LEMBAGA KETAHANAN NASIONAL
REPUBLIK INDONESIA

PENGAMANAN INFORMASI DIGITAL TERHADAP KONTEN NEGATIF GUNA MEWUJUDKAN KETAHANAN NASIONAL

Oleh :

SUSILO RAHARJO, S.T.
KOLONEL LAUT (E) NRP. 11417/P

KERTAS KARYA ILMIAH PERSEORANGAN (TASKAP)
PROGRAM PENDIDIKAN REGULER ANGKATAN LXIV
LEMHANNAS RI
TAHUN 2022

LEMBAGA KETAHANAN NASIONAL
REPUBLIK INDONESIA

KATA PENGANTAR

Assalaamu'alaikum Wr. Wb., salam sejahtera bagi kita semua.

Dengan memanjatkan puji syukur ke hadirat Tuhan Yang Maha Esa atas segala rahmat, petunjuk dan karunia-Nya, penulis sebagai salah satu peserta Program Pendidikan Reguler Angkatan (PPRA) LXIV tahun 2022 telah berhasil menyelesaikan tugas dari Lembaga Ketahanan Nasional Republik Indonesia sebuah Kertas Karya Perorangan (Taskap) dengan judul: " **PENGAMANAN INFORMASI DIGITAL TERHADAP KONTEN NEGATIF GUNA MEWUJUDKAN KETAHANAN NASIONAL".**

Penetapan judul Taskap ini didasarkan oleh Surat Keputusan Gubernur Lembaga Ketahanan Nasional Republik Indonesia Nomor: 66 Tahun 2022 tanggal 17 Maret 2022 tentang Penetapan Judul Taskap peserta PPRA LXIV Tahun 2022 Lemhannas RI. Dalam kesempatan yang baik ini perkenankan Penulis menyampaikan ucapan terima kasih yang sebesar–besarnya terutama kepada Bapak Gubernur Lemhannas RI yang telah memberikan kesempatan kepada penulis untuk mengikuti PPRA LXIV di Lemhannas RI tahun 2022. Ucapan yang sama juga Penulis sampaikan kepada Tutor Taskap kami, Bapak Marsekal Muda TNI Indrianto Wibowo Leksono, M.Si.(Han), serta semua pihak yang telah membantu serta membimbing dalam pembuatan Taskap ini sampai selesai, sesuai ketentuan yang dikeluarkan oleh Lemhannas RI.

Penulis menyadari sepenuhnya bahwa dihadapkan dengan latar belakang Penulis dalam penguasaan akademis dan terbatasnya waktu penulisan, maka kualitas Taskap ini masih jauh dari kesempurnaan akademis, oleh karena itu dengan segala kerendahanan hati mohon adanya masukan dari semua pihak, guna penyempurnaan penulisan naskah ini. Besar harapan Penulis semoga Taskap ini dapat dimanfaatkan sebagai sumbangan pemikiran Penulis kepada Lemhannas RI, Pemerintah Republik Indonesia khususnya Kementerian Kominfo, Kementerian Pendidikan, Kebudayaan, Riset, dan bagi siapa saja yang barangkali

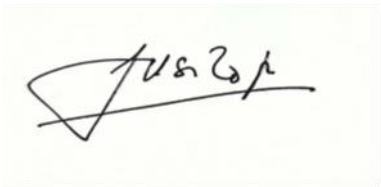
membutuhkannya dalam rangka membahas pengamanan informasi digital terhadap konten negatif guna mewujudkan ketahanan nasional.

Semoga Tuhan Yang Maha Esa senantiasa memberikan petunjuk dan bimbinganNya kepada kita, dalam melaksanakan tugas dan pengabdian kepada Bangsa dan Negara Kesatuan Republik Indonesia yang kita cintai Bersama.

Sekian dan terima kasih, Wassalamualaikum Wr. Wb.

Jakarta, September 2022

Penulis



Susilo Raharjo, S.T.
Kolonel Laut (E) NRP. 11417/P

LEMBAGA KETAHANAN NASIONAL
REPUBLIK INDONESIA

PERNYATAAN KEASLIAN

1. Yang bertanda tangan dibawah ini :

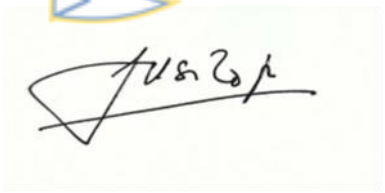
   Nama : Susilo Raharjo, S.T.
   Pangkat/NRP : Kolonel Laut (E) NRP. 11417/P
   Jabatan : Pamen Sahli Koarmada 2
   Instansi : TNI AL
   Alamat : Jl. Hang Tuah, Ujung, Surabaya, Jawa Timur.

   Sebagai peserta Program Pendidikan Reguler Angkatan (PPRA) ke LXIV tahun 2022 menyatakan dengan sebenarnya bahwa:

   a. Kertas Karya Perorangan (Taskap) yang saya tulis adalah asli.
   b. Apabila ternyata sebagian Tulisan Taskap ini terbukti tidak asli atau plagiasi, maka saya bersedia untuk dibatalkan.

2. Demikian pernyataan keaslian ini dibuat untuk dapat digunakan seperlunya.

Jakarta, September 2022
Penulis



Susilo Raharjo, S.T.
Kolonel Laut (E) NRP. 11417/P

LEMBAGA KETAHANAN NASIONAL
REPUBLIK INDONESIA

LEMBAR PERSETUJUAN TUTOR TASKAP

Yang bertanda tangan dibawah ini Tutor Taskap dari:

Nama	:	Susilo Raharjo, S.T.
Peserta	:	Program Pendidikan Reguler Angkatan (PPRA) LXIV Lemhannas RI Tahun 2022
Judul Taskap	:	Pengamanan Informasi Digital Terhadap Konten Negatif Guna Mewujudkan Ketahanan Nasional

Taskap tersebut di atas telah ditulis "sesuai/tidak sesuai" dengan Petunjuk Teknis tentang Penulisan Ilmiah Peserta Pendidikan Lemhannas RI Tahun 2022, karena itu "layak/tidak layak" dan "disetujui/tidak disetujui" untuk diuji.

""coret yang tidak diperlukan

Jakarta, September 2022
Tutor Taskap

Indrianto Wibowo Leksono, M.Si.(Han).
Marsekal Muda TNI

LEMBAGA KETAHANAN NASIONAL
REPUBLIK INDONESIA

DAFTAR ISI

Halaman

BAB I
PENDAHULUAN

1. Latar Belakang.

Dinamika perkembangan lingkungan strategis (lingstra) pada abad 21 sangat dipengaruhi perkembangan dan pemanfaatan teknologi informasi dan komunikasi yang telah mengakibatkan revolusi industri 4.0. Revolusi ini berkaitan dengan proses transformasi menyeluruh pada segala aspek produksi yang terjadi di dunia industri melalui penggabungan antara teknologi digital, internet dengan industri konvensional.[1] Saat ini, teknologi informasi dan komunikasi telah dimanfaatkan untuk menunjang berbagai aspek kehidupan manusia, sehingga mentransformasikan tatanan kehidupan sosial yang semakin mengarah pada transformasi digital.[2]

Perkembangan teknologi informasi dan komunikasi yang demikian telah berdampak positif terhadap pendistribusian informasi maupun pertukaran data. Sistem komunikasi dan informasi berbasis internet, telah dimanfaatkan sebagai sarana untuk mendistribusikan informasi secara mudah, cepat dan dalam jangkauan yang luas. Namun demikian, penyebaran informasi yang demikian pesat telah mengakibatkan fenomena *Post Truth* (pembenaran informasi), sehingga medorong perubahan secara radikal terkait pemanfaatan informasi.[3]

Pada saat ini, informasi tidak hanya dimanfaatkan untuk mendukung peningkatan pengetahuan, tetapi sebagai sumber kekuatan (*power*) yang dapat dimanfaatkan untuk mempengarui opini publik. Hal ini ditunjukan dengan semakin berkembangan dan intens penyebaran informasi hoaks maupun *fake news* melalui situs internet maupun media sosial dalam rangka mempengaruhi opini publik, sebagaimana ditunjukkan pada proses pemilihan

---

[1] Andrew, *Perjalanan Revolusi Industri 1.0 Hingga 5.0*, https://www.gramedia.com/best----------seller/perjalanan-revolusi-industri-1-0-hingga-5-0/

[2] Innay, *Transformasi Digital: Pengertian Lengkap untuk Solusi Bisnis*,---------- https://sasanadigital.com/digital-transformation/

[3] Dudi Hartono, " Era Post-Truth : Melawan Hoax dengan FactChecking," *Prosiding Seminar Nasional Prodi Ilmu Pemerintahan 2018*, hal. 71-73.

Presiden Amerika Serikat (AS) tahun 2016.[4] Selain itu, fenomena "*Arab Spring*" menunjukkan bagaimana pengaruh internet dan media sosial sebagai sarana mengorganisasikan masyarakat untuk melaksanakan demonstrasi, sebagai bentuk perlawanan terhadap pemerintah yang berkuasa, sehingga berdampak terhadap perubahan tatanan politik di Timur Tengah.[5]

Pada konteks nasional, internet maupun media sosial, juga telah dimanfaatkan untuk menunjang penyebaran informasi hoaks, ujaran kebencian maupun SARA dalam konstelasi politik nasional maupun daerah.[6] Kondisi tersebut dapat mengakibatkan perpecahan dan konflik antar warga masyarakat, sehingga berpotensi mengancam persatuan dan kesatuan bangsa.[7] Selain fenomena tersebut, internet maupun media sosial, juga telah digunakan untuk menyebarkan berbagai informasi bermuatan konten negatif/ konten ilegal seperti Informasi dan/atau Dokumen Elektronik yang memiliki muatan yang melanggar kesusilaan, perjudian, penghinaan atau pencemaran nama baik, pemerasan dan/atau pengancaman, penyebaran berita bohong dan menyesatkan sehingga mengakibatkan kerugian konsumen dalam Transaksi Elektronik, serta perbuatan menyebarkan kebencian atau permusuhan berdasarkan suku, agama, ras dan golongan, dan ancaman kekerasan atau menakut-nakuti yang ditujukan secara pribadi dapat diakses, didistribusikan, ditransmisikan, disalin, disimpan untuk didiseminasi kembali dari mana saja dan kapan saja.[8]

Untuk mengatasi permasalahan penyebaran informasi bermuatan negatif melalui media informasi digital, pemerintah telah menetapkan peraturan perundang-undangan yang dapat dijadikan dasar dalam upaya penegakan hukum, seperti Undang-Undang Informasi dan Transaksi

---

[4] Evaluating Information: Fake news in the 2016 US Elections----------, "https://libraryguides.vu.edu.au/evaluating_information_guide/fakenews2016," (akses 25 Juni 2022).

[5] Ahmad Rizky Mardhatillah Umar, dkk, "Media Sosial dan Revolusi Politik: Memahami Kembali Fenomena "*Arab Spring*" dalam Perspektif Ruang Publik Transnasional", *Jurnal Ilmu Sosial dan Ilmu Politik,* Vol. 18 , No.2, (November, 2014), hal.130.

[6] Mastel, Hasil Survei Wabah Hoax Tahun 2019, hal. 21

[7] Ni Putu Savitrya Maheswari, "Hoax dalam Dinamika Nilai Persatuan dan Kesatuan Bangsa", *Jurnal Kewarganegaraan,* Vol. 2 , No.1, (Juni, 2018), hal.6-7.

[8] Penjelasan UU RI No. 19 Tahun 2016 tentang ITE.

Elektronik (UU ITE),[9] maupun Permenkominfo terkait penanganan situs internet bermuatan negatif.[10] Namun demikian, regulasi tersebut belum dapat secara optimal diimplementasikan untuk mengatasi penyebaran konten bermuatan negatif pada situs internet maupun media sosial.

Menurut Zulfan, Lestari AKA dan Dewi Maya Sari dalam penelitian, Efektivitas Penerapan Undang-Undang ITE Terhadap Pelaku Penyebaran Hoaks Terkait Covid-19 di Media Sosial, menunjukkan bahwa UU ITE tidak sepenuhnya dapat mencegah terjadinya tindak pelanggaran hukum di dunia maya. Hal tersebut dapat dilihat dari semakin marak dan meningkatnya penyebaran informasi yang tidakbenar atau berita bohong *(hoaks)* di tengah masyarakat Indonesia. Berdasarkan data yang dirilis oleh Kemenkominfo, diketahui bahwa per tanggal 4 Oktober 2020 total isu hoaks terkait virus corona di Indonesia mencapai 1173 isu.[11]

Pada sisi lain, upaya pengamanan terhadap konten negatif lainnya yang dilakukan Kemenkominfo menunjukkan kondisi yang sama. Pada tahun 2020, menurut data Kemenkominfo, terdapat 1.219.904 aduan konten negatif yang didominasi oleh judi online dan pornografi.[12] Kemenkominfo sebagai lembaga yang bertanggung jawab terhadap pengamanan informasi digital, bahkan sudah merasa kewalahan dalam mengatasi penyebaran konten pornografi melalui situs internet maupun media sosial.[13] Kondisi tersebut apabila tidak mendapatkan perhatian yang serius serta penanganan yang tepat maka akan dapat memberikan dampak negatif pada tatanan kehidupan masyarakat yang merugikan ketahanan nasional khususnya pada gatra sosial dan budaya.

Berangkat dari penjelasan di atas, maka tulisan ini akan menganalisa lebih lanjut permasalahan tentang pengamanan informasi digital terhadap

---

[9] Undang-undang No. 19 Tahun 2016 tentang Perubahan Atas UU Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE)

[10] Peraturan Menteri Komunikasi dan Informatika Republik Indonesia Nomor. 19 Tahun 2014 tentang Penanganan Situs Internet Bermuatan Negatif

[11] Zulfan, Lestari AKA, dan Dewi Maya Sari, "Efektivitas Penerapan Undang-Undang ITE Terhadap Pelaku Penyebaran Hoaks Terkait Covid-19 di Media Sosial", *Jurnal Transformasi Administras,* Vol. 10, No.2, (2020), hal.198-211.

[12] Kemenkominfo, "Kominfo: Aduan konten negatif didominasi pornografi,"---------- https://www.kominfo.go.id/content/detail/11711/ini-konten-negatif-yang-dominan-di----------indonesia/0/sorotan_media, (akses 25 Juni 2022).

[13] Penulis Vitorio Mantalean, "Menkominfo Mengaku Tak Sanggup Batasi Akses Pornografi Pakai VPN," https://www.kominfo.go.id/content/detail/11711/ini-konten-negatif-yang-dominan-di----------indonesia/0/sorotan_media, (akses 25 Juni 2022).

maraknya penyebaran konten bermuatan negatif melalui situs internet maupun media sosial dengan judul **"Pengamanan Informasi Digital Terhadap Konten Negatif Guna Mewujudkan Ketahanan Nasional"**. Analisa dilakukan untuk mencari solusi dalam rangka menyelesaikan permasalahan-permasalahan yang ada guna mewujudkan ketahanan nasional aspek sosial budaya dalam menunjang kebijakan transformasi digital yang telah dicanangkan oleh Pemerintah.

2. Rumusan Masalah.

Perkembangan teknologi informasi dan komunikasi, terutama teknologi komunikasi berbasis internet, telah merevolusi bagaimana penyebaran informasi terjadi. Perkembangan tersebut telah mempermudah individu maupun masyarakat dalam mengakses dan menyebarkan berbagai informasi secara mudah, murah dan cepat, tanpa dibatasi ruang dan waktu, sehingga memberikan dampak yang positif diberbagai bidang kehidupan bermasyarakat, berbangsa dan bernegara. Saat ini, berbagai kegiatan bisnis, ekonomi, perkantoran, pembelajaran dapat dilaksanakan secara *online* dengan memanfaatkan sarana media digital. Pada sisi lain, hal tersebut juga berdampak negatif melalui penyebaran informasi yang tidak bertanggung jawab berupa konten negatif dalam media digital, misalnya informasi hoaks. Hal ini semakin dipengaruhi oleh kenyataan bahwa kebijakan perundangan dan kebijakan lainnya yang telah ditetapkan pemerintah belum secara efektif mengatasi penyebaran konten negatif informasi digital.

Indonesia, sebagai negara yang multikultural dan multietnis, pemanfaatan media digital untuk menyampaikan informasi hoaks terkait SARA maupun informasi hoaks lainnya merupakan hal sangat berbahaya dan mengancam kerukunan dalam kehidupan bermasyarakat. Berangkat dari kondisi tersebut diatas maka penulis akan membahas Kertas Karya Ilmiah Peseorangan (TASKAP) ini dengan rumusan masalah adalah **"Bagaimana Mengoptimalkan Pengamanan Informasi Digital Terhadap Konten Negatif Guna Mewujudkan Ketahanan Nasional?"**

Berdasarkan uraian latar belakang di atas, permasalahan penulisan Taskap ini dirumuskan dalam 3 (tiga) bentuk pertanyaan kajian yaitu :

a. Bagaimana implementasi pengamanan informasi digital terhadap konten negatif yang timbul sebagai dampak penggunaan media informasi digital saat ini.

b. Bagaimana kondisi yang diharapkan dalam pengamanan informasi digital sehingga mampu menciptakan keamanan informasi digital terhadap konten negatif yang timbul.

c. Bagaimana konsepsi pengamanan informasi digital terhadap konten negatif sehingga dapat mewujudkan ketahanan nasional.

3. Maksud dan Tujuan.

a. **Maksud.** Penulisan Taskap ini dimaksudkan untuk menganalisis dan menggambarkan permasalahan pengamanan informasi digital terhadap konten negatif berdasarkan pada aspek regulasi, institusi yang memiliki kewenangan, maupun sarana dan prasarana.

b. Tujuan. Penulisan Taskap ini bertujuan sebagai sumbangan pemikiran kepada pemangku kebijakan agar dapat dijadikan bahan pertimbangan pengambilan keputusan pada aspek regulasi, institusi yang memiliki kewenangan maupun sarana dan prasarana terkait pengamanan informasi digital terhadap konten negatif guna mewujudkan ketahanan nasional.

4. Ruang Lingkup dan Sistematika.

a. Ruang lingkup. Ruang lingkup penulisan Taskap dibatasi pada pengamanan informasi digital terhadap konten negatif guna mewujudkan ketahanan nasional pada gatra sosial budaya. Ruang lingkup pembahasan dibatasi pada aspek regulasi, institusi/kelembagaan yang memiliki kewenangan serta metode pengamanan yang terkait dengan kondisi sarana dan prasarana.

b. Sistematika penulisan. Sistematika penulisan Taskap ini disusun kedalam 4 (empat) bab, yang meliputi :

1) **Bab I Pendahuluan.** Pada bab ini akan diuraikan latar belakang terkait fakta-fakta permasalahan yang kemudian dirumuskan dalam bentuk pertanyaan penelitian.

2) **Bab II Tinjauan Pustaka.** Pada bab ini akan diuraikan berbagai ketentuan peraturan perundang-undangan, landasan teori maupun serta data terkait fakta-fakta yang berkaitan dengan permasalahan penelitian. sebelumnya terkait permasalahan penelitian.

3) **Bab III Pembahasan.** Pembahasan dilaksanakan merujuk pada pertanyaan penelitian yang telah dirumuskan, berdasarkan data-data yang ditemukan. Ketentuan peraturan perundang-undangan, landasan teori digunakan untuk menganalisis data-data yang ditemukan guna menjawab pertanyaan penelitian yang telah dirumuskan.

4) **Bab IV Penutup.** Berdasarkan pada solusi yang telah dianalisis pada bab sebelumnya, kemudian akan diambil kesimpulan berdasarkan analisis setiap pertanyaan penelitian. Selanjutnya disampaikan saran kepada berbagai pihak terkait langkah-langkah yang perlu diterapkan guna menjawab permasalahan penelitian yang telah dirumuskan pada bab I.

5. Metode dan Pendekatan.

a. Metode. Dengan mempertimbangkan permasalahan penelitian serta kerangka waktu yang tersedia, maka penyelesaian penulisan Taskap ini menggunakan metode analisis kualitatif/ deskriptif. Sementara data-data yang digunakan dalam penelitian ini menggunakan data sekunder yang diperoleh melalui studi literatur. Untuk penyajian pada penulisan Taskap ini digunakan analisa metode penyajian dengan menggunakan metodologi analisa SWOT, sehingga diharapkan dapat memberikan gambaran secara jelas terkait analisis setiap permasalahan yang telah dirumuskan.

b. Pendekatan. Penulisan Taskap ini menggunakan pendekatan kualitatif untuk menjawab permasalahan penelitian berdasarkan analisis data-data yang ditemukan dengan menggunakan berbagai kerangka teroritis.

6. Pengertian

Untuk menghidari kesalahpahaman sebagai akibat perbedaan definisi, maka diperlukan definisi beberapa istilah yang digunakan dalam penulisan Taskap ini, antara lain :

a. **Informasi.** Menurut Kamus Besar Bahasa Indonesia (KBBI), Informasi memiliki arti sebagai penerangan, pemberitahuan, kabar atau berita tentang sesuatu.[14]

b. **Pengamanan Informasi**. Pengamanan informasi menurut Agus Hermanto secara umum adalah seperangkat strategi, aturan, pedoman, praktik untuk melindungi kerahasiaan, ketersediaan, dan integritas data serta mencegah akses, penggunaan, modifikasi, pencatatan, dan penghancuran informasi yang tidak sah.[15]

c. **Konten negatif.** Definisi konten negatif menurut kemenkominfo adalah gambar porno, perjudian, penipuan, pelecehan, pencemaran nama baik dan berita bohong.[16]

d. **Transformasi digital.** Menurut Anang Sugeng Cahyono, transfomasi digital merupakan proses pemanfaatan teknologi informasi dan komunikasi untuk melakukan perubahan pada proses kegiatan masyarakat, dunia usaha, maupun pemerintah.[17]

e. ***Internet Service Provider (ISP).*** Menurut *Encyclopaedia Britannica,* ISP adalah perusahaan yang menyediakan koneksi dan layanan internet untuk individu dan organisasi.[18]

f. ***Virtual Private Network (VPN).*** Gramedia mendefinisikan VPN sebagai sebuah koneksi jaringan internet yang aman bagi penggunanya. Melalui VPN, akses yang di berikan ke website apapun dapat berjalan secara aman *(secure)* dan pribadi *(private)* yakni dengan mengubah jalur

---

[14] https://kbbi.web.id/informasi
[15] https://www.agus-hermanto.com/blog/detail/definisi-keamanan-informasi-3-aspek-di-dalamnya
[16] https://www.kominfo.go.id/content/detail/7606/melindungi-keluarga-dari-konten-negatif----------duniamaya
[17] Innay, *Transformasi Digital: Pengertian Lengkap untuk Solusi Bisnis*,----------https://sasanadigital.com/digital-transformation/
[18] https://www.britannica.com/

koneksi melalui server serta menyembunyikan adanya pertukaran data yang terjadi.[19]

g. **Media Sosial.** Menurut Andreas Kaplan dan Michael Haenlein, media sosial merupakan aplikasi berbasis internet yang memungkinkan penciptaan dan pertukaran *user-generated content*".[20]

h. **Media digital.** Media digital dapat diartikan sebagai media elektronik yang digunakan untuk menyimpan, memancarkan serta menerima informasi yang terdigitalisasi, sehingga identik dengan internet.[21]

i. **Hoaks.** Hoaks merupakan berita bohong yang tidak bisa dipertangung jawabkan kebenarannya dan dibuat dengan tujuan tidak baik, berisi informasi yang sengaja disesatkan kemudian dibuat seolah-olah sebagai kebenaran.[22]

j. **Sistem Elektronik**. Sistem elektronik adalah serangkaian perangkat dan prosedur elektronik yang berfungsi mempersiapkan, mengumpulkan, mengolah, menganalisis, menyimpan, menampilkan, mengumumkan, mengirimkan, dan/atau menyebarkan Informasi Elektronik.[23]

k. **Penyelenggaran Sistem Elektronik (PSE).** PSE adalah setiap orang, Badan Usaha dan masyarakat yang menyediakan, mengelola, dan/atau mengoperasikan Sistem Elektronik secara sendiri-sendiri maupun bersama-sama kepada Pengguna Sistem Elektronik untuk keperluan dirinya dan/ atau keperluan pihak lain.[24]

l. **Literasi Digital.** Literasi digital merupakan kemampuan untuk memahami dan menggunakan informasi dari berbagai sumber yang diakses melalui komputer. Literasi digital menjadi landasan penting bagi kemampuan memahami perangkat-perangkat teknologi, informasi dan komunikasi.[25]

---

[19] https://www.gramedia.com/literasi/apa-itu-vpn/
[20] Ibid.
[21] "Pengertian Media Digital dan Contohnya," https://www.rksbmajafm.com/2021/11/pengertian------media-digital-dan-contohnya.html, (akses 25 Juni 2022).
[22] Zulfan, Lestari AKA, dan Dewi Maya Sari, "Efektivitas Penerapan Undang-Undang ITE Terhadap Pelaku Penyebaran Hoaks", *Jurnal Transformasi Administras,* Vol. 10, No.2, (2020), hal.198-211.
[23] Pasal 1 ayat (1), Peraturan Pemerintah Republik Indonesia No. 71 Tahun 2019 tentang Penyelenggara Sistem dan Transaksi Elektronik.
[24] Ibid ayat (4).
[25] Hendra Kurniawan,dkk, *Pembelajaran : Literasi Menuju Society 5.0*, (Yogyakarta : Deepublish Publisher, 2019), hal. 35.

m. **Misinformasi.** Misinformasi merupakan informasi yang salah namun orang yang membagikannya percaya bahwa informasi itu benar. Misalnya, informasi yang disebarkan melalui media sosial tanpa mengetahui asal-usul informasinya.[26]

n. **Disinformasi.** Disinformasi merupakan informasi yang salah dan orang yang membagikannya tahu bahwa informasi itu salah dan biasanya terdapat kesengajaan atau motif terselubung. Contohnya, penyebaran hoaks sebagai alat propaganda politik di media sosial *twitter*.[27]

o. **Keadilan Restoratif.** Keadilan restoratif adalah penyelesaian perkara tindak pidana dengan melibatkan pelaku, korban, keluarga pelaku/korban, dan pihak lain yang terkait untuk bersama-sama mencari penyelesaian yang adil dengan menekankan pemulihan kembali pada keadaan semula, dan bukan pembalasan.[28]

p. **Keadilan Retributif.** Keadilan retributif yaitu keadilan yang memberikan penjatuhan pidana yang sesuai dengan kejahatan atau pelanggaran yang dilakukan.[29]

[26] Fatma Khosiah, Yuli Rohmiyati, “Kontrol Informasi Publik Terhadap *Fake News* dan *Hate Speech* Oleh Aliansi Jurnalis Independen”, *Jurnal ANUVA,* Vol. 3 , No. 3, (2019), hal.296.
[27] Ibid.
[28] Brilian Capera, “Keadilan Restoratif Sebagai Paradigma Pemidanaan di Indonesia”, *Jurnal LEX Renaissan,* Vol. 2 , No. 2, (April, 2021), hal.231.
[29] Ibnu Artadi, “Menggugat Efektivitas Penerapan Pidana Penjara Pendek Menuju Suatu Proses Peradilan Pidana Yang Humanis”, *Jurnal Hukum Pro Justitia,* Vol. 24 , No. 4, (Oktober, 2006), hal.379.

BAB II
TINJAUAN PUSTAKA

7. Umum.

Tinjauan pustaka dalam bab ini akan mencakup berbagai landasan hukum, data dan fakta yang berkaitan dengan permasalahan penelitian, serta kerangka teoritis yang digunakan sebagai pisau analisis untuk menganalisis berbagai perspektif, serta dinamika lingkungan strategis yang dapat mempengaruhi upaya pengamanan informasi digital terhadap konten negatif. Terkait dengan landasan hukum, akan diuraikan peraturan perundang-undangan yang terkait dengan pengamanan informasi digital, antara lain meliputi aturan mengenai Informasi dan Transaksi Elektronik dan turunanya berupa Peraturan Pemerintah dan Peraturan Menteri.

Selain itu, kerangka teoritis yang digunakan meliputi teori penanggulangan kejahatan, teori peperangan informasi, teori kebijakan publik di bidang komunikasi, serta analisis SWOT. Kerangka teoritis tersebut akan digunakan sebagai acuan dalam menganalisis berbagai data dan fakta yang ditemukan dalam rangka menjawab permasalahan penelitian.

8. Peraturan Perundang-undangan.

a. Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan Atas Undang-Undang Nomor. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE).

Secara prinsip, pengamanan informasi digital terhadap konten bermuatan negatif merupakan tugas pemerintah seperti diamanatkan pada pasa-pasal UU ITE, sebagai beriktut :

1) **Pasal 40 ayat (2)**: Pemerintah melindungi kepentingan umum dari segala jenis gangguan sebagai akibat penyalahgunaan Informasi Elektronik dan Transaksi Elektronik yang mengganggu ketertiban umum, sesuai dengan ketentuan peraturan perundangundangan.
2) **Pasal 40 ayat (2a)**: Pemerintah wajib melakukan pencegahan penyebarluasan dan penggunaan Informasi

Elektronik dan/ atau Dokumen Elektronik yang memiliki muatan yang dilarang sesuai dengan ketentuan peraturan perundang-undangan.

3) **Pasal 40 ayat (2b)**: Dalam melakukan pencegahan sebagaimana dimaksud pada ayat (2a), Pemerintah berwenang melakukan pemutusan akses dan/atau memerintahkan kepada Penyelenggara Sistem Elektronik untuk melakukan pemutusan akses terhadap Informasi Elektronik dan/ atau Dokumen Elektronik yang memiliki muatan yang melanggar hukum.

b. Peraturan Pemerintah Republik Indonesia Nomor 71 Tahun 2019 tentang Penyelenggara Sistem dan Transaksi Elektronik (PP PSTE).

Pengamanan informasi negatif terhadap konten bermuatan negatif, selain tugas pemerintah, juga merupakan tanggung jawab PSTE sebagaimana diamanatkan pada pasal-pasal PP PSTE, sebagai berikut :

1) **Pasal 5 ayat (1)**: Penyelenggara Sistem Elektronik wajib memastikan Sistem Elektroniknya tidak memuat Informasi Elektronik dan/atau Dokumen Elektronik yang dilarang sesuai dengan ketentuan perundang-undangan.

2) **Pasal 5 ayat (2)**: Penyelenggara Sistem Elekronik wajib memastikan Sistem Elektroniknya tidak memfasilitasi penyebarluasan Informasi Elektronik dan/atau Dokumen Elektronik yang dilarang sesuai dengan ketentuan perundang-undangan.

c. Peraturan Menteri Komunikasi dan Informatika Republik Indonesia Nomor 5 Tahun 2020 Tentang Penyelenggara Sistem Elektronik Lingkup Privat.

Untuk memastikan Penyelenggaraan Sistem Elektronik (PSE) Lingkup Privat, mematuhi kewajiban yang dipersyaratkan PP PSTE,

maka PSE wajib melaksanakan pendaftaran, sebagaimana diamanatkan pada pasal-pasal Peraturan Menteri (Permen) tersebut, yaitu :

1) **Pasal 2 ayat (1)**: Setiap PSE Lingkup Privat wajib melakukan pendaftaran.
2) **Pasal 2 ayat (3)**: Kewajiban melakukan pendaftaran bagi PSE Lingkup Privat dilakukan sebelum Sistem Elektronik mulai digunakan oleh Pengguna Sistem Elektronik.
3) **Pasal 2 ayat (4)**: Pendaftaran ISP sebagai PSE Lingkup Privat dilaksanakan melalui perizinan yang diselenggarakan oleh Kementerian sesuai dengan ketentuan peraturan perundang-undangan.

d. Peraturan Menteri Komunikasi dan Informatika Republik Indonesia Nomor. 19 Tahun 2014 tentang Penanganan Situs Internet Bermuatan Negatif.

Permen ini mengatur ruang lingkup pengamanan konten bermuatan negatif, sebagaimana dijelaskan pada pasal 3, sebagai berikut :

1) Penentuan situs internet bermuatan negatif yang perlu ditangani.
2) Peran Pemerintah dan masyarakat dalam penanganan situs internet bermuatan negatif.
3) Peran Penyelenggara Jasa Akses Internet dalam penanganan situs bermuatan negatif.
4) Tata cara pemblokiran dan normalisasi pemblokiran dalam penanganan situs internet bermuatan negatif.

9. Kerangka Teoritis.

a. Teori Penanggulangan Kejahatan.

Kebijakan penanggulangan kejahatan atau disebut juga politik kriminal memiliki tujuan akhir atau tujuan utama yaitu perlindungan

masyarakat untuk mencapai kesejahteraan masyarakat.[30] Kebijakan penanggulangan kejahatan dapat meliputi ruang lingkup yang cukup luas. Namun demikian, menurut G. Peter Hoefnagels, ruang lingkup "*criminal policy*" dalam upaya penanggulangan kejahatan terdiri dari 3 (tiga) metode penanggulangan, yaitu :[31]

1) Penerapan hukum pidana (*criminal law application*).
2) Pencegahan tanpa pidana (*prevention without punishment*).
3) Mempengaruhi pandangan masyarakat mengenai kejahatan dan pemidanaan di media massa (*influencing views of society on crime and punishment/mass media*).

Berdasarkan pada ketiga metode diatas, penerapan hukum pidana merupakan pendekatan represif, sementara pencegahan tanpa pidana dan pengaruhi pandangan masyarakat melalui media massa merupakan pendekatan yang bersifat preventif. Kedua pendekatan tersebut digunakan untuk menganalisis implementasi pengamanan informasi digital terhadap konten bermuatan negatif.

b. Teori Peperangan Informasi.

Peperangan informasi, berdasarakan penjelasan berbagai literatur, dapat dimaknai sebagai penggunaan media informasi sebagai sarana untuk menyebarkan informasi atau opini yang menjurus pada propaganda.[32] Penggunaan informasi untuk mempengaruhi opini telah semakin dipermudah seiring dengan perkembangan teknologi informasi dan komunikasi, terutama teknologi komunikasi berbasis internet. Oleh karena itu, menurut David Patrikarakos dalam *War in 140 Characters : How Social Media Is Reshaping Conflict in the Twenty First Century*, peperangan informasi dalam bentuk narasi atau kata-kata merupakan

[30] Tirta Raharja, *Strategi Penanggulangan Informasi Hoax Di Media Sosial Oleh Unit Cyber Crime Di Kota Makassar*, Skripsi Fakultas Ilmu Politik, Universitas Muhammadiyah Makassar, 2020, hal. 19-20.
[31] Ibid.
[32] Stein, George J. *"Information warfare"* (https://www.hsdl.org/?view&did=439935). Air University (U.S.). Press. Diakses 14 Mei 2022, 11.35 WIB.

salah satu bentuk konflik pada abad 21, selain konfik fisik yang melibatkan kekuatan militer.[33]

Definisi peperangan informasi yang menekankan penggunaan media informasi telah mengalami perubahan secara radikal seiring dengan penggunaan teknologi internet di bidang informasi dan komunikasi. Menurut P.W Singer dan Emerson T. Brooking, dalam *LikeWar : The Weaponization of Sosial Media*, internet tidak hanya berperan sebagai jaringan komunikasi, tetapi telah berubah menjadi medan perang (*battlefield*) yang melibatkan setiap individu tanpa memandang status sosial. Kondisi yang demikian, juga telah mengubah peran media sosial dari sarana komunikasi menjadi senjata (*weapon*).[34]

Peperangan yang dilaksanakan di internet, lebih lanjut menurut P.W Singer dan Emerson T. Brooking, berbeda dengan apa yang terjadi dengan peperangan secara umum. Kemenangan tidak diukur berdasakan kerusakan pada aspek fisik, tetapi terkait bagaimana mendapatkan perhatian (*attention*) dengan memanfaatkan media sosial sebagai senjata untuk menyebarkan berbagai informasi.[35] Oleh karena itu, bentuk peperangan yang terjadi di internet berkaitan dengan manipulasi psikologis masyarakat melalui penyebaran informasi yang bersifat viral.[36]

Pada sisi lain, menurut P.W Singer dan Emerson T. Brooking, kesuksesan mendapatkan perhatian melalui informasi viral di dunia virtual memiliki berdampak langsung di dunia fisik (realita) dalam skala yang lebih luas.[37] Fenomena "*Arab Spring*" menunjukkan bagaimana pengaruh media sosial sebagai sarana penyebaran informasi viral terkait perjuangan politik demokrasi di Tunisa, telah mendorong perjuangan

[33] David Patrikarakos, *War in 140 Characters : How Social Media Is Reshaping Conflict in the Twenty First Century*, (New York : Basic Books, 2017), hal. 2.
[34] P.W Singer, Emerson T. Brooking, *LikeWar : The Weaponization of Sosial Media*, (Boston : Houghton Mifflin Harcourt Publishing Company, 2018), hal. 22.
[35] Ibid.
[36] Ibid
[37] Ibid.

yang sama di Mesir, Libya, Yaman, dan Yordania, sehingga berdampak pada perubahan politik di Timur Tengah.[38]

Secara universal, untuk mengatasi penggunaan informasi untuk tujuan manipulasi psikologis masyarakat, pendekatan dalam penyelenggaran keamanan informasi pada domain siber dapat dilaksanakan melalui 3 (tiga) pendekatan, yaitu :

1) Pendekatan budaya. Pendekatan ini merujuk pada penyelenggaraan literasi digital untuk mendorong penggunaan sistem informasi dan komunikasi secara bijak dan bertanggungjawab.
2) Pendekatan Hukum. Penggunaan hukum dalam rangka menindak setiap pelanggaran terkait pemanfaatan sistem informasi dan komunikasi untuk menyebarkan informasi yang melanggar ketentuan perundang-undangan yang berlaku.
3) Pendekatan Teknologi. Penggunaan teknologi sebagai sarana dan prasarana dalam rangka meningkatkan perlindungan informasi maupun sistem informasi dan komunikasi.

Menurut Anisa Rizki Sabrina, literasi digital bertujuan untuk meningkatkan kemampuan kritis individu dalam memanfaatan media digital, termasuk media sosial, secara bijak dan bertanggungjawab dalam pemprosesan informasi, yang melibatkan kompetensi teknologi, kognitif dan sosial. Peningkatan kemampuan kritis merupakan bentuk *self control* sebagai solusi dalam mencegah kasus peredaran hoaks, maupun berbagai konten negatif lainnya yang tersebar pada ruang digital.[39] Sementara peningkatan sarana dan prasarana teknologi diperlukan untuk melakukan pengawasan terhadap informasi yang tersebar pada situs internet maupun media sosial.[40]

---

[38] Ahmad Rizky Mardhatillah Umar, dkk, "Media Sosial dan Revolusi Politik: Memahami Kembali Fenomena "*Arab Spring*" dalam Perspektif Ruang Publik Transnasional", *Jurnal Ilmu Sosial dan Ilmu Politik,* Vol. 18 , No.2, (November, 2014), hal.130.

[39] Anisa Rizki Sabrina , " Literasi Digital Sebagai Upaya Preventif Menanggulangi Hoax," *Journal of Communication Studies*, Vol. 5, No. 2 (Desember, 2018), hal. 42-44.

[40] Ibid.

c. Teori Kebijakan Publik

Menurut Syafiie, kebijakan publik didefinisikan sebagai jawaban terhadap suatu permasalahan. Permasalahan apapun, terutama yang menyangkut kepentingan publik, memerlukan upaya untuk menyelesaikan, mengurangi, serta mencegah faktor-faktor yang merupakan akar penyebab permasalahan tersebut. Oleh karena itu, kebijakan publik merupakan faktor yang menentukan dalam penyelesaian permasalahan apapun, sehingga dibutuhkan inovasi, cara terbaik dan tindakan yang terarah.[41]

Untuk itu, pengaturan terhadap permasalahan bagaimana komunikasi yang harus dilaksanakan dalam kehidupan bermasyarakat, merupakan bagian dari kebijakan publik yang terkait dengan kebijakan komunikasi. Menurut L. Sommeriad, seperti dikutip Ana Nadhya Abr, kebijakan komunikasi didefinisikan sebagai : "*The ways in which communication is used, the networks through which it flows, the structures of media system, the regulatory framework for the system, and the decision of people who operate it, are all the outcome of communication policies*."[42]

Berdasarkan pada definisi di atas, kebijakan komunikasi berkaitan dengan tata cara komunikasi, jaringan yang digunakan untuk berkomunikasi, struktur sistem media komunikasi, kerangka regulasi untuk sistem tersebut, dan keputusan orang yang mengoperasikan sistem komunikasi, semuanya merupakan hasil dari kebijakan komunikasi.[43] Sementara menurut UNESCO, kebijakan komunikasi merupakan kumpulan prinsip-prinsip dan norma-norma yang sengaja dibuat untuk mengatur perilaku sistem komunikasi.[44] Kebijakan komunikasi merupakan hal penting yang diperlukan dalam rangka pengamanan informasi digital terhadap konten bermuatan negatif melalui media digital, seperti situs internet maupun media sosial.

---

[41] Arifin Tahir, *Kebijakan Publik dan Good Governancy*, hal. 6-7.
[42] Ana Nadhya Abr, dkk, *Demokrasi Bermedia Online*, (Yogyakarta : Tiara Wacana Lokus, 2014), hal. 98-99.
[43] Ibid.
[44] Ibid.

d. Analisis SWOT

Menurut Pearce dan Robinson analisis SWOT didasarkan pada asumsi bahwa suatu strategi yang efektif akan memaksimalkan kekuatan (*strength*) dan peluang (*opportunity*), dan meminimalkan kelemahan (*weakness*) dan ancaman (*threat*). Untuk itu, penggunaan metode SWOT, mensyaratkan analisis terhadap faktor eksternal dan internal.[45] Faktor kekuatan dan kelemahan berkaitan dengan faktor internal organisasi, sementara peluang dan ancaman dipengaruhi oleh lingkungan eksternal atau terkait dengan kondisi yang terjadi di luar organisasi.[46]

Analisa SWOT merupakan metode yang efektif untuk membantu proses pengambilan keputusan dalam mewujudkan visi dan misi organisasi, dengan mempertimbangkan faktor internal dan eksternal yang mempengaruhi perkembangan organisasi. Untuk itu, penggunaan metode SWOT, mensyaratkan analisis terhadap faktor eksternal dan internal, sebagai berikut: [47]

1) **Faktor Eksternal.** Faktor eksternal merupakan faktor yang mempengaruhi peluang (*Opportunity*) dan ancaman (*Threath*), dan berkaitan langsung dengan kondisi yang terjadi di luar organisasi.
2) **Faktor Internal.** Faktor internal merupakan faktor yang mempengaruhi kekuatan (*Strenght*) dan kelemahan (*Weakness*), dan berkaitan langsung dengan kondisi yang terjadi dalam organisasi.

Analisis SWOT disusun untuk menggambarkan berbagai faktor internal dan eksternal yang mempengaruhi implementasi pengamanan informasi digital yang telah dilaksanakan pemerintah saat ini. Selain itu, analisis tersebut juga digunakan dalam rangka rumusan konsepsi

[45] Irham Fahmi, Manajemen Strategis Teori dan Aplikasi, 260
[46] Pearce Robinson, Manajemen Stratejik Formulasi, Implementasi dan Pengendalian, 229.
[47] Irham Fahmi, Manajemen Strategis Teori dan Aplikasi, 260

pengamanan informasi digital agar dapat mengoptimalkan pengamanan informasi digital terhadap konten negatif.

10. Data dan Fakta.

a. Penyedia Layanan Internet dan Pengguna Informasi Digital.

Penggunaan teknologi internet telah menjadi bagain sentral dalam kehidupan masyarakat Indonesia, dan terus mengalami peningkatan seiring pembangunan infrastruktur jaringan internet di seluruh wilayah Indonesia. Menurut data Asosiasi Penyelenggara Jasa Internet Indonesia (APJII), terdapat kurang lebih 175 juta pengguna internet pada tahun 2021, dan terus mengalami peningkatan sekitar 35 juta, atau kurang lebih terdapat 210 pengguna internet diawal tahun 2022, atau sekitar 77% dari total jumlah penduduk Indonesia.[48] Menurut APJII, berdasarkan pulau tingkat penetrasi cukup merata, meskipun tingkat penetrasi internet didominasi di Pulau Jawa sebesar 43,92%, dibandingkan wilayah di Sulawesi, Maluku maupun Papua.[49]

Sebagai negara dengan jumlah penduduk terbesar keempat secara global dan wilayah geografis yang luas, telah menjadikan Indonesia sebagai salah satu pasar menarik bagi industri telekomunikasi. Menurut Badan Pusat Statistik (BPS), terdapat 602 perusaha yang berkecimpung dalam bidang *Internet Service Provider* (ISP) atau sekitar 62,77% dari total 959 perusahaan yang telah mendapatkan izin menyelenggarakan layanan telekomunikasi di Indonesia pada 2020.[50] Sementara menurut APJII, diperkirakan akan terdapat sekitar 1.000 perusahan ISP yang beroperasional di Indonesia pada tahun 2022.[51]

---

[48] Intan Rakhmayanti Dewi, “Data Terbaru! Berapa Pengguna Internet Indonesia 2022?,” https://www.cnbcindonesia.com, (akses 16 Juni 2022).

[49] Agus Tri Haryanto, "Jumlah Pengguna Internet Indonesia Tembus 210 Juta" https://inet.detik.com/telecommunication/d-6119064/jumlah-pengguna-internet-indonesia-tembus-210-juta, (akses 16 Juni 2022).

[50] Monavia Ayu Rizaty, “Sebanyak 959 Penyelenggara Telekomunikasi Beroperasi di Indonesia pada 2020”, https://databoks.katadata.co.id/datapublish/2021/10/12/sebanyak-959-penyelenggara-telekomunikasi-beroperasi-di-indonesia-pada-2020, (akses 16 Juni 2022).

[51] Ibnu Naufal, “APJII: Jumlah Perusahaan Layanan Internet Bakal Mencapai 1.000”, https://www.inilah.com/apjii-jumlah-perusahaan-layanan-internet-bakal-mencapai-1-000, (akses 16 Juni 2022).

Berdasarkan data penelitan *Hootsuite (We are Social), Indonesian Digital Report 2022*, perangkat *mobile* merupakan sarana utama yang digunakan untuk mengakses jaringan internet dibandingkan dengan perangkat lainnya. Pada tahun 2022, terdapat 370,1 juta perangkat mobile yang digunakan untuk mengakses layanan internet, atau terdapat peningkatan sebesar 3,6% dari 345,3 juta perangkat mobile tahun 2021. Secara umum, masyarakat Indonesia menghabiskan kurang lebih 9 (sembilan) jam sehari untuk mengakses jaringan internet. Kebutuhan akan informasi merupakan faktor yang dominan mendorong digunakannya layanan internet atau sekitar 80,1%, dibandingkan dengan faktor-faktor lain, seperti menemukan ide-ide baru sebesar 72,9%, berhubungan dengan teman dan keluarga sekitar 68,2% maupun sekedar mengisi waktu luang sebesar 63,4%, [52]

Pada sisi lain, media sosial merupakan salah satu media digital yang digunakan selain situs internet, dan terus mengalami penggunaan. Menurut data penelitan Hootsuite, penggunaan media sosial mengalami peningkatan yang signifikan, dari sekitar 62 juta pengguna media sosial pada tahun 2014, menjadi sekitar 191,4 juta pengguna pada tahun 2022, atau sekitar 68,9% dari total penduduk Indonesia. Secara umum, rata-rata menghabiskan sekitar 3 jam, 17 menit setiap hari untuk menggunakan media sosial melalui perangkat *smart phone*, gadget maupun laptop. Secara umum, Whatsapp merupakan aplikasi media sosial yang paling banyak digunakan atau sekitar 88,7% dari jumlah penduduk Indonesia, dibandingkan dengan Instagram sebanyak 84,8%, Facebook sebanyak 81,3%.[53]

b. Konten-Konten Negatif.

Pemanfaatan teknologi komunikasi terutama teknologi digital, telah menjadikan media digital, situs internet dan media sosial, sebagai sarana utama yang dimanfaatkan dalam proses komunikasi. Sebagai sarana

[52] "Hootsuite (We are Social): Indonesian Digital Report 2022", https://andi.link/hootsuite-we-are-social-indonesian-digital-report-2022/, (akses 16 Juni 2022).
[53] Ibid.

pertukaran informasi yang dominan saat ini, media digital telah dikembangkan dan dimanfaatkan untuk hal-hal positif dalam rangka memajukan kehidupan bermasyarakat, berbangsa dan bernegara. Namun demikian, media digital telah dimanfaatkan untuk menyebarkan berbagai informasi yang dapat mengganggu ketertiban umum, maupun informasi yang berpotensi mengancam keamanan nasional, atau yang disebut konten bermuatan negatif.

Pelaksanaan penanganan terhadap konten negatif merupakan pewujudan UU ITE terhadap tindakan atau perbuatan yang dilarang untuk dilakukan di ruang internet atau siber. Hal ini merupakan kewajiban pemerintah untuk memfasilitasi pemanfaatan teknologi informasi dan komunikasi pada hal-hal yang positif, dalam rangka mewujudkan ruang digital yang aman, bersih dan bersahabat guna mendukung pencapaian kepentingan nasional. Untuk itu, dalam pengamanan terhadap konten negatif pada media digital, Kemenkominfo berdasarkan kententuan peraturan perundang-undangan, telah mengklasifikasikan konten negatif, sebagaimana ditunjukan pada Tabel I. Klasifikasi Konten Negatif.[54]

Berdasarkan pada gambaran konten negatif, hoaks merupakan salah satu permasalahan yang patut mendapat perhatian pemerintah, karena dapat memuat informasi yang dapat memecah bela bangsa, sehingga berpotensi merusak persatuan dan kesatuan.[55] Menurut data penelitian yang disampaikan Masyarakat Telematika Indonesia (MASTEL) pada tahun 2019, terdapat beragam jenis informasi hoaks yang disebarkan melalui berbagai media. Menurut penelitian tersebut, informasi bohong yang disengaja merupakan jenis informasi hoaks yang paling dominan sekitar 88%, dibandingkan dengan informasi lainnya, seperti berita yang menghasut sekitar 49%, maupun berita yang menyudutkan pemerintah 14%.[56] Selain itu, bentuk infomasi hoaks juga

[54] Lampiran II. Daftar Tabel
[55] Barman Tambunan, "Tantangan Merawat Kebhinnekaan di Era Digital," (Diskusi Panel SBS Bhinneka Tunggal IKA PPRA LXIV Tahun 2022, Jakarta, 3 Juni, 2022).
[56] Mastel, *Hasil Suvey Wabah Hoaks Nasional Tahun 2019*, hal. 9.

bervariasi dari tulisan tangan, editan foto maupun berita lama yang diposting pada media digital.[57]

Menurut penelitian tersebut, secara umum media sosial merupakan saluran penyebaran hoaks yang tertinggi sekitar 87,50%, dibandingkan dengan sarana lainnya, seperti aplikasi *chatting* sekitar 67,0%, maupun website sekitar 28,20%. Sementara penyebaran hoaks didominasi oleh informasi terkait sosial politik sekitar 93,20%, dibandingkan dengan informasi terkait SARA sekitar 76,20%, pemerintah sekitar 61%, maupun terkait penipuan keuangan sekitar 18,50%.[58]

Dalam hal penggunaan media sosial, menurut laporan database Kemenkominfo pada 2018-30 November 2021, Twitter merupakan aplikasi media sosial yang paling banyak digunakan untuk menyebarkan berbagai konten bermuatan negatif sejumlah 568,843 konten, Facebook sekitar 11,470 konten, Instagram sejumlah 11,470 konten, WhatsApp sekitar 11,470 konten, Google sekitar 1,757 konten, You Tube sekitar 1,492 konten, Telegram sekitar 1,077 konten, Tiktok sekitar 210 konten, maupun media sosial lainnya,[59] sebagaimana ditunjukan pada Tabel II. Media Sosial Bermuatan Konten Negatif.[60]

Berkaitan dengan konten negatif, menurut data Kemenkominfo dalam kurun waktu periode 2018-2021, pemblokiran konten negatif selama periode tersebut didominasi oleh konten ponografi berjumlah 1,107,547, dibandingkan dengan konten negatif, seperti perjudian online sekitra 423,453, penipuan sekitar 14,757, terorisme/radikalisme berjumlah 509, separatisme/organisasi terlarang berjumlah 14 konten, kekerasan pada anak sekitar 10 konten, maupun media sosial lainnya,[61] seperti ditunjukan pada Tabel III. Pemblokiran Konten Negatif Periode 2018-2021.[62]

---

[57] *Ibid*., hal. 23.
[58] *Ibid*., hal. 22.
[59] Agustin Setyo Wardani, "Kemenkominfo Takedown 1,5 Juta Konten Negatif, Ini Detailnya", https://www.liputan6.com/tekno/read/4726843/Kemenkominfo-takedown-15-juta-konten-negatif-ini----detailnya, (akses 16 Juni 2022).
[60] Lampiran II. Daftar Tabel
[61] https://www.kominfo.go.id/, (akses 16 Juni 2022).
[62] Lampiran II. Daftar Tabel

c. Pengamanan Konten Negatif Yang Dilaksanakan Negara Lain.

Pengamanan media informasi digital seperti situs internet maupun media sosial terhadap konten negatif yang dilaksanakan berbagai negara sangat bergantung terhadap sistem nilai budaya dan aturan yang mendasari kehidupan sosial masyarakat. Negara-negara penganut sistem nilai liberal sebagai nilai yang membentuk kehidupan sosial masyarakat, penyebaran konten ponografi dan perjudian merupakan hal yang legal serta merupakan suatu kegiatan industri. Sementara negara dengan sistem politik liberal demokrasi, yang sangat menjunjung nilai kebebasan berbicara (*freedom of speech*), penyebaran informasi seperti hoaks, *fake news* dan informasi lainnya, merupakan wujud dari bentuk kebebasan berbicara, sehingga bukan merupakan suatu perbuatan yang harus dilarang atau melanggar hukum. Pada sisi lain, negara-negara yang menganut sistem politik dan bentuk pemerintahan otoriter, memiliki kecenderungan untuk mengontrol arus informasi yang boleh diakses oleh setiap warga negara.

Perbedaan sistem nilai dan politik yang membentuk kehidupan sosial masyarakat telah mempengaruhi pengamanan informasi terhadap konten negatif yang diimplementasi oleh berbagai negara. Walaupun demikian, menurut P.W Singer dan Emerson T. Brooking, dalam *LikeWar : The Weaponization of Sosial Media*, secara umum kebijakan pengamanan yang diterapkan dalam pengamanan informasi, meliputi kebijakan pengontrolan terhadap sistem informasi dan komunikasi, maupun kebijakan penyensoran (*censorship*) terhadap berbagai informasi yang dapat mengancam keamanan nasional.[63]

Kebijakan pengontrolan dimaksudkan agar sistem informasi dan komunikasi tidak dapat dimanfaatkan untuk menyebarkan informasi secara luas, terutama informasi yang dapat berdampak negatif terhadap keamanan nasional. Kebijakan pengontrolan dapat berupa pemutusan akses jaringan komunikasi pada wilayah tertentu, seperti penyebaran informasi SARA yang dapat menyebabkan konflik. Misalnya, pemerintah

[63] P.W Singer, Emerson T. Brooking, Ibid., hal. 114-159.

India melakukan pemutusan jaringan internet selama seminggu, ketika terjadi konflik sosial di wilayah Rohtak pada tahun 2016. Hal tersebut dilakukan untuk menghindari penyebaran informasi negatif, seperti hoaks terkait konflik tersebut, agar tidak menimbulkan konflik sosial di wilayah lain di India.[64]

Selain itu, kebijakan pengontrolan juga berkaitan dengan pengaturan sistem informasi dan komunikasi dalam rangka mengontrol berbagai informasi yang dapat diakses oleh warga negara. Misalnya, pemerintah China telah menerapkan kebijakan penggunaan teknologi VPN, yang sesuai dengan lisensi yang telah ditetapkan pemerintah. Penggunaan teknologi VPN yang tidak sesuai atau tidak resmi akan dikenai denda sekitar US$145.[65] Kebijakan tersebut memudahkan pemerintah China melaksanakan pengawasan terhadap berbagai informasi yang diakses melalui media digital, walaupun menggunakan teknologi VPN. Kebijakan pengaturan VPN juga telah diimplementasikan oleh beberapa negara, seperti China, Rusia maupun Turki dan beberapa negara lainnya.[66]

Pada sisi lain, untuk mengatasi penyebaran konten negatif berupa hoaks, pemerintah Finlandia mengedepankan pelaksanaan literasi media digital sejak pendidikan dasar. Berdasarkan laporan The Guardian, Finlandia merupakan negara yang memiliki kemampuan menangkal informasi hoaks yang tinggi dibandingkan dengan negara-negara yang terdapat di kawasan Eropa. Hal tersebut juga sesuai dengan survei yang dilakukan oleh Statista pada tahun 2018, yang menunjukan bahwa Finlandia menjadi negara paling rendah terpapar informasi hoaks di antara negara anggota Uni Eropa.[67]

---

[64] Ibid.

[65] Marisa Dika Andini, dkk,"Penggunaan Aplikasi Virtual Private Network (VPN) Point To Point Tunneling Protocol (PPTP) Dalam Mengakses Situs Terblokir ," *Supremasi Hukum: Jurnal Penelitian Hukum*, Vol. 29, No. 2 (Agustus, 2020), hal. 161-162.

[66] Roy Franedya, “Rudiantara Pilih Melarang, Negara Ini Malah Blokir Total VPN”,---------- https://www.cnbcindonesia.com/tech/20190527114452-37-75232/rudiantara-pilih-melarang---------- negara-ini-malah-blokir-total-vpn, (akses 18 Juni 2022).

[67] Adya Rosyada Yonas, “Upaya Finlandia Melawan Hoaks : Ajar Literasi Media di Kurikulum Sekolah Dasar” https://kumparan.com/adya-yonas/upaya-finlandia-melawan-hoaks-ajarkan-literasi-media-di-kurikulum-sekolah-dasar-1wWVnHSypqP/full, (akses 18 Juni 2022).

11. Lingkungan Stategis.

a. Lingkungan Global.

Perkembangan teknologi informasi dan komunikasi telah merevolusi arus informasi dibandingkan dengan era sebelumnya. Perkembangan teknologi internet dan media sosial telah berdampak terhadap distribusi informasi yang dilaksanakan secara cepat, jangkauan luas, serta tidak dipengaruhi hambatan geografis. Oleh karena itu, pada saat ini kehidupan bermasyarakat dan bernegara dipengaruhi oleh berbagai informasi, baik dari situs internet, *platform* media sosial maupun *media mainstream.*

Pada satu sisi, kemudahan dalam memperoleh informasi dapat berdampak positif terhadap peningkatan pengetahuan. Namun, pada sisi lain, berbagai informasi yang terdapat pada dunia maya belum sesuai dengan realita yang sebenarnya, sehingga diperlukan kemampuan berpikir kritis. Kemampuan tersebut diperlukan untuk menilai kebenaran informasi berdasarkan pada fakta, dan bukan tergatung pada emosi atau keyakinan personal tertentu.

Post truth merupakan fenomena yang didefiniskan sebagai kondisi psikis yang mengedepankan emosi dan keyakinan personal, dibandingkan dengan fakta terhadap kebenaran informasi yang membentuk opini publik. Kondisi ini memuncak pada kontestasi politik, dimana terjadi peperangan informasi untuk memperoleh kekuasaan. Dalam kondisi yang demikian, berkembang berbagai informasi hoaks maupun *fake news* yang dapat mempengaruhi pandangan publik,[68] seperti ditunjukan pada pemilihan Presiden Amerika Serikat tahun 2016.[69]

Perkembangan fenomena *Post truth* tersebut akan berdampak negatif terhadap tatanan kehidupan sosial nasional melalui penyebaran informasi hoaks bermuatan SARA di berbagai platform media sosial,

---

[68] Dudi Hartono, " Era Post-Truth : Melawan Hoax dengan FactChecking," *Prosiding Seminar Nasional Prodi Ilmu Pemerintahan 2018*, hal. 71-73.

[69] Evaluating Information: Fake news in the 2016 US Elections----------, “https://libraryguides.vu.edu.au/evaluating_information_guide/fakenews2016,” (akses 25 Juni 2022).

terutama pada penyelenggaraan kontestasi politik baik nasional maupun daerah. Hal tersebut dapat mengakibatkan polarisasi dalam masyarakat berdasarkan SARA, sehingga berpotensi sebagai sumber konflik sosial antar warga masyarakat, yang dapat mengancam persatuan serta kesatuan bangsa dan negara.

Terkait dampak negatif tersebut, diperlukan upaya penegakan hukum yang sesuai dengan prinsip keadilan dan kesetaraan serta memperhatikan nilai demokrasi, hak asasi manusia (HAM) maupun nilai-nilai yang membentuk kehidupan sosial masyarakat. Selain itu, diperlukan upaya peningkatan literasi digital dalam rangka meningkatkan *self control* individu maupun masyarakat, agar dapat menilai secara kritis setiap informasi yang diterima melalui media sosial. Selain itu, literasi digital juga akan mampu mendorong dan meningkatkan kesadaran terhadap penggunaan media sosial secara bijak dan bertanggung jawab.

Penyelenggaran literasi digital dapat dilaksanakan melalui berbagai metode pendidikan baik informal seperti kursus, seminar maupun pelatihan. Selain itu, juga dapat dilaksanakan secara formal pada jenjang pendidikan dasar dan menengah dalam kurikulum sistem pendidikan. Oleh karena itu, diperlukan peningkatan infrastruktur jaringan internet maupun sarana dan prasarana pendukung, terutama di daerah yang memiliki keterbatasan akses internet, seperti pedesaan, daerah terpencil maupun daerah terluar, terdepan dan tertinggal, agar penyelenggaran literasi digital dapat dilaksanakan di seluruh wilayah negara.

b. Lingkungan Regional.

Perkembangan lingkungan strategis regional sangat dipengaruhi oleh berbagai potensi ancaman yang dapat menggangu stabilitas keamanan dan politik kawasan, baik ancaman militer maupun ancaman non militer. Pada bidang pemanfaatan teknologi informasi, China menerapkan kebijakan sangat membatasi akses internet kepada warga negaranya. Selain itu, upaya China untuk menganeksasi Taiwan yang

diwaranai perang informasi dan propaganda, dapat mengakibatkan konflik militer terbuka dengan Amerika Serikat.[70]

Selain ancaman militer, ancaman non militer yang merebak pada era *Post Truth* yaitu ancaman *misinformasi* dan *disinformasi*. Ancaman ini muncul sebagai dampak dari lahirnya revolusi industri 4.0 dan masyarakat 5.0, yang ditandai dengan kondisi mudah bergejolak (*volatility*). Hal tersebut berpontensi menimbulkan konfilk horizontal antar masyarakat yang berbeda latar belakang, politik, ekonomi, sosial maupun budaya,[71] dengan dipicu oleh penyebaran konten negatif.

Dalam rangka mengatasi ancaman kejahatan pada dunia siber pada tataran regional, Kemenkominfo telah meningkatkan kerja sama tingkat regional meliputi kerja sama kawasan ASEAN dan Asia Pasifik. Bentuk kegiatan berupa pertemuan, seminar dan peningkatan kapasitas, misalnya ASEAN SOMRI *Working Group Meeting on Information, Media and Training*. Salah satu agenda pertemuan tersebut membahas upaya kampanye literasi digital pada penduduk usia lebih muda, mengingat penetrasi internet pada kalangan tersebut sangat berisiko terhadap berbagai konten negatif, seperti *online-dating*, *online purchasing* dan *online gaming*, pertukaran data pribadi, kekerasan, penipuan dan *cyberbullying*.[72]

Kerja sama lintas negara, baik antar pemerintah maupun dengan pengembang aplikasi media digital, berpotensi memberikan dampak positif terhadap upaya pemerintah dalam menanggulangi ancaman konten negatif pada dunia siber. Hal ini dipengaruhi oleh faktor infrastruktur jaringan internet yang terkoneksi diantara berbagai negara di kawasan, baik regional maupun global, sehingga membutuhkan kerja

---

[70] AS: China Bangun Kekuatan Militer untuk Kuasai Taiwan,---------- "https://www.cnnindonesia.com/internasional/20220511160742-113-795571/as-china-bangun-------kuatan-militer-untuk-kuasai-taiwanunculkan-ancaman-nonmiliter," (akses 27 Juni 2022).

[71] Asni Ovier, Lingkungan Strategis Global yang Kian Dinamis Munculkan Ancaman Nonmiliter, "https://www.beritasatu.com/archive/740891/lingkungan-strategis-global-yang-kian-dinamis----------unculkan-ancaman-nonmiliter," (akses 27 Juni 2022).

[72] Pratiwi Agustini, Kerja Sama Regional, "https://aptika.kominfo.go.id/2020/02/kerja-sama-regional/," (akses 27 Juni 2022).

sama lintas negara untuk mengatasi ancaman siber pada dunia maya, termasuk ancaman penyebaran konten negatif.

Untuk itu, pemerintah perlu melaksanakan berbagai kerja sama, baik dengan aktor negara dan organisasi internasional dalam rangka mengatasi penyebaran konten negatif melalui teknologi media berbasis digital. Kerja sama tersebut dapat berupa *sharing knowledge* dalam rangka meningkatkan kualitas sumber daya manusia maupun bantuan teknologi yang dapat digunakan untuk melaksanakan tindakan pengawasan dan penyensoran terhadap konten negatif. Selain itu, juga diperlukan kerja sama yang baik dengan berbagai berbagai pihak terutama perusahan pengelola situs maupun pengembang platform media sosial yang berada di luar negeri. Kerja sama tersebut akan memudahkan upaya pemerintah, terkait kebijakan penyensoran, pengawasan maupun pemblokiran terhadap media digital asing yang memfasilitasi penyebaran konten negatif.

c. Lingkungan Nasional.

Penyelenggaraan pertukaran informasi menggunakan sarana komunikasi, selain mensyaratkan faktor kecepatan dan ketepatan, juga memperhatikan faktor keamanan. Berbagai sistem informasi dan komunikasi yang digunakan telah diperlengkapi dengan teknologi keamanan sebagai bentuk perlindungan sistem maupun informasi. Teknologi VPN merupakan salah satu teknologi yang dikembangkan untuk melindungi pertukaran informasi menggunakan jaringan internet.

Penggunaan teknologi VPN untuk mengakses jaringan internet bertujuan untuk menyediakan jalur khusus pertukaran data dengan cara enkripsi, sehingga menyulitkan pihak lain untuk memantau proses pertukaran informasi menggunakan jaringan internet, baik privat maupun publik. Keunggulan teknologi VPN telah menjadikan VPN sebagai pilihan utama dalam rangka meningkatkan keamanan pertukaran informasi menggunakan media digita, situs internet maupun media sosial.

Terkait penggunaan teknologi VPN, Indonesia merupakan negara yang menempati urutan ketiga dalam jumlah pengunduhan VPN,

mengalahkan China dan India pada tahun 2019, dan diawal tahun 2022, Indonesia menjadi negara teratas penggunaan VPN.[73] Namun demikian, penggunaan VPN, selain dimanfaatkan untuk melindungi informasi, juga telah dimanfaatkan untuk mengakses maupun menyebarkan informasi negatif melalui media digital. Penggunaan teknologi VPN dengan mengenkripsi data telah menyulitkan proses pengawasan terhadap informasi negatif yang diakses dan disebarkan melalui situs internet maupun media sosial. Selain itu, penggunaan teknologi VPN juga dapat dimanfaatkan untuk mengakses situs internet bermuatan negatif yang telah diblokir oleh Kemenkominfo, seperti situs ponografi, perjudian online maupun konten negatif lainnya.

Pada sisi lain, ketersediaan teknologi VPN yang sangat banyak dan ditawarkan secara gratis pada berbagai aplikasi, seperti *play store*, telah semakin memudahkan penggunaan teknologi tersebut. Oleh karena itu, hal ini dapat berdampak negatif terhadap upaya pemerintah dalam mengatasi ancaman penyebaran konten bermuatan negatif seperti pornografi dan judi online, maupun konten negatif lainnya.[74]

Dalam rangka mengatasi permasalahan penggunaan teknologi VPN terhadap penyebaran konten negatif, beberapa negara telah menerapkan aturan yang secara tegas melarang penggunaan teknologi tersebut, seperti China, Turki maupun rusia dan beberapa negara lainnya.[75] Kebijakan tersebut dapat dijadikan rujukan pemerintah dalam mengatasi peningkatan penggunaan teknologi VPN di Indonesia yang terus mengalami peningkatan. Untuk itu, diperlukan kerangka regulasi berupa ketentuan peraturan perundangan maupun peraturan menteri yang mengatur penggunaan teknologi VPN.

---

[73] Galuh Putri Riyanto, "Riset: Indonesia Pengguna VPN Terbesar Ketiga di Dunia," https://tekno.kompas.com/read/2022/05/11/11000087/riset--indonesia-pengguna-vpn-terbesar-ketiga-di-dunia?page=all (akses 23 Juni 2022).

[74] Ikhwan Hastanto, "Menkominfo Menyerah, Tak Sanggup Sensor Konten Pornografi Diakses Lewat VPN," https://www.vice.com/id/article/pkp9ev/menkominfo-johnny-g-plate-akui-negara-tak----------sanggup-cegah-konten-pornografi-diakses-lewat-vpn (akses 23 Juni 2022).

[75] Ibid., Marisa Dika Andini.

Kerangka regulasi tersebut diperlukan sebagai kontrol terhadap penggunaan teknologi VPN, serta sebagai landasan hukum bagi aparat penegak hukum untuk menindak individu maupun organsasi yang menggunakan teknologi VPN yang tidak sesuai dengan standar yang ditentukan. Hal ini dapat mengurangi, mengontrol maupun mencegah penggunaan teknologi VPN, baik yang berbayar maupun yang tidak atau gratis, untuk menyebarkan konten negatif melalui media digital atau bahkan mengakses sistus internet maupun media sosial yang telah diblokir Kemenkominfo.

BAB III
PEMBAHASAN

12. Umum.

Perkembangan teknologi informasi dan komunikasi, terutama yang berkaitan dengan internet maupun media sosial, selain telah berdampak positif terhadap proses pertukaran informasi, juga telah dimanfaatkan untuk menyebarkan berbagai konten negatif, sehingga berpotensi mengancam sendi-sendi kehidupan bermasyarakat, berbangsa dan bernegara. Oleh karena itu, diperlukan kebijakan dan strategi dalam rangka pangamanan media digital, agar dapat mewujudkan ruang digital yang aman, bersih dan bersahabat.

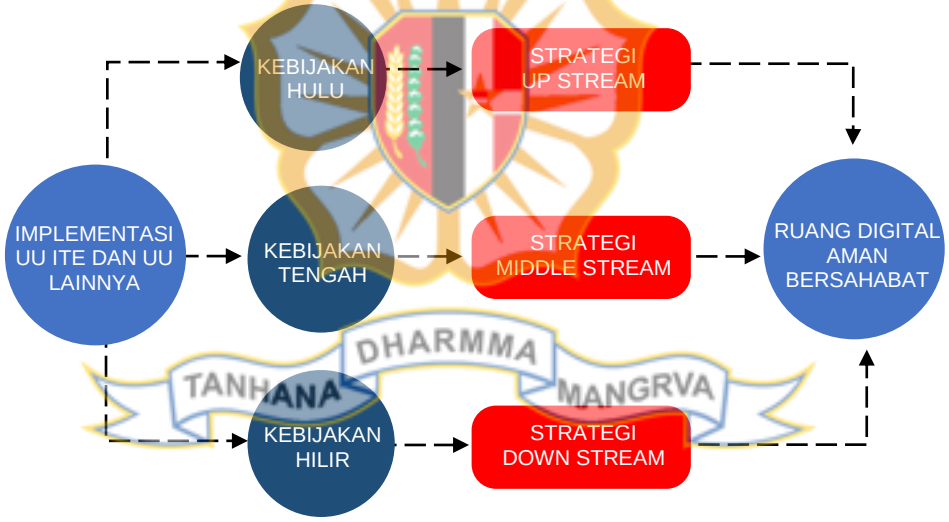
Pengamanan media digital telah diimplementasi oleh berbagai negara sesuai dengan sistem nilai dan politik yang mendasari dan membentuk perilaku kehidupan sosial masyarakat. Oleh karena itu, terdapat perbedaan implementasi kebijakan yang diterapkan oleh berbagai negara dalam rangka mengatasi penyebaran informasi bermuatan konten negatif. Namun demikian, secara umum implementasi kebijakan pengamanan informasi digital yang diterapkan berbagai negara, dapat meliputi kebijakan pengontrolan sistem komunikasi dan penyensoran, seperti pengaturan terhadap penggunaan teknologi VPN yang dilaksanakan oleh China, Rusia dan beberapa negara lainnya. Kebijakan tersebut dimaksudkan agar sistem informasi dan komunikasi tidak dimanfaatkan untuk memfasilitasi penyebaran konten negatif.

Selain itu, pendekatan pengamanan media digital terhadap konten negatif juga dilakukan melalui literasi media digital. Kebijakan tersebut telah diimplementasikan Finlandia dengan mengikutsertakan pendidikan literasi media pada kurikulum pendidikan dasar. Implementasi literasi media yang dilaksanakan sejak dini telah menjadikan Finlandia sebagai negara yang memiliki ketahanan yang baik terhadap penyebaran informasi hoaks, dibandingkan dengan negara-negara lain di kawasan Eropa. Oleh karena itu, untuk meningkatkan pengamanan media digital terhadap konten negatif, pemerintah Indonesia perlu menerapkan kebijakan yang terkait dengan

pengontrolan sistem komunikasi, pemblokiran maupun implementasi kegiatan literasi media digital sejak dini.

13. Implementasi Pengamanan Informasi Digital Terhadap Konten Negatif Saat Ini.

Perkembangan teknologi media informasi digital, seperti internet maupun media sosial, selain memberikan kemudahan dalam berkomunikasi, juga telah dimanfaatkan untuk mengakses dan menyebarkan berbagai informasi konten negatif yang dapat mengancam sendi-sendi kehidupan bermasyarakat, berbangsa dan bernegara. Untuk mengatasi permasalahan tersebut, pemerintah telah mengupayakan pendekatan preventif maupun represif, yang diimplementasikan melalui berbagai kebijakan dan strategi pengamanan media digital terhadap penyebaran berbagai konten negatif.



Gambar I. Kebijakan dan Strategi Pengamanan Informasi Digital
Sumber : Diolah dari berbagai sumber

Secara umum pelaksanaan pengamanan informasi digital terhadap konten bermuatan negatif yang telah dilaksanakan saat ini terdiri dari berbagai kebijakan dan strategi, seperti yang ditunjukkan pada Gambar I. Kebijakan dan Strategi Pengamanan Informasi Digital. Secara prinsip, pengamanan yang telah dilaksanakan saat ini memiliki kesamaan dengan metode praktek pengamanan yang dilakukan diberbagai negara, terkait pengontrolan sistem informasi dan komunikasi, penyensoran maupun literasi digital.

Kebijakan hulu mengacu pada pendekatan *preventif*, yang difokuskan pada tindakan pencegahan. Sementara kebijakan tengah dan hilir berfokus pada pendekatan *represif* berupa pengawasan, pemblokiran maupun penegakan hukum, dalam rangka penyelesaian penyebaran konten bermuatan negatif, baik melalui situs internet maupun media sosial. Hal tersebut bertujuan untuk mewujudkan ruang digital yang aman, nyaman, bersih, positif dan produktif dalam rangka mendukung pembangunan nasional.

a. Regulasi Pengamanan Informasi Digital Saat Ini.

Pengamanan informasi digital terhadap konten negatif dilaksanakan berdasarkan beberapa ketentuan peraturan perundang-undangan yang telah ditetapkan. Berbagai regulasi tersebut, telah mengatur perihal yang diperlukan dalam rangka mendukung penyelenggaran pengamanan konten bermuatan negatif pada sistem komunikasi berbasis teknologi internet. Hal-hal yang diatur dalam ketentuan perundangan, adalah sebagai berikut :

1) Pencegahan terhadap penyebaran konten bermuatan negatif.
2) Penegakan hukum terhadap penyebaran konten bermuatan negatif.[76]
3). Tata cara penanganan konten bermuatan negatif pada sistem komunikasi berbasis teknologi internet, baik situs internet maupun media sosial.
4) Pelibatan seluruh penyelenggara komunikasi untuk terlibat secara langsung dalam pengamanan informasi digital terhadap penyebaran konten negatif, baik pemerintah sebagai regulator, Penyelenggara Sistem Elekronik (PSE), *Internet Service Provider* (ISP) atau Penyelenggara Jasa Akses maupun masyarakat umum sebagai pengguna teknologi internet dan media sosial.

[76] Bab X, Pasal 42- 44, UU No. 19 Tahun 2016 tentang Perubahan Atas UU Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.

b. Institusi/Kelembagaan dan Kewenangan Pengamanan Informasi Digital Saat Ini.

Berdasarkan kerangka regulasi yang ada, terdapat beberapa institusi baik pemerintah maupun swasta yang terlibat secara langsung maupun tidak langsung dalam pelaksanaan pengamanan informasi digital terhadap konten bermuatan negatif, sebagai berikut :

1) Kementerian Komunikasi dan Informatika (Kemenkominfo)

Kemenkominfo merupakan lembaga negara yang berperan sebagai regulator yang mengatur penyelenggaraan komunikasi dan informasi, melaksanakan tindakan pencegahan, pengawasan maupun pemblokiran situs internet dan media sosial yang menyebarkan konten bermuatan negatif. Selain itu, Kemenkominfo juga berperan sebagai Penyidik Pegawai Negeri Sipil (PPNS) yang berwenangan melaksanakan penyidikan dan penindakan tindak pidana di bidang teknologi informasi dan transaksi elektronik.

2) Kepolisian RI

Kepolisian RI sebagai institusi negara berperan sesuai dengan kewenangan di bidang penegakan hukum, sebagai penyidikan tindak pidana di bidang teknologi informasi dan transaksi elektronik sesuai ketentuan peraturan perundang - undangan.[77]

3) Lembaga Pemerintah lainnya

Dalam penanganan terhadap konten negatif, kementerian atau lembaga pemerintah lainnya berperan untuk melaporkan berbagai konten negatif sesuai kewenangannya kepada Kemenkominfo.[78]

4) Penyelenggara Jasa Akses Internet

Penyelenggara Jasa Akses Internet yang merupakan bagian dari Penyelenggaraan Sistem Elektronik,[79] memiliki

[77] Pasal 13, UU No. 2 Tahun 2002 tentang Kepolisian Negara Republik Indonesia
[78] Pasal 5 ayat (2), Peraturan Menteri Komunikasi dan Informatika Nomor 19 Tahun 2014 tentang Penanganan Situs Internet Bermuatan Negatif.
[79] Pasal 1 ayat (6), UU No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.

kewenangan untuk melaksanakan pembokiran terhadap situs internet maupun media sosial yang bermuatan konten negatif.[80]

5) Masyarakat Umum

Masyarakat memiliki kewenangan untuk melaporkan situs internet maupun media sosial yang memuat informasi negatif kepada kementerian atau lembaga pemerintah terkait.[81]

c. Metode Pengamanan Informasi Digital Saat Ini.

Penyelenggaraan pengamanan informasi digital terhadap konten bermuatan negatif yang telah dilaksanakan sesuai dengan kebijakan dan strategi yang telah diimplementasikan. Pada tataran kebijakan dan strategi pengamanan informasi digital dilaksanakan dengan metode literasi digital. Sementara pada tataran kebijakan dan strategi tengah dan hilir, pengamanan informasi digital dilaksanakan dengan metode pengawasan, pemblokiran maupun penegakan hukum.

1) Literasi Digital.

Implementasi kegiatan literasi digital telah dilaksanakan Kementerian Pendidikan, Kebudayaan, Riset, dan Teknologi (Kemendikbudristek) pada jenjang pendidikan dasar di seluruh wilayah nasional.[82] Selain itu, Kemenkominfo, melalui Gerakan Nasional Literasi Digital (GNLD)/ Siberkreasi, juga telah melaksanakan kegiatan literasi digital melalui pendidikan non formal, seperti kursus, seminar maupun kegiatan lainnya.[83] Menurut data Kemenkominfo, pada tahun 2020, terdapat sekitar 205.000 orang yang telah mendapatkan pendidikan literasi digital. Jumlah tersebut

---

[80] Pasal 8 ayat (1), Peraturan Menteri Komunikasi dan Informatika Nomor 19 Tahun 2014 tentang Penanganan Situs Internet Bermuatan Negatif.
[81] Pasal 5 ayat (4), Peraturan Menteri Komunikasi dan Informatika Nomor 19 Tahun 2014 tentang Penanganan Situs Internet Bermuatan Negatif.
[82] Kemendikbudristek, Modul Literasi Digital Di Sekolah Dasar, 2021.
[83] Kementerian Kominfo, *Literasi Digital : Satu Data Untuk Percepatan Transformasi Digital*, 2020, hal. 12.

sangat kecil, jika dibandingkan dengan total penduduk Indonesia. Oleh karena itu, Kemenkominfo telah menyusun metode percepatan pelaksanaan literasi digital, sehingga dapat menjangkau sekitar 50 juta warga Indonesia pada 2024, atau sekitar 12 juta orang pertahun agar target tersebut dapat tercapai.[84]

Menurut peneliti *Center For Digital Society* (CFDS) UGM, Dewa Ayu Diah, tingkat literasi yang rendah dipengaruhi oleh kondisi yang disebut kesenjangan digital, yang didefinisikan sebagai kesenjangan antara individu, rumah tangga, bisnis, dan area geografis pada level sosial-ekonomi yang berbeda berkaitan dengan peluang dalam mengakses Teknologi Informasi dan Komunikasi (TIK) dan penggunaannya untuk berbagai kegiatan.[85] Sementara menurut Kemendikbudristek, faktor utama yang merupakan kendala pelaksanaan literasi digital di jenjang pendidikan dasar berkaitan dengan kendala akses jaringan internet maupun ketersediaan sarana pendukung, seperti laptop, komputer maupun sarana pendukung lainnya.[86] Kendala tersebut juga diakui Terkait hal tersebut, menurut laporan Kemenkominfo, terdapat sekitar 9.113 daerah yang tidak terjangkau jaringan 4G, dan 3.435 daerah non 3T yang juga tidak tercover jaringan 4G. Jika ditotal, ada sekitar 12.548 daerah *blankspot* di Indonesia.[87]

---

[84] Pratiwi Agustini, "Kominfo Targetkan 50 Juta Masyarakat Terliterasi Digital di 2024," https://aptika.kominfo.go.id/2020/10/kominfo-targetkan-50-juta-masyarakat-terliterasi-digital-di-2024/ (akses 16 Juni 2022).

[85] Leski Rizkinaswara, "Urgensi Literasi Digital bagi Masa Depan Ruang Digital Indonesia,"---------- https://aptika.kominfo.go.id/2020/06/urgensi-literasi-digital-bagi-masa-depan-ruang-digital---------- indonesia/ (akses 19 Juni 2022).

[86] Ibid., Kemendikbudristek, hal 7-10.

[87] "Kominfo Ungkap Masalah Internet di Indonesia,"---------- https://www.cnnindonesia.com/teknologi/20201215131630-213-582359/kominfo-ungkap-masalah--internet-di-indonesia (akses 18 Juni 2022).

2) Pengawasan dan Pemblokiran.

Kondisi saat ini tindakan pengawasan maupun pemblokiran dilaksanakan dengan memanfaatkan berbagai sarana dan prasarana yang dimiliki. Kemenkominfo (Direktorat Jenderal Aplikasi Informatika/ Ditjen Aptika) dan Kepolisian RI (Direktorat Tindak Pidana Siber Bareskrim Polri) mengandalkan peralatan yang memiliki keunggulan teknologi untuk mengawasi dan menganalisis konten bermuatan negatif yang tersebar pada situs internet maupun media sosial. Misalnya, Ditjen Aptika mengandalkan Perangkat Pengendali Proaktif (Mesin AIS) untuk melakukan tindakan pengawasan.[88]

Selain itu, juga mengandalkan sistem Trust+Positif yang digunakan sebagai rujukan bagi ISP maupun PSE untuk melaksanakan tindakan pemblokiran terhadap konten negatif yang termuat pada situs internet maupun media sosial.[89] Berdasarkan data Kemenkominfo, terdapat sekitar 2,679,352 berbagai konten negatif pada media digital, situs internet maupun media sosial, yang telah diblokir selama periode 2018-2021, sebagaimana Tabel III. Pemblokiran Konten Negatif Periode 2018-2021.[90]

Untuk meningkatkan pelaksanaan pengamanan, Kemenkominfo dan Kepolisian RI, telah menjalin kerja sama dengan berbagai institusi pemerintah lainnya dalam rangka pengawasan terhadap penyebaran konten negatif sesuai dengan tugas pokok. Misalnya, Kemenkominfo bekerja sama dengan BPPOM terkait konten negatif kesehatan, BNPT jika berkaitan dengan radikalisme dan dengan lembaga lainnya

---

[88] Ditjen Aptika, mengandalkan Perangkat Pengendali Proaktif (Mesin AIS) untuk melakukan tindakan pengawasan. Kementerian Kominfo, *Laporan Tahunan 2020 : Indonesia Terkoneksi, Semakin Digital, Semakin Maju*, hal. 36.

[89] "Trust+Positif,"https://www.kominfo.go.id/index.php/content/detail/3322/TRUSTPOSITIF/0/e_-----business (akses 20 Juni 2022).

[90] Lampiran II. Daftar Tabel

sesuai dengan tugas pokok.[91] Selain itu, juga melibatkan masyarakat, sebagai pengguna teknologi media digital, untuk mengawasi konten bermuatan negatif yang tersebar pada situs internet dan media sosial. Penemuan terhadap konten bermuatan negatif dapat dilaporkan kepada Kemenkominfo maupun Polri melalui berbagai aplikasi yang telah disediakan, seperti https://aduankonten.id/.[92]

Pada sisi lain, upaya pemblokiran situs maupun media sosial bermuatan konten negatif belum secara optimal dapat dilaksanakan. Hal ini dipengaruhi oleh penggunaan teknologi *Virtual Private Network* (VPN), sehingga menyebabkan Kemenkominfo mengalami kesulitan untuk memblokir berbagai situs yang bermuatan ponografi,[93] maupun perjudian online.[94] Selain itu, penggunaan teknologi VPN juga dapat dimanfaatkan untuk mengakses situs internet maupun media sosial yang telah diblokir Kemenkominfo.[95] Keberadaan teknologi VPN, menurut Marisa Dika Andini dkk, menunjukkan bahwa upaya pemblokiran konten bermuatan negatif merupakan suatu tindakan yang sia-sia.

c) Penegakan Hukum.

Implementasi kebijakan hilir berupa penegakan hukum dilaksanakan oleh Kemenkominfo (PPNS) dan Kepolisian RI, yang bertujuan memberikan efek jera pada pelaku pelanggaran hukum, sehingga diharapkan dapat mencegah penyebaran konten bermuatan negatif. Namun demikian,

---

[91] Kemal Faruq, "Atasi Konten Negatif, Kemenkominfo Gandeng 16 Pihak Terkait----------," https://ivoox.id/atasi-konten-negatif-Kemenkominfo-gandeng-16-pihak-terkait?tag_from=konten----------negatif (akses 20 Juni 2022).

[92] https://aduankonten.id/ (akses 20 Juni 2022).

[93] Hestin Untari, "Berantas Situs Porno, Kominfo: Penggunaan VPN Tidak Bisa Dikendalikan," https://techno.okezone.com/read/2020/02/04/207/2163057/berantas-situs-porno-kominfo-penggunaan-vpn-tidak-bisa-dikendalikan (akses 23 Juni 2022).

[94] "Menkominfo Akui Kewalahan Blokir Situs Judi Online,"---------- https://www.cnnindonesia.com/teknologi/20200311180408-185-482593/menkominfo-akui-kewalahan-blokir-situs-judi-online (akses 23 Juni 2022).

[95] Khulafa Pinta Winastya, "https://www.merdeka.com/trending/fungsi-vpn-di-android-simak-kegunaan-risiko-dan-cara-memasangnya-kln.html (akses 20 Juni 2022).

upaya penegakan hukum saat ini belum dapat dilaksanakan secara optimal. Hal ini dikarenakan sampai saat ini belum ada aturan hukum yang mengatur perihal penggunaan teknologi VPN, sehingga menyulitkan Kepolisian RI terkait upaya penegakan hukum.[96] Terkait hal tersebut, Kementerian Kominfo dan Asosiasi Penyelenggara Internet Indonesia (APJII) sedang mempertimbangkan penyusunan regulasi yang bersifat teknis terkait penggunan teknologi VPN yang harus memiliki izin di Indonesia.[97]

Upaya penegakan hukum terhadap konten negatif juga dipengaruhi oleh adanya pasal-pasal UU ITE yang dianggap kontroversi, sehingga mengakibatkan berbagai permasalahan,[98] seperti yang ditunjukan pada Tabel IV. Pasal Kontroversi dan Dampak Negatif UU ITE.[99] Kondisi yang demikian mendorong berbagai pihak mengusulkan agar dilaksanakan revisi atau perubahan terhadap pasal-pasal yang multitafsir dan kontroversi tersebut.[100] Selain dianggap kontroversi, menurut pengamat hukum pidana, Teuku Nasrullah, yang mewakili pandangan banyak pihak, menyatakan bahwa UU ITE sering digunakan sebagai alat untuk memukul lawan-lawan politik yang tidak sesuai, searah, sejalan dengan rezim yang berkuasa. Hal ini dapat digunakan oleh rezim penguasa selanjutnya.[101]

Dalam hal penegakan hukum, UU ITE telah mengakibatkan dampak negatif berupa keresahan dan

---

[96] Marisa Dika Andini, Ibid., hal. 159-160.
[97] Ibid.
[98] Yosephus Mainake dan Luthvi Febryka Nola, " Dampak Pasal-Pasal Multitafsir Dalam Undang-Undang Tentang Informasi Dan Transaksi Elektronik," *Kajian Singkat Terhadap Isu Aktual Dan Strategis*, Vol. XII, No. 16 (Agustus, 2020), hal. 1-4.
[99] Lampiran II. Daftar Tabel
[100] Leski Rizkinaswara, "Menkopolhukam: Presiden Menyetujui Adanya Revisi UU ITE," https://aptika.kominfo.go.id/2021/06/menkopolhukam-presiden-menyetujui-adanya-revisi-uu-ite/ (akses 25 Juni 2022).
[101] Aditya Budiman, "Pengamat Nilai UU ITE Jadi Alat Memukul Lawaan Politik," https://nasional.tempo.co/read/1404739/pengamat-nilai-uu-ite-jadi-alat-memukul-lawan-politik------- (akses 25 Juni 2022).

perselisihan warga masyarakat sehingga dengan mudah melaporkan kepada penegak hukum, sehingga menambah sumber konflik antara penguasa dan anggota masyarakat. Berbagai pihak telah mengusulkan penerapan prinsip keadilan restoratif dalam penyelesaian tindak pidana UU ITE terhadap tindakan pelanggaran hukum yang tidak termasuk kategori mengandung unsur SARA, kebencian terhadap golongan atau agama maupun diskriminasi ras dan etnis, serta penyebaran berita bohong yang menimbulkan keonaran.[102]

d. Analisa Terhadap Pengamanan Informasi Digital Saat Ini.

1) Analisa regulasi pengamanan informasi digital saat ini.

Menurut L. Sommeriad, pengelolaan komunikasi merupakan bagian dari kebijakan publik, yang berkaitan dengan tata cara komunikasi, jaringan yang digunakan untuk berkomunikasi, struktur sistem media komunikasi, kerangka regulasi untuk sistem tersebut, dan keputusan orang yang mengoperasikan sistem komunikasi. Sementara menurut UNESCO, kebijakan komunikasi merupakan kumpulan prinsip-prinsip dan norma-norma yang sengaja dibuat untuk mengatur perilaku sistem komunikasi. Terkait dengan pengamanan informasi digital, kebijakan komunikasi merupakan pengelolaan komunikasi yang diharapkan agar perilaku sistem komunikasi tidak memfasilitasi penyebaran konten bermuatan negatif.

Untuk memastikan sistem sesuai dengan perilaku yang dikehendaki, regulasi yang ada saat ini telah mensyaratkan bahwa setiap Penyelenggara Sistem Elektronik (PSE) wajib untuk tidak memuat maupun tidak memfasilitasi penyebarluasan informasi yang bermuatan konten negatif. Untuk itu, setiap PSE wajib

[102] Humas USN, "Banyak Warganet Dijerat UU ITE, Rektor UNS: Keadilan Restoratif Perlu dalam Regulasi Digital," https://uns.ac.id/id/uns-update/banyak-warganet-dijerat-uu-ite-rektor-uns----------keadilan-restoratif-perlu-dalam-regulasi-digital.html (akses 25 Juni 2022).

mendaftarkan ke Kemenkominfo untuk diverifikasi agar memperoleh ijin beroperasional di wilayah yurisdiksi nasional, baik PSE dalam negeri maupun asing. Selain itu, pengawasan terhadap informasi negatif dilakukan oleh seluruh penyelenggara, baik institusi pemerintah, ISP, PSE maupun masyarakat sebagai pengguna sistem. Oleh karena itu, regulasi yang ada saat ini seharusnya dapat secara holistik mengatur pengamanan terhadap informasi digital. Namun demikian, terdapat kekurangan pada aspek regulasi yang mengakibatkan pengamanan informasi digital saat ini belum terllaksana secara optimal, yaitu :

(a) Pasal-pasal yang multitafsir dalam UU ITE.

Keberadaan pasal-pasal dalam UU ITE yang dianggap multitafsir telah mengakibatkan berbagai dampak negatif seperti ketidakpastian hukum, kesewenang-wenangan para penegak hukum, memicu keresahan dan perselisihan warga masyarakat maupun berbagai permasalahan lainnya, seperti ditunjukkan pada Tabel 2.2 Pasal Multitafsir dan Dampak Negatif UU ITE.

(b) Ketiadaan regulasi yang mengatur penggunaan teknologi VPN.

Ketiadaan pengaturan perihal penggunaan teknologi VPN telah mengakibatkan kesulitan dalam upaya pengawasan, pemblokiran maupun penegakan hukum pengamanan informasi digital terhadap konten negatif.

2) Analisa institusi/kelembagaan dan kewenangan pengamanan informasi digital saat ini.

Menurut L. Sommeriad, kebijakan komunikasi merupakan kebijakan pengelolaan komunikasi yang tidak hanya terkait pengaturan sistem komunikasi yang digunakan, tetapi juga harus mencakup pengaturan perihal penyelenggara komunikasi untuk memastikan prilaku sistem

yang tidak dapat digunakan sebagai sarana penyebaran konten negatif. Secara umum, Kemenkominfo berperan sangat dominan pada setiap tataran kebijakan dan strategi pengamanan, baik tataran hulu, tengah maupun hilir. Sementara Kepolisian RI memiliki peran sesuai tugas pokok yang terkait dengan penegakan hukum pada tataran kebijakan hilir.

Selain itu, pada tataran kebijakan dan strategi tengah terkait metode pengamanan dalam bidang pengawasan dilakukan dengan melibatkan semua pihak penyelenggara, termasuk masyarakat umum. Namun demikian, belum terdapat institusi yang berwenangan untuk menentukan spesifikasi teknis terkait penggunaan teknologi VPN yang dapat dioperasionalkan di wilayah yurisdiksi nasional. Hal ini diperlukan agar dapat mencegah penggunaan teknologi VPN untuk mengakses maupun menyebarkan informasi konten negatif.

3) Analisa metode pengamanan informasi digital saat ini.

(a) Literasi Digital.

Upaya pengamanan informasi digital adalah salah satu bentuk peperangan informasi dalam rangka perlindungan sistem maupun informasi. Untuk itu diperlukan pendekatan budaya agar dapat mencegah penyebaran informasi negatif. Literasi digital yang telah dilaksanakan Kemendikbudristek dan Kemenkominfo, berdasarkan pada data-data penelitian, belum dapat dilaksanakan secara maksimal. Hal tersebut dipengaruhi oleh faktor kesenjangan digital terkait kesenjangan infrastruktur jaringan internet diantara daerah pulau Jawa dan luar P. Jawa, perkotaan dan pedesaan, maupun di daerah terdepan, terluar dan tertinggal. Selain itu, kesenjangan ekonomi dalam bentuk kemiskinan, juga berpengaruh terhadap

kemampuan daya beli berbagai peralatan teknologi, misalnya *smartphone* maupun kuota untuk mengakses situs maupun *platform* media sosial.

(b) Pengawasan dan Pemblokiran.

Pemanfaatan teknologi, dalam konteks peperang informasi, merupakan salah satu upaya perlindungan terhadap sistem, sehingga dapat mencegah penyebaran informasi yang tidak dikehendaki. Pemanfaatan teknologi diperlukan untuk memonitor berbagai informasi yang disebarkan melalui media informasi digital, seperti internet maupun media sosial. Namun demikian, kemampuan teknologi peralatan saat ini yang dimiliki Kemenkominfo dan Kepolisian RI belum dapat mengatasi penyebaran konten negatif dengan menggunakan teknologi VPN.

(c) Penegakan Hukum.

Penegakan hukum melalui penerapan hukum pidana, menurut G. Peter Hoefnagels merupakan bagian dari "*criminal policy*" dalam rangka penanggulangan kejahatan sebagai bentuk perlindungan untuk mencapai kesejahteraan masyarakat. Namun demikian, pengamanan informasi digital melalui metode penegakan hukum terhadap tindak pidana UU ITE, telah mengakibatkan berbagai permasalahan seperti yang ditunjukan pada Tabel IV. Pasal Kontroversi dan Dampak Negatif UU ITE.[103] Hal tersebut menunjukkan bahwa metode penegakan hukum dalam pengamanan informasi digital saat ini belum dapat memenuhi aspek perlindungan, berupa kepastian dan kesetaraan hukum, maupun kesejahteraan masyarakat.

[103] Lampiran II. Daftar Tabel

14. Kondisi Yang Diharapkan Dalam Pengamanan Informasi Digital Terhadap Konten Negatif.

a. Regulasi Pengamanan Informasi Digital Yang Diharapkan.

Berdasarkan pada kondisi regulasi saat ini seperti yang dijelaskan di atas, maka kondisi yang diharapkan dari aspek regulasi dalam rangka meningkatkan pengamanan penyebaran informasi digital terhadap konten negatif, yaitu :

1) Pengaturan norma pasal-pasal UU ITE yang jelas dan tidak ambigu atau multitafsir.

Kerangka regulasi berupa aturan merupakan bagian penting dalam penerapan hukum pidana, membutuhkan aturan hukum yang jelas dan tidak ambigu terhadap kriteria suatu tindak pidana melalui sistem komunikasi. Untuk itu, diperlukan pengaturan yang jelas terkait konten negatif, terutama hoaks, pencemaran nama baik, penghinaan maupun ujaran kebencian, yang dibedakan dengan informasi kritik. Hal ini diperlukan mengingat sebagai negara demokrasi, nilai kebebasan berbicara (*freedom of speech*), termasuk penyampaian kritik, merupakan nilai yang diakui dan dihormati dalam sistem negara demokrasi.

Oleh karena itu, pengaturan yang jelas, selain mempermudah penegakan hukum, juga melindungi hak masyarakat dalam menyampaikan kritik terhadap penyelenggara negara. Hal ini agar berbagai penyampaian kritik terhadap pihak tertentu, yang merupakan hal yang umum dalam sistem demokrasi, dapat dipidanakan karena dianggap telah mencermarkan nama baik pihak tertentu.

2) Regulasi yang mengatur penggunaan teknologi VPN.

Pengelolaan sistem komunikasi sebagai suatu kebijakan komunikasi memerlukan regulasi yang mengatur perihal penggunaan teknologi sistem komunikasi yang sesuai dengan prinsip maupun norma berkomunikasi. Untuk itu, diperlukan kerangka regulasi berupa ketentuan perundangan

yang mengatur perihal penggunaan teknologi VPN. Hal tersebut diperlukan dalam rangka meningkatkan pelaksanaan pengawasan, pemblokiran dan penegakan hukum terhadap penyebaran informasi berupa konten negatif melalui sistem komunikasi, baik situs internet maupun media sosial.

b. Institusi/Kelembagaan dan Kewenangan Pengamanan Informasi Digital Yang Diharapkan.

Pengaturan sistem komunikasi bertujuan agar teknologi yang digunakan tidak dimanfaatkan untuk memfasilitasi penyebaran informasi yang bermuatan melanggar hukum. Berdasarkan kondisi saat ini, untuk mewujudkan kondisi yang diharapkan terkait dengan institusi dan kewenangan dalam pengamanan informasi digital terhadap konten negatif, diperlukan institusi maupun lembaga negara sebagai *leading sector* digital nasional yang berwenangan untuk menentukan dan mengatur penggunaan sistem elektronika yang dapat dioperasionalkan di wilayah yurisdiksi nasional. Hal diperlukan untuk mencegah berbagai penggunaan teknologi VPN, baik berbayar maupun gratis, untuk mengakses maupun menyebarkan informasi negatif melalui media informasi digital, baik situs internet maupun media sosial.

c. Metode Pengamanan Informasi Digital Yang Diharapkan.

Untuk meningkatkan pelaksanaan pengamanan informasi digital pada tataran kebijakan dan strategi pada tataran hulu, tengah dan hilir, makan metode pengamanan informasi digital yang diharapkan adalah sebagai berikut :

1) Literasi Digital.

Untuk meningkatkan pelaksanaan metode pengamanan melalui literasi digital diperlukan perbaikan terhadap jaringan infrastruktur jaringan internet, terutama di daerah yang memiliki keterbatasan akses jaringan internet, seperti luar P. Jawa, pedesaan maupun daerah 3T. Selain itu, juga diperlukan ketersedian perangkat teknologi pendukung,

seperti komputer maupun laptop, pada sekolah dasar dan menengah serta fasilitas sosial masyarakat yang tersebar di seluruh Indonesia. Pada sisi lain, untuk meningkatkan partisipasi kelompok masyarakat miskin dan kurang mampu dalam literasi digital diperlukan peningkatan askse internet dan sarana pendukung secara gratis pada lokasi-lokasi publik, baik di daerah perkotaan maupun pedesaan.

2) Pengawasan dan Pemblokiran.

Perkembangan teknologi komunikasi dan informasi yang semakin memudahkan distribusi informasi melalui media digital, baik dari segi kecepatan maupun volume, membutuhkan kemampuan peralatan pengawasan maupun pemblokiran yang memiliki teknologi canggih. Untuk itu, dalam rangka mewujudkan metode pengawasan dan pemblokiran yang diharapkan, agar Kemenkominfo dan Kepolisian RI, perlu diperlengkapi dengan peralatan teknologi pencari konten negatif berbasis (*Artificial Intelligence*), sehingga dapat mendeteksi informasi konten negatif dengan volume yang sangat banyak, dalam waktu yang relatif singkat, pada media digital.

Selain itu, teknologi yang digunakan memiliki kemampuan untuk mengidentifikasi dan menindak individu maupun kelompok yang menyebarkan berbagai konten negatif dengan menggunakan identitas palsu. Pada sisi lain, perangkat teknologi yang digunakan juga memiliki kemampuan untuk mendeteksi penggunaan teknologi VPN untuk mengakses situs internet maupun media sosial yang bermuatan konten negatif. Dengan demikian, teknologi VPN tidak lagi digunakan untuk mengakses berbagai situs internet maupun media sosial yang telah diblokir pemerintah.

Pada sisi lain, peran pengawasan juga membutuhkan partisipasi masyarakat sebagai sarana langsung dalam upaya pengawasan konten negatif. Sebagai unsur pengguna media

informasi digital, baik situs internet maupun media sosial, masyarakat dapat secara langsung memantau berbagai informasi yang terdapat pada media informasi digital tersebut, dan dapat melaporkan kepada pihak yang berwenang.

3) Penegakan Hukum.

Penegakan hukum terkait UU ITE, telah berdampak pada perselisihan warga masyarakat yang dengan mudah melaporkan kepada penegak hukum, sehingga menambah sumber konflik antara anggota masyarakat, maupun warga negara dengan pejabat publik. Oleh karena itu, untuk mewujudkan pelaksanaan penegakan hukum yang meminimalkan fenomena konflik, diperlukan metode penegakan hukum berdasarkan prinsip keadilan restoratif. Penerapan prinsip keadilan restoratif dapat diterapkan terutama terhadap tindak pidana UU ITE yang tidak termasuk kategori mengandung unsur SARA, kebencian terhadap golongan atau agama maupun diskriminasi ras dan etnis, serta penyebaran berita bohong yang menimbulkan keonaran.

Selain itu, dibutuhkan peran lembaga pengawas institusi penegak hukum, untuk mengawasi proses penegakan hukum terhadap tindak pidana penyebaran konten negatif pada media digital. Hal ini diperlukan agar penegakan hukum dapat berlangsung sesuai prinsip keadilan, kesetaraan maupun kepastian hukum, dan tetap menjunjung nilai-nilai demokrasi.

d. Analisa Terhadap Pengamanan Informasi Digital Yang Diharapkan.

1) Analisa regulasi pengamanan informasi digital yang diharapkan.

Kebijakan komunikasi, menurut L. Sommeriad, merupakan pengelolaan komunikasi yang salah satu aspek pengelolaan mencakup pengaturan sistem komunikasi yang digunakan, agar perilaku sistem sesuai yang dikehendaki.

Untuk itu, pengaturan teknologi VPN merupakan bagian dari pengaturan sistem komunikasi agar teknologi VPN, baik berbayar maupun gratis, tidak dapat dimanfaatkan untuk mengakses dan menyebarkan informasi negatif melalui media sosial maupun situs internet. Selain itu, revisi terhadap UU ITE diperlukan untuk mewujudkan penegakan hukum yang berkeadilan, kesetaraan, kepastian hukum maupun menjunjung nilai-nilai demokrasi.

2) Analisa institusi dan kewenangan pengamanan informasi digital yang diharapkan.

Kebijakan komunikasi, menurut L. Sommeriad, merupakan pengelolaan komunikasi yang mencakup pengaturan sistem komunikasi agar sistem yang digunakan, tidak dimanfaatkan untuk menyebarkan konten negatif. Dengan adanya institusi sebagai *leading sector* digital nasional yang mengatur penggunaan teknologi internet yang dapat beroperasional di wilayah nasional, dapat mencegah penyebaran teknologi VPN yang illegal, baik yang gratis maupun berbayar. Selain itu, akan memudahkan upaya pengawasan maupun penegakan hukum terhadap penggunaan teknologi VPN yang illegal yang digunakan individu maupun kelompok masyarkat.

3) Analisa metode pengamanan informasi digital yang diharapkan.

(a) Literasi Digital.

Peningkatan infrastruktur jaringan internet maupun saran pendukung akan berdampak terhadap pelaksanaan literasi digital secara nasional, baik pendidikan formal maupun non formal. Hal tersebut juga dapat mewujudkan target pencapaian 50 juta penduduk yang telah terliterasi digital pada tahun 2024. Dengan demikian pendekatan literasi digital untuk menumbuhkan dan meningkatkan budaya penggunaan

media digital yang bijak dan bertanggung jawab dapat terealisasi dalam kehidupan bermasyarakat, berbangsa dan bernegara.

(b) Pengawasan dan Pemblokiran.

Peningkatan kemampuan teknologi pencarian konten negatif dapat meningkatkan perlindungan terhadap sistem informasi dan komunikasi terhadap penyebaran konten negatif. Hal ini sangat dibutuhkan dalam penyelenggaraan peperangan informasi, yang menekankan perlindungan terhadap sistem merupakan hal mutlak yang harus dilakukan. Selain itu, peningkatan partisipasi masyarakat, yang merupakan penggunaan media digital, baik internet maupun media sosial, dapat membantu pemerintah dalam tindakan pengawasan terhadap konten bermuatan negatif yang disebarkan melalui media digital.

(c) Penegakan Hukum.

Revisi terhadap pasal-pasal UU ITE, penggunaan metode prinsip keadilan restributif maupun pengawasan terhadap proses penegakan hukum, akan berdampak terhadap proses penegakan hukum yang sesuai dengan prinsip keadilan, kesetaraan, kepastian hukum maupun nilai-nilai demokrasi dan Hal Asasi Manusia (HAM). Hal tersebut dapat secara signifikan meningkatkan kepercayaan publik terhadap upaya pengamanan informasi digital terhadap konten negatif, yang diimplementasikan pemerintah melalui penegakan hukum. Dengan demikian, kebijakan penanggulangan konten negatif melalui metode penegakan hukum dapat mewujudkan tujuan "*criminal policy*" seperti yang disampaikan G. Peter Hoefnagels, sebagai bentuk perlindungan untuk mencapai kesejahteraan masyarakat dapat terwujud.

15. Konsepsi Pengamanan Informasi Digital Terhadap Konten Negatif Guna Mewujudkan Ketahanan Nasional.

Untuk mewujudkan konsepsi pengamanan informasi digital dalam rangka meningkatkan pengamanan informasi terhadap konten negatif pada media digital, baik aspek regulasi, institusi dan kewenangan serta metode pengamanan, diperlukan langkah pemecahan masalah. Secara umum, langkah pemecahan masalah ditunjukan pada Tabel V. Pemecahan Masalah.[104]

a. Kebijakan.

Kebijakan merupakan rangkaian konsep yang dijadikan pedoman atau rujukan dalam penyusunan suatu strategi. Berdasarkan pada landasan teori, kondisi lingkungan strategis dan kondisi saat ini implementasi pengamanan informasi digital terhadap konten bermuatan negatif, maka kebijakan yang dirumuskan adalah sebagai berikut :

"Terwujudnya pengamanan informasi digital terhadap konten negatif melalui norma pasal-pasal UU ITE yang tidak kontroversi, optimalisasi literasi digital, pengaturan penggunaan teknologi internet serta VPN, penguatan kelembagaan yang berwenang mengatur teknologi komunikasi yang digunakan, serta peningkatan infrastruktur jaringan internet dan perangkat pendukung guna mewujudkan ketahanan nasional."

b. Strategi.

Penyusunan strategi pada tulisan ini menggunakan metode analisis SWOT yang mensyaratkan analisis terhadap faktor eksternal dan internal. Faktor internal berkaitan dengan kekuatan

[104] Lampiran II. Daftar Tabel

(*strength*) dan kelemahan (*weakness*), sementara faktor eksternal berkaitan dengan peluang (*opportunity*) dan ancaman (*threat*).

1) Analisis faktor internal

a) Kekuatan.

(1) Pelibatan penyelenggara komunikasi.

Menurut L. Sommeriad, kebijakan komunikasi mensyaratkan pengaturan terhadap penyelenggara komunikasi yang bertanggung jawab terhadap operasional komunikasi, termasuk aspek keamanan. Untuk itu, pelibatan semua pihak penyelenggara komunikasi dalam pengamanan informasi merupakan upaya holistik yang diperlukan untuk menjamin kemanan dalam berkomunikasi.

(2) Regulasi komunikasi dan informasi.

Kebijakan komunikasi, menurut L. Sommeriad, terkait dengan regulasi sistem komunikasi dan informasi dalam rangka memastikan bahwa sistem yang digunakan tidak memfasilitasi penyebaran informasi yang bermuatan melanggar ketentuan perundang-undangan.

(3) *Self control* individu.

Peningkatan *self control* melalui literasi digital ditujukan untuk meningkatkan kemampuan kognitif individu agar memiliki kemampaun untuk menilai, menyaring dan memanfaatkan penggunaan teknologi informasi digital secara bijak dan bertanggungjawab.

b) Kelemahan.

(1) Pasal multitafsir UU ITE.

Kebijakan penerapan hukum pidana dalam mengatasi konten negatif pada media informasi digital, belum secara optimal dapat dilaksanakan. Hal ini dipengaruhi oleh pasal-pasal UU ITE yang dianggap multitafsir, sehingga mengakibatkan ketidakpastian hukum, kesewenang-wenangan para penegak hukum, serta permasalahan lainnya.

(2) Kesenjangan digital.

(a) Kesenjangan infrastruktur jaringan internet.

Kondisi jaringan internet yang belum memadai terutama di daerah luar P. Jawa, pedesaan maupun daerah 3T. Hal ini menyulitkan pelaksanaan literasi digital yang diakibatkan kendala keterbatasan akses terhadap jaringan internet di daerah-daerah tersebut.

(b) Kesenjangan sosial ekonomi.

Kesenjangan sosial ekonomi dalam bentuk kemiskinan, juga mempengaruhi kemampuan kelompok masyaratkat miskin untuk memperoleh perangkat teknologi, seperti komputer, *smartphone* dan kuota internet, yang merupakan sarana utama dalam mendukung kegiatan literasi digital.

(3) Ketiadaan regulasi penggunaan teknologi VPN.

Ketiadaan regulasi terkait penggunaa teknologi VPN, telah mengakibatkan penggunaan teknologi tersebut, baik yang berbayar maupun gratis, untuk mengakses

situs internet maupun media sosial yang diblokir pemerintah. Selain itu, hal tersebut juga telah berdampak negatif terhadap upaya penegakan hukum dikarenakan tidak terdapat dasar hukum yang mengatur penggunaan teknologi VPN yang dapat dioperasionalkan di wilayah yurisdiksi nasional.

(4) Belum terdapat institusi yang mengatur aspek teknis sistem komunikasi.

Menurut L. Sommeriad, pengelolaan komunikasi mencakup pengaturan sistem komunikasi yang digunakan. Pengaturan sistem komunikasi bertujuan agar teknologi yang digunakan tidak dimanfaatkan untuk memfasilitasi penyebaran informasi yang bermuatan melanggar hukum.

2) Analisis faktoe eksternal.

a) Peluang.

(1) Tingkat penggunaan internet yang tinggi.

Indonesia, secara umum, merupakan negara dengan tingkat penetrasi internet tinggi dibandingkan dengan negara berkembangan lainnya. Selain itu, partisipasi masyarakat cukup tinggi dalam menggunakan media informasi digital, internet maupun media sosial, untuk mendukung kebutuhan informasi.

(2) Sistem pendidikan nasional.

Sistem pendidikan nasional yang diselenggarakan secara terstruktur dan berkelanjutan, pendidikan dasar, menengah dan lanjutan, serta tersebar di seluruh

wilayah nasional, merupakan peluang yang dapat dimanfaatkan untuk literasi digital secara terstruktur dan berkelanjutan

(3) Kerja sama lintas negara.

Perkembangan teknologi informasi dan komunikasi telah melahirkan bentuk ancaman pada dunia siber. Ancaman siber merupakan ancaman lintas negara sehingga memerlukan kerja sama antar negara untuk mengatasi ancaman siber, termasuk ancaman penyebaran konten bermuatan negatif melalui dunia siber.

b) Ancaman.

(1) Penggunaan teknologi VPN yang terus meningkat.

Saat ini, berdasarkan data penelitian menunjukkan Indonesia merupakan salah satu negara dengan tingkat penggunaan teknologi VPN yang tinggi. Hal tersebut merupakan ancaman terhadap upaya pengamanan informasi digital terhadap konten bermuatan negatif.

(2) Fenomena *Post Truth.*

Penyebaran informasi dalam jumlah besar dan cepat, dapat menyulitkan individu maupun masyarakat dalam menilai keakuratan informasi. Hal ini dipengaruhi keterbasan pengetahuan maupun waktu, sehingga sebuah informasi sudah diyakini kebenarannya sebelum dikonfirmasi sesuai dengan kondisi emosi dan keyakinan personal. Hal ini dapat berdampak terhadap penyebaran informasi negatif yang dapat

mempengaruhi opini publik untuk tujuan propaganda, terutama informasi propaganda yang bermuatan SARA.

(3) Karakteristik sistem komunikasi.

Sistem komunikasi, terutama komunikasi berbasis internet bersifat sangat kompleks, dalam pengertian bahwa infrastruktur jaringan internet menghubungkan berbagai negara dengan sisitem nilai, kondisi sosial dan politik yang berbeda, sehingga dapat menghambat maupun menyulitkan berbagai upaya penanggulangan berbagai konten negatif.

Untuk menentukan strategi berdasarkan analisis SWOT, akan dilaksanakan perhitungan *Internal Strategic factor Analysis Summary* (IFAS) yang memperhitungkan faktor-faktor internal dan *External Strategic factor Analysis Summary* (EFAS) yang memperhitungkan faktor-faktor eksternal. Hasil perhitungan IFAS ditunjukkan pada Tabel VI. IFAS Analisis SWOT dan Tabel VII. EFAS Analisis SWOT.

Tabel VI. IFAS Analisis SWOT

	FAKTOR INTERNAL	BOBOT	RATING	SKOR
KEKUATAN				
1.	Pelibatan seluruh penyelenggara komunikasi	0.15	5	0.75
2.	Regulasi sistem komunikasi dan informasi	0.15	5	0.75
3.	*Self control* individu	0.15	3	0.45
Jumlah Faktor Kekuatan		**0.45**		**1.95**
KELEMAHAN				
1.	Pasal multitafsir UU ITE	0.10	1	0.10
2.	Kesenjangan digital	0.15	2	0.30
3.	Ketiadaan regulasi terkait teknologi VPN	0.15	1	0.15
4.	Belum terdapat institusi yang mengatur aspek teknis sistem komunikasi	0.15	1	0.15
Jumlah Faktor Kelemahan		**0.55**		**0.70**
Jumlah Keseluruhan		**1.00**	**Selisih**	**1.25**

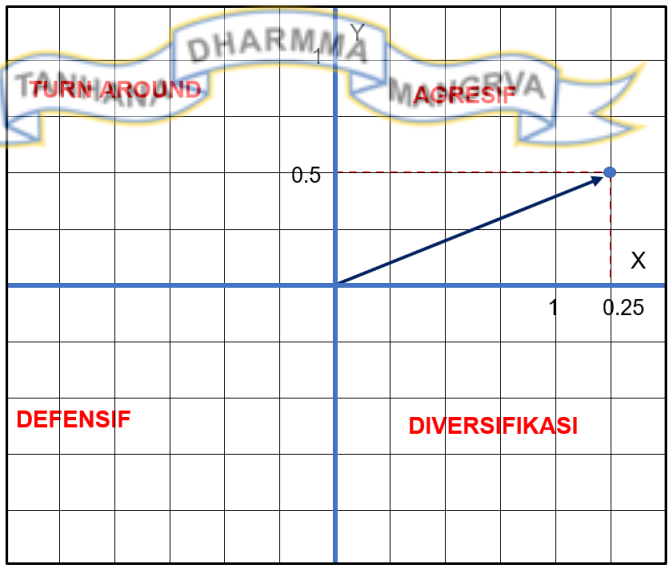
Sumber : Hasil Pengolahan Data Penulis

Tabel VII. EFAS Analisis SWOT

FAKTOR EKSTERNAL		BOBOT	RATING	SKOR
PELUANG				
1.	Tingkat penggunaan internet yang tinggi	0.21	2	0.43
2.	Sistem pendidikan nasional	0.21	2	0.43
3.	Kerja sama lintas negara	0.14	2	0.29
Jumlah Faktor Peluang		**0.57**		**1.14**
ANCAMAN				
1.	Penggunaan teknologi VPN yang terus meningkat	0.21	1	0.21
2.	Fenomena Post Truth	0.07	2	0.14
3.	Karakteristik sistem komunikasi	0.14	2	0.29
Jumlah Faktor Ancaman		**0.43**		**0.64**
Jumlah Keseluruhan		**1.00**	**Selisih**	**0.50**

Sumber : Hasil Pengolahan Data Penulis

Berdasarkan pada selisih nilai faktor internal dan faktor eksternal, seperti pada yang ditunjukkan pada Tabel VIII. Nilai Faktor Internal dan Eksternal,[105] maka hasil selisih kedua faktor tersebut dapat dituangkan pada kuadran SWOT dengan posisi sumbu (X,Y). Posisi sumbu X adalah nilai selisih faktor internal, dan sumbu Y adalah nilai selisih faktor eksternal. Untuk itu, posisi pada kuadran SWOT, yaitu (1.25,0.50), seperti ditunjukan pada Gambar II. Kuadran SWOT.



Gambar II. Kuadran SWOT.
Sumber : Hasil Pengolahan Data Penulis

[105] Lampiran II. Daftar Tabel

Berdasarkan hasil analisis SWOT pada gambar 3.2 Kuadran SWOT, kuadran terpilih adalah kuadran ke-1, sehingga strategi yang sesuai yaitu *Comparative Advantage*, merupakan strategi agresif yang menggunakan kemampuan atau kekuatan untuk memanfaatkan peluang yang ada. Sementara untuk menentukan strategi yang tepat atau strategi terpilih dilakukan dengan cara memperhitungkan setiap kombinasi *Strengt* (S)-*Opportunity* (O), seperti yang ditunjukkan pada Tabel IX. Penentu Strategi.[106]

Berdasarkan Tabel IX. Penentu Strategi, dapat dirumuskan beberapa strategi, yaitu sebagai berikut :

1) **Strategi I** : Meningkatkan *self control* individu melalui literasi digital dengan memanfaatkan tingkat penggunaan internet yang tinggi dan sistem pendidikan nasional yang melibatkan seluruh penyelenggara komunikasi guna mendukung tindakan pencegahan terhadap penyebaran informasi bermuatan konten negatif.
2) **Strategi II** : Menyusun regulasi sistem komunikasi dan informasi untuk memfasilitasi penggunaan internet yang tinggi dalam rangka pengamanan informasi digital terhadap penyebaran konten yang bermuatan melanggar ketentuan perundang-undangan.
3) **Strategi III** : Meningkatkan kerja sama lintas negara untuk mengatasi penyebaran konten negatif yang memanfaatkan teknologi sistem komunikasi dan informasi.

c. Upaya.

Untuk mewujudkan strategi-strategi yang telah ditetapkan, maka diperlukan upaya-upaya untuk mendukung pelaksanaan strategi tersebut, antara lain:

1) **Upaya Strategi I** : Meningkatkan *self control* individu melalui literasi digital dengan memanfaatkan tingkat penggunaan internet yang tinggi dan sistem pendidikan nasional yang melibatkan seluruh penyelenggara komunikasi guna mendukung tindakan pencegahan terhadap penyebaran informasi bermuatan konten negatif. Upaya-

[106] Lampiran II. Daftar Tabel

upaya yang dapat dilakukan untuk mewujudkan strategi I, antara lain adalah :

(a) Kemendikbudristek membuat peraturan menteri tentang pelaksanaan literasi digital pada kurikulum pendidikan nasional tingkat dasar dan menengah agar tingkat literasi digital nasional terstandarisasi.

(b) Pemerintah Daerah membuat peraturan daerah tentang alokasi dana pendidikan terkait penyiapan sarana dan prasarana yang dibutuhkan dalam penyelenggaraan literasi digital di daerah.

(c) Kemenkominfo menyusun peraturan tentang penghargaan yang diberikan kepada masyarakat dalam rangka meningkatkan partisipasi aktif masyarakat terkait pengawasan terhadap informasi bermuatan konten negatif.

(d) Kemendikbudristek bersama dengan Kemenkominfo untuk menyiapkan tenaga pendidik yang berkualitas melalui pelatihan dan materi literasi digital dalam rangka mendukung literasi digital sesuai jenjang pendidikan.

(e) Kemenkominfo dan Kemendikbudristek melaksanakan literasi digital sesuai empat (4) pilar kurikulum literasi digital, baik melalui pendidikan formal dan non formal dalam rangka meningkatkan kemampuan digital guna mewujudkan budaya digital serta masyarakat digital.

(f) Kemenkominfo untuk mengingkatkan penyelenggaran kegiatan literasi digital secara non formal melalui seminar, kursus, seminar, webinar maupun kegiatan lainnya dengan peserta yang berasal dari luar P. Jawa.

(g) Kemenkominfo dan Badan Perencanaan Pembangunan Nasional (Bappenas) segera menindak lanjuti rencana percepatan pembangunan infastruktur jaringan internet di daerah luar P. Jawa, pedesaan maupun 3T.

(h) Kementerian Keuangan dan DPR mengalokasikan anggaran pembangungan infrastruktur jaringan internet di daerah luar P. Jawa, pedesaan maupun 3T.

(i) Pemerintah daerah menyiapkan sarana dan prasarana teknologi pendukung di sekolah dasar maupun menengah, seperti komputer, laptop, gawai dan perangkat pendukung lainnya.

(j) Penyedia Jasa Internet menyediakan akses internet secara gratis di daerah perkotaan dan pedesaan maupun 3T agar memudahkan kelompok masyarakat miskin dan kurang mampu mendapatkan layanan internet.

(k) Penyedia Jasa Internet agar membantu pemerintah dalam pembangunan jaringan infrastruktur internet di daerah pedesaan maupun 3T dalam rangka percepatan pemerataan akses terhadap jaringan internet.

2) **Upaya Strategi II** : Menyusun regulasi sistem komunikasi dan informasi untuk memfasilitasi penggunaan internet yang tinggi dalam rangka pengamanan informasi digital terhadap penyebaran konten yang bermuatan melanggar ketentuan perundang-undangan. Upaya-upaya yang dapat dilakukan untuk mewujudkan strategi II, antara lain adalah :

(a) Kemenkominfo membuat peraturan menteri tentang standarisasi penggunaan teknologi sistem komunikasi dan informasi berbasis teknologi internet yang dapat dioperasionalkan di wilayah yurisdiksi nasional.

(b) Kemenkominfo, Badan Siber dan Sandi Negara (BSSN), Kepolisian RI, Kementerian Pertahanan (Kemhan) dan bersama APJII, menyusun standarisasi teknologi sistem komunikasi dan informasi berbasis teknologi internet yang dapat dioperasionalkan di wilayah yurisdiksi nasional.

(c) Pemerintah menetapkan Kemenkominfo sebagai *leading sector* digital nasional selanjutnya menunjuk BSSN sebagai institusi yang melaksanakan sertifikasi teknis terhadap peralatan teknologi komunikasi dan informasi yang dapat dioperasionalkan di wilayah yurisdiksi nasional.

(d) Badan Riset dan Inovasi Nasional (BRIN) agar membantu Kemenkominfo dengan melaksanakan riset terhadap berbagai teknologi komunikasi dan informasi yang secara aman dapat digunakan di wilayah yurisdiksi nasional.

(e) Kemenkominfo, Kementerian Hukum dan Hak Asasi Manusia (Kemenkumham) dan Dewan Perwakilan Rakyat (DPR), agar melaksanakan revisi terhadap pasal-pasal UU ITE yang dinilai multitafsir, ambigu, bertentangan dengan nilai demokrasi, dengan melibatkan universitas maupun perwakilan lembaga masyarakat.

(f) Kementerian Hukum dan Hak Asasi Manusia (Kemenkumham) dan Dewan Perwakilan Rakyat (DPR) agar menyusun ketentuan peraturan perundangan terkait penerapan prinsip keadilan restoratif dalam penyelesaian tindak pidana UU ITE.

(g) Kemenkominfo dan Kepolisian RI melaksanakan pengadaan peralatan deteksi teknologi berbasis *artificial intelligence (AI)* untuk meningkatkan kemampuan pengawasan informasi yang tersebar pada media informasi digital.

(h) Kementerian Keuangan dan DPR mengalokasikan anggaran pengadaan pembelian peralatan peralatan deteksi teknologi berbasis IA dalam rangka mendukung tugas pengawasan Kemenkominfo dan Kepolisian RI.

(i) Kepolisian RI agar menerapakan prinsip keadilan restoratif terhadap pelanggaran tindak pidana UU ITE yang sesuai dengan ketentuan peraturan perundangan yang berlaku.

(j) Komisi Kepolisian Nasional (Kompolnas) dan Komisi Nasional Hak Asasi (Komnas HAM) untuk mengawasi pelaksanaan penegakan hukum tindak pidana pelanggaran UU ITE dalam rangka mewujudkan kepastian hukum dan penegakan Hak Asasi Manusia (HAM)

3) **Upaya Strategi III** : Meningkatkan kerja sama lintas negara untuk mengatasi penyebaran konten negatif yang memanfaatkan teknologi sistem komunikasi dan informasi. Upaya-upaya yang dapat dilakukan untuk mewujudkan strategi III, antara lain adalah :

(a) Kementerian Luar Negeri (Kemenlu) dan Kemenkominfo menjalin kerja sama dengan berbagai negara, baik tingkat regional maupun global, dalam rangka mencegah penyebaran konten bermuatan negatif melalui sistem komunikasi dan informasi digital.

(b) Kementerian Luar Negeri (Kemenlu) dan Kemenkominfo melaksanakan sosialisasi terkait upaya Pemerintah Indonesia untuk mengatasi penyebaran konten negatif pada forum kerja sama global (PBB), kerja sama regional (ASEAN) maupun kerja sama antar negara.

(c) Kemenkominfo menjalin kerja sama melalui *Memorandum of Understanding* (MoU) dengan pengembang berbagai situs maupun platform media sosial di luar negeri, seperti seperti Youtube, Whatsapp, Facebook maupun aplikasi lainnya, untuk tidak memuat informasi konten bermuatan negatif yang dapat diakses atau dibuat oleh pengguna internet di Indonesia.

(d) Kemenkominfo menjalin kerja sama melalui *Memorandum of Understanding* (MoU) dengan berbagai negara terkait ekstradisi terhadap pelaku pelanggaran UU ITE yang berada di luar negeri, baik individu maupun organisasi, untuk diadili berdasarkan ketentuan peraturan perundangan yang berlaku.

(e) Kemenkominfo menjalin kerja sama dengan Penyelenggara Sistem Elektronik (PSE) Privat Asing untuk memastikan bahwa seluruh PSE Privat Asing yang beroperasional di wilayah yurisdiksi nasional mematuhi segala peraturan perundangan-undangan yang berlaku.

(f) Kepolisian RI menjalin kerja sama dengan institusi kepolisian negara lain untuk meningkatkan penegakan hukum terkait kejahatan lintas negara yang terjadi di dunia siber, misalnya judi online, radikalisme, terorisme, pornografi maupun kejahatan lainnnya.

Apabila konsepsi pengamanan informasi digital seperti yang telah diuraikan diatas dapat terselenggara dengan baik, maka permasalahan yang terjadi pada upaya pengamanan informasi digital saat ini akan dapat diatasi. Dengan demikian kondisi media digital yang aman, nyaman dan penuh manfaat seperti yang diharapkan akan dapat tercapai sehingga akan menciptakan tatanan sosial budaya masyarakat digital yang positif serta mendukung terwujudnya ketahanan nasional.

BAB IV
PENUTUP

16. Simpulan.

Berdasarkan pembahasan yang telah dilakukan pada bab-bab sebelumnya, maka dapat diambil kesimpulan sebagai berikut :

Pertama, Pengamanan informasi digital terhadap konten negatif yang telah dilaksanakan saat ini, belum dapat dilaksanakan secara optimal. Hal ini dipengaruhi oleh kendala sarana infrasturktur jaringan internet dan perangkat teknologi pendukung, sehingga menyulitkan pelaksanaan literasi digital terutama di daerah luar Pulau Jawa, pedesaan serta daerah 3T. Selain itu, metode pengamanan, pengawasan dan pemblokiran terhadap informasi bermuatan konten negatif belum dapat dilaksanakan secara maksimal. Hal tersebut dikarenakan oleh kondisi sarana dan prasarana yang dimiliki Kemenkominfo maupun Kepolisian RI, berupa peralatan pencari belum memiliki kemampuan mengawasi maupun memblokir akses serta penyebaran konten negatif dengan menggunakan teknologi VPN.

Pada sisi lain, upaya penegakah hukum terkendala oleh keberadaan pasal-pasal kontroversi yang terdapat pada UU ITE, sehingga mengakibatkan ketidakpastian penegakan hukum. Disamping itu juga terkendala dengan belum adanya kerangka hukum yang mengatur penggunaan teknologi VPN, yang menyulitkan aparat penegak hukum dalam menindak penggunaan teknologi VPN yang sangat tinggi di Indonesia.

Kedua, Dalam rangka mewujudkan pengamanan informasi digital yang diharapkan, diperlukan regulasi perihal pengaturan teknologi komunikasi dan internet yang dapat dioperasionalkan di wilayah yurisdikasi nasional. Oleh kerena itu, diperlukan lembaga atau institusi pemerintah sebagai *leading sector* digital nasional yang dapat melaksanakan sertifikasi teknis terhadap setiap peralatan teknologi komunikasi yang dapat dipasarkan untuk digunakan masyarakat dalam mendukung kegiatan komunikasi dan informasi. Selain itu, diperlukan aturan yang jelas tentang informasi yang dapat dikategorikan sebagai konten yang melanggar aturan hukum, sehingga tidak mengakibatkan berbagai permasalahan dalam penegakan hukum, terutama terkait

informasi yang dapat dikategorikan sebagai hoaks, pencemaran nama baik, penghinaan maupun ujaran kebencian.

Sementara itu untuk mengoptimalkan pelaksanaan literasi digital dalam rangka membentuk budaya dan masyarakat digital yang positif, diperlukan sarana dan prasarana berupa infrastruktur jaringan internet serta perangkat teknologi pendukung seperti komputer maupun laptop dan gawai, terutama di daerah luar P. Jawa, pedesaan maupun 3T. Hal ini diperlukan agar kegiatan literasi digital dapat dilaksanakan secara terstruktur melalui sistem pendidikan nasional maupun pendidikan non formal. Selain itu, diperlukan peran aktif pemerintah pusat maupun daerah serta penyedia jasa layanan internet untuk menyediakan sarana dan prasarana secara gratis agar dapat membantu kelompok masyarakat miskin dan kurang mampu dalam memanfaatkan teknologi media digital sebagai sarana berinteraksi.

Ketiga, untuk melaksanakan pengamanan informasi digital terhadap konten negatif secara optimal guna mewujudkan ketahanan nasional maka diperlukan upaya-upaya nyata pada aspek regulasi, kebijakan, sarana dan prasarana pendukung literasi digital serta dengan meningkatkan kerjasama internasional. Pada aspek regulasi diperlukan revisi terhadap pasal UU ITE yang kontroversial serta diperlukan aturan tentang standarisasi sistem elektronika digital yang dapat beroperasi di Indonesia dan penetapan *leading sector* pemanfaatan teknologi digital nasional.. Pada aspek optimalisasi literasi digital diperlukan peningkatan sarpras pendukung dan jaringan internet yang dapat menjangkau seluruh wilayah nasional serta perlu memasukkan pelajaran literasi digital kedalam kurikulum sistem pendidikan nasional. Pada aspek kerja sama internasional dapat dilaksanakan dengan membuat perjanjian kerjasama antar negara dalam menangani kejahatan berbasis internet, sosialisasi kebijakan ITE nasional kepada dunia internasional serta perjanjian ekstradisi pelaku kejahatan siber antar negara. Selain itu, untuk meningkatkan tindakan pengawasan dan pemblokiran, perlu dilaksanakan pengadaan peralatan baru yang berbasis teknologi kecerdasan buatan *(artificial intelligence).*

17. Rekomendasi.

Berdasarkan pada uraian kesimpulan, dalam rangka mengimplementasikan meningkatkan pengamanan informasi digital terhadap konten negatif guna mewujudkan ketahanan nasional, disampaikan beberapa saran sebagai berikut :

a. Pemerintah dalam hal ini Kemenkominfo dan Kemenkumham bersama DPR, perlu melaksanakan revisi terhadap pasal-pasal UU ITE yang dinilai multitafsir, bertentangan dengan nilai demokrasi, maupun Hak Asasi Manusia (HAM).

b. Pemerintah agar menetapkan Kemenkominfo sebagai *leading sector* pemanfaatan teknologi digital nasional selanjutnya bersama dengan BSSN, Kepolisian RI, Kemhan dan APJII menyusun standarisasi penggunaan teknologi sistem komunikasi data, terutama teknologi VPN yang dapat beroperasi di wilayah yurisdiksi nasional.

c. Kemenkominfo, Bappenas, Pemda bersama APJII, perlu melaksanakan percepatan pembangunan infastruktur jaringan internet dan sarana pendukung di daerah luar P. Jawa, pedesaan maupun 3T, serta memfasilitasi akses internet secara gratis untuk mendukung kegiatan literasi digital.

d. Kemenkominfo bekerjasama dengan Kemendikbud mendorong agar mata pelajaran literasi digital dapat masuk kedalam kurikulum pendidikan nasional tingkat dasar dan menengah sehingga kemampuan literasi warga negara dapat terstandarisasi serta *self control* pemanfaatan teknologi informasi digital dapat terbentuk sedini mungkin.

DAFTAR PUSTAKA

Buku

Barda Nawawi. 2007. Masalah Penegakan Hukum dan Kebijakan Hukum Pidana Dalam Penanggulangan Kejahatan. Jakarta: Kencana.

Kurniawan, Hendra, dkk. 2019. Pembelajaran : Literasi Menuju Society 5.0. Yogyakarta : Deepublish Publisher.

Nadhya, Ana Abr, dkk. 2014. Demokrasi Bermedia Online. Yogyakarta : Tiara Wacana Lokus.

Patrikarakos, David. 2017. *War in 140 Characters : How Social Media Is Reshaping Conflict in the Twenty First Century*. New York : Basic Books.

Singer, P.W Singer, Emerson T. Brooking. 2018. LikeWar : *The Weaponization of Sosial Media*. Boston : Houghton Mifflin Harcourt Publishing Company.

Peraturan Perundang-undangan

Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan Atas Undang-Undang Nomor. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE).

Peraturan Pemerintah Republik Indonesia Nomor 71 Tahun 2019 tentang Penyelenggara Sistem dan Transaksi Elektronik (PP PSTE).

Peraturan Menteri Komunikasi dan Informatika Republik Indonesia Nomor 5 Tahun 2020 Tentang Penyelenggara Sistem Elektronik Lingkup Privat.

Peraturan Menteri Komunikasi dan Informatika Republik Indonesia Nomor. 19 Tahun 2014 tentang Penanganan Situs Internet Bermuatan Negatif.

Skirpsi

Tirta Raharja, *Strategi Penanggulangan Informasi Hoax Di Media Sosial Oleh Unit Cyber Crime Di Kota Makassar*, Skripsi Fakultas Ilmu Politik, Universitas Muhammadiyah Makassar, 2020.

Jurnal

Ahmad Rizky Mardhatillah Umar, dkk, Media Sosial dan Revolusi Politik: Memahami Kembali Fenomena "*Arab Spring*" dalam Perspektif Ruang Publik Transnasional, *Jurnal Ilmu Sosial dan Ilmu Politik,* Vol. 18 , No.2, (November, 2014).

Amilin, S.E, Pengaruh Hoaks Politik dalam Era Post-Truth terhadap Ketahanan Nasional dan Dampaknya pada Kelangsungan Pembangunan Nasional, *Jurnal Kajian Lemhannas RI,* Edisi. 39, (September, 2019).

Anang Sugeng Cahyono, Pengaruh Media Sosial Terhadap Perubahan Sosial Masyarakat di Indonesia", *Jurnal Publicana*, Vol. 9, No.1, (2016).

Artadi Ibnu, "Menggugat Efektivitas Penerapan Pidana Penjara Pendek Menuju Suatu Proses Peradilan Pidana Yang Humanis", *Jurnal Hukum Pro Justitia*, Vol. 24 , No. 4, (Oktober, 2006), hal.379.

Capera Brilian, "Keadilan Restoratif Sebagai Paradigma Pemidanaan di Indonesia", *Jurnal LEX Renaissan*, Vol. 2 , No. 2, (April, 2021).

Denico Doly, Penegakan Hukum Kampanye Hitam (*Black Campaign*) di Media Sosial: Pembelajaran Pemilihan Umum Presiden Tahun 2019, *Jurnal Kajian*, Vol. 2, No.1, (2020).

Fendy E. Wahyudi, "Teatrikal Makroekonomisme Globalisasi", *Jurnal Ilmu Sosial*, Vol.14, No.2, (November 2015).

Ghulam Shabir, dkk, Mass Media, Communication and Globalization with the Perspective of 21st Century", *New Media and Mass Communication*, Vol. 34, (2015).

Khosiah Fatma, Yuli Rohmiyati, "Kontrol Informasi Publik Terhadap Fake News dan Hate Speech Oleh Aliansi Jurnalis Independen", *Jurnal ANUVA*, Vol. 3 , No. 3, (2019).

Lauder Siagian, Peran Keamanan Siber Dalam Mengatasi Konten Negatif Guna Mewujudkan Ketahanan Informasi Nasional, Jurnal Prodi Perang Asimetris, Vol. 4, No.3 (Desember, 2018).

Marisa Dika Andini, dkk,"Penggunaan Aplikasi Virtual Private Network (VPN) Point To Point Tunneling Protocol (PPTP) Dalam Mengakses Situs Terblokir ," Supremasi Hukum: Jurnal Penelitian Hukum, Vol. 29, No. 2 (Agustus, 2020).

Yosephus Mainake dan Luthvi Febryka Nola, " Dampak Pasal-Pasal Multitafsir Dalam Undang-Undang Tentang Informasi Dan Transaksi Elektronik," Kajian Singkat Terhadap Isu Aktual Dan Strategis, Vol. XII, No. 16 (Agustus, 2020).

Publikasi Elektronik

Anthonius Malau, Strategi Penanganan Hoaks Oleh Kementerian Komunikasi dan Informatika RI, 14 Pebruari 2019.

Dudi Hartono, " Era Post-Truth : Melawan Hoax dengan Fact Checking," Prosiding Seminar Nasional Prodi Ilmu Pemerintahan 2018.

Kementerian Kominfo, Laporan Tahunan 2020 : Indonesia Terkoneksi, Semakin Digital, Semakin Maju.

Kementerian Kominfo, Literasi Digital : Satu Data Untuk Percepatan Transformasi Digital, 2020.

Mastel, Hasil Survei Wabah Hoax Tahun 2019.

Usman Kansong, "Pancasila dalam Pembangunan Karakter Manusia Digital Indonesia di Era Globalisasi," (Dalam Diskusi Panel PPRA LXIV Tahun 2022 Lemhannas RI, Jakarta, 17 Mei, 2022).

Sumber Internet

Aditya Budiman, "Pengamat Nilai UU ITE Jadi Alat Memukul Lawaan Politik," https://nasional.tempo.co/read/1404739/pengamat-nilai-uu-ite-jadi-alat---------memukul-lawan-politik, (akses 25 Juni 2022).

Andika Primasiwi, "Peningkatan Literasi Digital, Ini Kendala Struktural yang Dihadapi,"https://www.suaramerdeka.com/nasional/pr04161444/peningkatan literasi-digital-ini-kendala-struktural-yang-dihadapi (akses 18 Juni 2022).

AS: China Bangun Kekuatan Militer untuk Kuasai Taiwan, "https://www.cnnindonesia.com/internasional/20220511160742-113-china----bangun-kuatan-militer-untuk-kuasai-taiwanunculkan-ancaman-nonmiliter,"--- (akses 27 Juni 2022).

Asni Ovier, Lingkungan Strategis Global yang Kian Dinamis Munculkan Ancaman Nonmiliter, "https://www.beritasatu.com/archive/740891/lingkungan-strategis-global-yang-kian-dinamis-unculkan-ancaman-nonmiliter," (akses 27 Juni 2022).

Aryo Putranto Saptohutomo, "Restorative Justice : Pengertian dan Penerapannya Dalam Hukum di Indonesia," https://nasional.kompas.com/read/2022/02/15/12443411/restorative-justice---pengertian-dan-penerapannya-dalam-hukum-di-indonesia?page=all/, (akses 25 Juni 2022).

Carnagie Endowment For International Peace, "Anthony Giddens Discusses the Globalization Debate", https://carnegieendowment.org/2000/07/05/anthony-giddens-discusses-globalization-debate-pub-8655.

Countries with the highest number of internet users as of February 2022, https://www.statista.com/statistics/262966/number-of-internet-users-in---------selectedcountries/#professional.

Evaluating Information: Fake news in the 2016 US Elections, "https://libraryguides.vu.edu.au/evaluating_information_guide/fakenews2016, " (akses 25 Juni 2022).

Galuh Putri Riyanto, “Riset: Indonesia Pengguna VPN Terbesar Ketiga di Dunia,” https://tekno.kompas.com/read/2022/05/11/11000087/riset--indonesia----------pengguna-vpn-terbesar-ketiga-di-dunia?page=all, (akses 23 Juni 2022).

Hasil Survei Mastel Catat 92,40 Persen Hoaks Lewat Medsos, https://infojateng.id/read/13336/hasil-survei-mastel-catat-9240-persen-hoaks-lewat-medsos/

Hendro D Situmorang, “Penanganan Kasus Pelanggaran UU ITE, Polri Gunakan Pendekatan Restorative Justice,” https://www.beritasatu.com/archive/819505/penanganan-kasus-pelanggaran-uu-ite-polri-gunakan-pendekatan-restorative-justice/, (akses 25 Juni 2022).

Hestin Untari, “Berantas Situs Porno, Kominfo: Penggunaan VPN Tidak Bisa Dikendalikan,”https://techno.okezone.com/read/2020/02/04/207/2163057/berantas-situs-porno-kominfo-penggunaan-vpn-tidak-bisa-dikendalikan, (akses 23 Juni 2022).

Humas USN, “Banyak Warganet Dijerat UU ITE, Rektor UNS: Keadilan Restoratif Perlu dalam Regulasi Digital,” https://uns.ac.id/id/uns-update/banyak-warganet-dijerat-uu-ite-rektor-uns-keadilan-restoratif-perlu-dalam-regulasi----digital.html (akses 25 Juni 2022).

https://datareportal.com/reports/digital-2022-indonesia, (akses 20 Juni 2022).

https://aduankonten.id/, (akses 20 Juni 2022).

Iba Nurkasihani, “Restorative Justice, Alternatif Baru Dalam Sistem Pemidanaan,” https://www.jdih.tanahlautkab.go.id/artikel_hukum/detail/restorative-justice----alternatif-baru-dalam----sistem-pemidanaan/, (akses 25 Juni 2022).

Ikhwan Hastanto, “Menkominfo Menyerah, Tak Sanggup Sensor Konten Pornografi Diakses Lewat VPN,” https://www.vice.com/id/article/pkp9ev/menkominfo-johnny-g-plate-akui-negara-taksanggup-cegah-konten-pornografi-diakses-----lewat-vpn, (akses 23 Juni 2022).

Kemal Faruq, “Atasi Konten Negatif, Kemkominfo Gandeng 16 Pihak Terkait,” https://ivoox.id/atasi-konten-negatif-kemkominfo-gandeng-16-pihak----------terkait?tag_from=konten-negatif, (akses 20 Juni 2022).

Khulafa Pinta Winastya, “https://www.merdeka.com/trending/fungsi-vpn-di-android-simak-kegunaan-risiko-dan-cara-memasangnya-kln.html, (akses 20 Juni 2022).

“Kominfo Ungkap Masalah Internet di Indonesia,” https://www.cnnindonesia.com/teknologi/20201215131630-213----------582359/kominfo-ungkap-masalah--internet-di-indonesia, (akses 18 Juni 2022).

Leski Rizkinaswara, “Menkopolhukam: Presiden Menyetujui Adanya Revisi UU ITE,” https://aptika.kominfo.go.id/2021/06/menkopolhukam-presiden----------menyetujui-adanya-revisi-uu-ite/, (akses 25 Juni 2022).

Leski Rizkinaswara, “Urgensi Literasi Digital bagi Masa Depan Ruang Digital Indonesia,” https://aptika.kominfo.go.id/2020/06/urgensi-literasi-digital-bagi-masa-depan-ruang-digital-indonesia/, (akses 19 Juni 2022).

“Menkominfo Akui Kewalahan Blokir Situs Judi Online,” https://www.cnnindonesia.com/teknologi/20200311180408-185----------482593/menkominfo-akui-kewalahan-blokir-situs-judi-online, (akses 23 Juni 2022).

Pratiwi Agustini, Kerja Sama Regional, “https://aptika.kominfo.go.id/2020/02/kerja-sama-regional/,” (akses 27 Juni 2022).

“Trust+Positif,”https://www.kominfo.go.id/index.php/content/detail/3322/TRUSTPOSITIF/0/e_business, (akses 20 Juni 2022).

Yudo Dahono, *Data: Ini Media Sosial Paling Populer di Indonesia 2020-2021*, https://www.beritasatu.com/digital/733355/data-ini-media-sosial-paling-populer-di-indonesia 2020-2021

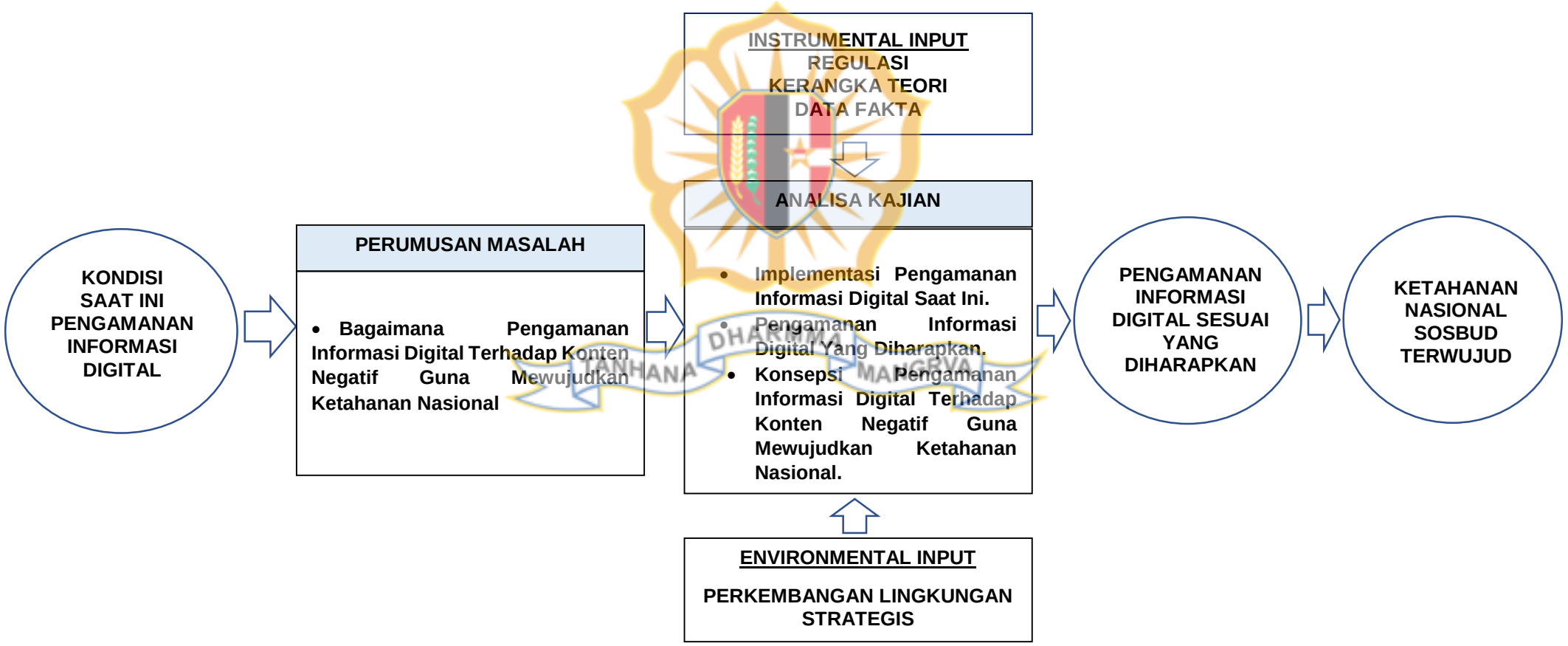
Yusuf, “Tiga Strategi Kominfo dalam Tangani Hoaks dan Misinformasi,” https://aptika.kominfo.go.id/2020/09/tiga-strategi-kominfo-dalam-tangani-------hoaks-dan-misinformasi/ (akses 16 Juni 2022).

LEMBAGA KETAHANAN NASIONAL
REPUBLIK INDONESIA

LAMPIRAN I

ALUR PIKIR

PENGAMANAN INFORMASI DIGITAL TERHADAP KONTEN NEGATIF GUNA MEWUJUDKAN KETAHANAN NASIONAL



LEMBAGA KETAHANAN NASIONAL
REPUBLIK INDONESIA

LAMPIRAN II

Tabel I. Klasifikasi Konten Negatif

NO	KONTEN NEGATF	KETERANGAN
1.	Informasi/dokumen elektronik yang melanggar Peraturan Perundang-Undangan	a) Pornografi/Pornografi Anak b) Perjudian c) Pemerasan d) Penipuan e) Kekerasan/Kekerasan Anak f) Fitnah/Pencemaran Nama Baik g) Pelanggaran Kekayaan Intelektual h) Produk dengan Aturan Khusus i) Provokasi SARA j) Berita Bohong k) Terorisme/Radikalisme l) Informasi/Dokumen Elektronik Melanggar UU
2.	Informasi/dokumen elektronik yang melanggar norma sosial yang berlaku di masyarkat	a) Informasi/dokumen elektronik yang meresahkan masyarakat b) Informasi/dokumen elektronik yang tidak sesuai dengan nilai-nilai kepantasan untuk ditampilkan di muka umum
3.	Informasi elektronik/dokumen elektronik tertentu yang membuat dapat diaksesnya konten negatif yang terblokir (web proxy, open proxy, open browser dan lainnya).	

Sumber : Kemkominfo : Ragam Konten Negatif

Tabel II. Media Sosial Bermuatan Konten Negatif

NO	MEDIA SOSIAL	KONTEN NEGATIF
1.	Twitter	568,843
2.	Facebook	11,470
3	Instagram	11,470
4.	WhatsApp	11,470
3.	Google	1,757
	YouTube	1,492
4.	File sharing	5,000
5.	Telegram	1,077
6.	Michat	165
7.	Tiktok	210
8.	Line	24

Sumber : Kemkominfo : Penanganan Konten Negatif

Tabel III. Pemblokiran Konten Negatif Periode 2018-2021

NO	KATEGORI KONTEN	JUMLAH PEMBLOKIRAN
1.	Pornografi	1,107,547
2.	Perjudian	423,453
3.	Penipuan	14,757
4.	Hak kekayaan intelektual (HKI)	7,660
5.	Konten negatif rekomendasi instansi	4,058
6.	Terorisme/radikalisme	509
7.	Pelanggaran keamanan informasi	325
8.	Suku, agama, ras, antargolongan (SARA)	188
9.	Perdagangan produk dengan aturan	128
10.	Pelanggaran nilai sosial dan budaya	26
11.	Berita bohong/hoaks	26
12.	Konten meresahkan masyarakat	23
13.	Separatisme/organisasi terlarang	14
14.	Fitnah	12
15.	Kekerasan pada anak	10
Total Pemblokiran Konten Negatif		**2,679,352**

Sumber : Kemkominfo : Penanganan Konten Negatif

Tabel IV. Pasal Kontroversi dan Dampak Negatif UU ITE

PASAL-PASAL KONTROVERSI	DAMPAK NEGATIF
1. Pasal 27 ayat (1) terkait kesusilaan. 2. Pasal 27 ayat (3) terkait penghinaan dan pencemaran nama baik. 3. Pasal 28 ayat (2) terkait ujaran kebencian dan SARA. 4. Pasal 29 terkait tindakan menakut-nakuti pada media elektronik.	1. Membatasi kebebasan berpendapat terutama dalam beropini dan memberikan kritik. 2. Menimbulkan kesewenang-wenangan dikarenakan para penegak hukum dalam menentukan orang yang tersandung UU ITE bersalah dan layak dipidanakan. 3. Menjadi instrumen sebagian sekelompok dalam rangka membalas dendam bahkan menjadi senjata untuk menjebak lawan politik. 4. Kurang menjamin kepastian hukum. Putusan terkait pasal-pasal multitafsir menjadi beragam dan bahkan bertolak belakang. 5. Memicu keresahan dan perselisihan warga masyarakat yang dengan mudah melaporkan kepada penegak hukum dan menambah sumber konflik antara penguasa dan anggota masyarakat. 6. Menyebabkan keresahan dan perselisihan warga masyarakat yang dengan mudah melaporkan kepada penegak hukum dan menambah

	sumber konflik antara penguasa dan anggota masyarakat.

Sumber : Yosephus Mainake dan Luthvi Febryka Nola, Dampak Pasal-Pasal Multitafsir dalam UU ITE, 2020

Tabel V. Pemecahan Masalah

1	ASPEK	PERMASALAHAN
1.	Regulasi	1. Pasal-pasal multitafsir dalam UU ITE 2. Ketiadaan ketentuan perundangan yang mengatur penggunaan teknologi penggunaan teknologi VPN.
2.	Institusi dan Kewenangan	1. Tidak terdapat institusi yang berwenang mengatur teknologi komunikasi yang digunakan.
3.	Metode Pengamanan	1. Kesenjangan digital, baik infrastruktur jaringan internet dan kesenjangan sosial ekonomi di daerah luar P. Jawa, pedesaan dan 3T.
PELUANG **KENDALA**		**ANALISIS SWOT** **FAKTOR INTERNAL DAN EKSTERNAL**
INDIKATOR KEBERHASILAN		**OPTIMALISASI ASPEK REGULASI, INTITUSI, SARANA DAN METODE PENGAMANAN**
		1. Norma pasal-pasal UU ITE yang jelas dan tidak ambigu atau multitafsir.
		2. Ketentuan perundangan perihal penggunaan teknologi VPN.
		3. Terdapat institusi yang berwenang untuk menentukan teknologi sistem komunikasi yang dapat dioperasilakan di wilayah NKRI.
		4. Ketersedian jaringan infrastruktur jaringan internet di daerah luar P. Jawa, pedesaan dan 3T.
		5. Ketersediaan fasilitas pendukung untuk kelompok sosial masyarakat yang kurang mampu atau miskin.

Sumber : Hasil Pengolahan Data Penulis

Tabel VIII. Nilai Faktor Internal dan Eksternal

FAKTOR INTERNAL (X)	NILAI	FAKTOR EKSTERNAL (Y)	NILAI
STRENGTH	1.95	OPPORTUNITY	1.14
WEAKNESS	0.70	THREAT	0.64
SELISIH	**1.25**	**SELISIH**	**0.50**

Sumber : Hasil Pengolahan Data Penulis

Tabel IX. Penentu Strategi.

KOMBINASI STRENGT (S)- OPPORTUNITY (O)	**OPPORTUNITY**
	1. Tingkat penggunaan internet yang tinggi
	2. Sistem pendidikan nasional
STRENGT	3. Kerja sama lintas negara
1. Pelibatan seluruh penyelenggara komunikasi	1. Meningkatkan self control individu dengan memanfaatkan tingkat penggunaan internet yang tinggi dan sistem pendidikan nasional yang melibatkan seluruh penyelenggara komunikasi guna mendukung tindakan pencegahan terhadap penyebaran informasi bermuatan konten negatif. 2. Menyusun regulasi sistem komunikasi dan informasi untuk memfasilitasi penggunaan internet yang tinggi dalam rangka pengamanan informasi digital terhadap penyebaran konten yang bermuatan melanggar ketentuan perundang-undangan. 3. Meningkatkan kerja sama lintas negara untuk mengatasi penyebaran konten negatif yang memanfaatkan sistem komunikasi dan informasi.
2. Regulasi sistem komunikasi dan informasi	
3. *Self control* individu	

Sumber : Hasil Pengolahan Data Penulis

ANALISA SWOT

1. Analisis SWOT

Analisa SWOT merupakan metode yang efektif untuk membantu proses pengambilan keputusan dalam mewujudkan visi dan misi organisasi, dengan mempertimbangkan faktor internal (Kekuatan dan Kelemahan) dan eksternal (Peluang dan Ancaman) yang mempengaruhi perkembangan organisasi. Menurut Billie Nordmeyer, keunggulan (*advantage*) penggunaan analisis SWOT diantaranya terkait dengan faktor kesederhanaan (*simplicity*) dan biaya (*cost*). Sementara kelemahan (*disadvantage*) analisis SWOT dipengaruhi oleh analisis yang bersifat subjektif (*subjective analysis*), atau sangat bergantung pada perspektif individu.[23] Analisis SWOT merumuskan 4 (empat) kelompok alternatif strategi yang disebut strategi SO, strategi ST, strategi WO, dan strategi WT, seperti ditunjukan pada Tabel 1. Matriks SWOT.

Tabel 1. Matriks SWOT

	STRENGHT	**WEAKNESS**
OPPORTUNITY	**STRATEGI SO**	**STRATEGI WO**
Daftar semua peluang yang dapat di identifikasi.	Gunakan semua kekuatan yang dimiliki untuk memanfaatkan peluang yang ada.	Atasi semua kelemahan dengan memanfaatkan peluang yang ada.
THREATH	**STRATEGI ST**	**STRATEGI WT**
Daftar semua ancaman yang dapat di identifikasi.	Gunakan semua kekuatan untuk menghindari ancaman.	Tekan semua kelemahan dan cegah semua ancaman.

Sumber: Freddy Rangkuti, Analisis SWOT: Teknik Membedah Kasus Bisnis

2. EFAS dan IFAS

Pemilihan strategi terpilih analisis SWOT berdasarkan pada EFAS (*External Factor Analysis Summary*) dan IFAS (*Internal Factor Analysis Summary*).

---

[23] Billie Nordmeyer, “Advantages & Disadvantages of SWOT Analysis,”---------- https://smallbusiness.chron.com/advantages-amp-disadvantages-swot-analysis-41398.html (akses 23 Juni 2022).

a. EFAS

EFAS merupakan alat analisis untuk mengukur seberapa seberapa penting faktor lingkungan eksternal dan seberapa baik manajemen maupun strategi menanggapi faktor eksternal tersebut. Analisis EFAS membantu mengorganisir faktor-faktor strategis eksternal ke dalam kategori peluang dan ancaman.[24]

1) Nilai Bobot EFAS

Nilai bobot menunjukkan seberapa penting faktor lingkungan eksternal bagai organisasi. Nilai bobot EFAS dimulai dari 0.0 (sangat tidak penting) sampai dengan mendekati 1.0 (penting). Pembobotan didasarkan pada kemungkinan setiap faktor eksternal tersebut mempengaruhi posisi strategis organisasi saat ini. Semua bobot harus berjumlah berjumlah 1.0, tanpa memperdulikan jumlah faktor lingkungan strategis.[25] Penentuan nilai bobot berdasarkan pada tingkat signifikan faktor-faktor lingkungan ekternal terhadap terhadap organisasi, seperti ditunjukan pada Tabel 2. Tabel Signifikan EFAS.[26]

Tabel 2. Tingkat Signifikan EFAS

NILAI SIGNIFIKAN	KETERANGAN
1	Signifikan
2	Moderat
3	Sangat Signifikan

Sumber : Emron Bandung, Perhitungan Bobot dan Rating Analisis SWOT

2) Nilai Rating EFAS

a)) Peluang

Nilai *rating* EFAS (*External Factor Analysis Summary*) pada faktor peluang menunjukkan seberapa besar efektifitas strategi saat ini yang diterapkan organisasi mampu merespon berbagai peluang dalam lingkungan eksternal. Dengan demikian, rating menggambarkan nilai peluang bagi organisasai. Penentuan nilai

[24] Erna Listiana, "Manajemen Strategi - Menyusun Tabel EFAS & IFAS",---------- https://www.youtube.com/watch?v=1lMCDvpfFmI, (akses 23 Juni 2022).
[25] Ibid.
[26] Emron Bandung, "Perhitungan Bobot dan Rating Analisis SWOT,"---------- - https://www.youtube.com/watch?v=f2PugGuznN4&t=2s, (akses 23 Juni 2022).

rating EFAS untuk faktor peluang ditunjukkan pada Tabel 3. Rating EFAS Untuk Faktor Peluang.[27]

Tabel 3. Rating EFAS Untuk Faktor Peluang

NILAI	KETERANGAN
1	Strategi organisasi saat ini memiliki kemampuan yang **tidak baik** untuk merespon peluang dalam lingkungan eksternal, sehingga nilai peluang dari faktor ini **sangat rendah** bagi organisasi
2	Strategi organisasi saat ini memiliki kemampuan yang **kurang baik** untuk merespon peluang dalam lingkungan eksternal, sehingga nilai peluang dari faktor ini **cukup rendah** bagi organisasi
3	Strategi organisasi saat ini memiliki kemampuan yang **rata-rata** untuk merespon peluang dalam lingkungan eksternal, sehingga nilai peluang dari faktor ini **sedang atau moderat** bagi organisasi
4	Strategi organisasi saat ini memiliki kemampuan yang **sudah cukup baik** untuk merespon peluang dalam lingkungan eksternal, sehingga nilai peluang dari faktor ini **cukup besar** bagi organisasi
5	Strategi organisasi saat ini memiliki kemampuan yang **sudah sangat baik** untuk merespon peluang dalam lingkungan eksternal, sehingga nilai peluang dari faktor ini **sangat besar** bagi organisasi

Sumber: Erna Listiana, Manajemen Strategi

b)) Ancaman

Nilai *rating* EFAS (*External Factor Analysis Summary*) pada faktor ancaman menunjukkan seberapa besar efektifitas strategi saat ini yang diterapkan organisasi mampu merespon berbagai ancaman dalam lingkungan eksternal. Dengan demikian, rating menggambarkan nilai ancaman bagi organisasi. Penentuan nilai rating EFAS untuk faktor ancaman ditunjukkan pada Tabel 4. Rating EFAS Untuk Faktor Ancaman.[28]

Tabel 4. Rating EFAS Untuk Faktor Ancaman

NILAI	KETERANGAN
1	Strategi organisasi saat ini memiliki kemampuan yang **tidak baik** untuk merespon ancaman dalam lingkungan eksternal, sehingga nilai ancaman dari faktor ini **sangat besar** bagi organisasi

[27] Ibid., Erna Listiana.
[28] Ibid., Erna Listiana.

2	Strategi organisasi saat ini memiliki kemampuan yang **kurang baik** untuk merespon ancaman dalam lingkungan eksternal, sehingga nilai ancaman dari faktor ini **cukup besar** bagi organisasi
3	Strategi organisasi saat ini memiliki kemampuan yang **rata-rata** untuk merespon ancaman dalam lingkungan eksternal, sehingga nilai ancaman dari faktor ini **sedang atau moderat** bagi organisasi
4	Strategi organisasi saat ini memiliki kemampuan yang **sudah cukup baik** untuk merespon ancaman dalam lingkungan eksternal, sehingga nilai ancaman dari faktor ini **cukup kecil** bagi organisasi
5	Strategi organisasi saat ini memiliki kemampuan yang **sudah sangat baik** untuk merespon ancaman dalam lingkungan eksternal, sehingga nilai ancaman dari faktor ini **sangat kecil** bagi organisasi

Sumber: Dr. Erna Listiana, Manajemen Strategi

b. Perhitungan EFAS

Perhitungan EFAS dilaksanakan terhadap faktor eksternal terkait peluang dan ancaman yang telah diuraikan pada Bab II. Berdasarkan pada data/fakta serta kondisi lingkungan strategis yang telah dianalisis menggunakan kerangka teoritis terkait kondisi saat ini dan kondisi yang diharapkan, serta merujuk pada Tabel 2, Tabel 3 dan Tabel 4 di atas, perhitungan analisis EFAS sebagaimana ditunjukan pada Tabel 5. EFAS SWOT.

Tabel 5. EFAS SWOT

FAKTOR EKSTERNAL		TINGKAT	BOBOT	RATING	SKOR
PELUANG		**SIGNIFIKAN**			
1.	Tingkat penggunaan internet yang tinggi	3	0.21	2	0.43
2.	Sistem pendidikan nasional	3	0.21	2	0.43
3.	Kerja sama lintas negara	2	0.14	2	0.29
Jumlah Faktor Peluang			**0.57**		**1.14**
ANCAMAN					
1.	Penggunaan teknologi VPN yang terus meningkat	3	0.21	1	0.21
2.	Fenomena Post Truth	1	0.07	2	0.14
4.	Karakteristik sistem komunikasi	2	0.14	2	0.29
Jumlah Faktor Ancaman			**0.43**		**0.64**
Jumlah Keseluruhan			**1.00**	**Selisih**	**0.50**

Sumber : Hasil Pengolahan Data Penulis

c. IFAS

IFAS (*Internal Factor Analysis Summary*) merupakan alat analisis untuk mengukur seberapa seberapa penting faktor lingkungan internal dan seberapa baik manajemen maupun strategi menanggapi faktor internal tersebut. Analisis IFAS membantu mengorganisir faktor-faktor strategis internal ke dalam kategori kekuatan dan kelemahan.[29]

1) Nilai Bobot IFAS

Nilai bobot menunjukkan seberapa penting faktor lingkungan internal bagai organisasi. Nilai bobot IFAS dimulai dari 0.0 (sangat tidak penting) sampai dengan mendekati 1.0 (penting). Pembobotan didasarkan pada kemungkinan setiap faktor internal tersebut mempengaruhi posisi strategis organisasi saat ini. Semua bobot harus berjumlah berjumlah 1.0, tanpa memperdulikan jumlah faktor lingkungan strategis.[30] Penentuan nilai bobot berdasarkan pada tingkat signifikan faktor-faktor lingkungan internal terhadap terhadap organisasi, seperti ditunjukan pada Tabel 6. Tabel Signifikan IFAS.[31]

Tabel 6. Tingkat Signifikan IFAS

NILAI SIGNIFIKAN	KETERANGAN
1	Signifikan
2	Moderat
3	Sangat Signifikan

Sumber : Emron Bandung, Perhitungan Bobot dan Rating Analisis SWOT

2) Nilai Rating IFAS

a)) Kekuatan

Nilai *rating* IFAS pada faktor kekuatan menunjukkan seberapa baik sumber daya saat ini dimiliki mampu dikelola oleh organisasi, sehingga menjadi kekuatan bagi organisasi. Dengan demikian, rating menunjukkan nilai kekuatan bagi organisasi. Penentuan nilai

[29] Ibid., Erna Listiana.
[30] Ibid.
[31] Ibid., Emron Bandung.

rating IFAS untuk faktor kekuatan ditunjukkan pada Tabel 7. Rating IFAS Untuk Faktor Kekuatan.[32]

Tabel 7. Rating IFAS Untuk Faktor Kekuatan

NILAI	KETERANGAN
1	Strategi organisasi saat ini memiliki kemampuan yang **tidak baik** untuk mengelola faktor lingkungan internal ini, sehingga faktor ini memberikan nilai kekuatan yang **sangat rendah** bagi organisasi
2	Strategi organisasi saat ini memiliki kemampuan yang **kurang baik** untuk mengelola faktor lingkungan internal ini, sehingga faktor ini memberikan nilai kekuatan yang **cukup rendah** bagi organisasi
3	Strategi organisasi saat ini memiliki kemampuan yang **rata-rata** untuk merespon kekuatan dalam lingkungan internal, sehingga nilai kekuatan dari faktor ini **sedang atau moderat** bagi organisasi
4	Strategi organisasi saat ini memiliki kemampuan yang sudah **cukup baik** untuk mengelola faktor lingkungan internal ini, sehingga faktor ini memberikan nilai kekuatan yang **cukup besar** bagi organisasi
5	Strategi organisasi saat ini memiliki kemampuan yang **sudah sangat baik** untuk merespon kekuatan dalam lingkungan internal, sehingga nilai kekuatan dari faktor ini **sangat besar** bagi organisasi

Sumber: Dr. Erna Listiana, Manajemen Strategi

b)) Kelemahan

Nilai *rating* IFAS pada faktor kelemahan menunjukkan seberapa baik sumber daya saat ini dimiliki mampu dikelola oleh organisasi. Dengan demikian, rating menunjukkan nilai kelemahan bagi organisasi. Penentuan nilai rating IFAS untuk faktor kelemahan ditunjukkan pada Tabel 8. Rating IFAS Untuk Faktor Kelemahan.[33]

Tabel 8. Rating IFAS Untuk Faktor Kelemahan

NILAI	KETERANGAN
1	Strategi organisasi saat ini memiliki kemampuan yang **tidak baik** dalam mengelola faktor lingkungan internal ini, sehingga faktor ini memberikan nilai kelemahan yang **sangat besar** bagi organisasi
2	Strategi organisasi saat ini memiliki kemampuan yang **kurang baik** dalam mengelola faktor lingkungan internal ini, sehingga

[32] Ibid., Erna Listiana.
[33] Ibid., Erna Listiana.

	faktor ini memberikan nilai kelemahan yang **cukup besar** bagi organisasi
3	Strategi organisasi saat ini memiliki kemampuan yang **rata-rata** dalam mengelola faktor lingkungan internal ini, sehingga faktor ini memberikan nilai kelemahan yang **sedang/moderat** bagi organisasi
4	Strategi organisasi saat ini memiliki kemampuan yang **cukup baik** dalam mengelola faktor lingkungan internal ini, sehingga faktor ini memberikan nilai kelemahan yang **cukup rendah** bagi organisasi
5	Strategi organisasi saat ini memiliki kemampuan yang **sudah sangat baik** dalam mengelola faktor lingkungan internal ini, sehingga faktor ini memberikan nilai kelemahan yang **sangat rendah** bagi organisasi

Sumber: Dr. Erna Listiana, Manajemen Strategi

d. Perhitungan IFAS

Perhitungan IFAS dilaksanakan terhadap faktor internal terkait kekuatan dan kelemahan yang telah diuraikan pada Bab II. Berdasarkan pada data/fakta serta kondisi lingkungan strategis yang telah dianalisis menggunakan kerangka teoritis terkait kondisi saat ini dan kondisi yang diharapkan, serta merujuk pada Tabel 6, Tabel 7 dan Tabel 8 di atas, perhitungan analisis IFAS sebagaimana ditunjukan pada Tabel 9. IFAS SWOT.

Tabel 9. IFAS SWOT

FAKTOR INTERNAL		TINGKAT	BOBOT	RATING	SKOR
KEKUATAN		**SIGNIFIKAN**			
1.	Pelibatan seluruh penyelenggara komunikasi	3	0.15	5	0.75
2.	Regulasi sistem komunikasi dan informasi	3	0.15	5	0.75
3.	*Self control* individu	3	0.15	3	0.45
Jumlah Faktor Kekuatan			**0.45**		**1.95**
KELEMAHAN					
1.	Pasal multitafsir UU ITE	2	0.10	1	0.10
2.	Kesenjangan digital	3	0.15	2	0.30
3.	Ketiadaan regulasi terkait teknologi VPN	3	0.15	1	0.15
4.	Belum terdapat institusi yang mengatur aspek teknis sistem komunikasi	3	0.15	1	0.15
Jumlah Faktor Kelemahan			**0.55**		**0.70**
Jumlah Keseluruhan			**1.00**	**Selisih**	**1.25**

Sumber : Hasil Pengolahan Data Penulis

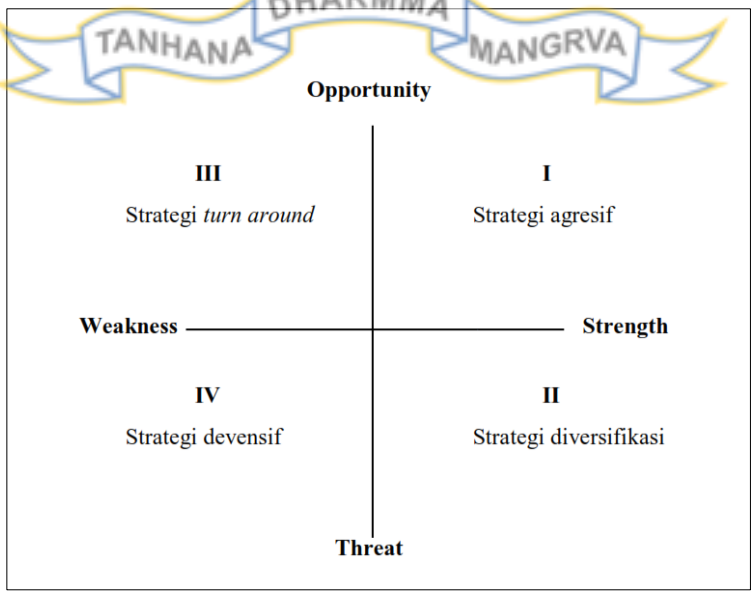
3. Penentuan Strategi Berdasarkan Kuadran SWOT

Penentuan strategi analisis SWOT berdasarkan pada posisi nilai EFAS dan IFAS pada kuadran SWOT, sebagaimana ditunjukan pada Gambar 1. Kuadran SWOT dan Tabel 10. Strategi dan Kuadran SWOT.

Tabel 10. Strategi dan Kuadran SWOT

NO	KUADRAN SWOT	KETERANGAN STRATEGI
1.	Kuadran I	Merupakan situasi yang sangat menguntungkan. Perusahaan memiliki peluang dan kekuatan sehingga dapat memanfaatkan peluang yang ada. Strategi yang harus diterapkan dalam kondisi ini adalah mendukung kebijakan pertumbuhan yang agresif (*growth oriented strategy*).
2.	Kuadran II	Meskipun menghadapi berbagai ancaman, perusahaan ini masih memiliki kekuatan dari segi internal. Strategi yang harus diterapkan adalah menggunakan kekuatan untuk memanfaatkan peluang jangka panjang dengan cara strategi diversifikasi (produk/pasar).
3.	Kuadran III	Perusahaan menghadapi peluang pasar yang sangat besar, tetapi dilain pihak, ia menghadapi berbagai kendala/ kelemahan internal. Fokus strategi perusahaan ini adalah meminimalkan masalah-masalah internal perusahaan sehingga dapat merebut peluang pasar yang lebih baik.
4.	Kuadran IV	Ini merupakan situasi yang sangat tidak menguntungkan, perusahaan tersebut menghadapi berbagai ancaman dan kelemahan Internal, sehingga fokus strategi perusahan adalah bertahan.

Sumber : Sondang P. Siagian, Manajemen Strategi, 175.



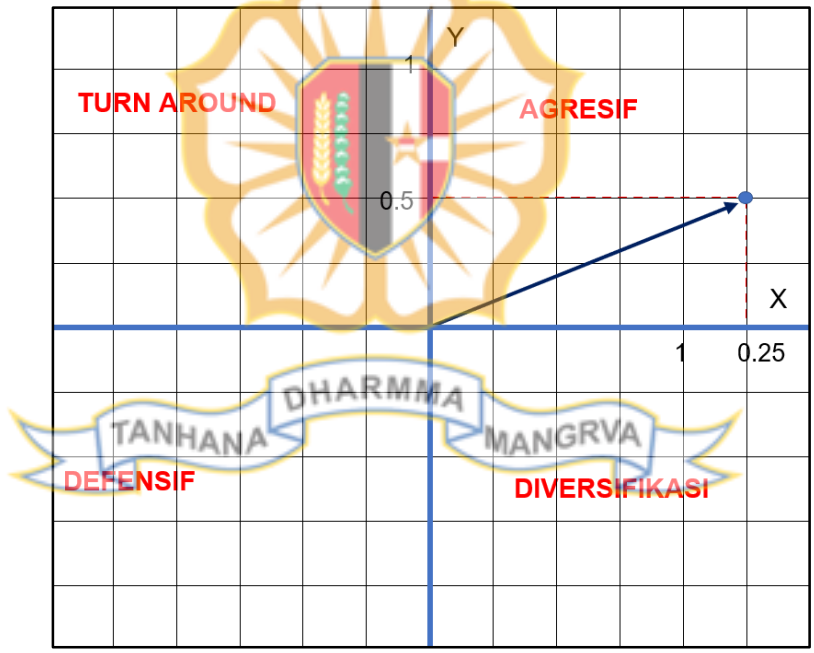
Gambar 1. Kuadran SWOT
Sumber : Sondang P. Siagian, Manajemen Strategi, 175.

Berdasarkan pada selisih nilai analisis EFAS dan IFAS, seperti pada yang ditunjukkan pada Tabel 11. Nilai Faktor Internal dan Eksternal, maka hasil selisih kedua faktor tersebut dapat dituangkan pada kuadran SWOT dengan posisi sumbu (X,Y). Posisi sumbu X adalah nilai selisih faktor internal, dan sumbu Y adalah nilai selisih faktor eksternal. Untuk itu, posisi pada kuadran SWOT, yaitu (1.25,0.50), seperti ditunjukan pada Gambar 2. Kuadran SWOT EFAS/IFAS

Tabel 11. Nilai Faktor Internal dan Eksternal

FAKTOR INTERNAL (X)	**NILAI**	**FAKTOR EKSTERNAL (Y)**	**NILAI**
STRENGTH	1.95	OPPORTUNITY	1.14
WEAKNESS	0.70	THREAT	0.64
SELISIH	**1.25**	**SELISIH**	**0.50**

Sumber : Hasil Pengolahan Data Penulis



Gambar 2. Kuadran SWOT EFAS/IFAS
Sumber : Hasil Pengolahan Data Penulis

LEMBAGA KETAHANAN NASIONAL
REPUBLIK INDONESIA

LAMPIRAN IV

RIWAYAT HIDUP

LEMBAGA KETAHANAN NASIONAL
REPUBLIK INDONESIA

RIWAYAT HIDUP PESERTA PPRA LXIV

A. Data Pokok

Nama	**: SUSILO RAHARJO, ST.**
Pangkat/Gol *	**: KOLONEL LAUT (E)**
Tempat/Tgl Lahir	**: SEMARANG, 26 APRIL 1973**
Jabatan	**: SAHLI PANGKOARMADA 2**
Instansi	**: TNI AL**
Agama	**: ISLAM**
Alamat Email	**: susiloraharjo40@gmail.com**

B. Pendidikan Umum

1. **SD Th. 1985**
2. **SMP Th. 1988**
3. **SMA Th. 1991**
4. **S1/STTAL Th. 2003**

C. Pendidikan Militer/Kursus/Khusus**

1. **AAL XL Th. 1994**
2. **DIKLAPA I Th. 1999**
3. **SESKOAL 48 Th. 2010**
4. **SESKO TNI 46 Th. 2019**

D. Pengalaman Jabatan

1. **PADIVLEKSEN KRI YOS 353 SATKOR ARMATIM Th. 1995**
2. **KADIVLISKAP KRI TMR 514 SATFIB ARMATIM Th. 1996**
3. **KADEPEKA KRI MDU 621 SATKAT ARMATIM Th. 1997**
4. **DPB DENMAKOARMATIM DIK STTAL Th. 2000**
5. **KADIVLEKSEN KRI AHP 355 SATKOR KOARMATIM Th. 2003**

6. KASIHAR SEWACO SATHARMAT SATKOR KOARMATIM Th. 2005
7. DPB DENMAKOARMATIM GASMILOBS UNOMIG GEORGIA Th. 2005
8. KASUBBAG SENKHUS ARSENAL DISSENLEKAL MABESAL Th. 2006
9. KASUBDISHAR SEWACO DISHARKAP KOARMABAR Th. 2010
10. KABAGREN DISKOMLEKAL MABESAL Th. 2013
11. PAWAS NAVKOM SATGAS KLL DISADAL MABESAL Th. 2015
12. KADISINFOLAHTA KOARMATIM Th. 2017
13. KADISINFOLAHTA KOARMADA II Th. 2018
14. KADISKOMLEK KOARMADA I Th. 2020

E. Data Keluarga

1. Nama Istri : SRI WILUJENG

2. Nama Anak : 1. A. KINANTI KUSUMA ARUM

2. A. CANTYA KIRANA

3. A. PUTRI KIRANI

Jakarta, 08 September 2022

Peserta

SUSILO RAHARJO, S.T.
Kolonel Laut (E) NRP 11417/P

*) Pangkat/Gol ASN/Non ASN menyesuaikan

**) Pendidikan ASN/Non ASN menyesuaikan