ABSTRACT

The research is a legal review based on the documentary research concept by comparing the development of legislative responses to fake news spread in Southeast Asia. Anti-fake news legislation focuses on the transmission of information by electronic means than print media. The analysis is carried out for each of the member states by including a clause-by-clause examination of the legislation and subsequent cases addressing legal issues associated with the laws. Several common factors should be addressed to provide a fairer and more transparent approach, including developing a clear-cut definition of fake news. Two key elements should be met in the definition of spreading of fake news: it should be the intentional spreading of misinformation or disinformation by design. The research suggests it would be better to develop anti-fake news legislation as either a standalone statute or a specific amendment to existing legislation than include fake news in omnibus legislation. Except in the most serious cases, creating, publishing, or distributing fake news illegality should be reduced from a criminal offence to an administrative offence, where the police issue a fine. Given the documented publishing and spreading of disinformation by state actors, their servants and agents, there should be an explicit “fake news” offence associated with the action of such persons.

Keywords: ASEAN, defamation, disinformation, fake news, hate speech, hoax news, legislation, misinformation, social media
INTRODUCTION

A recent paper research in Science argues that the rise of fake news shows the “erosion of long-standing institutional bulwarks against misinformation in the internet age”, with the concern of being global (Lazer et al., 2018). In response to the impact of fake news in their member states, the Association of Southeast Asian Nations (ASEAN) signed a Joint Declaration on the Framework to Minimise the Harmful Effects of Fake News. This research describes the diverse systems of government and legal systems of the ASEAN members as they may have a bearing on the governmental response with anti-fake news legislation and how it is used to prosecute offenders.

After addressing the issue of fake news as a modern internet attenuated issue, the research analyses the various approaches taken in the legislative responses to fake news as introduced by ASEAN members. In some cases, the legislation is fake news specific, whilst in other cases, it is part of a more general cybercrime law or amendment to the existing legal code. The key focus will be on the scope of the legislation, particularly the varying definitions of fake news, the control of the promulgation of fake news by state actors, the penalties attached to the violation of the new laws, and commentary in the media. The focus of anti-fake news legislation is material that is processed through electronic systems, which does not cover print media.

The Joint Declaration on the Framework to Minimise the Harmful Effects of Fake News, as its name suggests, is a framework only. As stated in its preamble, the parties acknowledge that online and social media improve information access and facilitate communication. They recognise that the propagation of fake news is a challenge that needed to be addressed to allow social media to be a reliable source of information and a safe space for all users. To assist this process, they agree to share best practices to educate citizens on the dangers of fake news. Under the founding philosophy of ASEAN, the countermeasures must respect national sovereignty, and be implemented nationally according to the requirements of the individual ASEAN member states. Key articles of the agreement include: 1) improve digital literacy (Item 3 and 4); 2) strengthen national capacity to detect and respond to fake news (Item 5); 3) encourage stakeholders to build on the existing industry anti-fake news norms and guides (Item 6), and 4) share best practices and experience (Item 7). The Declaration, however, does not propose a definition of fake news.

There is no agreed definition of fake news. At its most basic, in the post-Trump current COVID-19 era, “truth” and “facts” have become the victims of political identities where the view of your opponents becomes “fake” news (Tong et al., 2020). Wang (2020) has identified a series of words similar to “fake news”, namely “news satire, yellow journalism, junk news, pseudo-news, hoax news, propaganda news, advertorial, fake information, false information, misinformation, disinformation, rumour, mal-information, post-truth, and alternative fact”. To assist the identification of “fake news”, Molina et al. (2021) develop a detailed taxonomy. They consider that misinformation is essentially the spreading of incorrect information. Disinformation, on the other hand, is the spreading of incorrect messages to harm others.
deliberately. It occurs that the terms “disinformation” and “mal-information” are used interchangeably.

A more utilitarian matrix that has gained traction has been developed by Wardle (2017). The matrix has been adopted by the Australian Communications and Media Authority (ACMA) in developing their position paper on the development to guide the industry as they develop their codes on the management of online misinformation and news quality in Australia (“Online misinformation and news”, 2020). Wardle’s “fake news” matrix consists of seven types of misinformation and disinformation (Wardle, 2017):

a) Satire or parody — no intention to cause harm but with potential to fool;
b) Misleading content — misleading use of information to frame an issue or individual;
c) Imposter content — where genuine sources are impersonated;
d) Fabricated content — content is 100% false and designed to deceive and harm;
e) False connection — headlines, visuals, or captions do not support the content;
f) False context — genuine content is shared with false contextual information; and
g) Manipulated content — genuine information or imagery is manipulated to deceive.

Smith and Perry (2021) propose a modification of Wardle’s (2017) matrix in their suggestion to define the crime of spreading fake news. They recommend that satire or parody are not a crime. They furtherly recommend that spreading of “fake news” can only be an offence if it is deliberate.

In some jurisdictions, the definition of defamation is so broad that it can also be used to prosecute those who post or transmit what the authorities consider to be fake news. For instance, s. 326 of the Thai Criminal Code states:

“Whoever imputes anything to the other person before a third person in a manner likely to impair the reputation of such other person or to expose such other person to be hated or scorned is said to commit defamation and shall be punished with imprisonment not exceeding one year or fined not exceeding twenty thousand Baht, or both (italics added).”

Such legislation can be significantly effective in silencing critics when a juristic person can initiate a case of criminal “defamation” against an individual. The use of defamation legislation and lèse-majesté laws to silence critics is discussed by Smith and Perry (2020). However, the research focus on legislative responses to fake news, and not further consider defamation legislation.

**RESEARCH METHODS**

The research is a legal review based on the documentary research concept. It compares and contrasts the development of legislative responses to the spread of fake news in Southeast Asia. Analysis of the legislation in a multi-language region such as ASEAN faces two immediate challenges. Complications may occur when it comes to translating laws from one language to another since language constructs are attached to each of its culture and
understanding, which is explained in studies discussing the Thai laws (Smith & Perry, 2020). Moreover, court decisions are often unavailable, and researchers have to depend on “English language secondary sources such as news services and newspapers and their reporting of government press conferences, police press conferences, and court decisions”.

The research analysis includes a clause-by-clause examination of the legislation and subsequent cases addressing legal issues associated with the laws. The analysis is carried out for each of the member states. States of Emergency concerning the COVID-19 pandemic have only been discussed where they impose additional constraints on spreading fake news to those of the primary legislation. In most cases, English versions of the laws and judgments are available in English. In Brunei Darussalam, Malaysia, the Philippines, and Singapore, English is the official language of the law. In other jurisdictions, the English translations are considered unofficial despite being prepared within the government, so the national language version takes precedence.

**LEGISLATIVE RESPONSES TO FAKE NEWS**

Some ASEAN jurisdictions have fake-news specific legislation or cybercrime legislation, and others adapt their existing legislation. In addition, defamation laws, both criminal and civil, are sometimes misused to silence critics who have been accused of spreading “fake news”. When citing the specific legislation, the research uses the word that has been in the relevant translation.

**Brunei Darussalam**

Spreading fake news is covered by the *Public Order Act*. There are two offences:

(a) Spreading false reports or false statements ‘likely to cause public alarm or despondency’ (s. 34);
(b) Publishing or giving any person information known to be false ‘and which tends to give rise to apprehension for the safety of any person or property’ (s. 35(1)). In this case, where it is proved that the person published or gave false information, the onus is on the person charged to prove that they do not know such information is false (s. 35(2)).

**Cambodia**

A draft of cybercrime law has been under discussion for several years (Sovuthy, 2019). If the draft is adopted, offences under the law will include: 1) publishing contents deemed to hinder sovereignty and integrity of Cambodia (“Draft Cybercrime Law,” art. 28(1)); 2) publications deemed to incite or instigate the general population to anarchism (art. 28(2)); 3) publications deemed to generate insecurity, instability or political cohesiveness (art. 28(3)); or 4) publications “deemed to be non-factual which slanders or undermined the integrity of any governmental agencies, ministries, not limited to departments, federal or local levels” (art. 28(4)). In the meantime, prosecutions against posting fake news have been undertaken under...
the Criminal Code. With the increasing impact of the COVID-19 pandemic, the Parliament approves a law on emergency management which further strengthens criminal sanctions against posting fake news once a State of Emergency has been declared ("Law on Emergencies," art. 5).

False information is covered by art. 425 of the Criminal Code and is used to prosecute those who communicate or disclose false information, and is punishable by imprisonment and a fine. As seen from the English translation, the use of this section is problematic:

[The communication or disclosure of any false information with a view to inducing a belief that a destruction, defacement or damage dangerous to other persons will be carried out shall be punishable by imprisonment from one to two years and a fine . . .]

Between late January and April 2020, and before the law on the state of emergency had been enacted, there were 30 documented cases of arbitrary arrests under art. 494 and art. 495 on incitement to commit offences or to disturb social security (Human Rights Watch, 2020) using the same methods of offending as for defamation and insult ("Cambodian Criminal Code," 2009 art. 305 & art. 307).

In this case, the penalty is more severe, which includes imprisonment and a fine where the incitement has been ineffective (art. 495). If the incitement is ‘to discriminate, to be malicious, or be violent against a person or a group because of their membership or non-membership of a particular ethnicity, nationality, race or religion’ and has been ineffective, a longer prison term and a higher level of fine applies (art. 496). It is claimed that the legislation is being used to crack down on opposition supporters and critics whilst the population is distracted by the COVID-19 pandemic ("Cambodia: COVID-19 spurs", 2020; “Cambodia: State of Emergency Bill”, 2020).

The Law on Emergencies is much more explicit, which takes precedence over any law that contradicts it. It includes “bans or limits on distributing or broadcasting information that can cause public panic or turmoil, damage to national security, or confusion about the situation under the State of Emergency’ (art. 5). The penalty for intentionally failing to respect such measures is imprisonment and a fine (art. 8). A much heavier penalty applies if it causes public turmoil (art. 8). A State of Emergency may last no longer than three months, and may be extended by a further Royal Decree (art.3). In this case, the state of emergency is specific to the COVID-19 pandemic.

**Indonesia**

Indonesia has enacted the Law on Electronic Information and Transactions as amended in 2016 and Government Regulation on Trading Through Electronic Systems. In summary, the relevant offences under art. 27 of the Act are to knowingly and without authority distribute and/or transmit and/or cause to be accessible electronic content which offends against propriety (art. 27(1)), and/or affronts [sic] or defames (art. 27(3)), and/or extorts and/or threatens’ (art.
There is no clarification as to what constitutes an offence against propriety or what constitutes the offence of affronting. It is left open to the courts to decide.

Hate speech is the subject of Article 27(2) of the amended Electronic Information and Transactions Law. Despite the apparent widespread backlash at the time of enactment of the Law (Tapsell, 2019), only one application for review was lodged with the Constitutional Court ("Judicial Review of Law No. 11 of 2008,"). The review concerned Article 31(4), which provides for further provisions or procedures for interception of electronic information by law enforcement officials to be regulated by government regulation. The court found this to be unconstitutional (s. 5). Under the GR 80 2019, platform service providers are not held responsible for negative content if they are only conduits of information, only store the data/information, or act as a search engine (art. 22(3)-(4)). Article 207 of the Criminal Code is problematic (Gomez & Ramcharan, 2020). It is an offence for a person with deliberate intent to insult ‘in public, orally or in writing an authority or public body set up in Indonesia’ (art. 207). This article could easily be applied to anyone who makes a false claim against a public authority.

Kusumawardhani (2020) review the application of Electronic Information and Transactions Law during the 2019 election. She finds no substantial public support for eliminating the law. Changes are suggested, such as amending the law to focus on actual hate speech rather than cracking down on constructive criticism of corrupt officials. She considers that the Constitutional Court should review the law and void aspects liable to misuse. Sawitri and Wiratmaja (2019) consider that the difference between truth and falsehood, and between information and disinformation must be defined and included in the law. They suggest that there should be a “specific penal code for the producer and circulator of hoaxes.”

Further, Al-Fatih and Aditya (2019) argues that Article 28(2) of the Law does not provide an explanation of the three elements that must be met, as seen in the statement: the spreading of fake news is intentional, without right, and causes hatred and hostility. They argue that many judges ignore the element of intent deliberately. Regardless of the origins of the fake news and conspiracy theories, they have ‘clearly reduced trust between Indonesian citizens of different political, cultural, and religious affiliations, and between the government and its constituency’ (Hui, 2018).

Lao PDR

Publication and spreading of fake news are regulated by the Law on Resistance and Prevention of Cybercrime. The official English translation of the law states that it is an offence to enter into a computer system. Moreover, offences includes: 1) words that are slanderous, insulting or impolite; 2) data that are violent in character, false, cheating or untrue; 3) data which impacts national security, peace, social orderliness, culture, and tradition; and 4) data that persuades, exhorts, or encourages resistance to the Government or solidarity (art. 13).

Platform service providers and their users are subject to the Decree on Internet Information Management with the users responsible “for the content and information that are
developed, exchanged, sent, or forwarded through the website, online social media, or other forms on the Internet". During the first quarter of 2020, the government was taking action against fake news under the Law on Media and the Cybercrime Law.

**Malaysia**

The Communications and Multimedia Act regulates, amongst other actions, the transmission of false information (s. 233). The Act was complemented by the Anti-fake News Act of 2018. The latter Act was subsequently repealed in 2019 after a change of government ("Malaysia Parliament scraps law", 2019). As the Communications and Multimedia Act was not repealed, it is still in force and used to prosecute purveyors of fake news ("Content sharing on social", 2019). It is an offence to transmit a comment which is false with the intention to “annoy, abuse, threaten or harass another person” (s. 233(1)-(2)).

There is no definition as to what constitutes false information. Based on its consideration of Section 233 of the Act, the courts have set a three-part test that must be met in full for a successful prosecution: 1) Did the accused make the communication through a network facility?; Was the communication “obscene, indecent, false, menacing or offensive?”; 3) Was the communication intended “to annoy, abuse, threaten or harass another person” ("Rutinin Suhaimin v PP," para. 10)?

On 12 March 2021, the Emergency (Essential Powers) (No. 2) Ordinance entered into operation. The Ordinance addressed the spreading of fake news concerning COVID-19. Fake news “includes any news, information, data and reports, which is or are wholly or partly false relating to COVID-19 or the proclamation of emergency, whether in the forms of features, visuals or audio recordings or in any other form capable of suggesting words or ideas” (s. 2). The Ordinance has extra-territorial application regardless of the nationality or citizenship (s. 3(1)) provided it concerns Malaysia or “the person affected by the commission of the offence is a Malaysian citizen” (s. 3(2)). In summary, the offences under the ordinance include: 1) creating, offering and publishing fake news, including a publication containing fake news (s. 4); 2) providing financial assistance to those committing an offence under section 4 (s. 5); and 3) failing to remove a publication containing fake news (s. 6). Comparing the Ordinance with the repealed Anti-fake News Act shows that the only difference is the addition of the phrase “relating to COVID-19 or the proclamation of emergency” to the definition of fake news. It does not, however, include examples as were included in the repealed Act.

**Myanmar**

The fragility of democracy became apparent on 1 February 2021 when the Tatmadaw (Myanmar Defence Forces) arrested civilian leaders of the national and regional/state legislatures and declared a one-year state of emergency (“Myanmar: Military coup kills”, 2021).
Myanmar’s overall anti-cybercrime legislation is relatively rudimentary and largely dependent on its Telecommunications Law of 2013. The offences are: ‘[e]xtorting, coercing, restraining wrongfully, defaming, disturbing, causing undue influence or threatening to any person by using any Telecommunications Network’ (art. 66(d)), and ‘communications, reception, transmission, distribution, or conveyance of incorrect information with dishonesty or participation’ (art. 68(a)). The provisions have been criticised for being exceedingly broad and lacking legal certainty as they are “near-infinite in scope and hinge upon highly subjective terms that are open to a broad range of interpretation” (“Myanmar: Telecommunications law”, 2017). Two further laws are used to prosecute offences, including criminal defamation and arguably posters of fake news (“Myanmar: Briefing paper”, 2015). The Electronic Transaction Law specifies the offence of “creating, modifying, or altering of information or distributing of information created, modified or altered by electronic technology to be detrimental to the interest of or to lower the dignity of any organization or any person” (s. 34(d)). It is considered a truly loose and imprecise definition.

The role of social media in civil unrest in Myanmar incited by both the Tatmadaw and extremist Buddhist organizations is well-documented but denied by the various protagonists (Ibrahim, 2018; Irving, 2018; Wade, 2017). This is particularly the case of the continuing persecution of Muslims in Rakhine State, as reported by the Independent International Fact-Finding Mission on Myanmar (“Report of the detailed findings”, 2018). The Mission had “no doubt” that the prevalence of hate speech, including that on Facebook “significantly contributed to increased tension and a climate in which individuals and groups may become more receptive to incitement and calls for violence” (para. 1354).

Myanmar is unique amongst its ASEAN peers in that there is significant evidence that fake news is used by the Tatmadaw as a weapon against its enemies using Facebook as its medium (Douek, 2018; Gleicher, 2020; Mozur, 2018; Stecklow, 2018). A New York Times investigation found that the Tatmadaw was turning Facebook “into a tool for ethnic cleansing, according to former military officials, researchers, and civil officials in the country” (Mozur, 2018). In 2018 Facebook removed a large number of Facebook and Instagram accounts belonging to Tatmadaw for coordinated inauthentic behaviour (Gleicher, 2018). The sites were removed based on the behaviour of the actors due to false identity than on the contents of the posts. On 1 February 2021, following the coup d'état, the Tatmadaw quickly recognized that its opponents could also use the power of social media and blocked Facebook, at least temporarily (Potkin, 2021). After the action failed to deter protests, other social media platforms were blocked, and following widespread protests on 6 February, the entire internet was shut down (“Myanmar protesters take”, 2021).

Philippines

It has been widely reported that the Philippines National Police (Caliwan, 2020), especially during the COVID-19 crisis, are charging persons suspected of propagating fake news under s 4(c)4 of the Cybercrime Prevention Act and art.154 of the Revised Penal Code. Article 154(4)(1) of the Revised Penal Code states that it is a crime for a person “to publish or
cause to be published as news any false news which may endanger the public order, or cause
damage to the interest or credit of the State”.

The Cybercrime Prevention Act refers explicitly to online libel as a crime under the
Revised Penal Code (s. 4(c)(4)). The provisions of the Act concerning libel complement the
provisions in the Code. With limited exceptions, every defamatory imputation is presumed to
be malicious even if it is true (art. 354). Finally, libel can be committed by “writings or other
means” (art.355). The offence of libel in the Act can be “committed through a computer or any
other similar means which may be devised in the future” (s. 4(c)(4)). Penalties are one degree
higher than provided for in the Revised Penal Code ‘as amended, or special laws’ (s. 6). No
statute of limitations was included in the Cybercrime Prevention Act. The Department of
Justice has determined (Buan, 2019) that the Cybercrime Prevention Act is a special law and
therefore subject to the provisions of a 1926 Act. This results in a statute of limitations of 12
years ("Act to Establish Periods of Prescription for Violations," 1926 s. 1(d)).

The provisions of the Act were appealed to the Supreme Court ("Disni et al. v
Secretariat of Justice," 2014). The Court ruled that s 4(c)(4) is valid and constitutional in
relation to the original author of the post but not for those who only receive the post and react
to it (para. 48 Declaration 1). The offence of aiding and abetting under (s. 4(c)(4) and s. 4(c)(3))
was found to be void and unconstitutional (para. 48 Declaration 2). Furthermore, charging an
offender under s 4(c)(4) of the Act as well as Section 353 of the Revised Penal Code violates
the proscription against double jeopardy, and was therefore void and unconstitutional (para.
48-49).

**Singapore**

In January 2018, the Singapore Government tabled a Green Paper in Parliament
recommending that a Select Committee be appointed to consider options to address the problem
of online falsehoods (Ministry of Communications and Information and the Ministry of Law,
2018, para. 83-85). The Committee was specifically asked to address how Singapore could
“prevent and control online falsehoods”, including guiding principles and specific measures
such as legislation (para. 84(d)). The Committee recommended that the approach should
include nurturing an informed public, reinforcing social adhesion and trust, disrupting online
falsehoods, and dealing with threats to national security and sovereignty (Select Committee,
2018, para. 540). The Government responded with the Protection from Online Falsehoods and
Manipulation Act 2019 (POFMA).

Three important concepts are underpinning the Act, namely:

s 2(2)(a) a *statement of fact* is a statement which a reasonable person seeing, hearing or
otherwise perceiving it would consider to be a representation of fact; and

s 2(2)(b) a statement is false if it is false or misleading, whether wholly or in part, and whether
on its own or in the context in which it appears (s. 2(2)).

s 2(3)[A] person has *editorial control* over an online location if the person is able to decide
one or both of the following:
whether any statement may be included or excluded on the online location;
(b) where to place any statement on the online location (s. 2(3)).

The purpose of the Act is to prevent communications of false statements (s. 5(a)); suppress the operations of repeat offenders (s. 5(b)); detect, control and safeguard against coordinated actions and misuse of online accounts and bots (s. 5(c)); and enhance disclosure of paid political content (s. 5(d)). The law also covers providers of services that are used for communication of false statements of fact, whether in or outside Singapore (s. 9). Penalties for contravening the Act are heavy fines and/or imprisonment for individuals. For judicial persons, the maximum fine is at least ten times higher than for a natural person (ss. 7-9). Any Minister may instruct the Competent Authority to issue directives dealing with the communication of false statements of fact (pt. 3) and internet intermediaries (pt. 4). Action can be taken against declared online locations which contravene the Act by posting at least three false statements within the previous six months (pt. 5).

The Regulations name the prescribed internet intermediaries (s. 3); prescribed holders of press permits, broadcasting licenses, and telecommunications licenses (s. 4); and digital advertising intermediaries (s. 5) who are subject to the reporting provisions of the Act and are obliged to abide by associated Codes of Practice. An appeal under the penalty provisions of the Act is by way of a “rehearing” ("Protection from Online Falsehoods and Manipulation Rules," s. 5(1)).

Jayakumar, Ang, and Anwar (2021) note that major social media platforms had reservations but would abide by the Law. One group of objections saw POFMA as threatening civil liberties, particularly freedom of speech. The second group interpreted the law as giving the Minister the power to determine what is false. Jayakumar, Ang, and Anwar point out that this was not the case as the decisions can be challenged in court. Howe (2019) argues, however, that there were issues in relation to the appeals provision under s 17 of the Act. She considers that uncertainty “lies with s. 17(5)(b), on whether ‘the subject statement is not a statement of fact, or is a true statement of fact’” (Howe, 2019). Whilst an expedited appeals process significantly reduces the costs to the applicant in bringing a case to court, the applicant still deals with the costs of an appeal. In the result of the appeal failing, the applicant will have to meet the costs of the respondent unless it is a serious question of constitutional law, in which case costs may not apply.

As of 19 August 2020, there had been one appeal only that provides the basis of jurisprudence for future cases and is discussed below ("Singapore Democratic Party v Attorney-General,"). In brief, the Minister had found that the Singapore Democratic Party had posted misinformation on three occasions. Furthermore, Control Directives were issued. A request to the Minister to cancel the Directives was rejected (para. 2-7). The judge found that the assertion that there was a rising proportion of persons getting retrenched was a factual statement because no supporting data was cited or referenced (para. 27-32). He also found that the burden of proof to show that the statements subject to the Declarations arise and whether they are true or false rested with the respondent (i.e. the Attorney-General) (para. 44), and the standard of proof is on the balance of probabilities (para. 49). Hyperlinking to a previous article may, depending on the
circumstances, constitute re-publication of the main article (para. 51-56). The Act “necessitates an objective approach based on the wording of the material in question” (para. 128).

As of 1 July 2020, the Act had been used 55 times (Meyer, 2020). According to data reported by Meyer, the bulk of the orders under the Act aim at “political-oriented nongovernmental forces”, with less than 12% being ordinary social network users. Most of these posts (around 85%) cover criticism of the government, whilst the orders against social media posts were to tackle modest inaccuracies. During the nine-day June/July 2020 election campaign, won by the governing People’s Action Party, with 83 of the 93 seats and 61.23% of the total vote (GE2020, 2020), there were six referrals under the Act (Jaipragas, 2020). While the opposition parties had varying opinions of the Act’s impact on their campaigns, there was one significant action resulting from the Act. Google decided in December 2019 that it would not accept political advertising regulated by the Political Advertisements Code (Baker, 2019).

Thailand

Thailand regulates fake news under the Computer Crime Act, as amended, and the Criminal Code. The relevant section under Computer Crime Act (No. 2) states that it is an offence to bring into a computer system data “which is false, in such a manner likely to cause damage to the maintenance of national security, public safety, national economic security, or infrastructure for the common good of the nation, or to cause panic amongst the public” (s. 14 (1)(2)). It is also an offence to forward “computer data, with the knowledge that it is the computer data that is false” (s. 14 (2)).

There is no definition in either the Act or its amendment as to what constitutes data which are false. The application of the Act is discussed in detail by Anansaringkarn and Neo (2021) and Smith and Perry (2020). These articles also contain descriptions of several cases of the application of the Computer Crime Act and associated laws by Thai authorities.

Vietnam

Law 24 on Cybersecurity Law is wide-ranging in its application. There are a number of articles in the law that can be used to prosecute those who are considered to be communicating fake news. The Law also included prosecutions for those violating the principles of cybersecurity, including ‘ensuring the interest of the State and the lawful rights and interest of agencies, organizations, and individuals’ (art.4(1)), and ‘[l]eadership by the Vietnamese Communist Party and uniform administration by the State’ (art.4(2)). Strictly prohibited conduct under the Law includes: 1) undertaking activities to cause people to oppose the State; 2) distorting history and denying revolutionary achievements; and 3) providing false information causing confusion or harm (art. 8(1)(b) to (d)).

Depending on the seriousness of the breach, it could lead to an administrative offence or criminal prosecution and compensation (art. 9). In addition, the false, misleading, or violating information must be removed (art. 10(3)).
There is a wide range of political structures in ASEAN member states. The next task is to ascertain whether their legislation is as diverse. The information is summarized in Table 1. As the legislation is often broad in coverage with relatively ill-defined offences, it is sometimes difficult to determine the actual scope of the law. In that case, some cells in the table is filled with a “?".

Table 1. Comparison of Fake News Legislation across ASEAN

<table>
<thead>
<tr>
<th></th>
<th>Brunei Darussalam</th>
<th>Cambodia</th>
<th>Indonesia</th>
<th>Lao PDR</th>
<th>Malaysia</th>
<th>Myanmar</th>
<th>Philippines</th>
<th>Singapore</th>
<th>Thailand</th>
<th>Vietnam</th>
</tr>
</thead>
<tbody>
<tr>
<td>System of government</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Absolute monarchy</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Communist state</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Parliamentary democracy</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Presidential democracy</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Legal system</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Civil code</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Common law</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Legislative approach to fake news</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Fake news specific legislation</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Definition of fake news in legislation</td>
<td>✔</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Cybercrime/telecommunications legislation</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Criminal offence</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Administrative offence</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Safe-harbour provision for platform service providers</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Platform service providers specifically liable for content</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Broad definitions of offences open to wide interpretation</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Prescribed fake news offences</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Spreading false information likely to cause confusion, public harm, or panic</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Publishing or giving false information causing concern about safety of a person or property</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Inciting to commit offences or disturb social cohesion or damage to national security</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Publishing or spreading information believing it to be true is a defence</td>
<td>✓</td>
<td>?</td>
<td>?</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
<td>✓</td>
<td>✓</td>
</tr>
</tbody>
</table>

* fake-news specific legislation is in place either in a standalone document or explicitly included in other legislation.

Source: The authors.
Legislative Approach to Fake News

Essentially there have been two approaches to fake news. In all cases bar of Singapore, the jurisdictions have enacted cybercrime laws or have enacted or amended omnibus telecommunications legislation. The potential issue associated with adopting omnibus legislation is that it becomes quite complex as it tries to cover a plethora of issues and offences. Neither the system of government nor the legal system appears to have impacted the type of legislation used to prosecute publishers or distributors of fake news.

Criminal or Administrative Offence

In nine jurisdictions, spreading fake news is a criminal offence that can be punished by fines and/or imprisonment. Vietnam is the exception, although it has rigorous laws, the offences are treated as an administrative offence with police issuing a fine. There is a significant advantage in the Vietnamese approach that administrative fines are issued by the police and paid without the need for a court attendance, saving time, and costs for both parties.

In reality, the focus should be on removing the potentially dangerous fake news with legal action as a secondary consideration. In addition, there should be a lower threshold for the application of criminal sanctions.

Liability of platform service providers

One pressing issue associated with publishing and distributing “fake news” is the level of responsibility placed on the social media platform providers. Currently, they are primarily protected under safe harbour provisions. One of the most prominent examples of a safe harbour provision is the so-called Section 230 of Chapter 47 of the U.S. Code, which deals with the protection for private blocking and screening of offensive material. There is an interesting dichotomy in the United States with the Trump Republicans wanting it repealed so that action can be taken against the platforms removing content and the Democrats wanting it repealed so that the platforms are responsible for “fake news” posted on their sites (Siripurapu, 2020).

Indonesia is the only jurisdiction where safe harbour provisions explicitly apply. Four jurisdictions: Cambodia, Lao PDR, Philippines, and Singapore, explicitly mandate that platform providers are liable for the content on their platforms. The remainder has legislation that empowers the government with authority to order platform providers to remove content that is contrary to the law.

All major social media platforms have their own standards for users to post on their platforms. The user must accept them before using the platform. Whether or not those are actually read or understood, especially when the mother language is not English, is questionable. It is highly likely that very few users are actually cognizant of the requirements (“Community standards”, 2020; “The twitter rules”, 2021).
Prescribed Fake News Offences

In Singapore there is an explicit definition of fake news. This means that the police and prosecutors in the other jurisdictions have broad discretion in “defining” the offence and prosecuting offenders. The emphasis should be on the prompt removal of fake news than on charging offenders. Of particular concern is those who inadvertently publish or share information that they thought was true. There is an issue with the definition of “believing something to be true”. It can be overcome by setting a series of tests that must be met before such defence is accepted. The test could include questions such as: 1) Did the accused see something first-hand and misinterpreted it?; 2) Did the person do any fact-checking before the information was published?; and 3) Is the offence trivial and was not meant to cause offence? In the four former British colonies or protectorates (Brunei, Malaysia, Myanmar, and Singapore), publishing or spreading information believing it to be true is a defence. In the other jurisdictions, it is unclear.

Except for Singapore, no jurisdiction has attempted to regulate serious acts of misinformation or disinformation specifically published and spread by political parties. None of the jurisdictions has addressed the possible role of state actors in publishing and spreading misinformation or disinformation as a weapon to promote civil dissension against, for instance, minorities in the case of the Tatmadaw in Myanmar. It is considered that state actors should be held to higher account, especially in cases where they use fake news to promote communal unrest. More severe penalties should apply than in other cases.

Comparison between ASEAN Declaration and Legislation of ASEAN Member States

The key articles of the agreement include: 1) improve digital literacy; 2) strengthen national capacity to detect and respond to fake news; 3) encourage stakeholders to build on the existing industry anti-fake news norms and guides; and 4) share best practices and experience. The legislation of the member states address these factors in many practices.

In improving digital literacy, none of the State parties addressed this issue in their legislative response to fake news. In strengthening national capacity to detect and respond to fake news, each set of legislation has addressed the response, i.e. criminal sanctions and removal of offending material. The specific legislation does not include strengthened capacity to detect fake news. Meanwhile, most parties have adapted cybercrime or telecommunications than specific fake news legislation. The latter is covered by other legislative instruments and is outside the scope of the research.

To encourage stakeholders to build anti-fake news norms and guides, the legislation of each state party addresses this by defining the legislative framework through which fake news offences will be prosecuted rather than providing a positive guide as to how stakeholders should operate.
Regarding best practices and experience, only the Philippines has included a section on international cooperation in their legislation (s. 22). Undoubtedly it is because they are the only ASEAN member state that is a party to the Convention on Cybercrime.

The varying approaches taken by the ASEAN member states is not unexpected. Two of the overriding principles of ASEAN, as stated in its Charter, are: non-interference in the internal affairs of the other members (Charter of the Association of Southeast Asian Nations, 2007 art. 2(e)) and the right for every member to be free from external interference, subversion, and coercion (art. 2(f)).

CONCLUSIONS

From the overview of the legislative tools used by ASEAN member states to act against publishers and spreaders of misinformation and disinformation, it is clear that there are a number of common factors that should be addressed to provide a fairer and more transparent approach, namely: 1) Develop a concise definition as to what constitutes fake news; 2) Develop anti-fake news legislation as either a standalone statute or as a specific amendment to existing legislation; 3) Explicitly legislating that publishing or spreading information believing it to be true is a defence; 4) Except in the most serious cases, downgrade the offence from a criminal to an administrative offence where the police issue a fine; 5) Explicitly create the offence under the relevant fake news legislation of publishing and spreading of disinformation by state actors, their servants or agents. Such an approach will lead to a more transparent system focused on protecting the community from the malicious impacts of fake news.

ABOUT THE AUTHORS

Dr. Robert Brian Smith, graduated with a BSc in 1969 and, since that time, has undertaken postgraduate studies in Education, Engineering and Law. He holds a PhD in engineering, recently completed a MPhil in law investigating fake news in ASEAN and is currently a PhD candidate in law at the University of New England, Australia. Since April 2012 he has been a full-time international development consultant working in Southeast and South Asia. He has been a team leader in Bangladesh, India, Myanmar, Nepal, Sri Lanka and has spent shorter periods on projects in Cambodia, Indonesia, the Philippines, Thailand, and Timor Leste. This has given him unique insights into the development needs of least developed and developing economies.

Prof. Mark Perry, has been Professor, Faculty of Law, University of New England, Armidale, Australia, since 2012, and Emeritus Professor of Computer Science and Law at the University of Western Ontario. He is an academic leader, legal professional and computer scientist with strong governance, management, coordination, and negotiation skills. Member of the Academic Board of the University of New England from 2013-2021, and Council Member and Chair of Board for three years. He is an experienced author, presenter, and speaker of over 200 publications in both law and technology, advisor to governments, as well as expert opinions on law and technology.
Dr. Nucharee Nuchkoom Smith, graduated with degrees in Law and Political Science in Thailand. She graduated with a Master of International Trade and Commerce Law and a PhD in International Trade Law in Australia. Nucharee is an Assistant Professor in International Law at Walailak University, Thailand. From 1997 to 2011, she was an Academic/Legal Officer to the Standing Committee on Foreign Affairs of the House of Representatives, Thailand. This occurred during one of the most turbulent periods in Thai parliamentary history. Her current research interests focus on international trade law.

REFERENCES


Journal of ASEAN Studies 133


Smith, R. & Perry, M. (2020). “Fake News” legislation in Thailand: The good, the bad and the ugly. *Athens Journal of Law, 6*(3), 243-264. [https://dx.doi.org/10.30958/ajl.6-3-3](https://dx.doi.org/10.30958/ajl.6-3-3)

Smith, R. & Perry, M. (2021). Fake news and the convention on cybercrime. *Athens Journal of Law, 7*(3), 335-338. [https://doi.org/10.30958/ajl.7-3-4](https://doi.org/10.30958/ajl.7-3-4)


Legislation and Cases

47 U.S. Code § 230 - Protection for private blocking and screening of offensive material, (February 8, 1998).

Act to Establish Periods of Prescription for Violations Penalized by Special Acts and Municipal Ordinances and to Provide when Prescriptions will Begin to Run (Act No. 3326) 1926 (Philippines).

Anti-fake News Act 2018 (Malaysia).


Civil Code No 55/NA, dated 6 December 2018 (Lao PDR).


Code of Practice for Giving Prominence to Credible Online Sources of Information 2019 (Singapore).

Code of Practice for Preventing and Countering Abuse of Online Accounts 2019 (Singapore).

Code of Practice for Transparency of Online Political Advertisements 2019 (Singapore).

Communications and Multimedia Act 1998 (incorporating all amendments up to January 2006) (Malaysia)


Computer Crime Act (No 2) B.E. 2560 (2017) (Thailand) [tr Wikisource].


Criminal Code 1999 (Indonesia) [tr Hukumonline.com].

Criminal Code (Cambodia) [tr Buneng Cheung, May 2011].

Cybercrime Prevention Act of 2012 (Philippines).


Decree on Internet Information Management No 327/GOV, dated 16 September 2014 (Lao PDR).

Draft Cybercrime Law (Cambodia) Version 1 [tr Article 19].

Electronic Transactions Law 2004 (Myanmar).

Emergency (Essential Powers) (No. 2) Ordinance 2021. (Malaysia).

Government Regulation Number 80 Year 2019 on Trade Through Electronic System (Indonesia) [tr Minister of State Secretariat].


‘Fake News’ in Asean: Legislative
Jose Jesus M. Disni et al. v The Secretary of Justice et al. (Supreme Court, Republic of Philippines, en Banc, No GR 203335, February 21, 2014).

Law 24 on Cybersecurity 2018 (Vietnam) [tr Allens Linklaters].

Law Concerning Electronic Information and Transactions 2008 (as amended by Law 19 of 2016) (Indonesia) [tr Wishnu Basuki].

Law on the Management of the Nation in Emergencies 2020 (Cambodia) [tr Agence Kampuchea Presse].

Law on the Media No 01/NA, dated 25 July 2008 (Lao PDR).


Protection from Online Falsehoods and Manipulation Act 2019 (current version as at 21 June 2020) (Singapore).

Protection from Online Falsehoods and Manipulation Regulations 2019 (Singapore).


Revised Penal Code (Act No 3815) 1930 (Philippines).

Rutinin Suhaimin v PP, [2015] 3 CLJ 838 (High Court Sabah & Sarawak, Kota Kinabalu).


Supreme Court of Judicature (Protection from Online Falsehoods and Manipulation) Rules 2019 (Singapore).

Telecommunications Law 2013 (Myanmar).