

Analisis Yuridis Terhadap Penegakan dan Pengaturan Hukum Kejahatan Dunia Maya (*Cybercrime*) di Indonesia

Elok Harry Ari Dhani Putri

Magister Hukum Universitas Gorontalo

Ramdhan Kasim

Magister Hukum Universitas Gorontalo

Leni Dwi Nurmala

Magister Hukum Universitas Gorontalo

Korespondensi penulis: lenitsaina@gmail.com

Alamat: Jl. Sultan Botutihe, Tamalate, Kota Timur, Kota Gorontalo, Gorontalo

Abstract. *The aim of this research is to find out and analyze cybercrime law enforcement in Indonesia. The implementation of this research is normative research. Data analysis is an activity in research in the form of conducting studies or reviewing the results of data processing which is assisted by previously obtained theories. Cyber crime law enforcement in Indonesia can be carried out penal and non-penal. In general, seen from criminal policy (crime prevention policy), criminal law is not a strategic policy tool to prevent and eliminate causal factors or conditions that give rise to crime. We can see the positive criminal law provisions that are criminalized regarding cyber crime in Law Number 19 of 2016, amendments to Law Number 11 of 2008 concerning Information and Electronic Transactions. Meanwhile, non-penal measures are carried out through social methods or approaches such as information, appeals, educational channels, coaching, and also related matters of preventing cyber crime. In realizing law enforcement, law enforcement officers need an active role, namely by being equipped with special skills in handling cyber crime.*

Keywords: *Law enforcement, crime, computers, cyberspace.*

Abstrak. Tujuan Penelitian ini adalah Untuk mengetahui dan menganalisis penegakan hukum kejahatan dunia maya (*Cybercrime*) di Indonesia Pelaksanaan Penelitian ini merupakan penelitian normatif. Analisis data merupakan kegiatan dalam penelitian yang berupa melakukan kajian atau telaah terhadap hasil pengolahan data yang dibantu dengan teori-teori yang telah didapatkan sebelumnya. Penegakan Hukum *cyber crime* di Indonesia dapat dilakukan secara penal dan non penal. Secara penal, dilihat dari kebijakan kriminal (kebijakan penanggulangan kejahatan), hukum pidana bukan merupakan sarana kebijakan yang strategis untuk mencegah dan meniadakan faktor faktor penyebab atau kondisi yang menimbulkan kejahatan. Ketentuan hukum pidana positif yang dikriminalisasi terkait kejahatan mayantara (*cyber crime*) dapat kita lihat pada Undang-Undang Nomor 19 Tahun 2016 perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik. Sedangkan secara non penal dilakukan melalui metode atau pendekatan sosial seperti informasi, himbuan, jalur pendidikan, pembinaan, dan juga terkait hal-hal pencegahan *cyber crime* tersebut. Dalam mewujudkan penegakan hukum perlu peran aktif aparat penegak hukum yaitu dengan dibekali keahlian khusus dalam melakukan penanganan kejahatan mayantara (*cyber crime*) tersebut.

Kata Kunci: Penegakan hukum, kejahatan, komputer, dunia maya.

LATAR BELAKANG

Perkembangan masyarakat zaman sekarang ini semakin maju dan di dukung oleh pertumbuhan teknologi telekomunikasi (Zainuddin, Gassing, and Kurniati 2024). Namun perkembangan itu membawa dampak terhadap masyarakat Indonesia yang sedang membangun di era reformasi itu telah dihadapkan dengan berbagai krisis, baik politik,

ekonomi, dan sosial budaya, dan ini harus ditangani agar bangsa dan negara Indonesia tetap dipandang keberadaannya di antara bangsa-bangsa di dunia. Perkembangan teknologi informasi dan komunikasi terus berkembang pesat, kini dimungkinkan untuk menggunakan teknologi informasi dan komunikasi melalui perangkat mobile. Kegiatan yang biasanya dilakukan di dunia nyata kini banyak diperdagangkan melalui *gadget, smartphone, handphone*, dan laptop (Habibi and Liviani 2020).

Kita tidak lagi mengalami kesulitan untuk mengakses informasi dari seluruh penjuru dunia. Selain banyaknya teknologi informasi dan komunikasi yang telah memberikan dukungan untuk banyak perangkat mobile, juga karena banyak tersedianya hotspot gratis dibanyak tempat. Pesatnya perkembangan teknologi informasi dan komunikasi juga diiringi dengan meluasnya penyalahgunaan teknologi informasi dan komunikasi, sehingga menjadi masalah yang sangat meresahkan yaitu terjadinya kejahatan yang dilakukan di dunia maya atau yang biasa dikenal dengan istilah *cybercrime* (Marita 2015)

Cybercrime dewasa ini muncul ketika penyalahgunaan internet sudah di luar batas sehingga menjadi suatu kejahatan. Pengertian kejahatan computer atau kejahatan maya pada umumnya sebagai kejahatan melalui pengetahuan khusus tentang teknologi komputer. Hukum terlalu lambat untuk mengikuti perkembangan teknologi computer, kemudian bereaksi terhadap perubahan dan perkembangan teknologi yang demikian cepat (Amarini 2018). Bahkan undang-undang yang sekarang ini tidak mampu untuk menangani kejahatan dunia maya secara tuntas.

Berbagai kejahatan telah terjadi di dunia maya ini, kasus-kasus tersebut tentu saja merugikan dan berdampak negatif, kejahatan dunia maya semacam ini tidak hanya mencakup Indonesia, tetapi juga mencakup seluruh dunia. Beberapa kejahatan yang terjadi disebabkan oleh maraknya penggunaan *e-mail, e-banking* dan *e-commerce* di Indonesia. Menurut Heru Sutadi bahwa secara garis besar, kejahatan yang berkaitan dengan teknologi informasi dapat dibagi menjadi dua, yaitu: Pertama, kejahatan yang bertujuan merusak atau menyerang sistem atau jaringan komputer. Dan kedua, kejahatan yang menggunakan komputer atau internet sebagai alat bantu dalam melancarkan kejahatan. Namun begitu, mengingat teknologi informasi merupakan konvergensi telekomunikasi, komputer dan media, kejahatan jenis ini berkembang menjadi luas lagi (Sugriyo 2010).

Semakin banyaknya kasus *cybercrime* (khususnya di Indonesia) telah menarik perhatian pemerintah untuk segera memberlakukan undang-undang yang dapat digunakan untuk menjebak pelaku kejahatan di dunia maya. Pemerintah Indonesia sendiri telah memasukkan UU *Cybercrime* (UU Siber) ke dalam Undang-Undang Nomor 19 tahun 2016

perubahan atas UU ITE Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik begitu juga pada kitab Undang-Undang Hukum Pidana, dan berharap dengan adanya UU ITE Nomor 19 Tahun 2016 dapat mengatasi, mengurangi, dan menghentikan pelaku kejahatan di dunia maya.

Mengingat bahwa *cybercrime* tidak mengenal batas negara maka dalam upaya penanggulangannya memerlukan suatu kordinasi dan kerja sama antar negara. *Cybercrime* memperlihatkan salah satu kondisi yang kompleks dan penting untuk diadakannya suatu kerjasama internasional. Penanggulangan tindak pidana *cyber crime* sampai saat ini masih terdapat kendala-kendala yang dihadapi oleh para aparat penegak hukum dalam menjalankan tugasnya, khususnya terhadap pelaksanaan peran laboratorium forensik sebagai pendukung pembuktian kejahatan dunia maya secara ilmiah dalam sistem pradilan pidana di Indonesia.

Kendala-kendala yang dihadapi yaitu mengenai keterbatasan SDM, keterbatasan aparat penegak hukum dalam hal teknologi informasi, fasilitas yang belum memadai dan tidak *uptodate* yang mana juga mempengaruhi hasil kerja dan pemeriksaan seperti laboratorium digital forensik masih sangat terbatas yang dimiliki oleh lembaga-lembaga atau institusi yang menangani kejahatan *cybercrime* di Indonesia, begitu juga dengan anggaran yang terbatas dan lain sebagainya yang mana hal ini perlu diperhatikan oleh Pemerintah demi kemajuan kinerja aparat penegak hukum.

METODE PENELITIAN

Jenis penelitian yang digunakan adalah penelitian hukum yuridis normative yang menganalisis permasalahan berdasarkan perundang-undangan yang berlaku dan juga literatur yang membahas permasalahan yang dikaji. Adapun Pendekatan melalui Undang-Undang, yakni pendekatan yang dilakukan dengan menelaah semua undang-undang dan regulasi yang bersangkutan paut dengan isu hukum yang sedang diteliti. pengumpulan data utama di tempuh dengan melakukan penelitian kepustakaan dan studi dokumen-dokumen berupa peraturan-perundang-undangan.

HASIL DAN PEMBAHASAN

Pertanggungjawaban terhadap tindak pidana pada dunia maya (*Cyber crime*), pada hakikatnya mengandung makna tuntutan pidana pembuat (subjek hukum) atas tindak pidana yang telah dilakukannya. Oleh karena itu, pertanggungjawaban pidana mengandung di dalamnya pencelaan objektif dan pencelaan subjektif. Artinya, secara objektif si pembuat telah melakukan tindak pidana (perbuatan terlarang/melawan hukum dan diancam pidana menurut

hukum yang berlaku) dan secara subjektif si pembuat patut dicela atau dipersalahkan/dipertanggungjawabkan atas tindak pidana yang dilakukannya itu sehingga ia patut dipidana(Candra 2013).

Upaya Penegakan Hukum pada *Cyber Crime* di Indonesia dilakukan dengan melalui Sarana Penal dan Non Penal(Nuristiningsih 2023).

1. Melalui Sarana Penal.

Intrumen internasional yang berkaitan dengan kejahatan *cyber*. Intrumen internasional yang berkaitan dengan *cyber crime* adalah *Convention on Cyber Crime* tanggal 23 November 2001 di kota Budapest Hongaria telah membuat dan menyepakati *Convention on Cyber Crime* yang kemudian dimasukkan dalam *European Treaty Series* dengan nomor 185(Kurnia Putra 2014).

Convention on Cyber Crime 2001 dibentuk dengan pertimbangan antara lain: Pertama, masyarakat internasional menyadari perlunya kerjasama antara negara dan industri dalam memerangi kejahatan cyber dan adanya kebutuhan untuk melindungi kepentingan yang sah di dalam penggunaan serta pengembangan teknologi informasi. Kedua, Konvensi saat ini diperlukan untuk meredam penyalahgunaan sistem, jaringan dan data komputer untuk melakukan perbuatan kriminal. Dengan demikian perlunya adanya kepastian dalam proses penyelidikan dan penuntutan pada tingkat internasional dan domestik melalui suatu mekanisme kerjasama internasional yang dapat dipercaya dan cepat. Ketiga, saat ini sudah semakin nyata adanya kebutuhan untuk memastikan suatu kesesuaian antara pelaksanaan penegakan hukum dan hak azasi manusia sejalan dengan Konvensi Dewan Eropa untuk perlindungan Hak Azasi Manusia dan Kovenan Perserikatan Bangsa-Bangsa 1966 tentang Hak Politik dan Sipil yang memberikan perlindungan kebebasan berpendapat seperti hak berekspresi, yang mencakup kebebasan untuk mencari, menerima, dan menyebarkan informasi dan pendapat.

Dilihat dari kebijakan kriminal (kebijakan penanggulangan kejahatan), hukum pidana bukan merupakan sarana kebijakan yang strategis. Kebijakan yang strategis adalah mencegah dan meniadakan faktor faktor penyebab atau kondisi yang menimbulkan kejahatan. Dilihat dari sudut *criminal policy*, Upaya penanggulangan kejahatan (termasuk penanggulangan *cyber crime*) tentunya tidak dapat dilakukan secara parsial dengan hukum pidana (sarana penal), tetapi harus ditempuh pula dengan pendekatan integral/sistemik. Sebagai salah satu bentuk dari *high tech crime*, merupakan hal yang wajar jika upaya penanggulangan *cyber crime* juga harus ditempuh dengan teknologi (*techno prevention*).

Ketentuan hukum pidana positif yang dikriminalisasi terkait kejahatan mayantara (*cyber crime*) dapat kita lihat pada Undang-Undang Nomor 19 Tahun 2016 perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, sebagaimana yang dimuat pada Pasal 27 sampai dengan Pasal 36. Terdapat pula pada Undang-undang Nomor 20 Tahun 2001 tentang Perubahan atas Undang-undang Nomor 31 Tahun 1999 tentang Pemberantasan Tindak Pidana Korupsi, dimana sisi mayantara dari tindak pidana korupsi ini adalah bahwa kejahatan tersebut telah menggunakan media internet sebagai alat untuk melakukan korupsi ataupun memperlancar tindak dilakukannya tindak pidana tersebut meskipun tidak secara eksplisit diatur dalam undang-undang ini. Beberapa peraturan perundang-undangan yang mengkriminalisasi kejahatan mayantara di dalamnya adalah : Undang-undang Nomor 44 Tahun 2008 tentang Pornografi, Undang-undang Nomor 5 Tahun 2018 tentang Pemberantasan Tindak Pidana Terorisme, Undang-undang Nomor 8 Tahun 2010 tentang Pencegahan dan Pemberantasan Tindak Pidana Pencucian Uang, dan Undang-undang Nomor 35 Tahun 2009 tentang Narkotika.

2. Penegakan Hukum *Cyber Crime* Melalui Sarana Non Penal.

Pendekatan non penal menurut Hoefnagels adalah pendekatan pencegahan kejahatan tanpa menggunakan sarana pemidanaan (*prevention without punishment*), yaitu antara lain perencanaan kesehatan mental masyarakat (*community planning mental health*), kesehatan mental masyarakat secara nasional (*national mental health*), social worker and child welfare (kesejahteraan anak dan pekerja sosial), serta penggunaan hukum civil dan hukum administrasi (*administrative & civil law*)(Mulyadi 2011).

Kebijakan penanggulangan kejahatan lewat jalur “non penal” lebih bersifat tindakan pencegahan sebelum terjadinya kejahatan. Oleh karena itu, sasaran utamanya adalah menangani faktor-faktor kondusif penyebab terjadinya kejahatan yang berpusat pada masalah-masalah atau kondisi-kondisi sosial yang secara langsung atau tidak langsung dapat menimbulkan atau menumbuhkan suburkan kejahatan. Dengan demikian dilihat dari kebijakan penanggulangan kejahatan, maka usaha-usaha non penal ini mempunyai kedudukan yang strategis dan memegang peranan kunci yang harus diintensifkan dan diefektifkan(Sitta Saraya, Yusrina Handayani 2023).

Beberapa masalah dan kondisi sosial yang dapat merupakan faktor kondusif penyebab timbulnya kejahatan, jelas merupakan masalah yang tidak dapat diatasi semata-mata dengan “penal”. Di sinilah keterbatasan jalur “penal” dan oleh karena itu, harus ditunjang oleh jalur “non penal”. Salah satu jalur “non penal” untuk mengatasi masalah-masalah sosial seperti dikemukakan diatas adalah lewat jalur “kebijakan sosial” (*social*

policy), dimana G.P. Hoefnagels juga memasukkan dalam jalur “prevention without punishment”. Kebijakan sosial pada dasarnya adalah kebijakan atau upaya-upaya rasional untuk mencapai kesejahteraan masyarakat. Jadi identik dengan kebijakan atau perencanaan pembangunan nasional yang meliputi berbagai aspek yang cukup luas dari pembangunan.

Cyber Crime membutuhkan global action dalam penanggulangannya mengingat kejahatan tersebut seringkali bersifat transnasional. Beberapa langkah penting yang harus dilakukan setiap negara dalam penanggulangan *cyber crime* adalah:

- a) Melakukan modernisasi hukum pidana nasional beserta hukum acaranya, yang diselaraskan dengan konvensi internasional yang terkait dengan kejahatan tersebut.
- b) Meningkatkan sistem pengamanan jaringan komputer nasional sesuai standar internasional.
- c) Meningkatkan pemahaman serta keahlian aparaturnya mengenai upaya pencegahan, investigasi dan penuntutan perkara-perkara yang berhubungan dengan *cyber crime*.
- d) Meningkatkan kesadaran warga negara mengenai masalah *cyber crime* serta pentingnya mencegah kejahatan tersebut terjadi.
- e) Meningkatkan kerjasama antar negara, baik bilateral, regional maupun multilateral, dalam upaya penanganan *cyber crime*, antara lain melalui perjanjian ekstradisi dan mutual *assistance treaty*.
- f) Harmonisasi mengenai masalah yurisdiksi untuk menegakkan kedaulatan negara yang berlaku karena sifatnya transnasional.

Meskipun hukum pidana digunakan sebagai ultimum remidium atau alat terakhir apabila bidang hukum yang lain tidak dapat mengatasinya, tetapi harus disadari bahwa hukum pidana memiliki keterbatasan kemampuan dalam menanggulangi kejahatan. Keterbatasan-keterbatasan tersebut dikemukakan oleh Barda Nawawi Arief sebagai berikut:

- a) Sebab-sebab kejahatan yang demikian kompleks berada di luar jangkauan hukum pidana;
- b) Sebab-sebab kejahatan yang demikian kompleks berada di luar jangkauan hukum pidana;
- c) Hukum pidana hanya merupakan bagian kecil (*subsistem*) dari sarana kontrol sosial yang tidak mungkin mengatasi masalah kejahatan sebagai masalah kemanusiaan dan kemasyarakatan yang sangat kompleks (sebagai masalah *sosio-psikologis*, *sosio-politik*, *sosio-ekonomi*, *sosio-kultural* dan sebagainya);
- d) Penggunaan hukum pidana dalam menanggulangi kejahatan hanya merupakan “kurierenam symptom”, oleh karena itu hukum pidana hanya merupakan pengobatan simptomatik dan bukan pengobatan kausatif;

- e) Sanksi hukum pidana merupakan remedium yang mengandung sifat kontradiktif/paradoksal dan mengandung unsur-unsur serta efek sampingan yang negatif;
- f) Sistem pemidanaan bersifat fragmentair dan individual/personal, tidak bersifat struktural/fungsional;
- g) Keterbatasan jenis sanksi pidana dan sistem perumusan sanksi pidana yang bersifat kaku dan imperatif;
- h) Bekerjanya/berfungsingnya hukum pidana memerlukan sarana pendukung yang lebih bervariasi dan memerlukan “biaya tinggi”.

Keterbatasan-keterbatasan hukum pidana inilah yang tampaknya dialami oleh Polri yang menggunakan hukum pidana sebagai landasan kerjanya. Sebab kejahatan yang kompleks ini terlambat diantisipasi oleh Polri sehingga Ketika terjadi kasus yang berdimensi baru mereka tidak secara tanggap menanganinya. Untuk itu, pencegahan kejahatan tidak melulu harus menggunakan hukum pidana. Agar penegakan hukum cyber crime ini dapat dilakukan secara menyeluruh maka tidak hanya pendekatan yuridis atau penal yang dilakukan, tetapi dapat juga dilakukan dengan pendekatan non-penal.

Dari paparan penegakan hukum dengan sarana non-penal ini, maka menurut penulis cara non-penal inilah yang lebih diutamakan dari pada sarana penal dengan konsekwensi segera menyiapkan penegak hukum yang menguasai teknologi informasi. Atau lebih jelasnya kita sangat membutuhkan Polisi *cyber*, Jaksa *cyber*, Hakim *cyber* dalam rangka penegakan hukum cyber crime di Indonesia tanpa adanya penegak hukum yang mempunyai di bidang teknologi informasi, maka akan sulit menjerat penjahat-penjahat *cyber* oleh karena kejahatan *cyber* ini locus delicti bisa lintas negara.

Hukum sebagai gejala dalam kenyataan kemasyarakatan yang majemuk, yang mempunyai banyak aspek, dimensi dan faset. Hukum berakar dan terbentuk dalam proses interaksi berbagai aspek kemasyarakatan (politik, ekonomi, sosial, budaya, teknologi), dibentuk dan jkut membentuk tatanan masyarakat, bentuknya ditentukan oleh masyarakat dengan berbagai sifatnya, namun sekaligus ikut menentukan bentuk dan sifat-sifat masyarakat itu sendiri. Jadi, dalam dinamikanya, hukum itu dikondisikan dan mengondisikan masyarakat.

Karena menyandang tujuan untuk mewujudkan ketertiban dan keadilan secara konkret dalam masyarakat, maka dalam hukum terkandung baik kecenderungan konsewatif (mempertahakan dan memelihara apa yang sudah tercapai) maupun kecenderungan moderenisme (membawa, menganalisis dan mengarahkan perubahan).

Berdasarkan pandang ini, maka dapat dipahami bahwa hukum senantiasa berdialektika dengan aspek non hukum. Sejalan dengan pemahaman ini, tidak menutup kemungkinan juga hukum akan berdialektika dengan perkembangan teknologi.

Dalam posisi yang demikian ada tiga kemungkinan yang akan timbul, yakni, pertama, hukum akan dipengaruhi oleh perkembangan teknologi, kedua, hukum akan mempengaruhi perkembangan teknologi, dan ketiga, hukum dan teknologi akan saling mempengaruhi. Dalam konteks ini, umumnya fenomena berpengaruhnya perkembangan teknologi terhadap hukum berhubung langsung dengan pemanfaatan teknologi. Permasalahan yang mendasar disini bagaimana sebenarnya kedudukan hukum yang berlaku (hukum positif) terhadap semakin tidak dapat dikendalikannya perkembangan teknologi. Hal ini didasarkan pada kekhawatiran bahwa hukum yang berlaku tidak andequit dengan perkembangan teknologi.

Kalau melihat kepada perkembangan teknologi, nampak perubahan teknologi sangat berkembang dengan pesat dibanding dengan hukum sendiri yang selalu mengekor. Melalui perkembangan teknologi ini telah menimbulkan perubahan masyarakat, baik dalam konteks cara berperilaku individu maupun masyarakat itu sendiri.

Fenomena ini hendaknya menjadi suatu tantangan bagi kalangan hukum berkaitan dengan model pendekatan hukum yang selama ini dilakukan. Dengan kata lain bahwa perkembangan teknologi ini telah membawa manusia kepada suatu peradaban baru dengan struktur sosial beserta tata nilainya. Artinya, masyarakat berkembang menuju masyarakat baru yang berstruktur global dimana sekat-sekat negara mulai memudar.

Sistem tata nilai dalam masyarakat berubah, dari yang bersifat lokal- partikular menjadi global universal. Hal ini pada akhirnya akan membawa dampak pada pergeseran nilai, norma, moral dan kesusilaan.

Melihat fenomena di atas timbul persoalan apakah hukum pidana positif kita dapat menjangkau kejahatan yang terjadi di dunia *cyber* atau dunia maya mengingat teknologi internet yang membentuk relitas virtual merupakan sesuatu yang sama sekali baru. Sementara hukum pidana kita (KUHP) adalah buatan masa lalu di mana saat dibuat belum mengenal komputer apalagi internet.

KESIMPULAN

Semakin banyaknya kasus *cybercrime* (khususnya di Indonesia) telah menarik perhatian pemerintah untuk segera memberlakukan undang-undang yang dapat digunakan untuk menjebak pelaku kejahatan di dunia maya. Pemerintah Indonesia sendiri telah memasukkan *Cybercrime* dalam Undang-Undang Nomor 19 tahun 2016 perubahan atas

Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik begitu juga pada kitab Undang-Undang Hukum Pidana, dan berharap dengan adanya Undang-Undang Nomor 19 Tahun 2016 dapat mengatasi, mengurangi, dan menghentikan pelaku kejahatan di dunia maya.

Dalam mewujudkan penegakan hukum perlu peran aktif aparat penegak hukum yaitu dengan dibekali keahlian khusus dalam melakukan penyidikan dan penyelidikan guna memperlancar pembuktian kejahatan mayantara (cyber crime) tersebut. Peningkatan sarana prasarana dan kemampuan aparat penegak hukum di bidang teknologi dan informasi, pengetahuan, keyakinan dan pandangan yang luas hakim dalam menafsirkan hukum sebagai upaya penegakan hukum dunia mayantara di Indonesia. Dan perlu peningkatan kelengkapan alat teknologi informasi dan komunikasi untuk memperlancar proses pembuktian kejahatan tersebut serta peningkatan kerjasama internasional dalam rangka penegakan hukum untuk memberantas kejahatan mayantara (*cyber crime*).

REFERENSI

- Amarini, I. (2018). Pencegahan dampak negatif perkembangan teknologi informasi terhadap pengguna internet. *Kosmik Hukum*, 18(1). <https://doi.org/10.30595/kosmikhukum.v18i1.2340>
- Candra, S. (2013). Pembaharuan hukum pidana; konsep pertanggungjawaban pidana dalam hukum pidana nasional yang akan datang. *Jurnal Cita Hukum*, 1(1). <https://doi.org/10.15408/jch.v1i1.2979>
- Habibi, M. R., & Liviani, I. (2020). Kejahatan teknologi informasi (cyber crime) dan penanggulangannya dalam sistem hukum Indonesia. *Al-Qanun: Jurnal Pemikiran Dan Pembaharuan Hukum Islam*, 23(2), 400–426. <https://doi.org/10.15642/alqanun.2020.23.2.400-426>
- Kurnia Putra, A. (2014). Harmonisasi konvensi cyber crime dalam hukum nasional. *Jurnal Ilmu Hukum*, 95–109.
- Marita, L. S. (2015). Cyber crime dan penerapan cyber law dalam pemberantasan cyberlaw di Indonesia. *Jurnal Hukum Universitas Bina Sarana Informatika*, 18.
- Mulyadi, M. (2011). Penanggulangan tindak pidana korupsi dalam perspektif criminal policy (corruption reduction in criminal policy perspective). *Jurnal Legislasi Indonesia*, 8(2), 217–238.
- Nuristiningsih, D. (2023). Upaya penal dan non penal dalam menanggulangi tindak pidana teknologi informasi. *Majalah Keadilan*, 23, 62–90. <https://journals.unihaz.ac.id/index.php/keadilan/article/view/4153>

- Saraya, S., Handayani, Y., & Valentino, D. B. (2023). Penegakan hukum terhadap tindak pidana cyber di wilayah hukum Polda Jateng. *Jurnal Hukum Universitas Selamat Sri*, 4–19. <https://doi.org/10.48175/ijarsct-13062>
- Sugiaryo. (2010). Kebijakan regulasi hukum pidana dalam menangani kejahatan teknologi informasi. *Jurnal Serambi Hukum*, 4(2).
- Zainuddin, Q. G., & Kurniati. (2024). Manfaat dan mafsadat teknologi modern perspektif masalah. *UNES Law Review*, 6(2), 6782–6789.