Legal Dialogica
Volume 1 Issue 1

Analisis Hukum Tentang Pengaturan Pertanggung Jawaban Hukum Atas Konten Berbahaya dalam Media Sosial *Whatsapp (Link Phising)*

Aulia Andini[1], Aan Aswari[2], M.Azham Ilham[3]
[1]*Fakultas Hukum, Universitas Muslim Indonesia*
[2]*Fakultas Hukum, Universitas Muslim Indonesia*
[3]*Fakultas Hukum, Universitas Muslim Indonesia*
Email Correspondence : anandaadeliasaja321@gmail.com

***Abstract**:*

Aulia Andini. 04020210164: "Legal Analysis Regarding Legal Liability Arrangements for Malicious Content on WhatsApp Social Media (Phishing Links)", Under the Guidance of Aan Aswari. as chief supervisor and M. Azham Ilham. as a mentor member. Dangerous content on social media, especially phishing links, has become a serious threat to society. This research aims to analyze legal liability arrangements for dangerous content on WhatsApp social media and find solutions to improve these arrangements. The research method used is a normative legal research method, using primary and secondary data sources. The research results show that the regulation of legal responsibility for dangerous content on WhatsApp social media is still not effective and efficient, because there are still many weaknesses and limitations in its implementation. The conclusion of this research is that it is necessary to improve and increase the regulation of legal responsibility for dangerous content on WhatsApp social media, by increasing public awareness, increasing cooperation between the government and social media service providers, and increasing the capacity of law enforcement officials.

***Keywords**: legal liability arrangements, dangerous content, WhatsApp social media, phishing links.*

***Abstrak**:*

Aulia Andini. 04020210164: *"Analisis Hukum Tentang Pengaturan PertanggungJawaban Hukum Atas Konten Berbahaya dalam Media Sosial WhatsApp (Link Phishing)",* Dibawah Bimbingan Aan Aswari. sebagai ketua pembimbing dan M.Azham Ilham. sebagai anggota pembimbing. Konten berbahaya dalam media sosial, khususnya *link phishing*, telah menjadi ancaman serius bagi masyarakat Penelitian ini bertujuan untuk menganalisis pengaturan pertanggungjawaban hukum atas konten berbahaya dalam media sosial *WhatsApp* dan menemukan solusi untuk meningkatkan pengaturan tersebut.Metode penelitian yang digunakan adalah metode penelitian hukum normatif, dengan menggunakan sumber data primer dan sekunder. Hasil penelitian menunjukkan bahwa pengaturan pertangg-ungjawaban hukum atas konten berbahaya dalam media sosial WhatsApp masih belum efektif dan efisien,

karena masih banyak kelemahan dan keterbatasan dalam implementasinya. Kesimpulan penelitian ini adalah bahwa perlu dilakukan perbaikan dan peningkatan dalam pengaturan pertanggungjawaban hukum atas konten berbahaya dalam media sosial *WhatsApp*, dengan meningkatkan kesadaran masyarakat, meningkatkan kerja sama antara pemerintah dan penyedia layanan media sosial, dan meningkatkan kapasitas aparat penegak hukum.

Kata Kunci: pengaturan pertanggungjawaban hukum, konten berbahaya, media sosial *WhatsApp*, *link phishing.*

PENDAHULUAN

Indonesia adalah negara hukum. Hal tersebut sesuai dengan yang termaktub dalam Undang-Undang Dasar 1945 Pasal 1 Ayat (3) bahwa "Negara Indonesia Adalah Negara Hukum". Hukum memiliki peran sentral dalam hal mengatur kehidupan bernegara. Berdasarkan ketentuan tersebut, hukum menjadi sesuatu hal yang wajib ditaati dan dipatuhi oleh seluruh warga negara dan harus ditegakkan. Hukum menjadi pelindung hak-hak seluruh elemen bangsa dari berbagai tindakan yang bermaksud untuk merampasnya, tak terkecuali hak anak.

Di era digital seperti saat ini, keberadaan sosial media tidak bisa lepas dari kehidupan masyarakat modern. Perkembangan informasi dan komunikasi ini dapat memberikan kemudahan akses informasi dan komunikasi bagi setiap individu di seluruh dunia, sehingga setiap hal yang diunggah pada hasil daripada perkembangan teknologi dan informasi tersebut bisa diakses atau didapatkan oleh setiap individu di seluruh dunia.[1]

Pada era digital saat ini, kita tengah dihadapi dengan segala perkembangan *trend* serta *update* yang terjadi di dunia digital. Hal ini sangat berhubungan dengan kebutuhan manusia akan informasi dan teknologi. Guna melengkapi kebutuhannya, manusia menggunakan berbagai cara dan media. Tak terlepas juga dengan perkembangan media komunikasi yang semakin signifikan dengan kecanggihan teknologi di seluruh dunia. Media digital memiliki keunggulan dalam peyampaian pesan yang dapat dikirim dengan kapasitas data yang cukup besar dan media penyimpanannya yang tidak terbatas karena menggunakan jaringan internet. Perkembangan teknologi dan *internet* yang sangat pesat ini yang telah membantu masyarakat dalam mendapatkan dan menyampaikan informasi. Jangkauan dari media komunikasi digital ini memang bisa secara luas menjangkau khalayaknya.[2]

Platform pertemanan dan situs berbagi foto atau video sudah menjadi kebutuhan sehari-hari, terlebih bagi pegiat sosial media yang sering disebut dengan *influencer.* Sebut saja *Facebook, Twitter, , TikTok, YouTube WhatsApp, Instagram* dan lain sebagainya. Bagi mereka media sosial ini menjadi ladang pendapatan, karena beberapa *platform digital* tersebut memberikan fitur yang disebut monetisasi yaitu proses pada suatu kegiatan yang bisa mengubah sesuatu menjadi penghasilan.

Modernisasi sangat mempengaruhi perkembangan dan kemajuan *teknologi* dan informasi saat ini. Masyarakat saat ini sudah terbiasa menggunakan sistem dan perangkat elektronik. Penggunaan perangkat elektronik dewasa ini dibuat dan dirancang guna semakin *modern* untuk mewujudkan efisiensi tugas manusia yang terkait dengan pembuatan,

pemrosesan, dan penyimpanan informasi.[3]

Di era globalisasi, kemajuan teknologi sebagaimana disebutkan diawal, telah menjadi suatu realitas yang harus diterima oleh seluruh elmen lapisan masyarakat, fakta demikian telah mempertegas bahwa masyarakat dunia selalu berkembang secara dinamis mengikuti berbagai situasi dan kondisi perkembangan zaman.[4]

Salah satu kemajuan besar dalam teknologi dapat dilihat ketika saat ini banyak pekerjaan manusia yang dipermudah dengan kehadiran mesin dan peralatan digital, seperti hadirnya mobil, *handphone,* motor, komputer dan laptop merupakan suatu produk yang dihasilkan di era moderenisasi ini.[5]

Teknologi sendiri merupakan istilah yang sangat luas dan digunakan untuk merujuk pada berbagai bidang ilmu pengetahuan dan penelitian. Istilah "teknologi" sendiri berasal dari kata Yunani *"techne"* yang bearti "kerajinan" dan *"logia"* yang berarti "mempelajari sesuatu". Perkembangan teknis tersebut di atas telah membuka peluang bagi masyarakat untuk segera mengakses segala informasi di seluruh dunia tanpa ada batas wilayah. Menurut beberapa ahli, fenomena ini sering disebut istilah (*borderless word*), yaitu. dunia tanpa batas, karena setiap orang dapat mengakses berbagai perkembangan dan informasi global dimanapun dan kapanpun mereka mau.[6]

Di Indonesia, kita bisa melihat seberapa besar dampak perkembangan teknologi informasi terhadap nilai-nilai budaya masyarakat, baik di masyarakat perkotaan maupun pedesaan. Kemajuan teknologi seperti media *online* yang dilengkapi dengan jaringan *internet* tidak hanya menjangkau elmen masyarakat perkotaan tetapi juga telah dinikmati oleh masyarakat di pelosok desa.[7]

Fakta tersebut didukung oleh data penggunaan *internet* di Indonesia berdasarkan hasil survei yang dilakukan oleh Asosiasi Penyelenggara Jasa *Internet* Indonesia (APJII) pada triwulan I tahun 2019, menunjukan bahwa terdapat 196,7 juta pengguna *internet* di Indonesia, atau mencapai 73,3% dari kuartal kedua di tahun 2020. Angka ini naik sebesar 64,8% dibandingkan tahun 2018.

Namun demikian perkembangan atas teknologi informasi tidak hanya akan berdampak positif bagi manusia sebagaimana disebutkan, namun perkembangan itu juga telah membawa dampak negatif bagi manusia. Dampak negatif kemajuan teknologi informasi meliputi antaralain munculnya berbagai pelanggaran hukum dan kejahatan di dunia maya, seperti penyadapan, Penyebaran virus komputer, akses mudah atas Pornografi, perjudian, penipuan, serta tayangan kekerasan yang semakin marak. Dengan dampak negatif seperti itu dikhawatirkan akan menimbulkan kejahatan-kejahatan di dunia nyata yang disebabkan oleh karena mengkonsumsi informasi dengan tidak cermat dan bijak, terutama apabila pengguna itu adalah anak-anak.[8]

Dampak negatif dari kemajuan teknologi dan informasi saat ini dapat dilihat berdasarkan data pemblokiran situs yang memuat konten- konten ilegal seperti perjudian, porografi dan situs-situs lain yang sifatnya melanggar ketentuan hukum yang berlaku di Indonesia. Pada tahun 2022 contohnya, Kementerian Komunikasi dan Informatika, sebagai lembaga yang mengendalikan konten ilegal, memblokir dan menghentikan akses atas 3.716 konten pialang berjangka ilegal, penipuan atau investasi ilegal, konten pertukaran mata uang ilegal tentang *binary option.*

Dikemukakan pula bahwa kehadiran konten ilegal juga sudah diatur dalam beberapa pasal dalam UU ITE, dimulai dari Pasal 27 sampai Pasal 29. Pasal 27 ayat (1) menjelaskan mengenai larangan orang yang mentransmisi dan mendistribusi konten yang melanggar kesusilaan dalam konteks pornografi. Pasal 27 ayat (2) menjelaskan mengenai orang dilarang menyebar konten perjudian. Pasal 27 ayat (3) menerangkan mengenai penghinaan dan pencemaran nama baik. Pasal 27 ayat (4) menerangkan mengenai larangan terkait dengan pengancaman dan pemerasan. Pasal 28 ayat (1) mengatur mengenai *hoaks* yang merugikan konsumen. Pasal 28 ayat (2) menyebutkan mengenai masalah ujaran kebencian dan Pasal 29 mengatur larangan perundungan. Dari seluruh pasal tersebut, kata dia, menunjukkan bagaimana aturan hukum bisa membatasi terkait dengan penyebaran konten-konten ilegal yang berlebihan, melanggar hak untuk seseorang

Pada dasarnya, pengaturan hukum mengharapkan agar pengguna media sosial *WhatsApp* untuk mencegah atau melaporkan konten berbahaya yang melanggar hukum. Misalnya,jika seseorang mengetahui adanya penyebaran konten yang bersifat penipuan,penyebaran kebencian, *phising,* yang terjadi di media sosail *Whatsapp* agar supaya melaporkan konten tersebut kepada pihak berwenang atau mengambil langkah untuk menghindari distribusi konten tersebut lebih lanjut. Oleh karena itu, dalam hukum pidana Undang-Undang ITE (Informasi dan Transaksi Elektronik) ada ketentuan yang mengatur mengenai penyebaran konten berbahaya melalui media sosial termasuk *Whatsapp*. Pengguna yang sengaja menyebarkan konten yang melanggar hukum dapat di pidana.

Namun pada kenyataannya sering kali berbeda, pelaku penipuan yang terjadi di media sosial Whatsapp sering kali kita jumpai hingga saat ini, yang menunjukkan adanya kesenjangan antara harapan dan realita. Beberapa faktor yang mungkin menjadi penyebab tingginya angka penipuan, ujaran kebencian, serta hal hal serupa yang terjadi di media sosial *WhasApp* yaitu kurangnya kesadaran pelaku, ekonomi, dan kurangnya program rehabilitasi bagi pelaku. Maka dari itu baik penyelenggara *platform* maupun pengguna mematuhi kewajiban hukum untuk mencegah penyebaran konten berbahaya dalam media sosial *WhatsApp* lebih lanjut.

Penelitian ini dilatar belakangi oleh perhatian Al-Qur'an terhadap konten berbahaya dalam media sosial. Berdasarkan latar belakang di atas, penulis tertarik untuk membahas dan mengkaji permasalahan tentang Analisis Hukum Tentang Pengaturan Pertanggungjawaban Hukum Atas Konten Berbahaya Dalam media sosial.

Peningkatan pelaku tindakan mengunggah konten berbahaya dalam media sosial *WhatsApp* yakni penipuan, dapat disebabkan oleh beberapa faktor yaitu meningkatnya pengguna *WhatsApp*,kemudahan akses, fitur pemalsuan identitas, perkembanan teknologi, serta kurangnya pengawasan dan regulasi. Adapun faktor lain yaitu masalah ekonomi. Banyak individu yang mungkin mengalami kesulitan ekonomi yang memaksa mereka terlibat dalam tindakan kriminal seperti pencurian dan penipuan sebagai cara untuk memenuhi kebutuhan dasar. Kurangnya lapangan kerja yang memadai juga dapat menyebabkan orang ― orang merasa tidak memiliki pilihan lain selain beralih ke kejahatan dengan memanfaatkan perkembangan teknologi dengan cara negatif.

Peningkatan jumlah penipuan dengan cara mengunggah konten berbahaya dalam

media sosial *WhatsApp* menggunakan situs-situs ilegal, yang pada akhirnya dapat menciptakan rasa tidak aman dan rasa terhadap pesan pesan yang masuk di *WhatsApp* sesorang sekalipun itu benar (tidak berbahaya). Pelaku penipuan mengunggah konten berbahaya dalam media sosial *WhasApp* juga dapat memberikan tekanan tambahan pada sistem peradilan hukum dan penegakan hukum. Penipuan di media sosial tidak hanya berdampak pada individu yang menjadi korban tetapi juga dapat mengganggu beberapa aspek sistem teknis dan hukum yang lebih luas.

Perlu diperhatikan bahwa pelaku yang memposting konten yang berbahaya dimedia sosial adalah tindakan pidana, dan dapat dikenai sangsi pidana tergantung jenis konten yang dibagikan, dan untuk memahaminya diperlukan analisis komprehensif mengenai *actus reus* dan *mens rea*, serta kesadaran seseorang yang terlibat dalam tindakan tersebut.

Berdasarkan hal tersebut penulis tertarik membahas dan memahami sebuah penulisan karya ilmiah dengan judul **"Analisis Hukum Tentang Pengaturan Pertanggungjawaban Hukum Atas Konten Berbahaya Dalam Media Sosial WhatsApp (*Link Phising*)".**

METODE

Jenis penelitian ini adalah penelitian Hukum Normatif dalam mekanisme penyelesaian sengketa bagi para pihak jika salah sau pihak wanprestasi dan bentuk penyelesaian sengketa yang banyak digunakan dalam menyelesaikan sengketa waralaba. Penelitian ini bertujuan untuk mengetahui dan menganalisis hukum yang berlaku serta memberikan solusi mengenai mekanisme penyelesaian sengketa dalam kontrak *franchise* bentuk penyelesaian sengketa yang banyak digunakan dalam menyelesaikan sengketa waralaba. Peneltian hukum normatif menganalisis norma norma yang kontradiktif mengenai mekanisme penyelesaian sengketa, dan bentuk penyelesaian sengketa yang paling banyak digunakan dalam menyelesaikan sengketa waralaba.

HASIL DAN PEMBAHASAN

1. Pengaturan Hukum yang Ada di Indonesia Terkait PertanggungJawaban Hukum Atas Konten Berbahaya dalam Media Sosial WhatsApp (Link Phishing)

Memahami terdapat atau tidak terdapatnya suatu tindak pidana, maka rumusan di suatu peraturan perundang-undangan pidana mengenai tindakan yang dilaksanakan dengan sanksi yang menyertainya. Suatu rumusan terdapat beberapa syarat atau unsur yang menjadi ciri sehingga dengan jelas bisa membedakan tindakan lain yang dilarang.

Peristiwa pidana yang juga disebut tindak pidana (delict) merupakan suatu tingkah laku yang dilarang oleh aturan hukum serta mendapatkan sanksi apabila melanggarnya. Suatu peristiwa hukum ini adalah suatu insiden yang ada di masyarakat yang mendorong peraturan hukum tertentu, sehingga ketentuan yang tersemat di dalamnya terjadi. Terjadinya persitiwa hukum apabila memenuhi rumusan yang tersemat di peraturan tersebut. Rumusan atau unsur itu terdiri dari:

a. Subjektif, yakni seseorang yang bisa mempertanggungjawabkan atas kesalahannya.
b. Objektif, yakni perbuatan seseorang, akibat dari perbuatan tersebut, atau adanya peristiwa tertentu yang membarengi perbuatan tersebut. Berdasarkan rumusan tersebut, maka suatu tingkah laku yang diperbuat oleh seseorang patut memenuhi suatu kondisi, sehingga dapat dikatakan sebagai peristiwa pidana.

Seperti yang dialami nasabah Ibu Nurmatia merupakan Nasabah Bank Rakyat

Indonesia Cabang Watansoppeng. Ibu Nurmatia juga merupakan seorang guru yang berusia 53 Tahun. Pada salah satu *Group Whatssapp* Ibu Nurmatia, ada anggota group yang mengirim *link* undangan pernikahan. *Link* yang di kirim oleh salah satu anggota *group* tersebut adalah juga merupakan pesan terusan. Ibu Nurmatia setelah membuka *link* dari pesan itu semacam *mendownload file* APK. Tidak berselang lama ada satu lagi orang anggota group memperingatkan untuk tidak mengunjungi link undangan karna dapat *mendonwload file* APK. Ini merupakan modus *phising Via* APK yang mana jika *file* APK itu terdownload di HP seseorang, semua data di HP tersebut dapat di kendalikan oleh orang lain dan dapat mengurus isi saldo rekening seperti yang sedang marak di beritakan saat ini. Setelah membaca larangan dari temannya, ibu Nurmatia panik dan segera mengunjungi *customer service* Bank Rakyat Indonesia dan menceritakan masalahnya. *Customer service* kemudian mengambil langkah, mengecek mutasi rekening ibu Nurmiati yang ternyata masi sesuai saldo sebelumnya lalu melakukan pemblokiran sementara terhadap saldo tersebut atas permintaan ibu Nurmatia. Kemudian customer *service* membantu nasabah untuk menghapus *file* APK yang telah terdownload. *Customer service* menerangkan bahwa saldo nasabah aman dikarenakan Ibu Nurmatia tidak menggunakan *Internet Banking* di *Smartphone* nya, sehingga rekeningnya tidak bisa dikendalikan oleh pelaku dan customer service juga berterimakasih karna Ibu Nurmatia telah sigap melakukan pelaporan. Namun karna banyak anggota di group tersebut ibu Nurmatia menjadi khawatir kemungkinan teman-temannya telah *mendownload link file* APK karna kurangnya pengetahuan tentang bahaya *file* APK tersebut dan mengira bahwa itu adalah betul undangan pernikahan anak dari salah satu anggota *group*. *Customer service* Bank Rakyat Indonesia kemudian menyarankan untuk memberikan informasi ke groupnya untuk segera menghapus *file* APK yang terlanjut terdownload lalu melakukan pengecekan mutasi rekening, megubah user dan *password* untuk mengamankan saldo rekening.[9]

Adapun kasus serupa seperti pada kasus, terdakwa atas nama RIZKI RIANTO BIN TASWIRMAN sejak akhir tahun 2018 sampai tahun 2020, yang dengan sengaja dan tanpa hak atau melawan hukum mengakses *computer* atau *system* elektronik dengan cara apapun dengan tujuan untuk memperoleh informasi elektronik dan atau dokumen eletronik. Perbuatan tersebut terdakwa lakukan dengan cara-cara sebagai berikut: Bahwa pada hari Senin tanggal 27 Juli 2020 Tim *Cyber Ditreskrimsus* Polda Riau menemukan adanya kegiatan *Phishing* atau *Carding* VALIDATION // SPMRTERKUAD // *Market Place* dengan *uniform resource locator* (URL) https://www.facebook.com/messages/t/291234388882574 dengan beranggotakan 103 orang dari berbagai macam daerah.

Terdakwa melakukan *Phishing* atau *carding* dengan cara melakukan *search google* admin di pencarian *google* lalu lakukan *Log-in*, dengan memasukkan *username*, terdakwa melakukan *phishing* dan/atau *carding* dengan membeli *Username* dan *Password* di sebuah akun *facebook* dengan nama Pablo https://www.facebook.com/asique28, seharga Rp. 250.000,00 dan biaya harga sebuah *username* dan *password google* admin biasanya dihargai 250.000 — 1.000.000 tergantung dari usia admin dan billingnya. Semakin lama usia dan *billing* akun tersebut maka akun tersebut semakin bagus karena sudah lama terdaftar. Sehingga email phising yang dikirimkan pasti masuk atau tidak bounce. Untuk *email* dan

password yang terdakwa beli dan gunakan saat ini adalah *Username*: admin.admin@menarii-10.com. *Password*: reinkar1234.

Selanjutnya setelah *Log-in* maka klik *fitur users* atau pengguna untuk memasukkan atau meng-*upload* jumlah *user* yang kita inginkan. Setelah tahap pembuatan *users* atau pengguna selesai. Maka, selanjutnya terdakwa membeli akun *upcloud* untuk membuat VPS (*Virtual Private Server*) di sebuah *facebook* dengan nama Agung Satrio Kuy 4 https://www.facebook.com/admin.bocah, seharga Rp. 200.000,- dan biasanya dijual mulai dari Rp. 50.000,00 — Rp. 200.000,00 tergantung saldo yang ada didalam akun tersebut. Tujuan dari akun upcloud ini adalah untuk membuat VPS (*Virtual Private Server*).

Kemudian setelah data kartu kredit (CC) terbuka maka terdakwa bisa dapatkan antara lain : Nomor kartu kredit; Masa aktif kartu kredit; CVV kartu kredit; Nama dan alamat pemilik kartu kredit; Nomor telepon pemilik kartu kredit; Tanggal lahir pemilik kartu kredit dan terdakwa menjual *credit card* (CC) hasil *phishing* dan/atau *carding* tersebut melalui akun *facebook*, selanjutnya tempat tempat jual *credit card* (CC) hasil *phishing* dan/atau *carding* tersebut di *group chat facebook* dengan nama *group* VALIDATION // SPMRTERKUAD / Market I Place dengan URL https://faceboo.com/messages/t/2912343888835747.dan akun *facebook* dengan nama Ipul Ycb (*Officialpull*) https://www.facebook.com/010110C bahwa terdakwa menjual data *credit card* milik orang lain tersebut kepada orang lain dengan harga Rp. 45.000,- untuk 1 (satu) buah data *credit card.* Bahwa setelah terdakwa mendapatkan data *Credit Card* lalu terdakwa menjual data *credit card* dalam sehari sebanyak 50 (lima puluh) — 200 (dua ratus) *credit card* (CC) jika dihitung dalam sehari terdakwa bisa menghasilkan Rp. 2.250.000,00 — Rp. 9.000.000,00.

Dalam hal ini terdakwa di dakwakan Pasal berlapis yaitu, pasal 32 ayat (2) jo pasal 48 ayat (2) Undang-Undang ITE dan pasal 30 ayat (2) jo pasal 46 ayat (2) Undang-Undang ITE. Atas dakwaan tersebut hakim mengadili terdakwa Rizki Rianto bin Taswirman telah terbukti secara sah dan meyakinkan bersalah melakukan tindak pidana "ITE", sebagaimana dalam dakwaan Kesatu dan Menjatuhkan pidana kepada Terdakwa tersebut oleh karena itu dengan pidana penjara selama 1 tahun dan denda sejumlah Rp. 20.000.000,-

Beberapa langkah–langkah yang dilakukan pelaku kejahatan *phishing* sebagaimana pengalaman Ibu Lisda yang pernah mendapatkan pesan *phishing* dengan modus perubahan tarif administrasi dari Rp. 8.000 per bulan menjadi Rp. 150.000 per bulan yang membuat nasabah tidak berfikir panjang kemudian mengakses *link* yang mana merupakan *link* palsu sebagai pernyataan tidak setuju untuk kenaikan tarif administarsi.

1. Pesan *link* palsu masuk melalui WA (*WhatsApp*) kepada calon korban yang telah menjadi sasaran.
2. Dalam pesan tersebut berisi mengenai perintah permintaan informasi yang bersifat personal seperti *user id, pin* atau nomor kredit.
3. Tidak hanya memberikan pesan singkat kepada korban, para pelaku kejahatan *phishing* juga memberikan batas waktu untuk mengirimkan data informasi korban yakni satu kali 24 jam, apabila tidak segera mengirimkan data tersebut maka akan ada konsekuensi buruk pada korban yakni dianggap menyetujui perubahan kenaikan tarif administrasi Bank sebesar Rp.150.000/bulan

4. Korban yang tidak berpikir Panjang maka akan menyerahkan data personalnya kepada para penjahat. Dari data tersebut maka akan disalahgunakan oleh penjahat

Serangan *phishing* menarget pengguna *internet banking* biasanya disebarkan melalui *WhatsApp*. *WhatsApp* merupakan aplikasi pada selular dengan *basic* sama *blackberry messeger*, merupakan aplikasi pesan lintas platform dimana kita dapat bertukar pesan secara gratis. Sehingga cara menghindarkan serangan kejahatan phising mesti dipahami orang lain yang tidak mempunyai hak masuk pada akun *internet banking* orang lain. Perbankan merupakan salah satu sektor yang sering menjadi eksploitasi para *phisher* dan kejahatanini tidak hanya mengakibatkan kerugian nasabah saja sebagai korban, tapi juga pihak perbankan mengalami kerugian berupa kepercayaan

Pertanggungjawaban pidana mengarah kepada seseorang yang melakukan tindak pidana dan telah memenuhi unsur-unsur yang telah tersemat di dalam suatu peraturan. Hal ini dimaksudkan bahwa seseorang akan dipertanggungjawabkan pidana apabila telah melakukan perbuatan yang bersifat melawan hukum.[10]

Secara umum unsur-unsur dari pertanggungjawaban pidana, meliputi:

a. Kesalahan
b. Kemampuan bertanggung jawab
c. Tidak ada alasan pemaaf

Suatu tingkah laku yang dapat dipertanggungjawabkan pidana haruslah mengandung unsur kesalahan karena di dalam pertanggungjawaban pidana terdapat asas tidak bisa dipidana, apabila tidak mempunyai kesalahan *(geen straf zonder schuld; Actus non facit reum nisi mens sis rea)*. Kesalahan dalam tindak pidana terbagi menjadi dua jenis yaitu sengaja *(dolus)* dan kelalaian *(culpa)*.[11]

Kesengajaan terjadi apabila seseorang melakukan secara sengaja atau yang dikehendaki dalam melaksanakan suatu tindakan yang melawan hukum. Kebanyakan tindak pidana mempunyai unsur kesengajaan daripada unsur kelalaian, hal ini dikarenakan yang sering mendapatkan hukuman pidana adalah orang yang melaksanakan sesuatu secara sengaja. Kesengajaan ini bersangkutan dengan ketiga unsur tindak pidana, yaitu:

a. Perbuatan yang di larang;
b. Akibat yang menjadi alasan diadakan larangan itu; dan
c. Bahwa perbuatan itu melanggar hukum.

Kelalaian terjadi karena kesalahan yang timbul sebab pelakunya tidak memenuhi kriteria tingkah laku yang telah ditetapkan oleh undang- undang yaitu terjadi karena tingkah laku orang itu sendiri. kesimpulannya, kelalaian bisa terjadi karena kurangnya berhati-hati dalam melakukan suatu perbuatan.[12]

Kriteria seseorang dikatakan telah melaksanakan tindak pidana ialah dengan mengamati apakah tindakan, kegiatan, perbuatan, atau aktivitas seseorang tersebut pada peraturan perundang-undangan telah diatur atau belum, jika suatu peraturan mengaturnya sebagai tindak pidana, maka orang tersebut telah melaksanakan tindak pidana.[13]

Berikut beberapa pengaturan hukum di Indonesia terkait pertanggungjawaban hukum atas konten berbahaya dalam media sosial *whatsapp:*

Undang-Undang

1. Undang-Undang No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (ITE):

Mengatur tentang pertanggungjawaban penyedia layanan internet dan pengguna atas konten ilegal. Pasal 27: Tindak pidana penyebaran informasi yang melanggar hukum dan Pasal 45 : Tindak pidana penyalahgunaan sistem elektronik.

2. Undang-Undang No. 19 Tahun 2016 tentang Perubahan atas Undang- Undang No. 11 Tahun 2008: Memperluas pengaturan tentang konten ilegal dan pertanggungjawaban penyedia layanan. Pasal 1: Mengatur tentang perubahan atas undang-undang No.11 Tahun 2008, dan Pasal 2: Mengatur tentang tujuan perubahan UU ITE. Perubahan UU ITE ini bertujuan untuk meningkatkan perlindungan hak-hak masyarakat, meningkatkan keamanan dan keselamatan transaksi elektronik, serta meningkatkan efektivitas pengawasan dan penindakan terhadap tindak pidana di bidang informasi dan transaksi elektronik.
3. Undang-Undang No. 27 Tahun 2022 tentang Perlindungan Data Pribadi: Mengatur tentang perlindungan data pribadi dan pertanggungjawaban atas pelanggaran. Pasal 6: Mengatur tentang hak-hak pemilik data pribadi. Pasal 26: Mengatur tentang pengawasan dan pengendalian data pribadi.

Peraturan Pemerintah

1. Peraturan Pemerintah No. 82 Tahun 2012 tentang Penyelenggaraan Sistem dan Transaksi Elektronik: Mengatur tentang keamanan dan keselamatan transaksi elektronik.
2. Peraturan Pemerintah No. 71 Tahun 2019 tentang Penyelenggaraan Sistem Elektronik: Mengatur tentang pengawasan dan pengendalian konten ilegal.

Peraturan Menteri

1. Peraturan Menteri Komunikasi dan Informatika No. 20 Tahun 2016 tentang Perlindungan Data Pribadi dalam Penyelenggaraan Sistem Elektronik: Mengatur tentang perlindungan data pribadi.

   Peraturan menteri komunikasi dan informatika republik indonesia nomor 20 tahun 2016 tentang perlindungan data pribadi dalam sistem elektronik dengan rahmat tuhan yang maha esa menteri komunikasi dan informatika republik indonesia,

   Menimbang : bahwa untuk melaksanakan ketentuan Pasal 15 ayat (3) Peraturan Pemerintah Nomor 82 Tahun 2012 tentang Penyelenggaraan Sistem dan Transaksi Elektronik, perlu menetapkan Peraturan Menteri Komunikasi dan Informatika tentang Perlindungan Data Pribadi dalam Sistem Elektronik;

   Mengingat : 1. Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (Lembaran Negara Republik Indonesia Tahun 2008 Nomor 58, Tambahan Lembaran Negara Republik Indonesia Nomor 4843); 2. Undang-Undang Nomor 39 Tahun 2008 tentang Kementerian Negara (Lembaran Negara Republik Indonesia Tahun 2008 Nomor 166, Tambahan Lembaran Negara Republik Indonesia Nomor 4916); 3. Peraturan Pemerintah Nomor 82 Tahun 2012 tentang Penyelenggaraan Sistem dan Transaksi Elektronik (Lembaran Negara Republik Indonesia Tahun 2012 Nomor 189, Tambahan Lembaran Negara Republik Indonesia Nomor 5348);

   Peraturan Menteri Komunikasi dan Informatika No. 5 Tahun 2020 tentang Standar Pengamanan Sistem Elektronik: Mengatur tentang keamanan sistem elektronik.

Menimbang; bahwa untuk memenuhi kebutuhan pengaturan dalam penyelenggaraan sistem elektronik lingkup privat, serta untuk melaksanakan ketentuanPasal 5 ayat (3), Pasal 6 ayat (4), Pasal 97 ayat (5), Pasal 98 ayat (4), dan Pasal 101 Peraturan Pemerintah Komunikasi dan Informatika tentang Penyelenggara Sistem Elektronik Lingkup Privat;Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik, perlu menetapkan Peraturan Menteri Mengingat;

Pasal 17 ayat (3) Undang-Undang Dasar Negara Republik Indonesia Tahun 1945;

Undang-Undang Nomor 39 Tahun 2008 tentang Kementerian Negara (Lembaran Negara Republik Indonesia Tahun 2008 Nomor 166, Tambahan Lembaran Negara Republik Indonesia Nomor 4916); Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik (Lembaran Negara Republik Indonesia Tahun 2019 Nomor 185, Tambahan Lembaran Negara Republik Indonesia Nomor 6400);

Peraturan Presiden Nomor 54 Tahun 2015 tentang Kementerian Komunikasi dan Informatika (Lembaran Negara Republik Indonesia Tahun 2015 Nomor 96);

Peraturan Menteri Komunikasi dan Informatika Nomor 6 Tahun 2018 tentang Organisasi dan Tata Kerja Kementerian Komunikasi dan Informatika (Berita Negara Republik Indonesia Tahun 2018 Nomor 1019);

Peraturan Menteri Komunikasi dan Informatika Nomor 13 Tahun 2019 tentang Penyelenggaraan Jasa Telekomunikasi (Berita Negara Republik Indonesia Tahun 2019 Nomor 1329);

Kriminalisasi

1. Pasal 27 ayat (3) Undang-Undang ITE: Mengatur tentang pertanggungjawaban hukum atas konten ilegal, termasuk ujaran kebencian, pornografi, dan fitnah.
2. Pasal 28 ayat (1) Undang-Undang ITE: Mengatur tentang pertanggungjawaban hukum atas penyebaran konten ilegal.
3. Pasal 45 ayat (2) Undang-Undang ITE: Mengatur tentang sanksi pidana atas pelanggaran.

Adapun sanksi yang dikenakan terhadap pelaku tindak pidana tersebut yaitu:

1. Sanksi pidana: Penjara paling lama 4 tahun dan/atau denda paling banyak Rp 750.000.000 (Pasal 45 ayat (2) Undang-Undang ITE).
2. Sanksi administratif: Pemblokiran akses, pencabutan izin, dan/atau denda.

Tindakan yang dapat dilakukan bagi pengguna *WhatsApp* yaitu:

1. Melaporkan konten berbahaya ke Kemenkominfo atau Polri.
2. Menggunakan *fitur* pelaporan di *WhatsApp.*
3. Menghindari penyebaran konten berbahaya.

B. . Bagaimana Mekanisme Penegakan Hukum Terhadap Konten Berbahaya yang Tersebar di Media Sosial *WhatsApp (Link Phishing*

Perkembangan teknologi dan media sosial memicu peningkatan kasus penyebaran konten berbahaya, seperti *phishing*, di *WhatsApp*. Konten ini dapat merugikan masyarakat dan mengancam keamanan informasi pribadi. Perkembangan teknologi dan media sosial memicu peningkatan kasus penyebaran konten berbahaya, seperti *phishing*, di *WhatsApp*. Konten ini dapat merugikan masyarakat dan mengancam keamanan informasi pribadi.

Meningkatnya kejahatan *siber*, pemerintah melalui penegak hukum berupaya untuk melakukan penegakan hukum. Penegakan hukum merupakan suatu proses, pada hakikatnya merupakan penerapan diskresi yang menyangkut membuat keputusan yang tidak secara ketat diatur oleh kaidah hukum, akan tetapi mempunyai unsur penilaian pribadi. Secara konsepsional, inti dari penegakkan hukum terletak pada kegiatan meyerasikan hubungan nilai-nilai terjabarkan didalam kaidah-kaidah yang mantap dan sikap tindak sebagai rangkaian penjabaran nilai tahap akhir, untuk [14]menciptakan, memelihara dan mempertahankan kedamaian pergaulan hidup. Penegakan hukum adalah suatu usaha untuk menanggulangi kejahatan, memenuhi rasa keadilan dan berdaya guna untuk menanggulangi kejahatan terhadap berbagai sarana dan sebagai reaksi yang dapat diberikan kepada pelaku kejahatan, berupa hukum pidana maupun non hukum pidana, yang dapat diintegrasikan satu dengan yang lainnya.

Secara terminologis, perlindungan hukum dapat dijelaskan dari himpunan dua pengertian, yaitu "perlindungan" serta "hukum". KBBI mendefinisikan perlindungan sebagai objek atau tindakan perlindungan. Hukum kemudian dapat dipahami sebagai peraturan atau kebiasaan yang mengikat secara resmi, disahkan oleh otoritas atau pemerintah yang berwenang. Menurut pengertian ini, perlindungan hukum dipahami sebagai usaha untuk memberikan perlindungan berdasarkan aturan yang telah disahkan pihak yang berkuasa atas itu. Secara singkat, melindungi hukum merupakan fungsi dari hukum. Salah satu bentuk kejahatan siber ialah phising. Kejahatan ini dilakukan dengan menarik perhatian korban tanpa mengenal batas waktu yang membuat korban lebih mudah terjaring. Hal ini menyebabkan jumlah korban kejahatan *phising* meningkat. Atas dasar inilah perlindungan hukum diperlukan untuk menjamin kehidupan masyarakat. Tugas ini menjadi bentuk tanggung jawab negara sebagai negara hukum.

Kasus *phishing* sendiri telah pernah diadili. Salah satunya ialah kasus dalam Putusan PN Pekanbaru No: 958/Pid.Sus/2020/PNPbr. Diketahui bahwa kejahatan ini dilakukan dengan meniru *website* resmi dan kemudian disebarkan ke alamat *e-mail* korban. Korban yang mengklik tautan yang dikirimkan ke *e-mail* maka datanya akan dicuri, seperti id pengguna, kata sandi, hingga alamat dan identitas lainnya. Kejahatan *phishing* ini menargetkan untuk mendapatkan data kartu kredit korban. Setelah memperoleh data tersebut, pelaku menjualnya melalui akun media sosial *Facebook*. Perbuatannya ini didakwa atas Pasal 32 (2) serta 48 (2) UU ITE. Kejahatannya diancam kurungan 1 tahun 2 bulan serta denda Rp. 20.000.000.

Undang-Undang Nomor 27 tahun 2022 tentang Perlindungan Data Pribadi (UU PDP) penting dalam menanggulangi *phishing* di Indonesia. UU ini memberikan perlindungan bagi informasi pribadi seseorang serta memberikan sanksi tegas bagi pelaku kejahatan *siber*, termasuk pelaku *phishing* dan Kemudian, saksi serta korban yang dalam kejahatan ini juga memperoleh perlindungan. Tata cara perlindungannya diatur dalam UU No 31 tahun 2014. UU mengenai perlindungan saksi dan korban ini dijelaskan di pasal (4). Di dalamnya dijelaskan bahwa perlindungan ini dilakukan agar saksi dan korban mampu memberikan keterangan yang dibutuhkan pada proses penegakan hukum. Perlindungan hukum diberikan untuk saksi dan korban atas kriteria yang telah ditetapkan dalam Pasal 28 UUPSK, yaitu:

1. Sifat pentingnya keterangan saksi dan/atau korban;
2. Tingkat ancaman yang membahayakan saksi dan/korban;
3. Hasil analisis tim medis atau psikologi terhadap saksi dan/atau korban; dan
4. Rekam jejak kejahatan yang pernah dilakukan oleh saksi dan/atau korban.

Korban *phishing* pada dasarnya membutuhkan kompensasi untuk kerugian atas penipuan yang dialaminya. Keberadaan UUPSK memberikan perlindungan kepada saksi maupun korban kejahatan. Bentuk perlindungannya dapat berupa kompensasi, restitusi, serta bantuan. Pengaturan perlindungan ini dinyatakan dalam aturan berikut ini:

1. Pasal 28 D (1) UU 1945 menegaskan "Setiap orang berhak atas pengakuan, jaminan, perlindungan dan kepastian hukum yang adil serta perlakuan yang sama dihadapan hukum."
2. Pasal 40 (2) UU ITE berbunyi "Pemerintah melindungi kepentingan umum dari segala jenis gangguan sebagai akibat penyalahgunaan Informasi Elektronik dan Transaksi Elektronik yang mengganggu ketertiban umum, sesuai dengan ketentuan Peraturan Perundang- undangan."
3. Pasal 1 (8) UU No 31 Tahun 2014 yang merupakan perubahan atas UU No 13 Tahun 2006 mengenai Perlindungan Saksi dan Korban, menjelaskan "Perlindungan adalah segala upaya pemenuhan hak dan pemberian bantuan untuk memberikan rasa aman kepada Saksi dan/atau Korban yang wajib dilaksanakan oleh LPSK atau lembaga lainnya sesuai dengan ketentuan Undang-Undang ini."[15]

Namun, dari Pasal 45 hingga 52 UU ITE menetapkan bahwa pelaku kejahatan yang melakukan kejahatan yang dilarang berdasarkan UU ini akan dipidana karena melakukan perbuatan yang dilarang dalam UU, yang berarti bahwa mereka akan dikenakan pidana penjara atau denda sebagai bentuk penyelesaian perkara untuk melindungi hak para korban dalam transaksi elektronik/*cybercrime*. Restitusi adalah pendekatan yang tepat untuk mengurangi kerugian finansial bagi korban phising. Menurut Pasal 1 (11), "Restitusi adalah ganti kerugian yang diberikan kepada Korban atau Keluarganya oleh pelaku atau pihak ketiga." Dalam mendapatkan perlindungan melalui LPSK, korban kejahatan harus melewati tahap pengajuan dan mematuhi persyaratan dalam Pasal 21 PP No. 7 Tahun 2018.

Meskipun tidak ada undang-undang atau peraturan yang secara khusus mengatur tentang phishing. Namun, pelaku dapat dijerat dengan ketentuan Kitab Undang-Undang Hukum Pidana ("KUHP") dan UU ITE beserta perubahannya, seperti contoh kasus di atas. Penegakan Hukum Terhadap Tindak pidana phising kejahatan dunia maya dapat ditemukan di pasal 378 kuhp. Tindak pidana *phishing* termasuk dalam tindak pidana penipuan menurut pasal 378 kuhp yang berbunyi: "Barangsiapa dengan maksud hendak menguntungkan diri sendiri atau orang lain dengan melawan hak, baik dengan memakai nama palsu atau kedaan palsu, baik dengan akal dan tipu muslihat, maupun dengan karangan perkataan- perkataan bohong, membujuk orang supaya memberikan sesuatu barang, membuat utang atau menghapus piutang, dihukum karena penipuan, dengan hukuman penjara selama-lamanya empat tahun."

Selain itu juga ada beberapa pasal-pasal yang telah dijelaskan di atas, pelaku

phishing juga bisa dijerat Pasal 40 UU No. 36 tahun 1999 tentang telekomunikasi dengan bunyi: "Bahwa setiap orang dilarang melakukan kegiatan penyadapan atas informasi yang disalurkan melalui jaringan telekomunikasi dalam bentuk apapun".

Tindak kejahatan berupa menyebarkan informasi ataupun dokumen elektronik korban maka pelaku dikenai Pasal 32 (2) jo. Pasal 48 (2) UU ITE, yaitu: "Setiap orang dengan sengaja dan tanpa hak atau melawan hukum dengan cara apa pun memindahkan atau mentransfer Informasi Elektronik dan/atau Dokumen Elektronik kepada Sistem Elektronik orang lain yang tidak berhak dipidana penjara paling lama 9 tahun dan/atau denda paling banyak Rp 3 miliar." Terhadap tindakan kejahatan berupa memasuki sistem elektronik tertentu menggunakan identitas yang dicuri maka akan dikenai Pasal 30 (3) jo. Pasal 46 (3) UU ITE, yakni: "Setiap orang dengan sengaja dan tanpa hak atau melawan hukum mengakses Komputer dan/atau Sistem Elektronik dengan cara apapun dengan melanggar, menerobos, melampaui, atau menjebol sistem pengamanan dipidana penjara paling lama 8 tahun dan/atau denda paling banyak Rp800 juta."

Berdasarkan unsur *phishing* dan putusan pengadilan, pengaturan tentang kejahatan dunia maya berupa *phishing* tercantum dalam Undang- Undang Nomor 1 Republik Indonesia. 11/2008 tentang perubahan atas UU No. 19/2016 tentang informasi dan transaksi elektronik dalam beberapa pasal yang dapat diatur, antara lain: 1. Pasal 28 (1) berbunyi: "Setiap orang dengan sengaja dan tanpa hak menyebarkan berita bohong dan menyesatkan yang mengakibatkan kerugian konsumen dalam hal Elektronik." sudah Sebagai ketentuan pidana Pasal 45 ayat 2 disebutkan: "Barang siapa memenuhi keadaan sebagaimana dimaksud dalam Pasal 28, ayat 1 atau ayat 2, dipidana dengan pidana penjara paling lama 6 (enam) tahun dan/atau denda paling banyak 1.000.000.000,00 (satu miliar rupiah)". 2. Pasal 35 berbunyi: "Setiap orang dengan sengaja dan tanpa hak atau melawan hukum mengolah, membuat, mengubah, menghapus, memusnahkan data elektronik dan/atau dokumen elektronik dengan maksud agar data elektronik dan/atau dokumen elektronik dianggap asli." sudah Pasal 51 sebagai ketentuan pidana, dimana "Setiap orang yang memenuhi ciri-ciri yang ditentukan dalam Pasal 35 dipidana dengan pidana penjara paling lama 12 (dua belas) tahun dan/atau denda paling banyak Rp12.000.000.000,00 (dua belas milyaran rupiah).

Mekanisme penegakan hukum dimulai dengan pelaporan konten berbahaya oleh masyarakat ke Kementerian Komunikasi dan Informatika (Kemenkominfo), Kepolisian Republik Indonesia (Polri) atau langsung ke *WhatsApp* melalui fitur "Laporkan". Pelaporan ini dapat dilakukan secara *online* atau *offline* dengan menyertakan bukti konten berbahaya tersebut.

Setelah pelaporan diterima, Kemenkominfo atau Polri melakukan verifikasi untuk memastikan keabsahan laporan. Verifikasi ini bertujuan untuk memastikan bahwa konten tersebut memang melanggar hukum dan tidak merupakan pelanggaran hak asasi manusia. Jika konten tersebut memenuhi kriteria, maka akan dilanjutkan ke tahap pemblokiran.

Jika konten tersebut memenuhi kriteria, Kemenkominfo memblokir akses ke *link phishing* untuk mencegah penyebaran lebih lanjut. Pemblokiran ini dilakukan untuk melindungi masyarakat dari potensi kerugian dan menghindari penyebaran konten berbahaya.

Polri melakukan penyelidikan untuk mengidentifikasi pelaku dan mengumpulkan bukti. Jika pelaku teridentifikasi, maka akan dilakukan penindakan hukum sesuai dengan ketentuan yang berlaku. Penindakan ini dapat berupa penangkapan, penuntutan, dan sanksi pidana.

Adapun Dasar Hukumnya yaitu:

Penegakan hukum terhadap konten berbahaya dalam media sosial *WhatsApp link phishing* didasarkan pada beberapa peraturan perundang- undangan, antara lain:

1. Undang-Undang No. 11 Tahun 2008 tentang informasi dan Transaksi Elektronik (ITE)
2. Undang-Undang No. 19 Tahun 2016 tentang Perubahan atas Undang- Undang No. 11 Tahun 2008. Pasal 1: Mengatur tentang perubahan atas UU No. 11 Tahun 2008.Pasal 2: Mengatur tentang tujuan perubahan UU ITE. Perubahan UU ITE ini bertujuan untuk meningkatkan perlindungan hak-hak masyarakat, meningkatkan keamanan dan keselamatan transaksi elektronik, serta meningkatkan efektivitas pengawasan dan penindakan terhadap tindak pidana di bidang informasi dan transaksi elektronik.
3. Peraturan Pemerintah No. 82 Tahun 2012 tentang Penyelenggaraan Sistem dan Transaksi Elektronik.
4. Peraturan Menteri Komunikasi dan Informatika No. 20 Tahun 2016 tentang Perlindungan Data Pribadi.

KESIMPULAN DAN SARAN

Phishing merupakan upaya untuk mendapatkan informasi data seseorang dengan teknik pengelabuan. Data yang menjadi sasaran phising adalah data pribadi (nama, usia, alamat), data akun (username dan password), dan data finansial (informasi kartu kredit, rekening). Untuk itu perlu perlindungan dan penegakan hukum yang ekpresif hingga kejahatan phising ini dapat diminimalisir agar tidak berdampak luas di Indonesia khususnya bagi pengguna smartphone. Tujuan dilakukannya penelitian ini untuk meminimalisir angka kejahatan phising dan khusus bagi pengguna smartphone untuk mewaspadai modus operandi yang dilakukan oleh oknum baik yang dikirimkan melalui link atau cara lainnya.Pengaturan pertanggungjawaban hukum atas konten berbahaya dalam media sosial, khususnya link phishing, masih belum efektif dan efisien. Meskipun telah ada beberapa peraturan perundang-undangan yang mengatur tentang pertanggungjawaban hukum atas konten berbahaya, namun masih banyak kelemahan dan keterbatasan dalam implementasinya. Oleh karena itu, perlu dilakukan perbaikan dan peningkatan dalam pengaturan pertanggungjawaban hukum atas konten berbahaya dalam media sosial.Untuk meningkatkan pengaturan pertanggungjawaban hukum atas konten berbahaya dalam media sosial, beberapa saran dapat diberikan. Pertama, perlu dilakukan perbaikan dan peningkatan dalam peraturan perundang-undangan yang mengatur tentang pertanggungjawaban hukum atas konten berbahaya dalam media sosial. Kedua, perlu dilakukan kampanye kesadaran dan pengetahuan masyarakat tentang bahaya konten berbahaya dan cara melaporkannya. Ketiga, perlu dilakukan peningkatan dalam sistem pelaporan konten berbahaya dan peningkatan dalam pengawasan dan pengendalian konten berbahaya. Keempat, perlu dilakukan kerja sama antara pemerintah, penyedia layanan media sosial, dan masyarakat untuk meningkatkan pengaturan pertanggungjawaban hukum atas konten berbahaya dalam media

sosial.Dengan demikian, diharapkan dapat tercipta suatu sistem yang lebih efektif dan efisien dalam mengatur pertanggungjawaban hukum atas konten berbahaya dalam media sosial, sehingga dapat melindungi masyarakat dari bahaya konten berbahaya.

UNGKAPAN TERIMAKASIH

Bersyukur kepada Allah SWT atas rahmat, taufik dan inayah-Nya penulis dapat menyelesaikan penelitian ini. Tak lupa penulis mengirimkan Shalawat beserta salam semoga tercurah limpahkan kepangkuan baginda tercinta, hakim termulya yang adil dan bijaksana, pengikis habis ajaran komunis dan kapitalis pejuang reformasi yang anti korupsi, yaitu baginda nabi besar Muhammad SAW. Terima kasih kepada kedua orang tua saya dan saudara/i yang sangat kontributif dalam proses penyelesaian penelitian ini. Tak lupa saya ucapkan terima kasih kepada Satrih Hasyim dan Dwi Handayani. Karena telah memberikan bimbingan dengan penuh keseriusan, kecermatan, dan kebijakan dalam penyusunan penelitian ini. Serta Bapak Mustamin dan Bapak La Ode Husein atas kritik dan saran yang diberikan terhadap penelitian ini. Terimakasih pula kepada teman-teman yang penulis tidak bisa disebutkan satu-persatu senantiasa menemani dan saling mendukung pada masa perkuliahan. Penulis mengucapkan terima kasih kepada semuanya semoga kebaikan kalian dibalas oleh Allah SWT.

REFERENSI

(1) Adrian Sutedi. 2008. Hukum Waralaba. Jakarta: Galia Indonesia

(2) Chrishans, R. M. *(2023). Efektifitas Alternatif Penyelesaian Sengketa Sebagai Upaya Penyelesaian Sengketa Franchise (WARALABA). Multilingual: Journal of Universal Studies, 3(3), 428-442.*

(3) Dungga, & Sarson,. (2023). *Perlindungan Hukum Terhadap Para Pihak Dalam Perjanjian Waralaba*. *Journal of Comprehensive Science (JCS)*, *2*(5), 1193-120

(4) Dwi Handayani, Yoga *" Penyelesaian sengketa bisnis arbitrase"*

(5) Fadillah, F. A., & Putri, S. A. (2021). Alternatif Penyelesaian Sengketa Dan Arbitrase (Literature Review Etika). *Jurnal Ilmu Manajemen Terapan*, *2*(6), 744-756.

(6) Herniati, S. H. (2019). *Sengketa Bisnis dan Proses penyelesaiannya Melalui Jalur Non Litigasi*. MEDIA SAHABAT CENDEKI.

(7) https://www.mahkamahagung.go.id/id/berita/6102/selama-2023-mahkamah-agung-berhasil-memutus-perkara-sebanyak-26903-perkara

(8) https://www.google.com/search?q=jumlah+penyelesaian+sengketa+melalui+jalur+mediasi

(9) https://quran.nu.or.id/an-nahl/90

(10) IyabuDungga, & Sarson,. (2023). *Perlindungan Hukum Terhadap Para Pihak Dalam Perjanjian Waralaba*. *Journal of Comprehensive Science (JCS)*, *2*(5), 1193-120

(11) Jayadi, H. (2023). Hukum Alternatif Penyelesaian Sengketa dan Teknik Negosiasi.

(12) Kartika, I.& Senastri, (2021). *Perlindungan Hukum Terhadap Penerima Hak dalam Perjanjian Waralaba di Indonesia. Jurnal Preferensi Hukum*, *2*(3), 459-464.

(13) Kusnadi, A., & Marpaung, D. S. H. (2022). Efektifitas Penyelesaian Sengketa Konsumen Melalui Proses Di Luar Pengadilan (Melalui Jalur Mediasi). *Wajah Hukum*, *6*(1), 80-85.Adrian Sutedi. 2008. Hukum Waralaba. Jakarta: Galia Indonesia

(14) Kurniawaty, Y. (2017). Efektivitas alternatif penyelesaian sengketa dalam sengketa kekayaan intelektual (alternative dispute resolution on intellectual property dispute). *Jurnal Legislasi Indonesia*, *14*(2), 163-169.

(15) Mulyana, D. (2019). Kekuatan Hukum Hasil Mediasi Di Dalam Pengadilan Dan Di Luar Pengadilan Menurut Hukum Positif. *Jurnal Wawasan Yuridika*, *3*(2), 177-198.

(16) Nita, T. (2019). Alternatif Dispute Resolution: Penyelesaian Sengketa dengan Model Mediasi, Arbitrase, Negosiasi dan Konsiliasi.

(17) RM, G. P. S. (2006). *Arbitrase dan mediasi di Indonesia*. Gramedia Pustaka Utama.

(18) Rosita, R. (2017). Alternatif Dalam Penyelesaian Sengketa (Litigasi dan Non Litigasi). *Al-Bayyinah*, *1*(2), 99-113.Rustan, Andi Tenri Sapada,Ega Aprilia "*Ana;isis Hukum Sengketa Perjanjian Waralaba (Fanchise)*

(19) Slamet,(2011). *Waralaba (franchise) di Indonesia*. *Lex Jurnalica*, *8*(2), 18075.

(20) Serlika Apita "Alternatif penyelesaian sengketa bisnis