BAB VI
PENUTUP

A. Kesimpulan

Berdasarkan pembahasan yang telah dijelaskan dalam bab-bab sebelumnya, dapat disimpulkan bahwa disertasi ini mencapai kesimpulan sebagai berikut:

1. Penegakan hukum tindak pidana siber saat ini belum terlaksana secara maksimal, disebabkan penyidik kepolisian belum mampu melakukan penindakan berkaitan dengan kejahatan siber global seperti *phising, malware,* serangan *ransomware,* dan jenis kejahatan siber tersebut tidak masuk kedalam kejahatan siber sebagaimana UU ITE. Meskipun telah memiliki sejumlah regulasi seperti UU ITE dan KUHP, namun pesatnya perkembangan teknologi dan variasi modus kejahatan siber sering kali tidak sebanding dengan kemampuan regulasi dan aparat penegak hukum dalam meresponsnya secara cepat dan efektif, dikarenakan keterbatasan dalam hal kompetensi sumber daya manusia, minimnya fasilitas forensik digital, serta belum optimalnya koordinasi antar lembaga penegak hukum menyebabkan proses penanganan kasus siber seringkali lambat dan belum maksimal.
2. Urgensi penguatan pengaturan penyidik dalam penegakan hukum tindak pidana siber sangat penting untuk menjawab tantangan perkembangan teknologi informasi, dikarenakan kejahatan siber perlu ditangani lebih cepat, akurat, dan tuntas guna melindungi kepentingan nasional. Tindak pidana siber memiliki karakteristik lintas batas, menggunakan modus operandi yang canggih, serta melibatkan bukti digital yang rentan dan cepat berubah. Dalam kondisi ini,

keberadaan penyidik harus memiliki kewenangan yang jelas, kompetensi teknis yang tinggi, serta didukung oleh regulasi yang memadai menjadi kunci efektivitas penegakan hukum.

3. Konstruksi *rasio legis* dalam penguatan kewenangan penyidik dalam penegakan hukum tindak pidana siber di Indonesia didasarkan pada kebutuhan hukum yang adaptif terhadap dinamika kejahatan di ruang siber yang berkembang sangat cepat dan kompleks. Penguatan kewenangan penyidik secara normatif harus diarahkan pada pembentukan aturan yang lebih jelas, tegas, dan komprehensif mengenai batas-batas kewenangan, tata cara pengumpulan dan validasi bukti digital, serta mekanisme kerja sama antar-lembaga baik di dalam maupun luar negeri. *Rasio legis* ini mencerminkan perlunya penyidik tidak hanya diposisikan sebagai pelaksana hukum, tetapi juga sebagai aktor strategis dalam menjaga keamanan siber nasional. Oleh karena itu regulasi ke depan perlu menitikberatkan pada pemberian kewenangan yang jelas dan terukur bagi penegak hukum dalam menyelidiki, membuktikan, dan menangani kasus siber, serta didukung oleh infrastruktur kelembagaan dan teknologi yang memadai.

B. Saran

Berdasarkan kesimpulan tersebut, peneliti memberikan saran untuk pembaharuan hukum dengan memperkuat kewenangan penegak hukum terhadap kejahatan siber di masa depan, sebagai berikut:

1. Perlu adanya revisi regulasi terkait perluasan penafsiran yang jelas mengenai definisi jenis-jenis kejahatan siber yang bersifat global seperti *phising, malware,* serangan *ransomware,* serangan DdoS (*Distributed Denial of Service*), serangan

Man in the Middle (MITM), serangan *Zero-Da,* serangan terhadap identitas, serangan terhadap aplikasi *web*, masuk dalam Undang-Undang Republik Indonesia Nomor 1 Tahun 2024 Tentang Perubahan Kedua Atas Undang-Undang Republik Indonesia Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik.

2. Segera revisi regulasi untuk penguatan kewenangan Badan Siber dan Sandi Negara (BSSN) sebagai Penyidik Pegawai Negeri Sipil (PPNS) ke dalam Undang-Undang Republik Indonesia Nomor 1 Tahun 2024 Tentang Perubahan Kedua Atas Undang-Undang Republik Indonesia Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik, melalui perubahan Pasal 43 ayat (1) UU ITE, yang semula berbunyi:

> Selain Penyidik Pejabat Polisi Negara Republik Indonesia, Pejabat Pegawai Negeri Sipil tertentu di lingkungan Pemerintah yang lingkup tugas dan tanggung jawabnya di bidang Teknologi Informasi dan Transaksi Elektronik diberi wewenang khusus sebagai penyidik sebagaimana dimaksud dalam Undang-Undang tentang Hukum Acara Pidana untuk melakukan penyidikan tindak pidana di bidang Teknologi Informasi dan Transaksi Elektronik.

Dengan memperluas untuk melengkapi atau menambah menjadi norma Pasal 43 ayat (1) UU ITE, yang berbunyi:

> Selain Penyidik Pejabat Polisi Negara Republik Indonesia, Pejabat Pegawai Negeri Sipil tertentu di **Kementerian yang lingkup tugas dan tanggung jawabnya di bidang keamanan siber dan sandi** diberi wewenang khusus sebagai penyidik sebagaimana dimaksud dalam Undang-Undang tentang Hukum Acara Pidana untuk melakukan penyidikan tindak pidana di bidang Teknologi Informasi dan Transaksi Elektronik.

Selanjunya dalam Penjelasan Pasal 43 ayat (1) UU ITE semula:

> Yang dimaksud dengan "Pejabat Pegawai Negeri Sipil tertentu" adalah Pejabat Pegawai Negeri Sipil kementerian yang urusan pemerintahan di

bidang komunikasi dan informatika yang telah memenuhi persyaratan berdasarkan ketentuan peraturan perundang-undangan.

Menjadi

Yang dimaksud dengan "Pejabat Pegawai Negeri Sipil tertentu" adalah Pejabat Pegawai Negeri Sipil **Kementerian yang lingkup tugas dan tanggung jawabnya di bidang Komunikasi dan Informatika serta Badan Pemerintah yang lingkup tugas dan tanggung jawabnya di bidang keamana siber dan sandi** yang telah memenuhi persyaratan berdasarkan ketentuan peraturan perundang-undangan.

3. Para penegak hukum baik penyidik kepolisian maupun penyidik pegawai negeri sipil sebaiknya melakukan harmonisasi dan sinkronisasi pengaturan antar lembaga pemerintahan dan lembaga yang berwenang termasuk kerjasama dalam penegakan hukum tindak pidana siber di Indonesia.