Jurnal Hukum dan Keadilan
P-ISSN :
E-ISSN :
https://ojs.jurnaladsiindonesia.com/index.php/hk

ARTIKEL RISET

Kebijakan Penal dan Non – Penal dalam Penanggulangan Kejahatan Siber

[1]Syamsul Bachri
[1] Program Pascasarjana, Universitas Indonesia Timur
Email : syamsulbachri1975@gmail.com

ABSTRAK

Perkembangan teknologi informasi dan komunikasi telah mendorong transformasi digital di berbagai sektor kehidupan masyarakat. Di sisi lain, perkembangan tersebut juga melahirkan berbagai bentuk kejahatan siber (cybercrime) yang semakin kompleks, transnasional, dan sulit dideteksi menggunakan pendekatan penegakan hukum konvensional. Kejahatan siber tidak hanya mengancam keamanan data dan sistem elektronik, tetapi juga berdampak terhadap stabilitas ekonomi, keamanan nasional, serta perlindungan hak asasi manusia. Oleh karena itu, penanggulangan kejahatan siber memerlukan kebijakan hukum pidana (penal policy) yang efektif sekaligus didukung oleh kebijakan di luar hukum pidana (non-penal policy) yang bersifat preventif. Penelitian ini bertujuan menganalisis implementasi kebijakan penal dan non-penal dalam penanggulangan kejahatan siber di Indonesia serta merumuskan model kebijakan yang lebih integratif. Penelitian menggunakan metode hukum normatif dengan pendekatan perundang-undangan (statute approach), pendekatan konseptual (conceptual approach), dan pendekatan perbandingan (comparative approach). Data diperoleh melalui studi kepustakaan terhadap peraturan perundang-undangan, literatur, serta jurnal ilmiah. Hasil penelitian menunjukkan bahwa kebijakan penal melalui pengaturan dalam Undang-Undang Informasi dan Transaksi Elektronik, Kitab Undang-Undang Hukum Pidana Nasional, serta berbagai regulasi sektoral telah memberikan dasar hukum yang cukup dalam penindakan kejahatan siber. Namun demikian, pendekatan represif tersebut belum mampu mengimbangi perkembangan modus operandi kejahatan digital. Oleh sebab itu, kebijakan non-penal berupa peningkatan literasi digital, penguatan keamanan siber nasional, kolaborasi lintas sektor, pengembangan kapasitas aparat penegak hukum, dan kerja sama internasional menjadi faktor yang sangat menentukan efektivitas penanggulangan kejahatan siber di masa mendatan

Kata kunci: Kebijakan Penal; Kebijakan Non-Penal; Kejahatan Siber; Cybercrime; Hukum Pidana

ABSTRACT

The rapid advancement of information and communication technology has significantly transformed various aspects of modern society. However, this transformation has also generated increasingly sophisticated forms of cybercrime that pose serious threats to individuals, businesses, and national security. Cybercrime has evolved into a transnational crime characterized by anonymity, technological complexity, and cross-border operations, making conventional criminal law enforcement insufficient. Consequently, combating cybercrime requires not only effective penal policies but also comprehensive non-penal measures emphasizing prevention and public participation. This research aims to analyze the implementation of penal and non-penal policies in combating cybercrime in Indonesia and to formulate an integrated policy framework. The study employs normative legal research using statutory, conceptual, and comparative approaches. Data were collected through library research involving legislation, legal doctrines, books, and scientific journals. The findings indicate that Indonesia has established an adequate legal framework through the Electronic Information and Transactions Law, the new Criminal Code, and other sectoral regulations. Nevertheless, punitive approaches alone remain insufficient due to the rapid evolution of cyber threats. Therefore, preventive strategies such as digital literacy enhancement, cybersecurity awareness, institutional strengthening, law enforcement capacity building, and international cooperation are essential to achieving comprehensive cybercrime prevention.

Keywords: *Penal Policy; Non-Penal Policy; Cybercrime; Criminal Law; Cybersecurity*

Jurnal Hukum dan Keadilan
P-ISSN :
E-ISSN :
https://ojs.jurnaladsiindonesia.com/index.php/hk

1. PENDAHULUAN

Transformasi digital telah mengubah berbagai aspek kehidupan masyarakat, mulai dari ekonomi, pendidikan, pemerintahan, pelayanan publik hingga interaksi sosial. Perkembangan teknologi informasi memberikan manfaat berupa efisiensi, kemudahan akses informasi, peningkatan produktivitas, dan konektivitas global. Namun, ketergantungan terhadap teknologi juga meningkatkan risiko penyalahgunaan teknologi untuk melakukan tindak pidana. Kejahatan siber (cybercrime) merupakan perbuatan melawan hukum yang menggunakan komputer, jaringan komputer, sistem elektronik, atau internet sebagai sarana maupun sasaran kejahatan (Laudon & Laudon, 2022; Wall, 2007). Cybercrime memiliki karakteristik berbeda dari kejahatan konvensional karena bersifat lintas batas negara, menggunakan identitas anonim, memanfaatkan teknologi yang berkembang cepat, dan melibatkan jaringan pelaku lintas negara (Brenner, 2010). Perkembangan layanan digital seperti e-commerce, internet banking, financial technology, media sosial, cloud computing, dan kecerdasan buatan turut memperluas peluang terjadinya kejahatan siber (Yar, 2019). Bentuknya meliputi hacking, pencurian identitas, penipuan daring, malware, phishing, ransomware, perjudian daring, eksploitasi seksual terhadap anak, serta pencurian data pribadi. Dampaknya tidak hanya merugikan individu dan dunia usaha, tetapi juga dapat mengganggu pelayanan publik, keamanan nasional, dan infrastruktur kritis seperti perbankan, rumah sakit, jaringan listrik, dan sistem pemerintahan (Clough, 2015).

Perkembangan tersebut menjadi tantangan bagi sistem hukum pidana Indonesia yang pada awalnya lebih banyak dirancang untuk menghadapi kejahatan konvensional. Cybercrime membutuhkan pengaturan yang adaptif, khususnya terkait pembuktian elektronik, identifikasi pelaku, penyitaan data digital, dan kerja sama lintas negara (Brenner, 2010). Indonesia telah merespons perkembangan tersebut melalui berbagai instrumen hukum, antara lain Undang-Undang Nomor 1 Tahun 2024 tentang perubahan atas Undang-Undang Informasi dan Transaksi Elektronik, Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi, Undang-Undang Nomor 1 Tahun 2023 tentang Kitab Undang-Undang Hukum Pidana, serta regulasi sektoral mengenai keamanan siber dan sistem elektronik.

Meskipun kerangka hukum pidana telah berkembang, pendekatan represif belum sepenuhnya mampu menghadapi dinamika cybercrime. Kebijakan penal pada dasarnya bekerja melalui kriminalisasi, penyidikan, penuntutan, peradilan, dan pemidanaan, sehingga cenderung bersifat represif setelah kejahatan terjadi. Barda Nawawi Arief menegaskan bahwa penanggulangan kejahatan tidak cukup menggunakan sarana hukum pidana, tetapi perlu dipadukan dengan kebijakan sosial yang bersifat preventif (Arief, 2018). Oleh karena itu, kebijakan non-penal diperlukan melalui peningkatan literasi digital, penguatan keamanan informasi, peningkatan kapasitas kelembagaan dan aparat penegak hukum, pengawasan teknologi, serta partisipasi masyarakat. Pendekatan integral antara kebijakan penal dan non-penal juga berkembang dalam konteks internasional melalui kerja sama dan harmonisasi hukum, termasuk Convention on Cybercrime (Budapest Convention). Pendekatan tersebut menunjukkan bahwa penanggulangan cybercrime membutuhkan sinergi antara hukum, teknologi, kelembagaan, pendidikan, dan kerja sama internasional. Dengan demikian, kebijakan penal dan non-penal bukanlah pendekatan yang saling menggantikan, melainkan saling melengkapi untuk membangun sistem keamanan siber yang efektif.

Permasalahan utama penelitian ini berangkat dari masih adanya kesenjangan antara perkembangan cybercrime dan kemampuan sistem hukum dalam meresponsnya. Rendahnya literasi digital, lemahnya keamanan informasi, kurangnya koordinasi antarinstansi, keterbatasan sumber daya manusia di bidang forensik digital, serta hambatan kerja sama internasional menjadi faktor yang memperbesar kerentanan terhadap kejahatan siber (Clough, 2015). Dalam perspektif kebijakan kriminal, Marc Ancel memandang penanggulangan kejahatan sebagai bagian dari kebijakan sosial

yang menggunakan sarana penal dan non-penal. Pandangan tersebut sejalan dengan Barda Nawawi Arief yang menempatkan hukum pidana sebagai salah satu instrumen dalam perlindungan masyarakat (social defence). Sementara itu, Hoefnagels menekankan pentingnya penerapan hukum pidana, pencegahan tanpa pidana, serta pembentukan kesadaran masyarakat dalam penanggulangan kejahatan.

Penelitian mengenai cybercrime telah banyak membahas efektivitas Undang-Undang Informasi dan Transaksi Elektronik, pertanggungjawaban pidana, perlindungan data pribadi, dan pembuktian elektronik. Namun, masih terdapat ruang penelitian mengenai integrasi kebijakan penal dan non-penal sebagai model kebijakan kriminal yang terpadu. Kebaruan penelitian ini terletak pada analisis harmonisasi kedua kebijakan tersebut dalam membangun sistem penanggulangan cybercrime yang integratif, dengan memperkuat sinergi antara aparat penegak hukum, pemerintah, sektor swasta, akademisi, dan masyarakat.

Penelitian ini bertujuan menganalisis pengaturan kebijakan penal dalam hukum positif Indonesia, mengkaji implementasi kebijakan non-penal dalam pencegahan cybercrime, serta merumuskan model kebijakan kriminal yang integratif dan adaptif terhadap perkembangan teknologi informasi. Secara teoritis, penelitian diharapkan memperkaya kajian hukum pidana, khususnya kebijakan kriminal dan hukum siber. Secara praktis, hasil penelitian diharapkan dapat menjadi masukan bagi pembentuk undang-undang, aparat penegak hukum, BSSN, penyelenggara sistem elektronik, dan pemangku kepentingan lainnya.

Kerangka pemikiran penelitian menggunakan teori kebijakan kriminal (criminal policy) Marc Ancel, teori perlindungan masyarakat (social defence) Barda Nawawi Arief, teori sistem hukum Lawrence M. Friedman yang menekankan hubungan antara substansi, struktur, dan budaya hukum, serta teori pencegahan kejahatan (crime prevention theory) G. Peter Hoefnagels. Keempat teori tersebut menjadi dasar untuk menganalisis efektivitas kebijakan penal dan non-penal serta merumuskan model penanggulangan cybercrime yang komprehensif, terpadu, dan berkelanjutan.

2. METODE

Penelitian ini menggunakan metode penelitian hukum normatif (normative legal research), yaitu penelitian yang menempatkan hukum sebagai norma atau kaidah yang berlaku dalam sistem hukum positif serta mengkajinya melalui pendekatan terhadap peraturan perundang-undangan, doktrin, asas hukum, putusan pengadilan, dan berbagai literatur ilmiah yang relevan. Penelitian hukum normatif dipilih karena fokus penelitian diarahkan pada analisis kebijakan penal dan non-penal dalam penanggulangan kejahatan siber berdasarkan ketentuan hukum positif Indonesia serta perkembangan teori kebijakan kriminal. Menurut Soerjono Soekanto dan Sri Mamudji (2019), penelitian hukum normatif bertujuan mengkaji asas, sistematika, taraf sinkronisasi, sejarah, serta perbandingan hukum melalui studi kepustakaan sebagai sumber data utama.

Pendekatan utama yang digunakan adalah pendekatan perundang-undangan (statute approach), yaitu dengan menelaah berbagai peraturan perundang-undangan yang berkaitan dengan penanggulangan kejahatan siber. Peraturan yang menjadi objek kajian meliputi Undang-Undang Dasar Negara Republik Indonesia Tahun 1945, Undang-Undang Nomor 1 Tahun 2023 tentang Kitab Undang-Undang Hukum Pidana, Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi, serta berbagai peraturan pelaksana yang berkaitan dengan keamanan siber, penyelenggaraan sistem elektronik, dan perlindungan data. Pendekatan ini bertujuan untuk mengetahui kesesuaian norma hukum yang berlaku dengan kebutuhan penanggulangan cybercrime yang terus berkembang. Selain pendekatan perundang-undangan, penelitian ini menggunakan pendekatan konseptual (conceptual approach). Pendekatan konseptual

dilakukan dengan mengkaji berbagai teori dan doktrin hukum yang berkembang dalam literatur mengenai kebijakan kriminal (criminal policy), kebijakan penal (penal policy), kebijakan non-penal (non-penal policy), hukum pidana, hukum siber (cyber law), serta teori pencegahan kejahatan (crime prevention). Pendekatan ini penting untuk memberikan landasan teoretis dalam menganalisis efektivitas kebijakan hukum yang telah diterapkan di Indonesia sekaligus merumuskan model kebijakan yang lebih adaptif terhadap perkembangan teknologi informasi.

Selanjutnya, penelitian ini juga menerapkan pendekatan perbandingan (comparative approach) dengan membandingkan pengaturan dan kebijakan penanggulangan kejahatan siber di Indonesia dengan berbagai instrumen internasional maupun praktik beberapa negara lain. Instrumen internasional yang menjadi bahan analisis antara lain Convention on Cybercrime (Budapest Convention), rekomendasi Perserikatan Bangsa-Bangsa mengenai cybercrime, serta berbagai praktik terbaik (best practices) dalam pengembangan kebijakan keamanan siber. Pendekatan perbandingan dimaksudkan untuk memperoleh gambaran mengenai perkembangan hukum internasional serta kemungkinan harmonisasi pengaturan hukum nasional dengan standar global.

Bahan hukum yang digunakan dalam penelitian ini terdiri atas bahan hukum primer, bahan hukum sekunder, dan bahan hukum tersier. Bahan hukum primer meliputi peraturan perundang-undangan, konvensi internasional, dan dokumen resmi pemerintah yang berkaitan dengan penanggulangan kejahatan siber. Bahan hukum sekunder terdiri atas buku-buku ilmiah, artikel jurnal nasional dan internasional, hasil penelitian, disertasi, tesis, prosiding ilmiah, serta pendapat para ahli yang membahas hukum pidana, kebijakan kriminal, keamanan siber, dan teknologi informasi. Adapun bahan hukum tersier berupa kamus hukum, ensiklopedia hukum, indeks peraturan perundang-undangan, dan sumber referensi lainnya yang mendukung penafsiran terhadap bahan hukum primer dan sekunder. Teknik pengumpulan bahan hukum dilakukan melalui studi kepustakaan (library research), yaitu dengan menginventarisasi, mengidentifikasi, dan mengkaji berbagai dokumen hukum maupun literatur ilmiah yang relevan dengan objek penelitian. Studi kepustakaan dilakukan secara sistematis terhadap berbagai sumber yang memiliki otoritas akademik sehingga mampu memberikan landasan teoritis dan normatif dalam menjawab rumusan masalah penelitian. Pengumpulan data juga dilakukan melalui penelusuran jurnal ilmiah yang telah dipublikasikan pada pangkalan data nasional maupun internasional untuk memperoleh perkembangan terkini mengenai kebijakan penanggulangan cybercrime.

Analisis bahan hukum dalam penelitian ini menggunakan metode analisis kualitatif dengan pendekatan deskriptif-analitis. Analisis deskriptif dilakukan untuk menggambarkan secara sistematis mengenai pengaturan hukum yang berlaku, bentuk kebijakan penal dan non-penal, serta implementasinya dalam penanggulangan kejahatan siber. Selanjutnya, analisis dilakukan secara normatif melalui proses interpretasi terhadap ketentuan hukum, asas hukum, teori hukum, dan doktrin yang berkembang guna memperoleh argumentasi hukum yang komprehensif. Hasil analisis kemudian disusun secara deduktif, yaitu menarik kesimpulan dari ketentuan hukum yang bersifat umum menuju penyelesaian terhadap permasalahan yang bersifat khusus.

Dalam rangka menjaga validitas penelitian, digunakan teknik triangulasi sumber hukum, yaitu membandingkan berbagai ketentuan peraturan perundang-undangan dengan doktrin para ahli, hasil penelitian terdahulu, serta perkembangan praktik penegakan hukum di bidang kejahatan siber. Triangulasi ini bertujuan menghasilkan analisis yang objektif dan dapat dipertanggungjawabkan secara akademik. Selain itu, penelitian juga memperhatikan perkembangan kebijakan keamanan siber global sehingga rekomendasi yang dihasilkan tidak hanya sesuai dengan sistem hukum nasional, tetapi juga relevan dengan dinamika hukum internasional. Dengan metode tersebut, penelitian diharapkan mampu memberikan analisis yang komprehensif mengenai efektivitas kebijakan penal dan non-penal dalam penanggulangan kejahatan siber di Indonesia serta merumuskan model kebijakan kriminal yang lebih integratif, adaptif, dan berorientasi pada perlindungan masyarakat di era digital.

3. HASIL DAN PEMBAHASAN

3.1 Kebijakan Penal dalam Penanggulangan Kejahatan Siber di Indonesia

Kebijakan penal (penal policy) merupakan bagian integral dari kebijakan kriminal (criminal policy) yang menggunakan hukum pidana sebagai instrumen utama dalam menanggulangi kejahatan. Dalam perspektif hukum pidana modern, kebijakan penal tidak hanya berkaitan dengan pemberian sanksi pidana kepada pelaku, tetapi juga mencakup proses kriminalisasi, penegakan hukum, pemidanaan, serta pelaksanaan pidana sebagai satu kesatuan sistem perlindungan masyarakat. Barda Nawawi Arief menjelaskan bahwa kebijakan penal merupakan upaya rasional negara dalam menggunakan hukum pidana sebagai sarana untuk mencapai tujuan perlindungan masyarakat (social defence) sekaligus mewujudkan kesejahteraan sosial (social welfare). Dengan demikian, kebijakan penal dalam penanggulangan kejahatan siber tidak hanya berfungsi sebagai instrumen represif, tetapi juga sebagai mekanisme untuk menciptakan kepastian hukum, efek jera, dan perlindungan terhadap kepentingan masyarakat di ruang digital.

Perkembangan teknologi informasi telah mengubah karakteristik tindak pidana yang semula didominasi oleh kejahatan konvensional menjadi kejahatan berbasis teknologi informasi (technology-enabled crime). Cybercrime memiliki karakteristik yang berbeda dibandingkan tindak pidana konvensional karena dilakukan melalui jaringan komputer, menggunakan identitas anonim, memanfaatkan kelemahan sistem elektronik, serta tidak mengenal batas yurisdiksi negara (borderless crime). Karakteristik tersebut menyebabkan pendekatan hukum pidana konvensional sering kali menghadapi kesulitan dalam proses pembuktian, identifikasi pelaku, penangkapan, hingga pelaksanaan putusan pengadilan. Oleh sebab itu, pembentukan kebijakan penal menjadi kebutuhan mendesak agar sistem hukum mampu mengikuti perkembangan teknologi informasi yang sangat dinamis.

Dalam konteks Indonesia, kebijakan penal terhadap kejahatan siber berkembang seiring meningkatnya pemanfaatan internet dalam berbagai aspek kehidupan. Sebelum lahirnya regulasi khusus mengenai informasi dan transaksi elektronik, berbagai bentuk kejahatan siber hanya dapat dijerat menggunakan ketentuan dalam Kitab Undang-Undang Hukum Pidana (KUHP) yang pada dasarnya disusun untuk mengatur kejahatan konvensional. Kondisi tersebut menimbulkan berbagai kendala karena banyak bentuk cybercrime belum memiliki rumusan delik yang secara eksplisit mengakomodasi karakteristik tindak pidana berbasis teknologi informasi. Akibatnya, proses penegakan hukum sering kali menghadapi kesulitan dalam menerapkan asas legalitas (nullum crimen sine lege) karena belum tersedia dasar hukum yang spesifik.

Perubahan mendasar terjadi dengan diundangkannya Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, yang kemudian mengalami beberapa perubahan dan terakhir disempurnakan melalui Undang-Undang Nomor 1 Tahun 2024. Kehadiran undang-undang tersebut menjadi tonggak penting dalam perkembangan hukum siber di Indonesia karena memberikan dasar hukum yang lebih komprehensif mengenai penyelenggaraan sistem elektronik, transaksi elektronik, alat bukti elektronik, serta berbagai bentuk tindak pidana yang dilakukan melalui media elektronik. Melalui regulasi tersebut, negara memperluas ruang lingkup perlindungan hukum terhadap masyarakat dengan mengkriminalisasi berbagai perbuatan yang sebelumnya belum diatur secara tegas dalam hukum pidana nasional. Kebijakan kriminalisasi yang terdapat dalam Undang-Undang Informasi dan Transaksi Elektronik mencakup berbagai bentuk kejahatan siber, antara lain akses ilegal terhadap sistem elektronik (illegal access), intersepsi ilegal (illegal interception), gangguan terhadap sistem elektronik (system interference), manipulasi data elektronik (data interference), penyebaran informasi bermuatan melanggar hukum, penipuan elektronik, perjudian daring, pemerasan melalui media elektronik, distribusi konten yang melanggar kesusilaan, serta berbagai bentuk penyalahgunaan

teknologi informasi lainnya. Kriminalisasi tersebut menunjukkan bahwa pembentuk undang-undang telah berupaya mengakomodasi perkembangan modus operandi cybercrime yang semakin kompleks.

Selain Undang-Undang Informasi dan Transaksi Elektronik, kebijakan penal juga diperkuat melalui Undang-Undang Nomor 1 Tahun 2023 tentang Kitab Undang-Undang Hukum Pidana. Meskipun KUHP Nasional tidak mengatur secara rinci seluruh bentuk kejahatan siber, berbagai ketentuan mengenai tindak pidana terhadap harta benda, pemalsuan, penipuan, pencurian data, serta pertanggungjawaban pidana korporasi memberikan dasar hukum yang dapat diterapkan terhadap perkembangan bentuk kejahatan digital. Pembaruan KUHP menunjukkan adanya orientasi hukum pidana nasional yang lebih adaptif terhadap perkembangan masyarakat, termasuk perkembangan teknologi informasi dan komunikasi.

Dalam perkembangan terbaru, negara juga mengesahkan Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi sebagai bentuk penguatan kebijakan penal terhadap penyalahgunaan data pribadi. Perlindungan data pribadi menjadi sangat penting karena sebagian besar cybercrime bermula dari pencurian, penyalahgunaan, atau perdagangan data elektronik milik individu maupun korporasi. Pengaturan mengenai sanksi pidana terhadap penyalahgunaan data pribadi menunjukkan bahwa hukum pidana tidak hanya diarahkan untuk menghukum pelaku, tetapi juga memberikan perlindungan terhadap hak privasi sebagai bagian dari hak asasi manusia di era digital.

Meskipun demikian, efektivitas kebijakan penal dalam penanggulangan cybercrime masih menghadapi berbagai tantangan. Salah satu tantangan utama adalah sifat cybercrime yang bersifat lintas negara (transnational crime). Pelaku dapat melakukan serangan dari negara lain dengan menggunakan jaringan virtual yang sulit dilacak, sementara korban berada di Indonesia. Perbedaan yurisdiksi hukum, mekanisme ekstradisi, serta belum seragamnya pengaturan hukum antarnegara sering kali menghambat proses penegakan hukum. Kondisi tersebut menunjukkan bahwa keberhasilan kebijakan penal tidak hanya bergantung pada kualitas regulasi nasional, tetapi juga pada efektivitas kerja sama internasional.

Tantangan berikutnya berkaitan dengan pembuktian tindak pidana siber. Berbeda dengan alat bukti konvensional, pembuktian cybercrime sangat bergantung pada alat bukti elektronik (electronic evidence) yang memerlukan keahlian khusus dalam proses identifikasi, pengamanan, analisis, dan penyajiannya di persidangan. Aparat penegak hukum dituntut memiliki kompetensi di bidang digital forensik agar mampu menjaga integritas alat bukti elektronik sehingga memiliki kekuatan pembuktian yang sah menurut hukum acara pidana. Oleh karena itu, penguatan kapasitas sumber daya manusia menjadi bagian yang tidak terpisahkan dari implementasi kebijakan penal.

Selain persoalan teknis, tantangan lain adalah keseimbangan antara penegakan hukum dan perlindungan hak asasi manusia. Dalam praktiknya, penegakan hukum terhadap cybercrime sering kali bersinggungan dengan hak atas kebebasan berekspresi, hak atas privasi, dan perlindungan data pribadi. Oleh karena itu, kebijakan penal harus dilaksanakan berdasarkan prinsip due process of law, proporsionalitas, legalitas, dan akuntabilitas agar tidak menimbulkan penyalahgunaan kewenangan oleh aparat penegak hukum. Penegakan hukum yang efektif harus tetap menjamin perlindungan hak-hak konstitusional warga negara sebagaimana diatur dalam Undang-Undang Dasar Negara Republik Indonesia Tahun 1945.

Dari perspektif kebijakan kriminal, penggunaan hukum pidana seharusnya ditempatkan sebagai ultimum remedium, yaitu sarana terakhir setelah berbagai upaya pencegahan tidak berhasil. Pendekatan represif memang penting untuk memberikan efek jera terhadap pelaku, namun tidak dapat berdiri sendiri dalam menghadapi perkembangan cybercrime yang sangat cepat. Hal ini sejalan dengan pandangan Hoefnagels yang menyatakan bahwa penanggulangan kejahatan tidak cukup dilakukan melalui penerapan hukum pidana, tetapi juga harus didukung oleh strategi pencegahan dan pembentukan kesadaran hukum masyarakat.

Berdasarkan analisis tersebut, dapat dipahami bahwa kebijakan penal di Indonesia telah mengalami perkembangan yang signifikan melalui pembentukan berbagai regulasi yang mengatur tindak pidana siber, penguatan sistem pembuktian elektronik, serta perluasan pertanggungjawaban pidana terhadap pelaku maupun korporasi. Namun demikian, efektivitas kebijakan tersebut masih memerlukan dukungan berupa peningkatan kapasitas aparat penegak hukum, harmonisasi regulasi, penguatan kerja sama internasional, serta sinergi dengan kebijakan non-penal. Dengan demikian, kebijakan penal harus diposisikan sebagai salah satu komponen dalam sistem penanggulangan cybercrime yang bersifat komprehensif dan terintegrasi.

3.2 Kebijakan Non-Panel dalam Penanggulangan Kejahatan Siber

Selain melalui pendekatan hukum pidana (penal policy), penanggulangan kejahatan siber juga memerlukan kebijakan non-penal yang berorientasi pada pencegahan (preventive approach). Pendekatan non-penal merupakan bagian integral dari kebijakan kriminal (criminal policy) yang bertujuan menghilangkan atau meminimalkan faktor-faktor penyebab terjadinya kejahatan sebelum perbuatan pidana terjadi. Dalam perspektif hukum pidana modern, penggunaan sarana pidana semata tidak akan mampu mengatasi perkembangan cybercrime yang semakin kompleks, karena hukum pidana pada hakikatnya bersifat represif dan baru bekerja setelah suatu tindak pidana dilakukan. Oleh sebab itu, kebijakan non-penal menjadi instrumen strategis dalam membangun sistem perlindungan masyarakat yang lebih komprehensif dan berkelanjutan.

Barda Nawawi Arief menjelaskan bahwa kebijakan kriminal harus dipahami sebagai bagian dari kebijakan sosial (social policy) yang diarahkan untuk menciptakan kesejahteraan masyarakat (social welfare) sekaligus memberikan perlindungan kepada masyarakat (social defence). Dalam konteks tersebut, kebijakan non-penal memiliki fungsi untuk mengurangi faktor-faktor kriminogen dan viktimogen yang berpotensi melahirkan tindak pidana. Pada kejahatan siber, faktor-faktor tersebut meliputi rendahnya literasi digital, lemahnya sistem keamanan informasi, kurangnya kesadaran masyarakat mengenai perlindungan data pribadi, minimnya koordinasi antarinstansi, serta keterbatasan kapasitas sumber daya manusia di bidang keamanan siber. Karakteristik cybercrime yang berbasis teknologi menjadikan kebijakan non-penal memiliki kedudukan yang sangat penting. Berbeda dengan kejahatan konvensional, kejahatan siber memanfaatkan kelemahan sistem elektronik, kelalaian pengguna, dan rendahnya tingkat keamanan digital sebagai pintu masuk untuk melakukan tindak pidana. Dengan demikian, upaya pencegahan harus diarahkan pada peningkatan ketahanan sistem (cyber resilience) serta pembangunan budaya keamanan siber (cybersecurity culture) di seluruh lapisan masyarakat.

1. Peningkatan Literasi Digital sebagai Upaya Preventif

Salah satu bentuk kebijakan non-penal yang paling fundamental adalah peningkatan literasi digital. Literasi digital tidak hanya dimaknai sebagai kemampuan menggunakan perangkat teknologi informasi, tetapi juga mencakup kemampuan memahami risiko keamanan digital, melindungi data pribadi, mengenali modus penipuan daring, serta menggunakan internet secara aman, etis, dan bertanggung jawab. UNESCO mendefinisikan literasi digital sebagai seperangkat kompetensi yang memungkinkan individu mengakses, memahami, mengevaluasi, menciptakan, dan mengomunikasikan informasi melalui teknologi digital secara efektif dan bertanggung jawab. Rendahnya literasi digital menjadi salah satu penyebab meningkatnya angka kejahatan siber di Indonesia. Banyak korban penipuan daring, phishing, social engineering, maupun pencurian data pribadi berasal dari kelompok masyarakat yang belum memahami teknik manipulasi yang digunakan oleh pelaku. Kondisi tersebut menunjukkan bahwa kelemahan manusia (human vulnerability) sering kali menjadi sasaran utama dibandingkan kelemahan teknologi itu sendiri. Oleh karena itu, edukasi kepada masyarakat merupakan langkah strategis dalam mengurangi peluang terjadinya cybercrime. Pemerintah Indonesia telah mengembangkan berbagai program literasi digital melalui kementerian dan lembaga terkait, termasuk

Kementerian Komunikasi dan Digital (Komdigi), Badan Siber dan Sandi Negara (BSSN), lembaga pendidikan, serta organisasi masyarakat sipil. Program tersebut bertujuan meningkatkan pemahaman masyarakat mengenai keamanan digital, etika bermedia sosial, perlindungan data pribadi, dan kewaspadaan terhadap berbagai modus kejahatan siber. Namun demikian, efektivitas program tersebut masih memerlukan evaluasi karena tingkat literasi digital masyarakat Indonesia masih menunjukkan kesenjangan antardaerah, kelompok usia, dan tingkat pendidikan.

2. Penguatan Sistem Keamanan Siber Nasional

Kebijakan non-penal juga diwujudkan melalui pembangunan sistem keamanan siber nasional (national cybersecurity system). Keamanan siber tidak hanya berkaitan dengan perlindungan jaringan komputer pemerintah, tetapi juga mencakup perlindungan terhadap infrastruktur informasi kritis, sistem keuangan, layanan kesehatan, transportasi, energi, pendidikan, dan berbagai sektor strategis lainnya. Menurut International Telecommunication Union (ITU), keamanan siber merupakan serangkaian kebijakan, teknologi, standar, prosedur, dan praktik yang bertujuan melindungi sistem informasi dari berbagai ancaman digital. Oleh karena itu, penguatan keamanan siber tidak cukup dilakukan melalui pembentukan regulasi, tetapi harus didukung oleh pengembangan teknologi, peningkatan kapasitas kelembagaan, serta investasi pada sistem keamanan informasi yang memadai. Di Indonesia, Badan Siber dan Sandi Negara (BSSN) memiliki peran strategis dalam membangun sistem keamanan siber nasional. BSSN bertanggung jawab melakukan deteksi dini terhadap ancaman siber, koordinasi penanganan insiden keamanan siber, pengembangan standar keamanan informasi, serta pembinaan penyelenggara sistem elektronik. Kehadiran BSSN menunjukkan bahwa pendekatan non-penal diarahkan untuk memperkuat kemampuan negara dalam mencegah serangan siber sebelum menimbulkan kerugian yang lebih besar.

Namun demikian, tantangan yang dihadapi masih cukup besar. Serangan siber terhadap instansi pemerintah maupun sektor swasta menunjukkan bahwa standar keamanan informasi belum diterapkan secara merata. Banyak organisasi masih memiliki kelemahan dalam pengelolaan akses pengguna, pembaruan sistem (system update), enkripsi data, maupun mekanisme pencadangan (backup) sehingga rentan menjadi sasaran serangan ransomware maupun pencurian data.

3. Penguatan Kapasitas Aparat Penegak Hukum

Efektivitas kebijakan non-penal juga bergantung pada peningkatan kualitas sumber daya manusia, khususnya aparat penegak hukum. Penanganan cybercrime memerlukan kompetensi khusus di bidang digital forensik, investigasi siber, analisis bukti elektronik, keamanan jaringan, serta teknologi informasi. Aparat penegak hukum yang tidak memiliki kemampuan teknis yang memadai akan mengalami kesulitan dalam mengidentifikasi pelaku maupun mengumpulkan alat bukti elektronik yang sah. Pengembangan kapasitas tersebut dapat dilakukan melalui pendidikan berkelanjutan (continuous legal education), pelatihan digital forensik, sertifikasi profesi, pertukaran pengalaman dengan lembaga internasional, serta pembentukan satuan tugas khusus yang menangani kejahatan siber. Menurut Casey (2011), keberhasilan investigasi cybercrime sangat ditentukan oleh kualitas sumber daya manusia yang memahami karakteristik bukti digital serta prosedur penanganannya.

Selain kepolisian, peningkatan kapasitas juga diperlukan bagi jaksa, hakim, advokat, auditor teknologi informasi, serta penyidik pegawai negeri sipil yang memiliki kewenangan di bidang keamanan informasi. Pendekatan multidisipliner menjadi penting karena kejahatan siber melibatkan aspek hukum, teknologi, ekonomi, dan hubungan internasional.

4. Kerja Sama Nasional dan Internasional

Cybercrime merupakan bentuk kejahatan lintas negara sehingga penanggulangannya memerlukan kerja sama yang erat, baik di tingkat nasional maupun internasional. Banyak pelaku menggunakan server yang berada di negara lain, jaringan virtual (Virtual Private Network), mata uang

kripto, maupun identitas palsu sehingga proses penegakan hukum memerlukan koordinasi lintas yurisdiksi.

Dalam konteks nasional, kerja sama dilakukan antara Kepolisian Negara Republik Indonesia, Kejaksaan Republik Indonesia, Mahkamah Agung, BSSN, Komdigi, Otoritas Jasa Keuangan, Bank Indonesia, Pusat Pelaporan dan Analisis Transaksi Keuangan (PPATK), serta berbagai penyelenggara sistem elektronik. Sinergi tersebut diperlukan agar pertukaran informasi, penanganan insiden, dan perlindungan terhadap korban dapat dilakukan secara cepat dan efektif. Pada tingkat internasional, kerja sama diwujudkan melalui pertukaran informasi intelijen, mutual legal assistance, ekstradisi, investigasi bersama (joint investigation), serta kerja sama dengan organisasi internasional seperti INTERPOL, ASEANAPOL, UNODC, dan berbagai forum keamanan siber internasional. Pendekatan kolaboratif tersebut menjadi sangat penting mengingat sebagian besar cybercrime memiliki dimensi transnasional yang tidak dapat diselesaikan hanya melalui yurisdiksi nasional.

5. Peran Sektor Swasta dan Partisipasi Masyarakat

Penanggulangan cybercrime tidak dapat sepenuhnya dibebankan kepada pemerintah. Sektor swasta, khususnya perusahaan teknologi, penyedia layanan internet, lembaga keuangan, platform perdagangan elektronik, dan penyelenggara sistem elektronik memiliki tanggung jawab besar dalam menjaga keamanan sistem yang mereka kelola. Penerapan standar keamanan informasi internasional seperti ISO/IEC 27001, penggunaan autentikasi multifaktor (multi-factor authentication), enkripsi data, audit keamanan berkala, serta pelaporan insiden keamanan merupakan bentuk kontribusi sektor swasta dalam mendukung kebijakan non-penal. Selain itu, perusahaan juga memiliki tanggung jawab untuk meningkatkan kesadaran keamanan digital bagi karyawan maupun pengguna layanan.

Partisipasi masyarakat juga menjadi unsur penting dalam pencegahan cybercrime. Kesadaran untuk tidak membagikan data pribadi secara sembarangan, menggunakan kata sandi yang kuat, melakukan pembaruan perangkat lunak secara berkala, serta melaporkan dugaan tindak pidana siber kepada aparat penegak hukum merupakan bentuk keterlibatan masyarakat dalam membangun ekosistem keamanan digital. Konsep community policing di ruang siber menunjukkan bahwa masyarakat bukan hanya objek perlindungan hukum, tetapi juga subjek yang memiliki peran aktif dalam pencegahan kejahatan.

Analisis Kebijakan Non-Penal

Berdasarkan uraian di atas, dapat dipahami bahwa kebijakan non-penal memiliki kedudukan yang sama pentingnya dengan kebijakan penal dalam penanggulangan kejahatan siber. Pendekatan non-penal tidak berorientasi pada penghukuman pelaku, melainkan pada pengurangan peluang terjadinya kejahatan melalui pembangunan sistem keamanan, peningkatan literasi digital, penguatan kelembagaan, peningkatan kapasitas sumber daya manusia, serta kerja sama lintas sector (Grabosky, 2007). Meskipun berbagai kebijakan telah dilaksanakan, efektivitasnya masih menghadapi sejumlah tantangan, antara lain belum meratanya tingkat literasi digital masyarakat, keterbatasan sumber daya manusia di bidang keamanan siber, belum optimalnya koordinasi antarinstansi, serta cepatnya perkembangan teknologi yang sering kali melampaui kemampuan regulasi. Oleh karena itu, kebijakan non-penal harus terus dikembangkan secara adaptif melalui pendekatan kolaboratif (whole-of-government dan whole-of-society approach) agar mampu menjawab dinamika ancaman siber yang terus berkembang (von Solms & van Niekerk, 2013).

Dengan demikian, keberhasilan penanggulangan kejahatan siber tidak dapat dicapai hanya melalui penegakan hukum pidana. Integrasi antara kebijakan penal dan non-penal merupakan prasyarat utama dalam membangun sistem perlindungan hukum yang efektif, berkelanjutan, dan berorientasi pada keamanan ruang digital nasional..

4. KESIMPULAN

Berdasarkan hasil penelitian mengenai Kebijakan Penal dan Non-Penal dalam Penanggulangan Kejahatan Siber, dapat ditarik beberapa kesimpulan sebagai berikut.

Pertama, kebijakan penal dalam penanggulangan kejahatan siber di Indonesia telah mengalami perkembangan yang cukup signifikan melalui pembentukan berbagai instrumen hukum yang mengatur tindak pidana di ruang siber. Keberadaan Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, Undang-Undang Nomor 1 Tahun 2023 tentang Kitab Undang-Undang Hukum Pidana, Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi, serta berbagai peraturan pelaksana menunjukkan komitmen negara dalam memberikan kepastian hukum terhadap berbagai bentuk cybercrime. Kebijakan penal tersebut telah mengatur kriminalisasi berbagai tindak pidana siber, mekanisme pertanggungjawaban pidana, alat bukti elektronik, serta pemberian sanksi pidana kepada pelaku. Namun demikian, efektivitas penerapan kebijakan penal masih menghadapi berbagai kendala, antara lain perkembangan modus operandi cybercrime yang sangat cepat, keterbatasan kemampuan digital forensik, perbedaan yurisdiksi antarnegara, serta kompleksitas pembuktian dalam tindak pidana berbasis teknologi informasi.

Kedua, kebijakan non-penal memiliki peranan yang sangat strategis dalam mencegah terjadinya kejahatan siber sebelum menimbulkan kerugian bagi masyarakat. Pendekatan non-penal diwujudkan melalui peningkatan literasi digital, penguatan keamanan siber nasional, perlindungan data pribadi, peningkatan kapasitas aparat penegak hukum, pembangunan budaya keamanan digital, serta penguatan kerja sama nasional dan internasional. Penelitian ini menunjukkan bahwa sebagian besar cybercrime tidak hanya dipengaruhi oleh kelemahan regulasi, tetapi juga oleh rendahnya kesadaran masyarakat terhadap keamanan digital, lemahnya sistem perlindungan informasi, serta belum optimalnya koordinasi antarlembaga. Oleh karena itu, kebijakan non-penal harus ditempatkan sebagai instrumen preventif yang memiliki kedudukan sama pentingnya dengan kebijakan penal dalam sistem penanggulangan kejahatan siber.

Ketiga, penanggulangan kejahatan siber yang efektif memerlukan harmonisasi antara kebijakan penal dan non-penal dalam suatu sistem kebijakan kriminal (integrated criminal policy). Pendekatan represif melalui penegakan hukum pidana tidak dapat bekerja secara optimal tanpa didukung oleh langkah-langkah preventif yang berorientasi pada pembangunan kapasitas kelembagaan, penguatan teknologi keamanan informasi, peningkatan literasi digital, serta partisipasi aktif masyarakat dan sektor swasta. Harmonisasi tersebut juga harus diwujudkan melalui sinkronisasi regulasi, peningkatan koordinasi antarlembaga, penguatan kerja sama internasional, serta pemanfaatan teknologi digital dalam proses penegakan hukum. Dengan demikian, kebijakan kriminal di bidang kejahatan siber tidak hanya bertujuan memberikan efek jera kepada pelaku, tetapi juga menciptakan sistem perlindungan hukum yang adaptif terhadap perkembangan teknologi informasi dan mampu menjamin keamanan ruang siber nasional secara berkelanjutan.

DAFTAR PUSTAKA

Journal article

Flanagan, A. (2005). The law and computer crime: Reading the script of reform. International Journal of Law and Information Technology, 13(1), 98–117.
DOI: https://doi.org/10.1093/ijlit/eai004

Hutchinson, T., & Duncan, N. (2012). Defining and describing what we do: Doctrinal legal research. Deakin Law Review, 17(1), 83–119.
DOI: https://doi.org/10.21153/dlr2012vol17no1art70

Hunton, P. (2010). The growing phenomenon of crime and the internet: A cybercrime execution and analysis model. Computer Law & Security Review, 25(6), 528–535.
DOI: https://doi.org/10.1016/j.clsr.2009.09.005

Katagiri, N. (2021). Why international law and norms do little in preventing non-state cyber attacks. Journal of Cybersecurity, 7(1), tyab009.

DOI: https://doi.org/10.1093/cybsec/tyab009
Khan, S., Saleh, T., Dorasamy, M., et al. (2022). A systematic literature review on cybercrime legislation. F1000Research, 11, 971.
DOI: https://doi.org/10.12688/f1000research.123098.1
Nurse, J. R. C. (2018). Cybercrime and you: How criminals attack and the human factors that they seek to exploit. In A. Attrill-Smith et al. (Eds.), The Oxford Handbook of Cyberpsychology (pp. 663–690). Oxford University Press.
DOI: https://doi.org/10.1093/oxfordhb/9780198812746.013.35
Pavlik, K. (2017). Cybercrime, hacking, and legislation. Journal of Cybersecurity Research, 2(1), 13–16.
DOI: https://doi.org/10.19030/jcr.v2i1.9966
Manatova, D., McGrath, C., & Camp, L. J. (2026). The organizational anatomy of cybercrime: A multilayer framework for modeling resilience. Journal of Cybersecurity, 12(1), tyag014.
DOI: https://doi.org/10.1093/cybsec/tyag014
Serour, I. (2025). International cooperation in pursuing cybercrime perpetrators, according to the United Nations Convention against Cybercrime. Journal of Law and Emerging Technologies, 5(2).
DOI: https://doi.org/10.54873/jolets.v5i2.234
Juku, J., & Riala, Z. N. (2026). Pertanggungjawaban pidana pelaku kejahatan siber di era digital. Indonesian Journal of Criminal Law, 8(1), 20–29.
DOI: https://doi.org/10.31960/ijocl.v8i1.3462
Nguyen, C. L., & Golman, W. (2021). Diffusion of the Budapest Convention on cybercrime and the development of cybercrime legislation in Pacific Island countries: “Law on the books” vs. “law in action”. Computer Law & Security Review, 40.
DOI: https://doi.org/10.1016/j.clsr.2020.105521
Kerr, O. S. (2005). Digital evidence and the new criminal procedure. Columbia Law Review, 105(1), 279–318.
Untuk versi bab buku yang memiliki DOI resmi penerbit, lihat: https://doi.org/10.18574/nyu/9780814739334.003.0013

Book References

Clough, J. (2015). *Principles of Cybercrime* (2nd ed.). Cambridge University Press. https://doi.org/10.1017/CBO9781139540803
Hoefnagels, G. P. (1973). *The Other Side of Criminology: An Inversion of the Concept of Crime*. Springer. https://doi.org/10.1007/978-94-017-4495-9
ed, M. (2008). *Metode Penelitian Kepustakaan*. Yayasan Obor Indonesia