



Freedom of Expression in the Digital Age: Can Hacking Government Websites Be Justified?

Ricky Saputra

Faculty of Law, Universitas Sriwijaya, Palembang, Indonesia

✉ corresponding author: rickysaputra@fh.unsri.ac.id

DOI: 10.37893/jv.v2i2.949

Keywords:

Cybersecurity;
Cyber Law;
Digital Protest;
Limits of Freedom of
Speech

ABSTRACT

In today's internet era, hacking the official government website has become a controversial event that raises questions about the limits of freedom of expression. This article examines the debate surrounding the hacking of government websites as a form of online expression. In the virtual world, individuals or groups can express their opinions, express their dissatisfaction, or criticize the government. However, the hacking of official government websites has become something interesting to discuss. In situations where groups or individuals convey their messages or protest online, these actions can be regarded as a form of freedom of expression. On the other hand, it can be seen as a threat to cybersecurity and the integrity of government institutions. This research aims to give a better understanding of the complexity of the problem by dealing with it from different perspectives. It also aims to provide a basic understanding for a deeper discussion of the limits of freedom of expression in the virtual world. The results of this research are expected to help the parties involved in making policies, which allow people to speak online while maintaining the cybersecurity and the integrity of government agencies.

A. INTRODUCTION

The right to freedom of expression is among the most fundamental human rights norms because the right to free speech and expression is a key to democracy and an indicator of accountable governance (Nasution, 2020). The right to freedom of expression and expression is the right to express or express opinions either orally, in writing, in illustrations or images, and certain other ways.

One of these forms of freedom of expression and expression can be seen in demonstrations in any country. These activities are common in Indonesia, there are many ways that people or societies do to channel their aspirations and opinions. It is not uncommon for these aspiration dissemination activities to be brought to the world of the internet and social media, to the point that the government website is a means of disseminating the aspirations of the people who do not approve the policies made by the government. One form of this action is the hacking of the official website of the Indonesian government. Hacking starts from what is considered minor to what has a



serious impact, from the abbreviation of government agencies to hacking that ends with data leaks. It has a background where the majority of social media users are young but have been critical of the political situation in Indonesia. The hackers themselves are dominated by young people who are often on the side of society.

These actions make some individuals believe that their actions can represent their opinions and represent their disagreement with government decisions. However, from a legal perspective, hackers may pose significant threats to national security and public order. The hacking itself has caused a lot of different reactions. On the one hand it's conspicuous because many consider it to be one way to offend the government in general, and on the other it can be difficult for people who really need data from the official website because this data is potentially to be a hoax.

Because of this case, the author argues to write this topic for a journal because basically the question that the writer wants to answer is whether this hacking can be justified and how the law can be enforced and what law could be applied.

B. METHOD

In legal research, the approach is typically doctrinal (library-based) or empirical. For this particular study. Through doctrinal research, this study analyzes existing laws, international agreements, and legal frameworks that define freedom of expression and the regulations around hacking. This includes the Universal Declaration of Human Rights, the ICCPR, and national laws such as Indonesia's Law No. 11 of 2008 on Electronic Information and Transactions (ITE Act). Empirical research, the study may include data on hacking incidents, public reactions, and legal cases in Indonesia and globally.

The literature review should cover existing legal commentary and judicial interpretations of laws related to freedom of expression, especially in online contexts. Sources can include academic articles, case law, and international legal reports on the regulation of hacking.

Legal theories related to freedom of expression and cybersecurity should be used to frame the discussion. Theories on the limits of expression in democratic societies will help justify the conclusions drawn in the research.

C. RESULTS AND DISCUSSION

Freedom of Expression in General

Freedom of speech and expression, or freedom of expression and opinion, has been established in various laws, both nationally and internationally, including Article 19 of The Universal Declaration of Human Rights, Article 23 of The International Covenant of Civil and Political Rights (ICCPR), Article 28 of The ASEAN Human Rights Declarations, and more. And there is A Law Number 9 of 1998 on the Freedom to Express Opinions in Public. The right to freedom of expression encompasses the rights to express opinions without interference and to seek, receive, and impart information, through any media, without the boundaries of the territory to be communicated orally, in writing, in artistic or cultural forms, or through other media. Freedom of expression and expression

is both an individual and a collective right, which allows people to have the opportunity to communicate, seek, receive, and share a variety of information, which can develop and express their opinions.

Some also referred to this right as the right to freedom of expression and opinion. As has been quoted from the Public Policy Press written by Bagir Manan, freedom of speech and expression and the right to freedoms of expression are the same thing. Article 19 of the Universal Declaration of Human Rights states that everyone has the right to have an opinion, and therefore everyone has a right to express it as well. Everyone is encouraged to share their opinions with others, both nationally and internationally, in any way or format.

For Information Activists published by UNESCO, freedom of expression is closely linked to press freedom and covers wider expression, including freedom to express itself through various ways. This freedom of expression is not absolute and must also be done with the obligation by the restrictions laid down by law. This right also protects the right of a person both as speaker and as listener (Hüfner, 2010).

In order not to cause conflict, people must be able to properly express their opinion in a way that does not contain ethnicity, religion, race, and inter-group relations (known as SARA in Indonesia). Use subtle language and give advice on a problem. A conflict can also occur from a person who is unwilling to receive critics and advice and causing miscommunication between the subject and the problem. In this kind of activities, one should be able to accept criticism and advice, and to correct, not to exaggerate the problem (Sabela & Pritaningtias, 2017).

Freedom of expression is essential as it guarantees individual self-fulfillment or achieving their maximum potential, to seek the truth and progress of knowledge, to be able to participate in the decision-making process, and to the stability and adaptability of a country and a society (Sabela & Pritaningtias, 2017).

Freedom of expression is essentially a right and a responsibility of a democratic state. The public is expected to be able to perform the control and supervision functions of the government of a country by actively participating and sharing their opinions and views on the policies established by the government. These actions can be either approval or criticism to the policies (Antari, 2017). If in the practice, the people can already channel their aspirations and can fully declare that the freedom of expression is already fulfilled, then the country can be said to have performed its rights well and it can also be said as democracy. However, it is important to remember that a state must be able to restrict when freedom of expression has overtake the limits laid down by national law or even international law.

The Restriction of Freedom of Expression

According to John Stuart Mill (Warburton, 2009), the wider the freedom of expression opened up in a society, the more advanced that society or civilization would be. Freedom of expression and expression is guaranteed in a democratic country like Indonesia, but there are a few things that we can know when freedom of expression is

threatened, including when permission to publish or broadcast is refused, when physical or emotional intimidation occurs, when access to information is unlawfully denied or restricted, when there are restrictive laws and regulations.

As freely as a person expresses their opinion, there must be restrictions on this right, because as we know, excessive freedom can cause a bad impact. In this kind of rights are known the terms limitations or restrictions and these are permitted as long as they meet the prescribed conditions. This restriction can be seen in the rights to civil and political freedoms. The limitation of these rights can be seen from Article 70 of Law Number 39 of 1999 on Human Rights. This limitations can also be seen in Article 29 of The Universal Declaration of Human Rights which states that these limitations are “prescribed by law”, or establishes the law in force with a view to respecting the rights of others, in accordance with justice, order and general well-being, and in conformity with the principles of the United Nations. And then there is Article 19, Paragraph 3 of The International Covenant on Civil and Political Rights (ICCPR), which states that freedom of expression must respect the right of others and does not threaten national security, order, and general health and morality ([Marwandianto & Nasution, 2020](#)).

Freedom of Expression on the Internet

Freedom of expression getting more attention and becoming widely open with the advances of information and communication technology and new innovations. Especially on the internet, which have had a major impact on the beneficiaries of the right of freedom to expression ([Perdana, 2016](#)).

According to Frank William La Rue ([La Rue, 2011](#)), the relevance of the Internet and freedom of opinion are media capable of being an important means in the fulfilment of the right of opinion and expression. Quoting Yanuar Nugroho’s point of view, the Internet also provides an opportunity for everyone to express their opinions, even in ways unimaginable before ([Antari, 2017](#)).

There are several laws about freedom of expression and expression on the Internet, including the Declaration of Expression and Information, the Declaration of Freedom of Communication on the internet, the Joint Declarations on Freedom and Expression, the Charter on Human Rights and Principles in the Internet and many more.

The Protection of Freedom of Expression

It should be noted that the protection of the right to freedom of expression has been regulated by the United Nations. The United Nations publishes rules about the protection of freedom of expression by arising resolutions that equate the freedom to expression in ‘offline’ or ‘online’ activities must be protected ([Lembaga Studi dan Advokasi Masyarakat, 2013](#)). In addition to recognize the access to the Internet as a human right, the United Nations has also arised a resolution on the transmission, protection, and enjoyment of human rights on the Internet, this topic also issued in the Declaration of Expression and Information, which has recognized that with the advancement of information technology, then the right to freedom of expression must be protected.

Demonstration

Demonstration is a movement carried out by a group of people in the form of a public protest. These activities are usually performed in order to protest a governmental policy or to convey the aspirations of a particular group of society. According to The Indonesian Dictionary, a demonstration has two meanings, the first is a statement of protest made in the wake of the demonstration, and the second is a rally carried out by an agency or group (Sabela & Pritaningtias, 2017).

Demonstration is a democratic right that is carried out in an orderly and peaceful manner and is also a form of public protest against the lack of public position in government. Freedom of expression can encourage people to appreciate differences of opinion and accept criticism in order to be able to develop the way people think and also can occur a country to become a more democratic state (Sabela & Pritaningtias, 2017).

Demonstration is an effective way of expressing opinions in order to satisfy interests and is an important element of communication in freedom of expression and in public use to raise a matter to be of public interest. Demonstration is one of the ways to convey the aspirations or opinions of people in a way of gathering. Demonstrations is a form of concern of the public as a citizen. The right to demonstrate is permitted whenever it is carried as long as the act is provided by the regulations or rules. From freedom of expression, both the public and the government become more aware of the shortcomings or surpluses, either in the process of government or the government themselves.

Opinions can be submitted in two ways, orally and in writing, but people prefer to express their aspirations orally through demonstration because it is considered more effective than writing. In addition, they also feel that by speaking their opinions orally this will be more channeled and heard by the government.

The Hacking of the Official Government Website

Hacking in General

Hacker, according to the Wikipedia website, is someone who studies, analyzes, modifies, breaks into computers and computer networks, either for profit or motivated by challenge. According to the Indonesian dictionary, a hacker is a person who is obsessed with learning more about computers or someone who accesses other people's computers without permission, which is usually done with the help of communication technology.

Hacking is very common, either hacking public sites, personal blogs, social media accounts, online games, even ATM cards can be hacked (Nugroho, 2015). When there's been a hacking, we can't completely blame the service provider or provider of this site because they have also tried to protect their site and not rarely make updates or updates to the site or application they manage.

Hackers are generally active and actually deliberately trying to mess up even damage the system. They also have a variety of ways to get data and take over the administration of a site or application. Hacking is not a legal act anywhere because it is dangerous to

people as consumers, governments, and providers of services. There have been many hacking regulations, such as Articles 30 and 46 of Law No. 11 of 2008 on Electronic Information and Transactions, but due to many obstacles and difficulties in tracking offenders, the enforcement of these actions is still said to be rather difficult.

Positive Impacts of Hacking

It is important to remember that hacking or cyber-criminal acts are generally unjustifiable and often have a serious negative impact. However, there are some situations where hacking and cyber activity carried out with positive or ethical intentions can have a positive impact, such as:

1) Enhanced Cyber Security

Some hackers or cybersecurity experts can undertake ethical attacks to identify and close security gaps in a system or network. By exposing these vulnerabilities, companies or organizations can strengthen their security and protect sensitive data from more dangerous attacks.

2) Enhanced Security Awareness

Ethically-directed cyber attacks can raise awareness of the importance of cyber security among users and organizations. By involving ethical hackers, people and companies can better understand risks and implement better security practices.

3) Security Skills Development

Ethical hacking activities can provide opportunities for cybersecurity professionals to develop and enhance their skills. They can work with companies or organizations to design and implement more effective security solutions.

4) Consumer protection

In some cases, ethical hackers can help protect consumers by identifying and addressing security issues on the platforms or services they use. This can prevent data leaks and protect user privacy.

Resilience to Future Threats: By identifying and correcting vulnerabilities, ethical hackers help organizations become more resilient to future cyber threats. This contributes to the development of systems and networks that are more secure and resistant to attacks.

Although there are some positive impacts as mentioned above, it is important to note that unauthorized and malicious hacking has the potential to harm individuals, companies, and society as a whole. Therefore, ethical hacking carried out within the legal and ethical framework is a much better preference to positive results without causing unnecessary losses.

Negative Impacts of Hacking

Besides the positive impact, it is worth noting that hacking also causes a lot of negative impact. Hacking or cyberattacks can have a serious negative impact, both at the individual and organizational levels. Here are some of the negative effects of hacking:

1) Loss of Personal Data

A cyber attack can result in the leakage of personal data, including identity information, financial information, and other personal data. This can lead to identity theft, fraud, or misuse of personal information.

2) Financial Losses

Hacking can result in significant financial losses for a company or organization. This can include costs to recover data, secure systems, and replace losses resulting from data breaches.

3) Service Disruption

A cyber attack can result in a service disruption on a critical system or infrastructure. This can affect the availability of the service, and in some cases, can stop the operation of a business or critical service.

4) Reputation loss

Cyber security violations can damage the reputation of a company or organization. Consumers' and business partners' confidence can be crushed, and restoring a reputation takes considerable time and effort.

5) National Security Threat

Cyber attacks targeting critical infrastructure or government agencies can constitute a serious threat to national security. It can damage the stability of the country and cause huge losses in terms of security and stability.

6) Loss of Intellectual Property Rights

Hacking may result in theft or loss of intellectual property rights, such as a business plan, product design, or software source code. It can destroy the competitive advantage of a company or a country.

7) Misuse of Sensitive Information

Information obtained through hacking may be used for criminal or other abuses, including blackmail, threats, or terrorist activities.

8) Dependency on digital security

Successful cyber attacks can cause public concerns about dependence on digital technology. This can trigger mistrust of online systems and services.

From these negative impacts, it is important for individuals, companies, and governments to prioritize cybersecurity, implement best security practices, and continue to improve their defences against the ever-increasing cyber attacks.

The Hacking of the Official Government Website

Freedom of expression can be expressed in a variety of ways, both verbally and in writing. The most common act of hackers is to make the website crash or inaccessible for a while until it is repaired. The next is to change the look of the website by replacing the

existing images, changing the abbreviation of official government agencies, and not forgetting they also left a 'signature' as a proof that the hackers have successfully hacked into the site. There is a regulatory basis for web hacking, such as Article 30, Paragraph 1, of Law No. 1 of 2008 on Electronic Information and Transactions. Then there are also Articles 32 and 35 of similar laws that may relate to this action. During the demonstrations, the hacking of the official website was very violent and it was related to the circumstances, plus the hackers usually viewed it as a challenge to their side.

Regulations About Hacking in Indonesia

In Indonesia, hacking or cyber attacks are governed by a number of laws that have provisions relating to information and communication security. Here are some relevant laws:

1) Law No. 11 of 2008 on Electronic Information and Transactions (ITE Act):

Article 30 regulates illegal access to electronic systems. Article 31 regulates hacking. Article 32 regulates the creation and/or distribution of malicious computer programs.

2) Law No. 19 of 2016 on Amendments to the ITE Act:

The bill amends some of the ITE's articles relating to cybersecurity, including the addition of provisions related to cybercrime.

3) Law No. 36 of 1999 on Telecommunications:

Article 4 provides for the protection of information transmitted through telecommunications networks, and Article 40 provides for prohibition of unauthorized access to telecoms networks.

4) Law No. 24 of 2013 on Amendments to Act No. 15 of 2003 on Punishment of Terrorism:

Article 4A paragraph (1) provides for the prohibition of the use of information and/or electronic technology in support of acts of terrorism.

5) Law No. 5 of 2018 on Punishment of Trafficking in Persons:

Article 31 regulates the prohibition of the use of information and communication technology in criminal acts of trafficking in persons.

It is important to remember that the ITE Act has been at the centre of concern because it has sparked a debate around freedom of expression and legal action that is considered controversial.

In addition to these laws, other regulations and regulations can also play a role in regulating cybersecurity in Indonesia. Cybersecurity is becoming increasingly important as information and communication technology develops, and governments are continuously working to update existing regulations to address the growing cyber security challenges.

D. CONCLUSION

The hacking of the government's official website is not new. This has been going on for a long time since the advent and development of the Internet in the 1990s. Hacking started from what was thought to be trivial to what had a serious impact, from the replacement of government agencies to hacking that ended in data breaches. It's obvious to some people because most internet users, especially social media users, don't think it's just a joke until it gets viral. But he has been critical of the political situation in Indonesia. The hackers themselves are dominated by young people.

Hacking incidents have elicited varied legal and public responses, particularly regarding their potential legality as a form of protest under freedom of expression laws. On the one hand, it's commendable because a lot of people consider it to be a way to offend legislators or governments in general, and on the other hand it can be difficult for people who really need data from official websites because this data is potentially a hoax.

Demonstration activities are common in Indonesia. From small demos, to demos that involve the whole country. There are many ways or forms that society does to channel their aspirations and opinions. It is not uncommon for these aspirations to be disseminated onto the Internet and social media, until the government website becomes a means of disseminating the aspirations of people who do not approve of the policies made by the government. One of them was the hacking of the Indonesian government's official website.

REFERENCES

- Antari, P. E. D. (2017). Tinjauan Yuridis Pembatasan Kebebasan Berpendapat Pada Media Sosial di Indonesia. *Jurnal Hukum Undiknas*, 4(1).
- Hüfner, K. (2010). UNESCO – United Nations Educational, Scientific And Cultural Organization. In *A Concise Encyclopedia of the United Nations* (pp. 715–718). Brill | Nijhoff. <https://doi.org/10.1163/ej.9789004180048.i-962.616>
- La Rue, F. (2011). Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression. *Human Rights Council 17th Session, Agenda Item, 3*.
- Lembaga Studi dan Advokasi Masyarakat. (2013). *Buku Saku Kebebasan Berekspresi di Internet*. ELSAM.
- Marwandianto, M., & Nasution, H. A. (2020). Hak Atas Kebebasan Berpendapat dan Berekspresi Dalam Koridor Penerapan Pasal 310 dan 311 KUHP. *Jurnal Ham*, 11(1), 1. <https://doi.org/10.30641/ham.2020.11.1-25>
- Nasution, L. (2020). Hak Kebebasan Berpendapat dan Berekspresi Dalam Ruang Publik di Era Digital. *Adalah: Buletin Hukum dan Keadilan*, 4(3), 38–39. <https://doi.org/10.15408/adalah.v4i3.16200>
- Nugroho, I. Y. (2015). Sanksi Hukum Kejahatan Peretasan Website Presiden Republik Indonesia. *Al-Daulah: Jurnal Hukum dan Perundangan Islam*, 5(1), 171–203.

<https://doi.org/10.15642/ad.2015.5.1.171-203>

Perdana, H. (2016). *Kebebasan Berekspresi di Indonesia; Hukum, Dinamika Masalah, dan Tantangannya*. ELSAM.

Sabela, A. R., & Pritaningtias, D. W. (2017). Kajian Freedom of Speech and Expression Dalam Perlindungan Hukum Terhadap Demonstran di Indonesia. *Lex Scientia Law Review*, 1(1), 81–92.

Warburton, N. (2009). *Free Speech: A Very Short Introduction* (Vol. 200). Oxford University Press, USA. <https://doi.org/10.1093/actrade/9780199232352.001.0001>