by researchers, surveillance has occurred since 2014 targeting the mainstream online media, *Tempo.co*. The group calling itself *Zone Injector* wrote the phrase "we have warned you but you did not respond to our good intentions". As a result of this action, the *Tempo.co* website was down for five minutes. This case was also reported to law enforcement officials.

Not yet finished the case was disclosed, surveillance action took place again with a larger target group. For example, the actions that befell anti-corruption activists such as Oce Madril and Rimawan at the end of 2019, University of Indonesia epidemiologist Pandu Riono, democracy activists Ravio Patra and Ainun Najib, were also experienced by online media institutions such as *Tirto* and *Tempo.co* in 2020. This condition is described by *Kompas* (Rahayu, Yogatama & Patricia, 2019) as an action that indicates a pattern to silence criticism.

In an article entitled What's New about the new surveillance? Classifying for change and continuity, Marx (2004) defined surveillance in the digital era as activities that are carried out secretly by involving visual and physical aspects, and utilizing new technology to collect personal data. The goal is to influence or manage the data that has been collected (Lyon, 2003). Similar to the explanation above with the deepening of the parties who carry out supervisory actions, McQuail (2010) defined supervisory action as something that involves "authority" either from the government, law enforcement or business entities to certain individuals or groups to collect certain information. The party who collects the information will compile it into data to be analyzed for a specific purpose.

In fact, if investigated further, the emergence of surveillance in the digital space that has occurred recently can be said to be the 4.0 version of the surveillance actions that have been happening so far. In the past, these acts were carried out by means of blackmail as experienced by (1) *Kompas Daily* in 1965 and 1978; (2) *Tempo Magazine* in 1982 and 1994, and (3) *Editor Magazine* and *Detik Tabloid* in 1994. These acts are currently undergoing changes in "packaging" although

with the same spirit, namely attacking those with critical voices against the ruler. *Tirto* and *Tempo.co* can be examples of how this happens in cyberspace.

Specifically, for *Tempo.co*, which represents *Tempo* in the digital world, hacking in the past decade has occurred twice, namely in 2014 and 2020. Comparing the conditions that occurred, if in 1982 and 1994 the perpetrators of raids were very clear and bright, in the era of 4.0, hackers are not certainly known. In fact, in several recent cases, the attacks that have come about have not only targeted media institutions but also targeted groups of journalists who write stories.

Regardless of the purpose of surveillance, in principle, this action will have an effect on the behavior and social conditions of those who are becoming the object (Brivot & Gendron, 2011). Through the Panopticon framework developed by Michel Foucault, it was hoped that those who experience supervision will submit to the authority (Foucault, 2012). The outcome that was expected by the authorities from this framework is the existence of social order and efficiency in the social system in society (Richards. 2012), although this sometimes has a negative impact on the dynamics of democracy in civil society.

This paper intends to reveal the perceptions, responses, and impacts of surveillance on journalist activism. The basis that was built was taken from previous research which revealed that surveillance has the potential to damage the relationship between journalists and sources. This occurs because of the risk of disruption in the informants' lives, if they are willing to be interviewed to describe topics that have high sensitivity to government activities (Waters, 2018).

METHODS

This research was conducted through a qualitative approach functioning to discover and understand phenomena, as well as how people interpret their experiences (Merriam & Tisdell, 2015). Exploration in this research was held on a small number of cases rather than quantitative research, which was performed through several incremental measurements to collect the correct formulation for a large number of cases. Almost all qualitative research tried to build representations based on the depth and detail of knowledge about a case (Neuman, 2014).

To complete the process design, this study utilized a descriptive type to describe phenomena in real life (Yin, 2016). Descriptive case studies have a function to describe a symptom, fact or reality (Raco, 2010) and try to examine as much data as possible, to describe in "thick" and explain various aspects related to Mulyana's research subject (2006). The analysis was carried out based on data obtained from interviews, observations, documentation, impressions, and statements of a person on the case under study.

The choice of this method was held to analyze the extent to which the surveillance actions experienced by journalists were perceived, responded to, and had an impact on them. For this reason, the researcher conducted in-depth interviews with a number of sources who were related to the topic being taken. The method of selecting sources was purposive sampling, namely the selection based on certain considerations. Then the

Table 1. Perceptions, Responses, and Impacts of Surveillance

No.	Variable	Journalist A	Journalist B
1	Perception on surveillance	Surveillance is perceived as something that is allowed to occur in the public sphere provided that the principles and criteria are carried out based on the values of transparency, accountability, and accountability. However, with the conditions that have occurred recently in Indonesia, the action seems unacceptable because "certain individuals" who are on the side of the government use surveillance only to benefit their interests.	The surveillance is perceived as something that is not allowed to occur in the public sphere because of its nature that causes disturbances to democracy and is closely related to forms of authoritarianism.
2	Responses on surveillance	The surveillance befalling me coincided with the writing of an article regarding the alleged use of "Pegasus" by Indonesian authorities. The chronology is one day after meeting at the office to discuss the written plan, I received an SMS containing the OTP code twice. The same thing happened to my colleague who was helping me finish the writing. To control the existing conditions so as not to "spread" to other parties, I informed what happened and asked my colleagues to be introspective and take preventive steps.	Supervision action took place in mid-2019 in conjunction with plans to carry out discussions within the Independent Journalists Alliance (AJI). Presenting a figure from Vietnam, AJI held a discussion at the secretariat office at that time. Prior to the discussion, my Facebook account was hacked and sent "pervert" information produced by invisible hands. During the discussion there were a number of parties who came to the discussion location and asked to disband the activity. At the time of the surveillance, I immediately contacted my colleagues through several other channels to inform them about what was going on. I warned them to be alert. I have to convince myself that this will not interfere with my position in conveying the public interest. Then related to the fear of a number of sources to convey messages after the digital violence that befell them, I have to further convince them that the interviews will be conducted through safe channels that have low potential for certain parties to monitor them.

Source: Interviews.

researcher drew conclusions based on the collected data.

FINDINGS AND DISCUSSION

Technological developments are not only having a profound effect on how we communicate but also talking about how surveillance occurs. Data taken by those who have "authority" in intervening in the digital world to be retrieved or stored indefinitely (Taekke, 2011) has become a separate dynamic in the digital world. This is ironic, as freedom from surveillance is an important part that becomes a critical point in ensuring the existence of the press as one of the pillars of democracy.

Rusbridger (2017), the former editor in chief of *The Guardian,* stated:

> "Every journalist should understand the information that Snowden delivered regarding digital security—this is because democracy, even in liberal countries, has the ability to intercept, store, and analyze all forms of electronic communication. They can perform human recognition based on the information stored in their database. Authorities appointed by the ruler can read text messages against

some of the targets they are devising. Authorities can even access all contacts and carry out location tracking of the targeted party".

This then led journalists to understand digital security, including the risks and threats that might arise from surveillance. All of these actions are carried out to help them protect themselves from surveillance and maintain communication security with colleagues, resources (interviewees), and other editorial members (Lashmar, 2017). However, this is admittedly quite difficult to do.

In Indonesia, the practice of violence against journalists also goes on its track. We actually had received fresh air after the collapse of the New Order regime by means of Law No. 40 of 1999, stating press freedom is guaranteed as a human right of citizens (Ruswandi, 2004). However, instead of giving birth to change, conditions that occurred in the field were stagnant. The Alliance of Independent Journalists (AJI) stated that press freedom is almost non-existent. If in the 1980s there was a "telephone culture" as part of surveillance (Susilastuti, 2000), the actions that are happening these days have shifted to digital platforms as has happened at the global level.

Based on in-depth interviews conducted by the author of two national print media journalists who did not wish to be named with questions about perceptions, responses, and the impact of surveillance, the following table 1.

Referring to the results of the interview, it can be seen that monitoring acts are perceived by journalists as something that is not possible in today's public space. The accountability factor and transparency of the unclear use of supervisory tools, plus the confusion of the parties appointed to carry out the supervision are the causes. If adequate action is not taken, it is feared that the presence of surveillance in the digital world will only narrow the movement of democracy and make us threatened with authoritarianism.

Finding a common consensus to answer the challenge of surveillance in the public sphere is not easy. Regan (2012), in her article entitled *Regulating Surveillance Technologies: Institutional Arrangements*, explained that in the last 40 years, there has been a lot of debate about the types of involvement of the parties, especially the government, and the possible institutional arrangements formed to ensure that surveillance technology is used in a legal manner and can be socially accepted in the practice of social life. However, the practice of surveillance, which is often carried out on the grounds of determining power, in the sense that certain parties can extract implied and express information from within the device and destroy the privacy of its users, is still a challenge. Any surveillance that exists without clarity of regulations has the potential to eliminate individual control over the information they have.

Then responding to the surveillance actions that occurred, the two journalists immediately took a position to inform their colleagues and other members of the editorial team. This is to prevent the act from spreading to other parties. According to Anderson (2001), there are several things that influence users to understand digital security, namely economics and psychology. Whitten and Tygar (1999) mentioned that the experience factor of using software also has an influence, beyond

the user's perception of the experience of using the security network itself (Kang et al., 2015).

Third, related to the impact of surveillance activities, it was felt by journalists to interfere with their work and potentially damage their relationship with a number of sources or interviewees. This is because the pressure comes not only on them but also on interviewees who are threatened subtly through physical and digital attacks. In an interview session conducted by the author to one of the SafeNet members, it was stated that any action that could potentially interfere with freedom of expression was primarily related to digital rights which include: (1) the right to access, (2) the right to expression, and (3) the right to feel safe. Violations cannot be tolerated because they have the potential to silence those who speak critically. For example, this can directly be seen from the incident experienced by one of the band's Banda Neira personnel, as its vocalist Gigih was arrested in the period KPK Bill demonstrations at the end of 2019. The "critical voice" that he often made seemed to fade when the Omnibus Law on Job Creation was rolled out in mid-2020. It seems that the action of pressure and intimidation was carried out by a number of elements in the warning "label" according to journalist A, which has a significant impact on those concerned. The same condition also happened to one of the founders of *KawalPemilu* who is currently struggling to provide information to the public regarding the dangers of Covid-19. The dissemination of information that some government supporters perceive as noise that interferes with government work processes has resulted in a number of threats. As experienced by the band personnel, this co-founder of Kawal Covid-19 finally decided to reduce his intensity in voicing critical voices from August to September 2020.

Even though they are under a lot of pressure, for the journalists who are the sources in this research, surveillance will not make them trapped in the Panopticon putting them submit to the "line" determined by the ruling authority. Both said that they would continue to convey voices in favor of the public interest and the truth. They also began to adapt to the environment. One way performed is by downloading several communication channels such as a wire application which ensures end-to-end encryption.

For those who agree with the Editor of Tempo (2020), the act of hacking and terrorizing civil society should be regarded as cowardly because civil liberties are not only a matter of public rights to be heard, but also the state's need to be straightened out. The community must also be equipped with the ability to understand the basis for such supervisory actions to be permitted by the authorities.

CONCLUSION

Surveillance, especially towards journalists, is actually not a new thing. In Indonesia, in the 1980s there were a "telephone culture" and bans as part of surveillance measures. Now, there is a hack in cyberspace that can be said to be version 4.0 of surveillance. Despite undergoing changes in "packaging", both are carried out with the same spirit, namely attacking those whose voices are critical of authority.

Referring to the results of the interview, it can be seen that surveillance is something that is not possible to happen in public spaces

at this time. The accountability factor and transparency of the unclear use of supervisory tools, plus the confusion of the parties appointed to carry out the supervision are the causes. If adequate action is not taken, it is feared that the presence of surveillance in the digital world will only narrow the movement of democracy.

Indeed, democracy requires the parties involved, especially the government, to inform what techniques are used to carry out surveillance, how the results of these acts are stored, for how long, and who has access to the data.

REFERENCES

Anderson, R. (2001). Why information security is hard-an economic perspective. In *Seventeenth Annual Computer Security Applications Conference* (pp. 358-365). IEEE.

Asfinawati. (2020). *Peretasan Digital Apa Benar Untuk Bungkam Kritik? Satu Meja The Forum (Bag 3)*. Retrieved from YouTube: https://www.youtube.com/watch?v=kJNasiIY_BU.

Brivot, M., & Gendron, Y. (2011). Beyond panopticism: On the ramifications of surveillance in a contemporary professional setting. *Accounting, Organizations and Society*, *36*(3), 135-155.

DRM. (2019). *DRM Investigates: Twitter Accounts Behind the Hashtag #ArrestAntiPakJournalists*. Retrieved from Digital Rights Monitor: https://www.digitalrightsmonitor.pk/drm-investigates-twitter-accounts-behind-the-hashtag-arrestantipakjournalists.

Foucault, M. (2012). *Discipline and punish: The birth of the prison*. Vintage.

Gellman, B., & Poitras, L. (2013). *US, British Intelligence Mining Data from Nine USInternet Companies in Broad Secret Program*. Retrieved from Washington Post: https://www.washingtonpost.com/investigations/us-intelligence-mining-data-from-nine-us-internet-companies-in-broad-secret-program/2013/06/06/3a0c0da8-cebf-11e2-8845-d970ccb04497_story.html.

Kang, R., Dabbish, L., Fruchter, N., & Kiesler, S. (2015). "My Data Just Goes Everywhere:" User mental models of the internet and implications for privacy and security. In *Eleventh Symposium On Usable Privacy and Security ({SOUPS} 2015)* (pp. 39-52).

Lashmar, P. (2017). No more sources? The impact of Snowden's revelations on journalists and their confidential sources. *Journalism Practice*, *11*(6), 665-688.

Lyon, D. (Ed.). (2003). *Surveillance as social sorting: Privacy, risk, and digital discrimination*. Psychology Press.

Marx, G. T. (2004). What's new about the "new surveillance"?: Classifying for change and continuity. *Knowledge, Technology & Policy*, *17*(1), 18-37.

McQuail, D. (2010). *McQuail's mass communication theory*. Sage Publications.

Merriam, S. B., & Tisdell, E. J. (2015). *Qualitative research: A guide to design and implementation*. John Wiley & Sons.

Mulyana, D. (2006). *Metodologi penelitian kualitatif: paradigma baru ilmu*

komunikasi dan ilmu sosial lainnya. PT Remaja Rosdakarya.

Neuman, W. L. (2014). *Social Research Methods: Qualitative and Quantitative Approaches: Pearson New International Edition*. Pearson Education Limited.

Raco, J. R. (2010). Metode Kualitatif (Jenis, Karakteristik, dan Keunggulannya). *Jakarta: PT. Gramedia Widiasaranan Indonesia*.

Rahayu, K. Y., Yogatama, B. K., & Patricia, S. (2019). *Yang Vokal yang Diretas (1)*. Retrieved from Kompas: https://kompas.id/baca/utama/2019/09/24/yang-vokal-yang-diretas-1.

Regan, P. M. (2012). Regulating Surveillance Technologies. New York: Routledge.

Richards, N. M. (2012). The dangers of surveillance. *Harv. L. Rev.*, *126*, 1934.

RSF. (2018). *Kazakhstan escalates harassment of media, confines blogger to clinic*. Retrieved from Reporters Without Borders: https://rsf.org/en/news/kazakhstan-escalates-harassment-media-confines-blogger-clinic.

Rusbridger, A. (2017). *Journalism after Snowden. In: Bell E and Owen T (eds) Journalism after Snowden: The Future of the Free Press in the Surveillance State*. New York: Columbia University Press.

Ruswandi, A. (2004). Menakar Kadar Kebebasan Pers Indonesia. *Mediator: Jurnal Komunikasi*, *5*(2), 265-274.

Shahbaz, A., & Funk, A. (2019). *Freedom on the Net 2019 Key Finding: Governments harness big data for social media surveillance*. Retrieved from Freedom House: https://freedomhouse.org/report/freedom-on-the-net/2019/the-crisis-of-social-media/social-media-surveillance.

Stein, S. (2013). *Obama Administration on PRISM Program: Only Non-US Persons Outside the US are Targeted*. Retrieved from Huffington Post: https://www.huffingtonpost.com.au/entry/obama-administration-prism-program_n_3399858?ri18n=true.

Susilastuti, D. N. (2000). Kebebasan Pers Pasca Orde Baru. *Jurnal Ilmu Sosial dan Ilmu Politik*, *4*(2), 221-242.

Taekke, J. (2011). Digital panopticism and organizational power. *Surveillance & Society*, *8*(4), 441-454.

Tempo. (2020). Cara Pengecut Berangus Kebebasan. Retrieved from Tempo: https://kolom.tempo.co/read/1360644/cara-pengecut-berangus-kebebasan.

Waters, S. (2018). The effects of mass surveillance on journalists' relations with confidential sources: a constant comparative study. *Digital Journalism*, *6*(10), 1294-1313.

Whitten, A., & Tygar. J. D. (1999). Why Johnny can't encrypt: A usability evaluation of PGP 5.0. USENIX Security Symposium. Retrieved from Usenix: https://www.usenix.org/conference/8th-usenix-security-symposium/why-johnny-cant-encrypt-usability-evaluation-pgp-50.

Woodhams, S. (2019). *Social Media in Asia: A New Frontier for Mass Surveillance and Political Manipulation*. Retrieved from The Diplomat: https://thediplomat.com/2019/11/social-media-in-asia-a-new-frontier-for-mass-surveillance-and-political-manipulation.

Yin, R. K. (2016). Quantitative Research from Start to Finish. New York: The Guilford Press.