LEGAL: Journal of Law
Vol. 5 No. 1, Mei 2026, 117-125 / ISSN 2829-6672
DOI: https://doi.org/10.67032/ljl.v5i1.177

Pengaturan Hukum Tentang Tindak Pidana *Cyberstalking* Terhadap Pejabat Penting Negara di Sulawesi Selatan

Martono[1], Andi Bau Ria Anugrah[2], Ismail Ali[3], Andi Nail Ijlal Zaki[4]

[1-2-3-4]Institut Ilmu Hukum dan Ekonomi Lamaddukelleng

Abstrak

Penelitian ini bertujuan untuk mengetahui bentuk pengaturan tentang tindak pidana pelaku penyebaran *cyberstalking* berdasarkan ketentuan pasal-pasal dalam UU ITE dan KUHP, dan untuk mengetahui faktor-faktor yang menghambat penegakan hukum terhadap kejahatan tersebut. Metode penelitian yang digunakan adalah pendekatan hukum normatif-empiris dengan memadukan analisis terhadap peraturan perundang-undangan dan data lapangan. Data primer diperoleh melalui wawancara dengan penyidik di Polda Sulawesi Selatan, sedangkan data sekunder diperoleh dari literatur hukum, jurnal ilmiah, dan peraturan perundang-undangan yang relavan. Teknik analisis data dilakukan secara kualitatif dengan mengkaji kesesuaian antara norma hukum dan praktik penegakan hukum di lapangan. Hasil penelitian menunjukkan bahwa secara normatif penyebaran *link cyberstalking* dapat dijerat melalui beberapa ketentuan dalam UU ITE dan KUHP, antara lain Nomor 1, Tahun 2008, dan UU nomor 1Tahun 2023 yang berkaitan dengan penyebaran informasi menyesatkan, akses ilegal terhadap sistem elektronik, serta penguntitan. Namun, dalam praktik penegakan hukum masih ditemukan berbagai hambatan, seperti kesulitan memperoleh bukti digital, penggunaan identitas anonim pelaku, keterbatasan sarana teknologi forensik digital, tidak adanya korban yang ingin melapor, serta rendahnya kesadaran masyarakat dalam menjaga bukti elektronik. Temuan ini menunjukkan adanya kesenjangan antara norma hukum yang berlaku dengan implementasinya dalam praktik penegakan hukum. Meskipun kerangka hukum untuk menjerat pelaku *cyberstalking*,telah tersedia dalam UU ITE dan KUHP, efektivitas penerapannya masih memerlukan penguatan melalui peningkatan kapasitas aparat penegak hukum, penyediaan sarana teknologi investigasi digital, serta peningkatan literasi dihital masyarakat.

Kata Kunci: *cyberstalking, pejabat negara, pengaturan hukum, tindak pidana*

Abstract

This study aims to determine the form of regulation regarding the criminal act of spreading cyberstalking based on the provisions of the articles in the ITE Law and the Criminal Code, and to determine the factors that hinder law enforcement against this crime. The research method used is a normative-empirical legal approach by combining analysis of laws and regulations and field data. Primary data was obtained through interviews with investigators at the South Sulawesi Regional Police, while secondary data was obtained from legal literature, scientific journals, and relevant laws and regulations. Data analysis techniques were carried out qualitatively by examining the conformity between legal norms and law enforcement practices in the field. The results of the study indicate that normatively the spread of cyberstalking links can be

ensnared through several provisions in the ITE Law and the Criminal Code, including Law Number 1 of 2008 and Law Number 1 of 2023 relating to the dissemination of misleading information, illegal access to electronic systems, and stalking. However, various obstacles remain in law enforcement practice, such as difficulties in obtaining digital evidence, the use of anonymous perpetrator identities, limited digital forensic technology, the absence of victims willing to report, and low public awareness of safeguarding electronic evidence. These findings indicate a gap between applicable legal norms and their implementation in law enforcement practice. Although a legal framework for prosecuting cyberstalkers is available in the ITE Law and the Criminal Code, its effective implementation still requires strengthening through capacity building of law enforcement officers, provision of digital investigative technology, and increased public digital literacy.
Keywords**:** *cyberstalking, state officials, legal regulations, criminal acts*

PENDAHULUAN

Cyberstalking merupakan salah satu bentuk tindak pidana yang dilakukan secara sengaja oleh seseorang melalui tindakan mengikuti, memantau, mencari tahu informasi pribadi milik korban tanpa izin, dan mengancam korban, tindakan ini dapat mencakup pengumpulan data sensitif seperti alamat rumah, nomor telepon, kegiatan sehari-hari, Nomor Induk Kependudukan (NIK) pada KTP maupun Kartu Keluarga, serta berbagai informasi identitas lainnya yang bersifat rahasia. Tidak hanya terbatas pada pengintaian fisik, pelaku *cyberstalking* juga memanfaatkan media digital untuk mengakses atau mencoba memperoleh informasi yang jauh lebih sensitif, termasuk nomor rekening ATM, kata sandi, riwayat mutasi rekening, hingga catatan transaksi keuangan.

Praktik seperti ini biasanya menyasar individu tertentu, terutama orang-orang yang memiliki posisi publik atau jabatan penting, seperti pejabat negara, sehingga mereka lebih rentan menjadi target karena memiliki nilai strategis bagi pelaku. Seluruh aktivitas *stalking* tersebut dilakukan tanpa sepengetahuan korban, sehingga memperlihatkan adanya pelanggaran serius terhadap privasi dan keamanan data pribadi.

Dampaknya sangat signifikan karena dapat mengganggu ketenangan, kenyamanan, dan kehidupan sehari-hari korban, mengingat informasi pribadi seharusnya tidak diketahui, diakses, ataupun disalahgunakan oleh pihak lain tanpa persetujuan. Selain menganggu kenyamanan pribadi tindakan tersebut juga menganggu tugas dan tanggung jawab sebagai pejabat negara seperti kebocoran data sensitif pemerintahan, pelaku juga bisa mengetahui jadwal rapat, jadwal perjalanan dinas dan lokasinya. Oleh karena itu, *cyberstalking* dipandang sebagai kejahatan yang tidak hanya menyerang privasi, tetapi juga dapat mengancam keamanan fisik, psikologis, maupun sosial dari korban. Di kota besar seperti Makasar, masyarakat sangat aktif dalam menggunkan media sosial, dan sebagai pejabat publik mereka sering menggunakan media sosial untuk transparansi, seperti memposting kegiantan harian, penyampaian kebijakan secara terbuka, perkembangan program kerja, tetapi kondisi ini juga membuka peluang terjadinya kejahatan seperti *cyberstalking*.

Kejahatan *cyberstalking* pernah terjadi di kota Makassar, pada tahun 2024 oleh Kepala Dinas Kominfo yang berinisial (R) mengalami gangguan digital yang intens dari seseorang yang tidak dia kenal berinisial (F), yang diawali oleh pelaku sering mengomentari unggahan korban (R) mengenai program digitalisasi kota. Namun dalam beberapa minggu tindakan yang dilakukan oleh F sudah termasuk tindakan *cyberstalking*, karena: 1) mengirim pesan ancaman melalui instagram, whatsapp bisnis

kantor, dan email dinas, dengan nada marah dan intimidatif karena F tidak setuju dengan kebijakan tertentu, 2) Mengambil foto R dari media sosial, lalu mengeditnya dan menyebarkannya untuk mempermalukan R secara *online*, 3) Melacak lokasi R melalui unggahan *story* pegawai lain, kemudian menuliskan lokasi tersebut di akun palsu, 4) Membuat 3 akun palsu dengan tujuan untuk mantau aktivitas R setelah R memblokir akun utamanya, 5) Mengirim pesan ke keluarga R di mana pesan tersebut dikirim ke anak R yang masih sekolah yang berisi ancaman dan informasi pribadi.

Tindakan yang telah dilakukan oleh F telah mengganggu kenyamanan dan menimbulkan tekanan psikologis dan membuat R meningkatkan pengaman pribadi. Ini hanya salah satu contoh kasus dari banyaknya kasus *cyberstalking* yang terjadi, dan di kasus ini menggambarkan bagaimana bahaya *cyberstalking* dalam kehidupan sehari-hari, namun dalam praktiknya, pertanggung jawaban pidana *cyberstalking* sering kali menemui kendala di tingkat penyidikan, karena sulitnya mengumpulkan butik digital, pelaku menggunkan identitas palus, keterbatasan aparat penegak hukum, platfom media sosial sering tidak responsif.

Walapun tidak ada undang-undang khusus yang mengatur langsung tentang hak dan perlindungan pejabat negara yang megalami tindak pidana *cyberstalking*, namun dari prinsip umum perlindungan warga negara, karena pejabat negara tetaplah warga negara, sehingga dilindungi oleh UUD 1945. Secara konstitusional yang bersifat umum dalam UUD 1945, dasar konstitusional yang mengatur perlindungan dari *cyberstalking* walau tidak menyebut "*cyberstalking*", UUD 1945 memberikan perlindungan melalui pasal-pasal tentang:

1. Perlindungan Diri dan Rasa Aman (Pasal 28G Ayat (1)) bahwa "Setiap orang berhak atas perlindungan diri pribadi, keluarga, kehormatan, martabat, dan harta benda".
2. Hak untuk Melindungi Diri (Pasal 28A) bahwa "Setiap orang berhak untuk hidup serta mempertahankan hidup dan kehidupannya".
3. Hak atas Informasi dan Komunikasi Pribadi (Pasal 28F) bahwa "Setiap orang berhak untuk berkomunikasi dan memperoleh Informasi".
4. Kepastian Hukum dan Perlindungan (Pasal 28D Ayat (1)) bahwa "Setiap orang berhak atas pengakuan, jaminan, perlindungan, dan kepastian hukum".
5. Kewajiban Negara Melindungi HAM (Pasal 28I Ayat (4)) bahwa Perlindungan, penegakan, dan pemenuhan HAM adalah tanggung jawab negara.
6. Tugas Polri (Pasal 30 Ayat (4)) bahwa "Kepolisian bertugas menjaga keamanan dan ketertiban Masyarakat".

Berdasarkan hal tersebut, perlu dilakukan analisis yuridis terhadap pertanggungjawaban pidana dalam tindak pidana *cyberstalking* dengan memperhatikan khusus pada ketentuan KUHP (ancaman, pencemaran, pemerasan) dengan perhatian khusus pada aspek pembuktian bukti digital dan kebijakan yang diterapkan oleh Polrestabes makasar sebagai salah satu lembaga penegak hukum di daerah. Penelitian ini diharapkan dapat memberikan pemahaman yang lebih mendalam mengenai bagaimana hukum pidana diterapkan terhadap *cyberstalking*, apa saja hambatan yang dihadapi dalam proses penegakan hukum, serta langkah-langkah yang dapat ditempuh untuk memperkuat efektivitas hukum dalam pemberantasan *cyberstalking* di tingkat kota, dengan mempertimbangkan perkembangan regulasi seperti KUHAP 2023.

Permasalahan yang angkat dalam penelitian ini adalah 1) Untuk mengetahui bentuk pengaturan tentang tindakan pidana *cyberstalking* terhadap pejabat penting negara, dan 2) Untuk mengetahui faktor-faktor bentuk pengaturan tentang tindakan pidana *cyberstalking* terhadap pejabat penting negara.

Pentingnya pengaturan hukum yang jelas untuk menangani tindak pidana *cyberstalking* sangat relevan, terutama mengingat dampak negatif yang ditimbulkan terhadap individu dan masyarakat.

Diperlukan langkah-langkah konkret untuk merumuskan undang-undang yang efektif dalam melindungi masyarakat dari tindakan stalking di dunia maya.Langkah-langkah ini harus mencakup penegakan hukum yang lebih ketat dan peningkatan kesadaran masyarakat tentang bahaya *cyberstalking*.Upaya ini juga harus melibatkan kolaborasi antara pemerintah, lembaga penegak hukum, dan masyarakat untuk menciptakan lingkungan yang lebih aman bagi semua individu. Dengan adanya regulasi yang jelas, diharapkan masyarakat dapat merasa lebih aman dan terlindungi dari ancaman *cyberstalking*, sehingga menciptakan rasa aman dalam kehidupan sehari-hari

METODE PENELITIAN

Penelitian ini berlokasi di Polda Sulawesi Selatan, dipilih karena merupakan lembaga yang berwenang melakukan penyelidikan dan penyidikan terhadap tindak pidana *cyber stalker*, termasuk yang melibatkan *cyber stalker* dalam pengadaan. Selain itu, Polda Sulawesi Selatan menangani beberapa kasus *cyber stalker*, sehingga memungkinkan peneliti memperoleh data yang relevan mengenai penerapan pertanggungjawaban pidana korporasi serta hambatan-hambatan yang muncul dalam proses penegakan hukumnya. Lokasi ini dinilai paling tepat untuk mendapatkan informasi empiris sesuai dengan tujuan penelitian.

Data Primer diperoleh langsung dari Kapolda Sulawesi Selatan, melalui wawancara dengan penyidik, observasi proses penyidikan, serta penelaahan dokumen perkara yang berkaitan dengan dugaan tindak pidana *cyberstalking*, pengadaan barang dan jasa. Data ini digunakan untuk mengetahui penerapan pertanggungjawaban pidana korporasi dalam praktik. Data Sekunder diperoleh melalui studi kepustakaan berupa peraturan perundang-undangan terkait, seperti UUD 1945.

Analisis data dalam penelitian ini dilakukan dengan menggunakan analisis deskriptif-kualitatif berdasarkan data primer dan data sekunder yang dianalisis secara sistematis untuk memahami penerapan pertanggungjawaban pidana *cyberstalker*.

PEMBAHASAN

Bentuk Pengaturan Tentang Tindakan Pidana Cyberstalking Terhadap Pejabat Penting Negara

Berdasarkan hasil penelitian lapangan yang dilakukan di Polda Sulawesi Selatan, diperoleh informasi bahwa kasus tindak pidana *cyberstalking* terhadap pejabat negara sudah sering terjadi, tetapi para korban tidak melaporkan tindakan tersebut di kepolisian, sebagaimana yang dikatakan oleh Bapak X bahwa memang benar sudah banyak berita atau media yang menginformasikan tentang tindak pidana *cyberstalking*, tetapi para korban atau pejabat yang mengalami kejadian tersebut tidak melaporkannya, karena mungkin mereka memikirkan beberapa hal seperti, dampak yang akan terjadi jika dia melapor, nama baik mereka yang akan rusak, jika pelaku menyebarkan informasi yang seharusnya tidak diketahui olah masyarakat.

Temuan tersebut menunjukan bahwa telah terjadi kasus *cyberstalking*, tetapi para korban tidak pernah melapor, karena mempertimbangkan beberapa hal, yang bisa saja merusak nama baik dan reputasinya sebagai pejabat negara, dan temuan informasi yang didapatkan oleh pelaku disebarkan.

Berdasarakan teori pengaturan tindak pidana, pada dasarnya suatu perbuatan

dapat diatur, dilarang, dan diberikan sanksi pidana oleh hukum, jika memenuhi unsur perbuatan melawan hukum, adanya kesalahan *(mens-rea)* serta kemampuan bertanggung jawab, dalam konteks *cyberstalking*,unsur kesalahan dapat dilihat dari kesengajaan pelaku dalam merencanakan tindakan *stalking* terdapat pejabat negara, untuk memperoleh ketentuan secara melawan hukum.

Pelaku biasanya melakukan beberapa tindakan yang menunjukkan adanya unsur kesengajaan, antara lain:

1. Merencanakan tindakan *cyberstalking* terhadap pejabat negara.
2. Merugikan atau membahayakan pejabat negara.
3. Mencari informasi tentang korban, baik itu informasi pribadi, kesalahan ataupun kekurangan pada saat meduduki jabatan.
4. Mengancam korban mengunakan informasi tersebut.

Serangkaian tindakan tersebut, menunjukkan adanya kesengajaan *(dolus)* karena pelaku secara sadar. Mengetahui bahwa perbuatannya dapat menimbukan kerugian bagi koran.

Dasar Hukum Nasional (UU ITE & KUHP)

Secara normatif, perbuatan *cyberstalking*, dapat dikualifikasikan sebagai tindakan pidana, berdasarkan beberapa ketentuan dalam undang-undang.

1. Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (jo. UU No. 19 Tahun 2016) Pasal yang relevan:
   a. Pasal 27 ayat (1): Melarang penyebaran konten asusila (sering digunakan jika penguntitan melibatkan konten seksual).
   b. Pasal 27 ayat (3): Penghinaan atau pencemaran nama baik secara online.
   c. Pasal 29: Ancaman kekerasan atau menakut-nakuti secara elektronik.
   d. Pasal 30: Akses ilegal (misalnya mengakses akun korban tanpa izin).
2. Undang-Undang Nomor 1 Tahun 2023 tentang Kitab Undang-Undang Hukum Pidana.
3. Undang-Undang Nomor 31 Tahun 2014 tentang Perlindungan Saksi dan Korban. Undang-Undang ini tidak mengatur pidana *cyberstalking* secara langsung, tetapi memberikan perlindungan bagi korban, termasuk korban kejahatan siber.

Pengaturan Khusus Jika Korban adalah Pejabat Negara

Jika korban adalah pejabat penting negara, terdapat lapisan perlindungan hukum tambahan, meskipun beberapa pasal telah dibatalkan atau diubah oleh Mahkamah Konstitusi (MK) untuk menjaga iklim demokrasi:

1. Penghinaan terhadap Lembaga Negara (Pasal 349-350 KUHP Baru): Mengatur pidana bagi setiap orang yang menghina kekuasaan umum atau lembaga negara (seperti DPR, Polri, atau Pemerintah Daerah). Namun, pasal ini merupakan delik aduan, artinya pejabat yang bersangkutan harus melaporkan sendiri.
2. Pasal Penyerangan Kehormatan Presiden/Wakil Presiden: Terdapat perlindungan khusus dalam KUHP bagi simbol negara, namun interpretasinya sangat dibatasi untuk kepentingan kritik publik.
3. Skala Prioritas Penegakan Hukum: Di Sulawesi Selatan, aparat kepolisian (seperti Polda Sulsel) cenderung memberikan atensi tinggi pada kasus yang melibatkan pejabat daerah guna menjaga stabilitas pemerintahan.

Implementasi dan Kasus di Sulawesi Selatan

Wilayah Sulawesi Selatan memiliki catatan penegakan hukum yang cukup ketat

terkait interaksi digital antara masyarakat dan pejabat publik.

1. Kasus Kritik Pejabat di Gowa (Contoh Kasus Fadli Rahim): Seorang PNS di Gowa pernah diproses hukum menggunakan Pasal 27 ayat (3) UU ITE karena dianggap menghina Bupati Gowa dalam sebuah grup pesan privat. Kasus ini menunjukkan bahwa kritik yang dianggap melampaui batas (bahkan di ruang privat) dapat dikategorikan sebagai tindak pidana di wilayah ini.
2. Fokus Polda Sulsel: Unit *Cyber Crime* Ditreskrimsus Polda Sulsel aktif melakukan patroli siber. Selain penanganan *cyberstalking*, mereka juga fokus pada peretasan akun *(hacking)* milik pejabat dan penyebaran berita bohong (hoax) yang menargetkan stabilitas politik lokal.
3. Respon Organisasi Pers (AJI Makassar): Aliansi Jurnalis Independen (AJI) Makassar sering menyoroti ancaman serangan digital (*doxing* dan intimidasi siber) yang dialami oleh pihak-pihak yang mengkritik pejabat atau kebijakan di Sulawesi Selatan, yang menunjukkan bahwa *cyberstalking* juga digunakan sebagai alat tekanan politik.

Secara hukum sebenarnya perbuatan *cyberstalking*, sudah memenuhi unsur pidana dalam KUHP dan UU ITE, tetapi dalam praktik sering kali sulit ditangani, karena pelaku biasanya menggunakan akun anonim atau identitas palsu, selain itu bukti yang dimiliki korban baik bukti digital ataupun non digital, sering kali tidak lengkap.

Jika dibandingkan antara norma hukum dan praktik di lapangan, dapat dilihat bawah secara normatif UU, ITE dan KUHP, telah menyediakan dasar hukum yang cukup dalam menjerat pelaku *cyberstalking*, namun dalam praktik penegakan hukum masih terdapat kesenjangan antar norma dan implementasi.

Dari perspektif teori penegakan hukum, kondisi tersebut menunjukkan bahwa keberadaan norma hukum saja tidak cukup untuk menjamin efektifitas penegakan hukum, efektifitas juga dipengaruhi oleh faktor struktur hukum, sarana prasarana, serta kesadaran hukum masyarakat,

Dalam konteks ini, aparat kepolisian sering menghadapi kesulitan dalam mengidentifikasi pelaku karena karakteristik kejahatan *cyberstalking* yang bersifat anonim, serta selain itu alat bukti digital yang bersifat mudah diubah atau dihapus, juga menimbulkan tantangan tersendiri dalam proses pembuktian. Ketidaksesuaian antara norma hukum dan praktik penegakan hukum memiliki beberapa implikasi penting.

Secara sosiologis,meningkatnya kasus cyberstalking, menujukan bahwa tingkat literasi digital masih relatif rendah, banyak korban yang tidak menyadari bahwa, situasi yang mereka alami sekarang sangatlah berbahaya, dan jika tidak dilaporkan ke pihak yang berwenang bisa saja kejadian tersebut terjadi ke pejabat yang lain, hal ini menyebabkan pejabat menjadi kelompok yang rentan terhadap kejahatan *cyberstalking*.

Secara yuridis, kurangnya kesadaran pejabat untuk melaporkan tindakan tersebut, membuat pelaku merasa aman jika melakukan hal tersebut ke pejabat lain, dan kesulitan pembuktian dalam kasus *cyberstalking*, dapat menyebabkan banyak perkara tidak dapat dilanjutkan hingga tahap pengadilan,

Kondisi ini dapat menimbulkan kesan bahwa pejabat negara masih mementingkan nama baiknya dibandikan melapor ke pihak berwajib dan hukum belum mampu memberikan perlindungan yang optimal terhadap korban kejahatan *cyberstalking*.

Secara praktis, aparat penegak hukum memerlukan peningkatan kapisitas teknis, khususnya dalam bidang forensik digital dan pelacakan jejak elektronik. Tanpa dukungan teknologi dan sumber daya manusia yang memadai, penegakan hukum

terhadap kejahatan siber akan sulit dilakukan secara efektif.

Temuan penelitian ini menunjukkan bahwa pertanggungjawaban pidana terhadap pelaku penyebaran *cyberstalking* pada dasarnya telah memiliki landasan hukum yang kuat dalam UU ITE dan KUHP, namun efektifitas penerapannya masih menghadapi berbagai kandala teknis dan struktural.

Penelitian ini memberikan kontribusi penting dalam memahami bagaimana norma hukum yang bersifat abstrak diterapkan dalam praktik penegakan hukum di tingkat daerah. Selain itu, temuan ini juga menunjukkan perlunya pendekatan yang lebih komprehensif dalam penanggulangan kejahatan *cyberstalking*, tidak hanya melalui penegakan hukum yang represif tetapi juga melalui upaya preventif seperti peningkatan literasi digital masyarakat.

Faktor-Faktor Pengaruh Penerapan Pengaturan Tentang Tindakan Pidana Cyberstalking Terhadap Pejabat Penting

Secara menyeluruh, baik dari sisi regulasi, aparat penegak hukum, maupun kesadaran masyarakat, penerapan pengaturan tentang tindak pidana *cyberstalking* terhadap pejabat penting dipengaruhi oleh berbagai faktor yang saling berkaitan, baik dari aspek substansi hukum, struktur penegakan hukum, maupun budaya hukum masyarakat.

Dari segi substansi hukum, belum adanya pengaturan yang secara khusus mengatur *cyberstalking* menyebabkan penegak hukum masih bergantung pada ketentuan umum dalam Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik dan Undang-Undang Nomor 1 Tahun 2023 tentang Kitab Undang-Undang Hukum Pidana, sehingga berpotensi menimbulkan multitafsir dalam penerapannya. Selain itu, faktor struktur hukum juga berperan penting, di mana kemampuan dan pemahaman aparat penegak hukum terhadap kejahatan siber, termasuk keterampilan dalam digital forensik, masih belum merata, yang berdampak pada efektivitas penanganan perkara.

Di sisi lain, faktor sarana dan prasarana turut mempengaruhi, khususnya keterbatasan teknologi dalam melacak pelaku yang menggunakan identitas anonim atau sarana digital tertentu, sehingga menyulitkan proses pembuktian. Faktor budaya hukum masyarakat juga menjadi kendala, karena masih rendahnya kesadaran hukum serta kecenderungan untuk menganggap tindakan *cyberstalking* sebagai hal yang biasa di ruang digital, termasuk oleh pejabat sebagai korban yang terkadang enggan melaporkan kasus tersebut. Lebih lanjut, perkembangan teknologi informasi yang sangat pesat menyebabkan hukum sering tertinggal dalam mengantisipasi modus kejahatan baru, sehingga menciptakan celah bagi pelaku.

Selain itu, faktor politik dan kedudukan pejabat juga tidak dapat diabaikan, karena status pejabat penting dapat mempengaruhi proses penegakan hukum, baik dalam bentuk percepatan penanganan maupun potensi adanya intervensi kepentingan tertentu. Terakhir, faktor pembuktian menjadi aspek yang krusial, mengingat bukti digital dalam kasus *cyberstalking* mudah dihapus atau dimanipulasi serta memerlukan keahlian khusus untuk mengungkapnya secara sah di pengadilan. Dengan demikian, berbagai faktor tersebut menunjukkan bahwa penerapan pengaturan tindak pidana *cyberstalking* terhadap pejabat penting masih menghadapi tantangan yang kompleks dan memerlukan pembenahan.

Tantangan dan perlindungan korban diperlukan edukasi hukum pada masyarakat khususnya di Sulsel yang belum menyadari bahwa aktivitas "memantau" akun pejabat secara berlebihan disertai komentar intimidatif dapat berujung pidana.

Sosialisasi UU Pelindungan Data Pribadi (UU PDP): Jika *cyberstalking* melibatkan pengambilan data pribadi pejabat secara ilegal, pelaku juga dapat dijerat dengan UU PDP yang memiliki sanksi denda sangat berat.

SIMPULAN

Pengaturan tentang tindak pidana *cyberstalking*, secara normatif telah diatur dalam ketentuan UUD walapun belum ada pengaturan secara khusus mengenai tentang cyberstalking, menyebabkan penegakan hukum masi bergantung pada ketentuan umum dalam undang-undang nomor 11 tahun 2008 tentang informasi dan transaksi elektronik, dan undang-undang nomor 1 tahun 2023 tentang kitab undang-undang hukum pidana,

Penerapan pengaturan terhadap tindak pidana *cyberstalking* yang ditujukan kepada pejabat penting negara dipengaruhi oleh berbagai faktor yang bersifat kompleks dan saling berkaitan. Faktor utama terletak pada aspek substansi hukum, para pejabat negara tidak ingin melaporkan kasus yang mereka alami dikarenakan faktor yaitu, nama baik meraka, jabatan yang mereka duduki, dan informasi yang didapatkan oleh pelaku disebarkan, sehingga bisa mempengaruhi kepercayaan masyarakat kepada mereka, dan juga belum ada pengaturan khusus mengenai *cyber stalking* menyebabkan penegakan hukum masih bertumpu pada ketentuan umum dalam Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik dan Undang-Undang Nomor 1 Tahun 2023 tentang Kitab Undang-Undang Hukum Pidana, sehingga menimbulkan potensi multitafsir dalam implementasinya.

DAFTAR PUSTAKA

Andi Bau Mallarangeng, Andi Wahyuddin Nur, Martono, & Muhammad Syahbana. (2025). Penegakan Hukum Terhadap Penyebarluasan Foto Vulgar di Media Sosial Disertai Pemerasan dan Pengancaman di Kabupaten Wajo. *Legal Journal of Law*, 4(1), 65–76. Diambil dari https://jurnal.lamaddukelleng.ac.id/index.php/legal/article/view/128.

Andi Wahyuddin Nur, Rijal, B. M. D. M. ., Dewi Wahyuni Mustafa, & Nelvi. (2024). Tanggung Jawab Pelaksana Sistem Elektronik dalam Melindungi Informasi Pemakai Media Sosial Menurut Undang-undang Nomor 19 Tahun 2016 Mengenai Informasi dan Transaksi Elektronik. *Legal Journal of Law*, 3(1), 18–29. Diambil dari https://jurnal.lamaddukelleng.ac.id/index.php/legal/article/view/24

Anisah, A. P., & Nursman, Eko. (2024). Cyberstalking: Kejahatan Terhadap Perlindungan Data Pribadi Sebagai Pemicu Tindak Pidana. *Krtha Bhayangkara*, 16(1). https://doi.org/10.31599/krtha.v16i1.1203.

Azhari, M. R. (2019). Aspek pidana mayantara (cyberstalking). *Badamai Law Journal*, 4(1), 150-163.

Eka, Agung (ed). (Maret 9, 2026). Diskusi Publik AJI Makassar, Soroti Kekerasan dan Serangan Digital kepada Jurnalis. *www.gosulsel.com.* Diakses dari https://gosulsel.com/03/2026/diskusi-publik-aji-makassar-soroti-kekerasan-dan-serangan-digital-kepada-jurnalis/.

Djamil, M. N., & Djafar, T. M. (2016). Etika Publik Pejabat Negara dalam Penyelenggaraan Pemerintahan yang Bersih. *Jurnal Kajian Politik Dan Masalah Pembangunan*, 12(01), 1775-1760.

Fatimah, S. (2025). Penerapan Sanksi Pidana Terhadap Pelaku Tindak Pidana Cyberstalking Di Indonesia. *Journal Of Business Law Research*, 1(2), 308-328.

ICJR. (Januari 9, 2015). Mengkritik Bupati Gowa, Pasal 27 Ayat (3) UU ITE Kembali Disalahgunakan Untuk Membungkam Fadli. *Institute For Criminal Justice Reform,* diakses dari https://icjr.or.id/mengkritik-bupati-gowa-pasal-27-ayat-3-uu-ite-kembali-disalahgunakan-untuk-membungkam-fadli/.

Khoirul Huda, S. H. (2014). Pertanggungjawaban hukum tindakan mal-administrasi dalam pelayanan publik. *Jurnal Heritage*, 2(2), 30-42.

Mustameer, Hamdan. (2022). Penegakan Hukum Nasional dan Hukum Internasional Terhadap Kejahatan Cyber Espionage Pada Era Society 5.0. *Jurnal Yustika: Media Hukum dan Keadilan,* 25(1), 40-53. Diakses dari https://journal.ubaya.ac.id/index.php/yustika/article/view/5090.

Partisya, R. (2024). Pertanggungjawaban Pelaku Cyberstalking Sebagai Perbuatan Melawan Hukum Pidana Indonesia. *Jurnal Rectum*, 5(1), 342-354. doi:10.46930/jurnalrectum.v5i1.4766.

Rumlus, M. H., Kusmiadi, M. E., Rajab, A. M., & Pamungkas, A. C. (2023). Kebijakan Penangguangan Tindak Pidana Cyberstalking pada Media Elektronik. *Equality Before The Law*, 3(2). https://doi.org/10.36232/equalitybeforethelaw.v3i2.461.

Sulaeman, Yustiana, Martono, & Herawati. (2025). Perlindungan Hukum Terhadap Penyerbarluasan Data Pribadi Pelaku Pinjaman Online di Kabupaten Wajo. *Legal Journal of Law*, 4(1), 55–64. Diambil dari https://jurnal.lamaddukelleng.ac.id/index.php/legal/article/view/127.

Taufiq, M. (2021). Konsep dan sumber hukum: Analisis perbandingan sistem hukum Islam dan sistem hukum positif. *Istidlal: Jurnal Ekonomi Dan Hukum Islam*, 5(2), 87-98.