BAB V

KESIMPULAN DAN SARAN

5.1 Kesimpulan

Undang-undang keamanan siber atau *Cybersecurity Law* (CSL) Tiongkok yang mulai berjalan efektif pada 1 Juni 2017, bertujuan untuk memperkuat tata kelola dunia maya melalui sejumlah inisiatif termasuk perlindungan khusus untuk infrastruktur informasi kritis, penyimpanan data secara lokal, dan peraturan pemerintah tentang keamanan siber di Tiongkok. Secara keseluruhan, CSL menunjukkan karakteristik khas dari Tiongkok. Undang-undang tersebut didasarkan pada konsep kedaulatan dunia maya dan menekankan keamanan atas aliran data yang bebas.

Dalam konteks CSL, beberapa kepentingan nasional muncul sebagai fokus utama. Pertama, Tiongkok memprioritaskan kedaulatan wilayahnya dalam domain siber. Konsep "*core interest*" menjadi landasan bagi kebijakan-kebijakan Tiongkok, dan dalam CSL, hal ini tercermin dalam upaya untuk menjaga kendali atas wilayah maya negaranya. Salah satu aspeknya adalah dengan mengatur arus data dan informasi yang masuk dan keluar dari wilayahnya serta melindungi infrastruktur informasi kritis. Ini mencerminkan tekad Tiongkok untuk mengendalikan dan melindungi wilayah maya negaranya.

Kedua, stabilitas politik merupakan prioritas utama bagi Tiongkok, yang dikelola oleh Partai Komunis Tiongkok. CSL memberikan pemerintah alat yang lebih kuat untuk mengawasi dan mengendalikan komunikasi *online* serta merespons

ancaman terhadap stabilitas politik. Dalam konteks ini, kontrol informasi menjadi elemen penting yang memungkinkan pemerintah Tiongkok untuk memantau dan mengatur informasi yang diterima oleh masyarakat sesuai dengan pandangan pemerintah.

Ketiga, upaya Tiongkok untuk mengurangi ketergantungannya pada teknologi asing juga tercermin dalam CSL. Melalui kebijakan yang mendorong perusahaan asing untuk menempatkan server data di dalam wilayah Tiongkok, Tiongkok berusaha untuk mengembangkan teknologi domestik dan mengurangi ketergantungannya pada teknologi asing. Selain itu, kolaborasi dengan perusahaan teknologi informasi domestik membantu menciptakan standar teknologi yang sesuai dengan kebutuhan nasionalnya.

Dalam keseluruhan, CSL adalah instrumen yang penting dalam upaya Tiongkok untuk mencapai kepentingan nasionalnya dalam kedaulatan wilayah siber, stabilitas politik, dan pengembangan teknologi, meskipun kebijakan tersebut juga menciptakan ketegangan dalam hubungan internasional.

CSL juga telah mengubah lanskap keamanan siber negara tersebut secara signifikan. Sebelumnya, terdapat sejumlah undang-undang dan peraturan yang mengatur aspek keamanan sistem dan infrastruktur jaringan, namun, CSL memberikan fondasi hukum yang lebih komprehensif dan terintegrasi untuk menghadapi tantangan semakin rumit dalam dunia maya. Pentingnya kedaulatan data menjadi poin fokus dalam CSL, dengan perusahaan yang beroperasi di Tiongkok diwajibkan untuk menyimpan data penting di dalam negeri dan mematuhi

regulasi keamanan data yang ditetapkan oleh pemerintah. Hal ini mencerminkan tekad Tiongkok untuk mengendalikan dan melindungi data sensitif yang berkaitan dengan kepentingan nasional.

Selain itu, CSL juga telah meningkatkan pengawasan terhadap konten *online*. Tiongkok telah memiliki sistem sensor dan pengawasan *online* yang ketat sebelum CSL, dan dengan pemberlakuan CSL, negara ini semakin memperluas kendali atas konten dan aktivitas *online*. Hal ini mencakup aturan-aturan terkait keamanan data, perlindungan informasi pribadi, moderasi konten, dan tinjauan keamanan siber.

Pengawasan ini diberikan kepada *Cyberspace Administration of China* (CAC), regulator utama pengawasan konten *online* di Tiongkok, yang kini memiliki kewenangan dan tanggung jawab yang lebih besar untuk memantau, memeriksa, dan memberikan sanksi terhadap pelanggaran hukum. CAC dapat memerintahkan operator jaringan untuk menghapus atau memblokir konten yang melanggar hukum, serta mengenakan denda atau mencabut lisensi bagi pelanggar serius.

Dengan demikian, diberlakukannya CSL telah mengubah cara Tiongkok mengelola dan mengatur lingkungan keamanan siber dan aktivitas *online*. Hal ini mencerminkan upaya Tiongkok untuk menjaga kedaulatan siber, melindungi data penting, dan mengontrol aliran informasi secara ketat sesuai dengan kepentingan nasionalnya.

Beberapa isi dan aspek yang diatur dalam CSL Tiongkok yang disoroti AS yang mengacu dari dokumen suatu laporan yang disampaikan oleh pemerintah AS

kepada Organisasi Perdagangan Dunia (WTO) yaitu; konsep infrastruktur informasi kritis; penyimpanan data lokal; ketentuan baru tentang perlindungan jaringan; pengawasan pemerintah, tinjauan keamanan, dan dukungan teknis.

Dalam respon awal AS terhadap CSL, AS dan kelompok bisnis asing telah dengan tegas mengkritik CSL, menyatakan keprihatan dan keberatan mereka terhadap berbagai ketentuannya. AS merasa bahwa CSL memiliki potensi untuk menghambat perdagangan, investasi, inovasi, dan komunikasi lintas batas yang sangat penting bagi bisnis internasional. Di sisi lain, Tiongkok menekankan pentingnya keamanan nasional dan kontrol atas data dalam negeri, dan mereka mengklaim bahwa CSL sejalan dengan praktik internasional.

Terdapat dua dokumen terkait bagaimana AS menunjukkan keberatannya mengenai beberapa ketentuan yang diatur dalam CSL, pertama, melalui dokumen S/C/W/374 yang dirilis pada tanggal 26 September 2017 AS menyoroti beberapa hal dalam CSL yang mana AS menyebutkan bahwa CSL hanya akan menganggu, menghalangi, dan melarang transfer informasi lintas batas dalam kegiatan bisnis pada umumnya. Dokumen kedua melalui S/C/W/376 yang dirilis pada tanggal 23 Februari 2018, dokumen tersebut merupakan komunikasi lanjutan AS yang mencakup topik yang sama. Dalam hal ini, terlihat bahwa respon awal AS terhadap implementasi Tiongkok terbilang cukup aktif.

Dalam menanggapi hal ini, Tiongkok telah memposting melalui akun media sosial resmi yang tampaknya tidak disampaikan melalui media pemerintah, tanggapan tersebut semacam klarifikasi Tiongkok yang menyebutkan bahwa

mereka telah mengeluarkan beberapa dokumen dan pedoman dan telah melakukan revisi antara draf pertama dan draf kedua dalam rangka merespons keprihatinan asing termasuk AS. Tiongkok juga mengakui bahwa dalam implementasi CSL terdapat berbagai pemangku kepentingan yang mewakili pendekatan dan kepentingan yang berbeda, yang menyebabkan kurangnya kesepakatan dalam birokrasi terkait penegakan hukum terhadap perusahaan multinasional yang beroperasi di Tiongkok.

Hingga pada akhirnya, AS telah memutuskan beberapa kebijakan terkait CSL, pada tahun 2017, Presiden Amerika Serikat, Donald Trump, memulai penyelidikan terhadap Tiongkok terkait pelanggaran hak kekayaan intelektual dan transfer teknologi yang dianggap tidak adil oleh Tiongkok. Penyelidikan ini dimulai berdasarkan Section 301 dari Trade Act tahun 1974 melalui lembaga pemerintah federal AS yang bertanggung jawab untuk mengembangkan dan mempromosikan kebijakan perdagangan AS, yaitu USTR.

Hasil penyelidikan USTR menemukan bahwa Tiongkok terlibat dalam praktik yang merugikan perusahaan AS, termasuk persyaratan usaha patungan, pembatasan investasi asing, tekanan untuk mentransfer teknologi, dan serangan siber.

Sebagai respons terhadap temuan ini, AS mengenakan tarif tambahan pada produk Tiongkok sekitar $50 miliar, terutama produk yang terkait dengan teknologi industri. Tiongkok merespons dengan menerapkan tarif tambahan pada produk impor AS.

AS juga mengeluarkan perintah eksekutif untuk melindungi rantai pasokan teknologi informasi dan komunikasi (TIK) dari ancaman asing, yang terutama ditujukan kepada perusahaan teknologi Tiongkok seperti Huawei. Pada tahun 2021, Presiden Joe Biden menggantikan perintah eksekutif sebelumnya dengan pendekatan yang lebih berbasis bukti, tetapi tetap mempertahankan larangan terhadap aplikasi perangkat lunak terhubung yang dimiliki atau dikendalikan oleh musuh asing, termasuk Tiongkok

Diberlakukannya Undang-Undang Keamanan Siber (CSL) Tiongkok telah memicu perdebatan intensif dalam hubungan bilateral antara Tiongkok dan Amerika Serikat. Perdebatan yang terjadi antara kedua negara tersebut juga mencerminkan erbedaan mendasar dalam pendekatan Tiongkok dan AS terhadap tata kelola keamanan siber. Tiongkok menganut prinsip *cyber sovereignty*, yang mengutamakan kontrol pemerintah atas ruang siber dalam wilayahnya. Di sisi lain, AS mendorong konsep ruang siber yang bebas dan terbuka, mendukung kerja sama internasional, dan menekankan pentingnya norma-norma internasional dalam menjaga keamanan siber global.

Akibatnya, hubungan bilateral antara Tiongkok dan AS, terutama dalam konteks keamanan siber dan perdagangan, mengalami ketegangan yang signifikan. Kebijakan dan respon agresif dari kedua negara ini telah berdampak negatif pada hubungan perdagangan dan investasi mereka. Ini adalah contoh konkret dari persaingan dan ketegangan yang ada antara kedua negara, dan kebijakan CSL telah menjadi salah satu titik fokus utama dalam ketegangan ini, terutama dalam konteks keamanan siber. Oleh karena itu, dengan diberlakukannya CSL, hubungan bilateral

Tiongkok-AS telah memburuk, dan ini menjadi tantangan besar dalam upaya mencapai kesepakatan dan kerja sama di masa mendatang.

5.2 Saran

5.2.1 Saran Teoritis

Berikut adalah beberapa saran teoritis yang diharapkan dapat memberikan pandangan yang lebih mendalam dan variatif bagi penelitian yang memiliki ketertarikan topik yang sama:

a. Penelitian selanjutnya dapat menulusuri potensi yang sekiranya dapat mengurangi ketegangan melalui dialog konstruktif dan kerja sama dalam upaya meningkatkan hubungan bilateral Tiongkok dan AS dalam bidang keamanan siber.
b. Penelitian selanjutnya dapat membandingkan pendekatan antara Tiongkok dan AS terhadap hukum keamanan siber. Hal ini dapat mengidentifikasi perbedaan dalam definisi keamanan siber, penegakan hukum, dan dampaknya terhadap perusahaan dan individu di kedua negara
c. Penelitian selanjutnya dapat mempertimbangkan pendekatan kebijakan yang lebih luas, selain hukum keamanan siber, apakah ada regulasi lain yang memiliki dampak serupa terhadap hubungan bilateral? Misalnya, kebijakan tentang investasi, teknologi, atau kekayaan intelektual.

5.2.1 Saran Praktis

Diberlakukannya Undang-Undang Keamanan Siber (CSL) Tiongkok telah memicu perdebatan intensif dalam hubungan bilateral antara Tiongkok dan Amerika Serikat. Perdebatan yang terjadi antara kedua negara tersebut juga mencerminkan perbedaan mendasar dalam pendekatan Tiongkok dan AS terhadap tata kelola keamanan siber. Berikut adalah beberapa saran praktis terkait implikasi kebijakan *cybersecurity law* Tiongkok terhadap hubungan bilateral Tiongkok-Amerika Serikat:

a. Meningkatkan dialog dan kerja sama: Kedua negara perlu meningkatkan dialog dan kerja sama dalam bidang keamanan siber untuk mengurangi ketegangan dan meningkatkan kepercayaan antara kedua belah pihak. Hal ini dapat dilakukan melalui pertemuan antara pejabat pemerintah, pertukaran ahli keamanan siber, dan kerja sama dalam investigasi kejahatan siber.
b. Menghindari tindakan yang merugikan: Kedua negara perlu menghindari tindakan yang merugikan satu sama lain dalam bidang keamanan siber. Tindakan seperti serangan siber dan pencurian data dapat memperburuk hubungan bilateral dan meningkatkan ketegangan antara kedua negara.
c. Membangun kepercayaan: Kedua negara perlu membangun kepercayaan antara satu sama lain dalam bidang keamanan siber. Hal ini dapat dilakukan melalui pertukaran informasi tentang ancaman keamanan siber, kerja sama dalam penanganan kejahatan siber, dan pengembangan standar keamanan siber yang dapat diterima oleh kedua belah pihak.

d. Menghormati kedaulatan dan privasi: Kedua negara perlu menghormati kedaulatan dan privasi satu sama lain dalam bidang keamanan siber. Hal ini dapat dilakukan dengan menghindari serangan siber yang melanggar kedaulatan negara dan menghormati privasi data pengguna.
e. Meningkatkan transparansi: Kedua negara perlu meningkatkan transparansi dalam bidang keamanan siber. Hal ini dapat dilakukan dengan mempublikasikan informasi tentang kebijakan keamanan siber dan tindakan yang diambil oleh kedua negara untuk mengatasi ancaman keamanan siber.

Dalam kesimpulannya, perdebatan antara Tiongkok dan Amerika Serikat tentang kebijakan keamanan siber mencerminkan perbedaan mendasar dalam pendekatan kedua negara terhadap tata kelola keamanan siber. Untuk mengurangi ketegangan dan meningkatkan kepercayaan antara kedua belah pihak, kedua negara perlu meningkatkan dialog dan kerja sama, menghindari tindakan yang merugikan, membangun kepercayaan, menghormati kedaulatan dan privasi, serta meningkatkan transparansi dalam bidang keamanan siber.