Jurisdiction Overview of Cyber Troops in Digital Campaigns

Amalia Syauket [1], Ida Budhiati [1], Bambang Karsono [1]

[1] Universitas Bhayangkara Jakarta Raya Jakarta, Indonesia
amalia.syauket@dsn.ubharajaya.ac.id

Abstract. Political elites often use paid cyber troops, also known as cybertroops, to manipulate public opinion on social media for their own benefit. These cyber troops emerged and evolved from electoral campaign organizations in Indonesia, ranging from winning teams in presidential elections to regional elections. One tactic that is considered successful to push public opinion is the use of cyber troops. The slanting of public opinion is done by invading cyberspace with false information that favors certain groups. In addition, cyber troops can be used to bring down the electability of one candidate through black or black campaigns, which trigger insults and/or defamation by creating rumors or gossip aimed at the opposing party without denying the facts. This normative research with a statutory approach aims to find out what types of data are the objects of cyber troops controlled by one of the candidates in the vortex of digital campaigns with the mode of insult and/or defamation for public knowledge? This study found that personal data used by mercenary cyber troops in the organization of campaigns is very sensitive and must be protected because it is an important component of a person's freedom and dignity, and is a strong driver of political, religious, expression, and privacy freedoms. Cybercrime with illegal modes carried out by paid cyber troops is a black campaign on social networks containing false information, slander, and insults.

Keywords: cyber troops, black campaigns in the digital era and types of personal data.

1 Introduction

General elections are an important part of the democratic state system in Indonesia, where they are conducted regularly every five years. Simultaneous Pilkada is the process of directly electing the president and vice president at the national level, as well as the election of governors and vice governors, mayors and vice mayors, and regents and vice regents.

Rapidly developing technology has many positive and negative effects on human life. This technological development can also pave the way for criminals, especially

A. Nurmandi et al. (eds.), *Proceedings of the 1st International Conference on Law, Social, and Political Science (ICSP 2023)*, Advances in Social Science, Education and Humanities Research 816,
https://doi.org/10.2991/978-2-38476-194-4_6

criminal cases that occur on the internet [1]. One of the factors that drives unlimited technological progress is globalization. A new term called the internet was created as a result of technological support, especially with regard to telecommunications systems.

The increasing number of internet users causes many problems. One of them is the emergence of a new type of criminality that occurs on the internet, also known as cybercrime, a criminal activity committed using the internet and other forms of digital communication. Both individuals and organizations are negatively impacted by these offenses.

Undoubtedly, digital crimes cause financial losses and loss of personal information, impacting lives and daily activities. The advancement of information technology has both positive and negative effects, including many insults and defamations. A study conducted by Linda Ismaya (2013) found that black campaigning is a type The formatter will need to create these components, incorporating the applicable criteria that follow.

Mayantara crime that involves defamation during campaigns through social media networks. which violates the Constitutional Court Decree (KUHP) and the Law of the Republic of Indonesia number 11 of 2008 on Information and Electronic Transactions (ITE).

As political elites campaign digitally during the campaign season, the phenomenon of cyber troops increases. Digital campaigning has many advantages, including increasing democratic participation and connecting candidates with voters. Nonetheless, it is important to stop digital campaigns that justify everything, what Linda Ismaya calls "social media smear campaigns”[2].

This research focuses on the cyber troops in the success teams of each presidential and vice presidential candidate, especially in the context of the 2019 election and the 2024 election phenomenon. With the increasingly sharp contestation for the presidential and vice presidential elections nationwide, every effort can be made to support and win one of the presidential candidate pairs, who will then enjoy power as president, head of state, and head of government, especially with the support of advances in technology and information.

2 Research Methods

The purpose of this normative research is to identify what type of data is used by cyber forces to control one of the candidates in a digital campaign with the mode of insult and/or defamation known to the public. Primary legal materials used in this method come from various sources, such as RI Law number 11 of 2008 [3] concerning Electronic Information & Transactions, RI Law number 27 of 2022 [4] concerning Personal Data Protection, and RI Law number 7 of 2017 [5] concerning General Elections. In addition, relevant and up-to-date secondary legal materials are taken from various reference books and research journals.

3 Result and Discussion

3.1 Cyber troops, success teams in the digital Campaign Period

Cyber troops, also known as "mercenary cyber soldiers" [6], are machines that utilize electronic equipment in direct contact with the internet, such as computers and mobile phones. In addition, cyber troops will access various social media sites, such as Facebook, YouTube, Twitter, Instagram and others.

The fact that Kampret Vs. Cebong occurred in the 2019 presidential election shows that cyber troops do exist and are involved in digital campaigns in Indonesia. It is possible that this phenomenon occurred due to the increasing use of the internet as a medium for campaigning and spreading false information in the political sphere. In addition, more and more cyber troops, also known as "cyber troops", are being used by political elites, including their success teams, to spread such misinformation. Its role then enters politics when politicians use social media as their campaign tool to sway public opinion and corner their political opponents.

Ward Barenshot stated in 2021 that Cyber troops are a growing phenomenon of election campaign organizations in Indonesia [7]. In other words, with an effective teamwork system in Indonesia. In addition, Ward stated that cyber troops perform four tasks: buzzers, who are responsible for spreading content, are the first. A buzzer usually has ten to hundreds of social media accounts. Second, content creators who are responsible for creating engaging content, such as through memes or hashtags spread by buzzers or cyber troops. Third, the coordinator who organizes the buzzers and ensures the right timing. Fourth, are influencers who are paid to support one of the candidates in the campaign and are not official members of the cyber troops.

After being intentionally recruited, cyber troops are assigned by influential political candidates or parties to spread propaganda or hoaxes. There is no need for an article because the forms are very diverse. Cybertroops usually gather material from buzzers and influencers. He then enters politics when politicians use social media for their campaigns.

During election campaigns, political opponents are often discredited by mentioning significant initials or nicknames.Since it only takes an email to create a social networking account, the culprit is usually anyone.

3.2 Social media black campaign in presidential election as a mayantara crime

The types of media used to campaign for presidential and vice presidential candidates are increasingly diverse as technology and time progress. In the past, campaigns were conducted through direct interaction between candidates and the public. Now, however, campaigns can be conducted through social networks, which today not only serve as communication tools but also provide information through the internet network.

According to Venus Antar [8], a political campaign is conveying a message to the public to inform them about what and how a party, its program, and vision so that they can understand the party's intentions and goals, and they can make a decision to make a choice or not.

Social networks that are in demand by the public, such as Facebook and Twitter, are widely used as digital campaign media because they are equipped with various features that are attractive to users, including the existence of dialog features that are closely related to support or rejection of an idea. In terms of election regulations, social media and internet campaign methods were first regulated for the 2019 elections through Law No. 7/2017. The provisions of Article 275 paragraph (1) letters e and f state that election campaign methods, among others, are carried out through social media and the internet. Meanwhile, the definition of social media in the Law is regulated in article 1 number 33, which reads: social media is a collection of communication channels on the internet network used for community-based interaction and content sharing.

Furthermore, the procedures for campaigning on social media as regulated in Law No.7 of 2017 are derived in Article 35 paragraph (1), (2) and Article 36 paragraph (1) of KPU Regulation No. 23 of 2018. In this provision, KPU regulates more technical procedures for campaigns on social media, namely Election Participants can conduct Campaigns through social media with a maximum of 10 (ten) accounts for each type of application. Campaign executors register official social media accounts with the KPU according to the type of election and its level. This provision has changed for the 2024 Election. The provisions of Article 37 paragraphs (1) and (2) of KPU Regulation No. 15 of 2023 state that Election Participants can conduct Election Campaigns through Social Media with a maximum of 20 (twenty) accounts for each type of application.

To organize the 2019 General Election, Law No. 7 Year 2017 does not regulate administrative sanctions for violations of campaign methods in social media. Therefore, within the limits of the KPU's authority, Article 74 of KPU Regulation No. 33/2018 on the Second Amendment to KPU Regulation No. 23/2018 states that violations of campaign provisions on social media are considered violations of campaign provisions on social media, before the start of the campaign period in the form of a. written warning; b. termination of the Campaign on social media. However, for the 2024 elections, the KPU actually removed administrative sanctions against campaign violations on social media. In terms of regulation, the regulation of sanctions for campaign violations on social media has regressed because there is only one type of criminal sanction as stipulated in Article 251 of Law No.7/2017.

Social reality shows that campaigns on social networks now do not only convey the vision, mission, programs and self-image of candidate pairs to the public. They now involve negative content that insults and defames other candidate pairs, resulting in their humiliation and defamation with false information or hoaxes intended to garner votes.

Such campaigns are called "black campaigns" or "smear campaigns". In the past, black campaigns were carried out by distributing or disseminating information through print media, such as brochures, pamphlets, narratives, freelance articles and banners, which conveyed negative information about their political opponents to the general public. Success teams and sympathizers of the relevant election participants disseminate such information through various media [9].

Black campaigning has actually been around for a long time. At first, black campaigns were carried out by spreading issues, gossip, or rumors through the media by word of mouth, so they were known as "word of mouth campaigns" [10].

In today's digital era, black campaigns are conducted using more sophisticated media thanks to advances in technology and information. This means that voters must be more innovative in using social media as their campaign medium to convey the candidates' vision, mission and self-image to the public. According to research conducted by Candra Ulfatun Nisa et al [11], the use of social media in political campaigns is certainly reasonable because social media is considered an easy and effective means of disseminating information, so that people can quickly and directly obtain information. Because social media is easily accessible to everyone, social media campaigns are relatively cheap and in demand by most people.

Spreading false rumors is part of a tactic to bring down political opponents by flooding social media with untrue stories [6]. In political campaigns, social media is often misused by irresponsible individuals by incorporating black campaigns to achieve desired political goals.

The purpose of Black Campaigning is to demonize people in order to make them look bad in the eyes of the public, harm, bring down, and attack their political opponents. This campaign is conducted in a way that violates political ethics, violates facts, and obtains information from unclear sources, which can even lead to slander and blasphemy. Black campaigns seem to be considered the right course of action to convince voters. This kind of campaign is definitely detrimental to election participants as they have to maintain their dignity, good name and honor during the campaign, as well as the public as recipients of information [11].

According to Rafli Fadilah Achmad, "black campaign" is a campaign whose focus is on spreading lies, slander, nonsense, or rumors deliberately created by the political opponent in question [12]. The term "character assassination" refers to this. Unlike negative campaigning, negative campaigning uses the weaknesses of political opponents to attack them. The similarity is that they attack political opponents or attack campaigns.

In terms of objectives, negative campaigning aims to demonize a person's character. Meanwhile, a black campaign aims to destroy a person's character with invalid, invalid or fabricated data. La Januru makes it clear that in addition to aiming at character assassination by directing bad public opinion towards political opponents, it is also a plan to reduce the chances of the election of the person concerned as a political opponent, in other words, as a form of elimination of the rival faced [13].

According to Candra Ulfatun Nisa et al., Instagram is the most widely used social media for black campaigning [11]. However, this social media is often misused by irresponsible individuals, who easily include other candidates and increase tensions between candidates. Instagram is a very effective social media to spread misinformation and influence people in their decision-making. While black campaigning does not guarantee victory in an election, it certainly creates a lot of havoc that can unsettle and worry the public.

Because they use social networks, black campaigns are classified as internet crimes or mayantara crimes. Petrus Reinhard Golose, Cybercrime is a type of computer crime that is influenced by the existence of the cyber world [14]. According to Barda Nawawi Arief in 2007, cybercrime is one of the new types or dimensions of modern crime, which is also referred to as cybercrime, high-tech crime, transnational crime, and white collar crime [15]. In 1996, Volodymyr Golubev called it a new type of anti-social behavior [16].

Of the various types of cybercrime, the use of social networks in black campaigns, the subjective element is intentionally with insulting content, slander and false news which is a mayantara crime with illegal content modus operandi. With objective elements as contained in Article 27 paragraph (3) of Law of the Republic of Indonesia number 11 of 2008 concerning Information and Electronic Transactions , namely 1. distributing, transmitting, making accessible, 2. without rights, 3. electronic information and / or electronic documents containing insults and/ or defamation.

To fulfill Article 27 paragraph (3) of Law No. 11/2008 on Electronic Information and Transactions, the perpetrator of a black campaign must intentionally and without rights disseminate, send, and distribute electronic documents and information containing insults or defamation. In the context of black campaigning, Article 69 letter c states that implementers, participants, and campaign teams are prohibited from insulting a person, whether religion, ethnicity, race, candidate group, or other election participants. Article 69 letter d also states that inciting and pitting someone, both individuals and communities, and dividing the community.

At the time of the election campaign, there have been many black campaigns, which means that the information disseminated is not based on facts and mostly tends to be slanderous, which can potentially lead to criminal acts. Because the information disseminated is not true and tends to be slanderous, political opponents will be defamed.

In the campaign ahead of the election, this cyber army is also used to bring down the electability of political opponents through black campaigns.

3.3 Types of Data worked on by Cyber Troops in carrying out black campaigns

Research by Sinta Dewi Rosadi, 2023: Personal data is essential to one's freedom and dignity. Political, religious and sexual freedoms are driven by data protection. Important rights that make us human are the right to self-determination, freedom of speech, and privacy. One's privacy is threatened by the collection and dissemination of personal data. Because there is a correlation between personal data and the level of trust a person has in their personal life.

Data from the Election Supervisory Agency (Bawaslu) shows that 1004 social media campaign violations, including hoaxes, negative content, and negative campaigns, were handled during the 2020 Simultaneous Regional Elections, including 734 violations on Facebook, 86 violations on Twitter, 182 violations on Instagram, 1 website, and YouTube. Based on verification by Bawaslu, 393 were sent to the Ministry of Information and Communication.

In Chapter I General Provisions, Law of the Republic of Indonesia number 27 of 2022 concerning Personal Data Protection, specifically in article 1 number 1, it is stated that personal data is data about an identified or identifiable individual individually or in combination with other information either directly or indirectly through electronic or non-electronic systems.

From the definition, it appears that personal data does not only refer to the unique identification given to a secured person. But it also extends to any information that a person can identify with, such as IP addres and location data. Daniel Rucker, 2018 explains that the definition of personal data must be flexible, adaptable and still be able to adopt the rapidly evolving developments in information technology [17].

Article 4 of Indonesian Law number 27 of 2022 concerning Personal Data Protection, concerning types of personal data.

(1) Personal data consists of:
  a. specific personal data; and
  b. general personal data.

(2) Specific personal data includes:
  a) health data and information;
  b) biometric data;
  c) genetic data;
  d) criminal record;
  e) child data; personal financial data;
  f) other data in accordance with the provisions of laws and regulations.

(3) General personal data, including:
  a) full name;
  b) Gender;
  c) citizenship;
  d) religion;
  e) marital status;
  f) personal data that is combined to identify an individual.

From article 4 above, Sinta Dewi Rosadi, 2023 divides 4 types of personal data, among others,

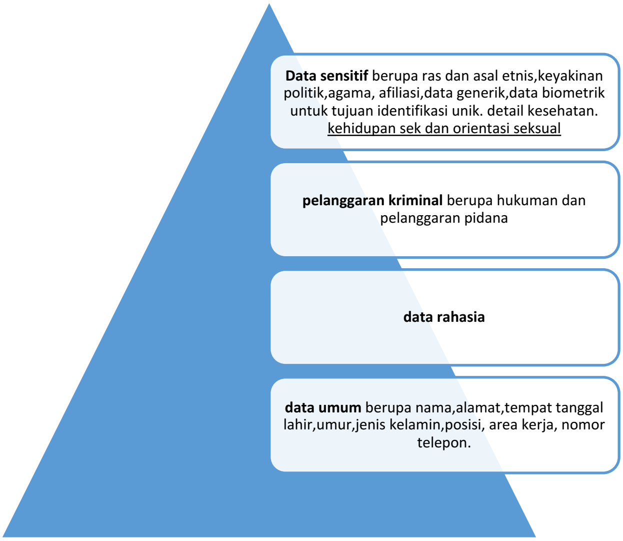
Data sensitif berupa ras dan asal etnis,keyakinan politik,agama, afiliasi,data generik,data biometrik untuk tujuan identifikasi unik. detail kesehatan. kehidupan sek dan orientasi seksual
pelanggaran kriminal berupa hukuman dan pelanggaran pidana
data rahasia
data umum berupa nama,alamat,tempat tanggal lahir,umur,jenis kelamin,posisi, area kerja, nomor telepon.

Fig. 1. Personal data protection

Research from Linda Ismaya et al, 2013 that electronic information used in black campaigns must be in the form of one or more electronic data, including, but not limited to, writings, images, maps, designs, photos, EDI, electronic mail, telegrams, telecopies or the like, letters, signs, numbers, access codes, symbols, or perforations that have been processed and have meaning or can be understood by people who are able to understand them [2].

Thus, Cyber troops paid by political parties or candidates understand that their actions are dangerous because they alter, add, subtract, send, damage, delete, move, or hide electronic information and electronic documents belonging to other people or the general public. And then incorporate black campaigns to achieve political goals.

4 Conclusions

Personal data used by mercenary cyber troops is within the election campaign organization and is specially protected because it is an important component of a person's freedom and self-esteem, and a strong driver of political, spiritual, expression and privacy freedoms. Cybercrime with illegal modes committed by mercenary cyber troops is a black campaign on social networks containing false information, slander, and insults.

Cyber troops manipulate public opinion online to gain votes and win elections, steering the public conversation to the story of one candidate who paid for it, using many fake accounts and bots to support the story.Acknowledgment

The author would like to thank to Rector of Universitas Brawijaya Malang Indonesia for the scholarship; Dean and colleagues of Faculty of Social and Political Science Universitas Brawijaya Malang Indonesia for all their support.

References

1. M. Ngafifi, “Technological Advances and Human Life Patterns in a socio-cultural perspective,” *J. Educ. Dev. Found. Appl.*, vol. 2, no. 1, pp. 33–47, 2014, doi: https://doi.org/10.21831/jppfa.v2i1.2616.
2. L. Ismaya and R. Sugiyantica, “Black Campaign on social networks in the 2014 presidential and vice presidential elections as a mayantara crime and defamation in the Criminal Code and Law number 11 of 2008 concerning ITE,” *Recidive*, vol. 2, no. 3, 2013.
3. R. Indonesia, *Law of the Republic of Indonesia number 11 of 2008 concerning Electronic Information & Transactions*. 2008.
4. R. Indonesia, *Indonesian Law number 27 of 2022 on Personal Data Protection*. 2022.
5. R. Indonesia, *Law of the Republic of Indonesia number 7 of 2017 concerning General Elections*. 2017.
6. Y. Sastramidjaya and Wijayanto, *Cyber Troops, online manipulation of public opinion and co-optation of Indonesia's cybersphere*. Singapore: ISEAS Publishing, 2022.
7. W. Barenshot, *Cyber troops, public opinion manipulation and the future of Indonesian Democracy*. ISEAS Publishing, 2021.
8. V. Antar, *Campaign Management*. Bandung: Simbiosa Rekatama Media, 2004.

9. A. B. D. Dodu, “Implementation of Black Campaign Political Regulations, a case study of the 2015 Banggai district election,” *J. Polit. Discourse*, vol. 2, no. 1, 2017.
10. Nimno and Dan, *Political Communication: Communicators, Messages and Media*. Bandung: Rosdakarya, 2009.
11. C. U. Nisa, H. S. Disemadi, and K. Roisah, “Legal aspects of Black Campaign on the Instagram social media platform. Mahkamah,” *J. Islam. Law Stud.*, vol. 5, no. 1, 2020.
12. R. F. Achmad, “Criminal threats for intellectual dader black campaign, study of decision number 17/Pid.Sus/2014/Pn.Bul,” *J. Law Dev.*, vol. 48, no. 4, 2018, doi: http://dx.doi.org/10.21143/jhp.vol48.no4.1799.
13. L. Januru, “Analysis Of Black Campaign Discourse In The 2014 Presidential Election In Kompas Media, Jaw Apos And People’s Sovereignty,” *Natapraja J.*, vol. 4, no. 2, 2017, doi: http://doi.org/10.21831/jnp.v4i2.12625.
14. P. R. Golose, *About Hacking Crime, theory and case studies*. Jakarta: Dharmaputra, 2008.
15. B. N. Arief and M. Crimes, *The development of cyber crime studies in Indonesia*. Jakarta: Raja Grafindo Persada, 2007.
16. V. Golubev, *Cyber crime and legal problems on internet usage*. Ministry of Interior of Ukraine, 1996.
17. D. Rucker and T. Kugler, *New European General Data Protection Regulation, a practitioner’s guide ensuring compliant corporate practice*. Germany: Nomos Verlaggsellschaft, 2018.