Volume 15. Number 2. December 2020 Page 228-241

Pandecta

http://journal.unnes.ac.id/nju/index.php/pandecta

Kebijakan Kriminal Non Penal dengan Techno Prevention (Analisis Pencegahan Konten Negatif Melalui Internet)

Cahya Wulandari[1]

[1]Program Doktor Hukum, Universitas Diponegoro, Semarang, Indonesia

[2]Fakultas Hukum, Universitas Negeri Semarang, Semarang, Indonesia

DOI: http://dx.doi.org/10.15294/pandecta.v15i2.23650

Article info

Article History:
Received : January 30td 2020
Accepted: August 15td 2020
Published: December 1st 2020

Keywords:
kebijakan kriminal; non penal; techno prevention; konten negatif

criminal policy; non penal; techno prevention; negative content

Abstrak

Pesatnya perkembangan teknologi informasi khususnya terkait dengan penggunaan internet selain memberikan dampak positif juga memberi dampak negatif. Dampak negatif dari penggunaan perkembangan teknologi dan adanya penyebaran konten negatif mendorong suatu kebijakan kriminal non penal melalui techno prevention. Penggunaan berbagai program dan aplikasi internet yang telah diciptakan oleh Kemenkominfo menjadi salah satu bentuk kebijakan kriminal non penal melalui upaya penggunaan techno prevention dalam penanggulangan penyebaran konten negatif. Artikel ini bertujuan menjabarkan kebijakan kriminal non penal melalui techno prevention sebagai upaya pencegahan konten negatif melalui internet dengan menggunakan metode penelitian hukum normatif (normative legal research) melalui statute approach yang didasarkan pada penelaahan peraturan hukum yang terkait dengan masalah yang dibahas. Kebijakan kriminal non penal lebih menitikberatkan pada sifat "preventif" yang bersifat pencegahan sebelum kejahatan terjadi. Bentuk kebijakan kriminal non penal sebagai upaya penanggulangan penyebaran konten negatif dilakukan melalui edukasi dan techno prevention.

Abstract

The rapid development of information technology, especially the use of the internet, has a positive and negative impact. The negative impact of technological developments and the spread of harmful content encourages a non-criminal criminal policy through techno prevention. The use of various internet programs and applications created by Kemenkominfo become one form of non-criminal policy through efforts to use techno prevention to overcome the spread of harmful content. This article aims to describe non-penal policy through techno prevention to prevent harmful content through the internet using normative legal research methods through a statute approach based on a review of legal regulations related to the issues discussed. Non-penal policy focuses more on the "preventive" nature of prevention before a crime occurs. The form of non-penal policy as an effort to overcome the spread of harmful content solved through education and techno prevention.

✉
Address : Jl. Prof. Soedarto, Tembalang, Kec. Tembalang, Kota Semarang, Jawa Tengah 50275
E-mail : cahyawulandari1984@gmail.com

ISSN 1907-8919 (Cetak)
ISSN 2337-5418 (Online)

1. Pendahuluan

Di Era milenial, kehidupan tidak dapat terpisahkan dari perkembangan teknologi. Teknologi selalu ada dan dibutuhkan di setiap waktu, setiap tempat dan oleh siapa pun. Perubahan besar dalam perkembangan teknologi telah mendorong Bangsa Indonesia sebagai Negara demokrasi modern untuk menjelmakan sistem elektroniknya guna kepentingan publik. Hal tersebut dikonkretkan dengan adanya Undang-Undang Nomor 14 Tahun 2008 tentang Keterbukaan Informasi Publik (UU KIP) dan Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE) jo Undang-Undang Nomor 19 Tahun 2016 (Makarim, 2009: 6).

Pengaturan lebih lanjut terkait dengan Sistem Elektronik tidak dapat dilepaskan dari hukum telematika. Terdapat simpang siur pendapat mengenai hukum yang memayungi segala peraturan di bidang telematika, mulai dari Undang-Undang ITE, UU Telekomunikasi ataukah peraturan perundang-undangan lain seperti KUHP. Penting tentunya untuk diketahui bersama, bertolak dari pemahaman mengenai telematika sebagai hukum terhadap perekembangan konvergensi TELEMATIKA (Telekomunikasi, Media dan Informatika) yang berwujud dalam penyelenggaraan suatu sistem elektronik, baik yang terkoneksi melalui internet (*cyberspace*) maupun yang tidak terkoneksi dengan internet meliputi aspek-aspek hukum yang terkait dengan keberadaan sistem informasi dan sistem komunikasi, khususnya yang dilakukan dengan penyelenggaraan sistem elektronik (Makarim, 2003: 8).

Teknologi telah mengubah dunia (Chiappetta, 2017), menjadikan hidup lebih mudah, terintegrasi dalam kehidupan setiap individu. Munculnya teknologi digital dengan perkembangan internet telah memungkinkan kemajuan umat manusia; Dunia Wide-Web telah merevolusi perusahaan yang ada merangkul dunia digital, sedangkan Web 2.0 dan sosial komunikasi media telah berubah secara dramatis dan dalam saat yang sama semua telah menjadi pengguna. Teknologi informasi dan komunikasi merupakan salah satu teknologi yang berkembang dengan sangat pesat. Pesatnya perkembangan teknologi informasi dan komunikasi akan menciptakan (*to create*), mengakses (*to access*), mengolah (*to process*), dan memanfaatkan (*to utilize*) informasi secara tepat dan akurat. Informasi merupakan suatu komoditi yang sangat berharga di era globalisasi untuk dikuasai dalam rangka meningkatkan daya saing suatu organisasi secara berkelanjutan (Hasibuan, 2007).

Perkembangan telematika terjadi sedemikian pesat bahkan tidak terlepas dari setiap bidang yang ada dalam masyarakat di suatu negara. Pesatnya perkembangan teknologi informasi khususnya terkait dengan penggunaan internet selain memberikan dampak positif juga memberi dampak negatif. Penggunaan internet secara tidak bertanggung jawab yang bersifat propaganda atau bahkan SARA oleh beberapa pihak seringkali mengganggu stabilitas keamanan negara. Salah satunya yang sedang marak adalah kasus *cyberbullying* terhadap anak. Diantaranya kasus terbaru terkait dengan *Cyberbullying* yang terjadi di Indonesia adalah kasus Betrand Peto, putra presenter Ruben Onsu sempat menjadi korban kejahatan dunia maya. Wajahnya diedit menjadi wajah hewan oleh oknum tak bertanggung jawab (Melvina, 2020).

Tersebarnya pemberitaan dengan sumber dan data yang tidak dapat dipertanggung jawabkan telah membuat keresahan di kalangan masyarakat bahkan menimbulkan pertikaian antar warga negara yang secara tidak langsung mengganggu stabilitas keamanan yang mempengaruhi kondisi perekonomian, sosial, budaya, politik, dan pertahanan keamanan. Hal tersebut mendorong Pemerintah untuk melakukan pembatasan penggunaan internet dengan alasan menjaga persatuan dan kesatuan Bangsa Indonesia, demi keamanan dan ketertiban yang tercipta di tengah masyarakat.

Dalam beberapa tahun terakhir, terjadi peningkatan pemblokiran situs-situs internet bermuatan negatif atau yang dianggap melanggar hukum (*illegal content*). Pada akhir Maret 2015, atas permintaan Badan Nasional Penanggulangan Terorisme (BNPT), Kementerian Komunikasi dan Informatika (Kemenkominfo) memblokir beberapa situs internet

yang menyerukan dakwah Islamiah yang dinilai bermuatan radikal. Dikatakan sebagai penyeru dakwah Islamiyah, karena dilihat dari nama-namanya, situs-situs itu menggunakan nama atau atribut yang berhubungan dengan Islam, seperti dakwatuna.com, dakwahmedia.com, voa-islam.com, eramuslim, dan sebagainya (Musyafak et al, 2017).

Ditahun 2016, Kemenkominfo sudah memblokir 773.097 situs bermuatan negatif yang sebagian besar berisi materi pornografi, lebih besar ketimbang tahun 2015 di mana sebanyak 766.394 situs diblokir Pemerintah (Setiyanti et al, 2017). Sementara itu, di tahun pertama 2017 Kemenkominfo memblokir 6.000 situs internet atau akun media sosial yang diduga menyebarkan ujaran kebencian, fitnah dan *hoax* (Republika, 2017).

Pemblokiran beberapa situs yang menyebarkan konten negatif ini sebagai salah satu upaya Pemerintah untuk mencegah terjadinya kejahatan sebagai akibat dari melihat tayangan dari situs tersebut. Tentunya, tidak hanya cukup sekedar melakukan pemblokiran situs-situs internet yang bermuatan negatif ataupun pembuatan peraturan perundang-undangan yang mengatur terkait dengan telematika akan tetapi juga perlunya suatu kebijakan kriminal yang bersifat preventif dari penyebaran konten negatif.

G P. Hoefnagels menguraikan beberapa upaya penanggulangan kejahatan , yaitu: penerapan hukum pidana (*criminal law application*); pencegahan tanpa pidana mengenai suatu kejahatan; pemidanaan melalui media masa *(influencing views of society on crime and punishment/mass media* (Muladi, 1995: 9-11). Kebijakan kriminal secara garis besar dapat dikelompokkan menjadi dua, yaitu: kebijakan kriminal dengan menggunakan sarana hukum pidana (*penal policy*); dan kebijakan kriminal dengan menggunakan sarana di luar hukum pidana (*nonpenal policy*). Kedua sarana ini (penal dan nonpenal) merupakan satu kesatuan yang tidak dapat dipisahkan, bahkan saling melengkapi dalam usaha penanggulangan kejahatan di masyarakat (Arief, 2010). T*echno prevention* dianggap dapat mengimbangi kecepatan perekembangan di bidang teknologi dan digunakan sebagai upaya preventif dalam penyebaran konten negatif di internet. Berdasarkan pada latar belakang sebagaimana telah dijabarkan, maka muncul permasalahan terkait dengan bagaimanakah kebijakan kriminal *non penal* melalui *techno prevention* sebagai upaya pencegahan konten negatif melalui internet?

2. Metode Penelitian

Metode Penelitian yang digunakan di dalam penulisan ini adalah metode penelitian hukum hukum normatif (*normative legal research*), dengan menggunakan pendekatan *statute approach*. Maksud dari *statute approach* adalah pendekatan yang didasarkan pada penelaahan peraturan hukum yang terkait dengan masalah yang dibahas. Peraturan hukum tersebut adalah data sekunder, yaitu data yang diperoleh secara tidak langsung sumbernya atau objek penelitiannya berupa bahan hukum primer, sekunder dan tersier (Suteki,. & Taufani, 2018: 163). Analisis dan pembahasan atas rumusan masalah yang ada dengan menggunakan studi kepustakaan (*library research*) yang kemudian dianalisis secara kualitatif sehingga diperoleh suatu kesimpulan.

3. Hasil Penelitian dan Pembahasan

Perkembangan dari teknologi informasi salah satunya membawa pengaruh terhadap semakin konvergennya sistem komputasi (*computing system*) dan sistem komunikasi yang mendorong terintegrasinya kedua sistem tersebut pada jarak jauh (*telecommunication system*). Secara pesat, teknologi ini mengubah cara hidup masyarakat, dimana internet sebagai salah satu bentuk perkembangan teknologi informasi membuat batas ruang dan waktu sudah tidak menjadi kendala besar (*boerdeless*) (Asshiddiqie, 2005: 225). Intrernet telah melahirkan konsep baru di berbagai bidang yaitu bidang perdagangan *(e-commerce),* bidang pendidikan *(e-learning),* bidang pemerintahan *(e-goverment),* dan bidang politik *(e-democracy)* (Subrata, 2004: 111).

Interconnecting networking atau internet secara sederhana dapat diartikan sebagai sebuah jaringan global dari jaringan-jaringan

komputer, dengan ciri khasnya bersifat mendunia dan menyebar dengan jangkauan tanpa batas secara global (Munir, 2017: 174). Internet dapat juga diartikan sebagai kumpulan jaringan global yang terhubung dan berbagi informasi melalui seperangkat protokol umum dengan fitur yang paling kuat, memungkinkan komputer terhubung ke jaringan komunikasi secara terbuka, efektif terlepas dari pembuatan, arsitektur, sistem operasi, atau lokasi dengan sumber daya dan manajemen jaringan didistribusikan secara luas tanpa titik pusat kendali (Miller, Gerri Sinclair, David Sutherland, Julie Zilber, 2009).

Sumber daya Internet dapat dibagi menjadi 2 (dua), yaitu: IP address dan Nama Domain. Sementara jika kita amati lebih jauh sumber daya yang tak terpisahkan adalah keberadaan setiap data dan/atau informasi yang melintasi internet, khususnya data pribadi setiap orang yang melakukan transaksi. Dalam tata kelola internet, ketentuan hukum yang berlaku ialah hukum komunitas. Pemerintah tidak memiliki kewenangan untuk melakukan pengaturan *IP Address* dan Nama Domain oleh karena itu dikenal kaedah ketentuan yang *self-regulatory*. Demikian pula keberadaan sistem pencatatan pengalamatan IP dan Nama Domain (Makarim, 2015).

Dalam prakteknya, pengguna dapat menggunakan sejumlah teknik dan program aplikasi untuk menyembunyikan jejak aktivitas online mereka. Meskipun alamat IP pengguna dicatat dalam aktivitas apa pun yang mereka tampil di internet, pengguna dapat menggunakan proxy server untuk menutupi Alamat IP ketika bertindak online. Oleh karenanya hampir sepertiga pengguna internet dapat memalsukan alamat IP sumbernya tanpa deteksi (Tran, 2018).

Ketiadaan kewenangan Pemerintah untuk pengaturan IP Address dan Nama Domain menyebabkan semakin maraknya penyalahgunaan internet, khususnya penyebaran konten negatif yang pada akhirnya berimbas pada terjadinya tindak pidana yang lainnya seperti tindak asusila, pelecehan seksual, pertentangan SARA dan efek lebih luas lagi memecah belah persatuan kesatuan bangsa.

Penyebaran konten negatif ini perlu didekati dengan kebijakan kriminal *non penal* sebagai upaya preventif. Hal tersebut akan lebih efektif dibanding dengan kebijakan kriminal penal yang baru diterapkan setelah terjadinya suatu tindak pidana. Dengan kebijakan kriminal *non penal* maka diharapkan dapat meminimalisir atau mencegah terjadinya tindak pidana yang ditimbulkan dari adanya penyebaran konten negatif oleh pihak tertentu. Bentuk kebijakan kriminal *non penal* sendiri dengan menggunakan *techno prevention* sebagai bentuk yang dimungkinkan untuk menghadapi penyebaran konten negatif melalui internet. Pergerakan teknologi yang sedemikian cepat membutuhkan upaya pencegahan yang cepat pula dengan menggunakan sarana teknologi juga.

Di dalam pembahasan lebih lanjut terkait dengan kebijakan kriminal *non penal* melalui *techno prevention* sebagai upaya pencegahan konten negatif melalui internet akan dibahas terkait dengan *techno prevention* dan kebijakan kriminal *non penal*.

1) Techno Prevention

Antara teknologi dan politik tentu saja berbeda, politik didasarkan pada nilai-nilai sementara teknologi tumbuh subur dalam pengetahuan ilmiah dan fakta-fakta obyektif. Padahal hukum dibuat dalam domain publik, regulasi teknis harus ditempatkan dalam kerangka kerja yang lebih luas yang merangkum keterikatan timbal balik antara budaya, politik dan teknologi. Seperti yang dikatakan Don Ihde: 'teknologi merupakan bagian dari kehidupan yang tidak dapat terpisahkan dari budaya, sama seperti budaya pada manusia, akal pasti menyiratkan teknologi'. Atau, seperti Andrew Feenberg menulis 'Teknologi harus dibawa ke ruang publik di mana ia semakin meningkat'. Setiap sistem hukum memiliki klaim legitimasi dalam arti bahwa sumber otoritas bergantung pada hak moral untuk memerintah. Dalam sistem demokrasi modern, prinsip supremasi hukum, sebagai pilar penting dari dimensi moral ini, mensyaratkan bahwa aturan diumumkan secara terbuka dengan aplikasi prospektif, dan memiliki karakteristik umum, persamaan, dan kepastian. Sebagai perlindungan hak, pencegahan kesewenang-wenangan dan meminta

pertanggungjawaban negara untuk tindakan yang melanggar hukum hanya mungkin dilakukan dengan cara yang dapat dipahami, andal dan dapat diprediksi ketertiban, universalitas, aplikasi yang relatif konstan dari waktu ke waktu secara prospektif dan cara non-kontradiktif dapat dianggap sebagai konstituen utama gagasan supremasi hukum. Hak dapat digunakan dengan batas dan ruang lingkupnya, bukan dengan sebebas-bebasnya (Bayamlıoğlu, 2018).

Teknologi tidak dapat terpisahkan dari budaya, tentunya dalam penggunaannya dilakukan secara bertanggungjawab dan tidak sewenang-wenang dengan mengganggap bahwa hal tersebut bagian dari hak setiap individu. Sebagaimana telah dijelaskan sebelumnya bahwa hak dibatasi dalam penggunaannya dan disesuaikan ruang lingkup keberlakuannya. Terkait dengan pembahasan dalam artikel ini, penggunaan *techno prevention* ini sebagai suatu upaya pencegahan terjadinya penyebaran konten negatif oleh individu-individu yang tidak bertanggungjawab menggunakan internet sesuai dengan batas dan ruang lingkup yang telah ditentukan.

Dalam hal penyebaran konten negatif melalui internet, hukum pidana tidak akan mampu bekerja sendiri. Sebagaimana telah dijelaskan sebelumnya, bahwa penyebaran konten negatif sangat berpengaruh tidak hanya secara individu semata tetapi bahkan pada keamanan suatu bangsa dan negara terkait dengan persatuan dan kesatuan. Penyebaran konten negatif ini tentu saja tidak terlepas dari penggunaan teknologi maju sebagai sarana dan prasarana. Oleh karena itu, upaya yang paling rasional dalam menghadapi penyebaran konten negatif tersebut adalah mengutamakan pendekatan teknologi (*techno prevention*).

Model prevensi ini menjadi aktual karena keterbatasan hukum pidana itu sendiri yang bersifat *post factum*. Maksudnya, respon hukum pidana lahir ketika kejahatan sudah terjadi. Model pendekatan ini tidak lagi strategis dan efektif untuk menjawab munculnya persoalan kejahatan yang relatif baru karena pengaruh langsung dari kemajuan teknologi (Ufran, 2014).Untuk menjawab tuntutan itu maka kedepan perlu dipikirkan beberapa upaya alternatif untuk melakukan kontrol terhadap penyebaran konten negatif. Salah satunya adalah pendekatan yang berbasis teknologi yaitu penggunaan *techno prevention***.**

Suatu kejahatan sejatinya bukan hanya sekedar permasalahan hukum tetapi tidak terlepas dari masalah-masalah sosial yang menjadi faktor penyebab terjadinya suatu kejahatan itu sendiri. Oleh karenanya dalam penanganan suatu kejahatan diperlukan suatu kebijakan integral yang menyeimbangkan antara penggunaan upaya penal dan non penal. Upaya non penal bersifat preventif, mencegah terjadinya suatu tindak pidana dan dianggap dapat mengikis penyebab terjadinya tindak pidana itu sendiri sampai pada akar masalah yang ada. Berdasarkan pada hasil penelitian, (Ufran, 2014) mengemukakan bahwa salah satu jenis kejahatan yang dapat berhasil diselesaikan di Indonesia dengan menggunakan *techno prevention* diantaranya adalah *cyberterrorism*. Upaya penanggulangan kejahatan menggunakan upaya penal dianggap tidak lagi efektif dan efisien dalam penyelesaian persoalan kejahatan yang relatif baru karena pengaruh langsung dari kemajuan teknologi. Salah satu bentuk alternatif sebagai upaya kontrol terhadap *cyberterrorism* melalui pendekatan yang berbasis teknologi yaitu *Biometric Technology* untuk mencegah terjadinya *cyberterrorism*.

Terkait dengan pembahasan artikel mengenai pencegahan terjadinya penyebaran situs negatif di internet yang seringkali menimbulkan kekacauan dalam masyarakat bahkan sampai mengancam persatuan dan kesatuan negara tentunya dengan pendekatan *techno prevention* akan lebih efektif dan tepat sasaran yang menjadi upaya preventif tidak terjadinya penyebaran konten negatif melalui media internet. Seiring dengan perkembangan teknologi dan adanya penyebaran konten negatif yang seringkali tidak dapat terbendung lagi, terdapat beberapa perangkat lunak (*software*) yang digunakan untuk memberikan perlindungan bagi anak ketika menggunakan *internet* dan terhubung di dalam dunia maya. Aplikasi *parental control*

dan penapis dapat digunakan untuk membantu melindungi keamanan anak di *internet* dan dipasang di berbagai jenis *gadget* yang digunakan. Beberapa aplikasi *parental control* yang dapat di pasang di antaranya adalah *Qustodio*, *K9 Web Protection*, *Kakatu* dan *DNS Nawala*.*Software* seperti *Kakatu* dan *DNS Nawala* adalah teknologi buatan Indonesia yang disarankan oleh Kemenkominfo dan komunitas yang peduli terhadap *internet* sehat dan menciptakan dunia maya yang aman (Mufid, 2018).

2) Kebijakan kriminal ***non penal*** *melalui* ***techno prevention*** *sebagai upaya pencegahan konten negatif melalui internet*

Menurut Kartini (Kartono, 2005: 139), kejahatan itu bukan merupakan peristiwa *herediter* (bawaan sejak lahir, warisan) juga bukan merupakan warisan biologis. Tingkah laku kriminalitas itu bisa dilakukan oleh siapapun juga, baik wanita maupun pria; dapat berlangsung pada usia anak, dewasa ataupun lanjut umur. Tindak kejahatan bisa dilakukan secara sadar misalnya, didorong oleh impuls-impuls yang hebat, didera oleh dorongan-dorongan paksaan yang sangat kuat (kompulsi-kompulsi), dan oleh obsesi-obsesi. Kejahatan bisa juga dilakukan secara tidak sadar sama sekali.

Upaya atau kebijakan untuk melakukan pencegahan dan penanggulangan kejahatan termasuk bidang "kebijakan kriminal". Kebijakan kriminal merupakan bagian dari kebijakan sosial yang terdiri dari "kebijakan/upaya-upaya untuk kesejahteraan sosial" (*social welfare policy*) dan "kebijakan/upaya-upaya untuk perlindungan masyarakat" (*social defence policy*). Kebijakan penanggulangan kejahatan (politik kriminal) dilakukan dengan menggunakan sarana *penal* (hukum pidana), maka kebijakan hukum pidana (*penal policy*), khususnya pada tahap kebijakan yudikatif/aplikatif harus memperhatikan dan mengarah pada tercapainya tujuan dari kebijakan sosial itu (Arief, 2010: 77). Analisis pendekatan sistem memperlihatkan bahwa kebijakan kriminal merupakan bagian integral dari kebijakan yang lebih besar, yaitu kebijakan perlindungan masyarakat, kebijakan kesejahteraan masyarakat dan secara makro bagian dari kebijakan sosial (Pujiono, 2012: 121).

Marc Ancel, seperti dikutip oleh Barda Nawawi Arief, merumuskan kebijakan kriminal sebagai *rational organitation of the control of crime by society* atau *the rational organization of the social reaction of crime by society* atau *the rational organiation of the social reaction of crime* (Muladi, 1995: 7). Sedangkan menurut Hoefnagels, kebijakan kriminal secara garis besar dapat dikelompokkan menjadi dua, yaitu: kebijakan kriminal dengan menggunakan sarana hukum pidana (*penal policy*); dan kebijakan kriminal dengan menggunakan sarana di luar hukum pidana (*non penal policy*). Kedua sarana ini (*penal* dan *non penal*) merupakan satu kesatuan yang tidak dapat dipisahkan, bahkan saling melengkapi dalam usaha penanggulangan kejahatan di masyarakat (Muladi, 1995: vii).

Kebijakan kriminal merupakan bentuk pembaharuan hukum pidana yang terpadu. Prof. Sudarto dalam bukunya Kapita Selekta Hukum Pidana, pernah mengemukakan tiga arti mengenai kebijakan kriminal, yaitu : (Jaya, 2017: 23).

a. dalam arti sempit, ialah keseluruhan asas dan metode yang menjadi dasar dari reaksi terhadap pelanggaran hukum yang berupa pidana;
b. dalam arti luas, ialah keseluruhan keseluruhan fungsi dari aparatur penegak hukum, termasuk di dalamnya cara kerja dari pengadilan dan polisi;
c. dalam arti paling luas, ialah keseluruhan kebijakan, yang dilakukan melalui perundang-undangan dan badan-badan resmi yang bertujuan untuk menegakkan norma-norma sentral dari masyarakat.

Pencegahan dan penanggulangan kejahatan harus dilakukan dengan pendekatan integral, ada keseimbangan sarana penal dan *non penal*. Dari sudut politik kriminal, kebijakan strategis melalui sarana *non penal* karena lebih bersifat preventif dan karena kebijakan penal mempunyai keterbatasan/kelemahan lebih bersifat represif/tidak preventif dan ha-

rus didukung oleh infrastruktur dengan biaya tinggi (Arief, 2010: 78). Sebagai usaha penanggulangan kejahatan, kebijakan kriminal dapat bersifat **pertama**, represif yang menggunakan sarana *penal*, **kedua**, usaha-usaha tanpa menggunakan sarana *penal* (*prevention without punishment*), dan **ketiga**, mendayagunakan usaha-usaha pembentukan opini masyarakat tentang kejahatan dan sosialisasi hukum melalui media (Muladi dan Barda Nawawi Arief, 2007: 9). Upaya penanggulangan kejahatan lewat jalur penal lebih menitikberatkan pada sifat "represif" sesudah kejahatan terjadi, sedangkan jalur *non penal* lebih menitikberatkan pada sifat "preventif" (pencegahan/penangkalan/pengendalian) sebelum kejahatan terjadi. Pada hakikatnya tindakan represif merupakan tindakan preventif dalam arti luas.

Salah satu jalur *non penal* untuk mengatasi masalah-masalah sosial adalah melalui kebijakan sosial (*social policy*), yang dalam skema G.Peter Hoefnagels dimasukkan dalam bagian *prevention without punishment*. Kebijakan sosial pada dasarnya dalah kebijakan atau upaya-upaya rasional untuk mencapai kesejahteraan masyarakat (Arief, 2010: 48-49). Wujud konkret dari penerapan upaya *non penal* ini salah satunya dalam bidang tindak pidana sektor perbankan sebagaimana dikemukakan oleh (Wulandari, 2013), penyelesaian sengketa melalui jalur non litigasi sendiri nampaknya mulai mendapat tempat dalam dunia perbankan, dengan dibentuknya Lembaga Mediasi Perbankan, Bank Indonesia (BI) bertugas melakukan penyelesaian secara non litigasi (di luar pengadilan) dengan menggunakan mediasi sebagai sarana penyelesaian sengketa.

Kebijakan kriminal secara *non penal* dapat ditempuh dengan melakukan pendekatan agama, budaya/kultural, moral/edukatif sebagai upaya preventif dengan melakukan serangkaian program kegiatan dengan fokus penguatan, penanaman nilai budi pekerti yang luhur, etika sosial, serta pemantapan keyakinan terhadap agama melalui pendidikan agama (Abdullah, 2012). Menurut M.Hamdan, upaya penanggulangan yang merupakan bagian dari kebijakan sosial pada hakikatnya juga merupakan bagian integral dari upaya perlindungan masyarakat (*social defence*) yang dapat ditempuh dengan 2 (dua) jalur, yaitu: (Hamdan, 1997: 19).

1. Jalur penal, yaitu dengan menerapkan hukum pidana (*criminal law application*)
2. Jalur *non penal*, yaitu dengan cara:
   a. Pencegahan tanpa pidana (*prevention without punishment*), termasuk di dalamnya penerapan sanksi administratif dan sanksi perdata.
   b. Mempengaruhi pandangan masyarakat mengenai kejahatan dan pembinaan lewat media massa (*influencing views of society on crime and punishment*)

Upaya penanggulangan kejahatan perlu ditempuh dengan pendekatan kebijakan, dalam arti ada ketepaduan (integralis) antara politik kriminal dan politik sosial serta ada keterpaduan antara upaya penanggulangan kejahatan dengan *penal* dan *non penal*. Penegasan tentang perlunya upaya penanggulangan kejahatan diintegrasikan dengan keseluruhan kebijakan sosial dan perencanaan pembangunan terlihat juga dalam pernyataan Sudarto yang menyatakan bahwa apabila hukum pidana hendak digunakan sebagai sarana untuk menanggulangi kejahatan, maka penggunannya tidak terlepas dalam hubungan keseluruhan politik kriminal atau "planning for social defence". *Social Defence Planning* ini pun harus merupakan bagian yang integral dari rencana pembangunan nasional (Sudarto, 1996: 96). Dari pendapat tersebut penanggulangan kejahatan secara umum dapat ditempuh melalui dua pendekatan yaitu penal dan *non penal*. Keduanya dalam fungsinya harus berjalan beriringan secara sinergis dan saling melengkapi. Ruang lingkup kebijakan kriminal sebagai bagian dari kebijakan atau "policy" (yaitu bagian dari politik hukum, politik hukum pidana dan politik sosial) maka diperlukan upaya baik dengan pendekatan *penal* maupun *non penal* (Ganesh et.al, 2019).

Terkait dengan pembahasan perkembangan teknologi, selain memberikan manfaat juga mempunyai dampak negatif. Beberapa dampak negatif yang ditimbulkan dari

penggunaan internet diantaranya: konten dewasa, tersebarnya berbagai informasi palsu, berita *hoax*, menampilkan sisi kekejaman, penipuan dan beberapa konten negatif lainnya.

Kejahatan bukanlah sekedar permasalahan hukum, melainkan termasuk masalah sosial dan masalah kemanusiaan. Oleh karenanya dalam penanggulangan kejahatan dibutuhkan sebuah kebijakan yang integral dengan menggunakan pendekatan *penal* (penerapan hukum pidana) dan pendekatan *non penal* (pendekatan di luar hukum pidana). Selain menggunakan peraturan perundang-undangan yang menjadi dasar dalam melakukan tindakan atas kejahatan di bidang teknologi, maka perlu juga dibuat kebijakan dengan pendekatan *non penal* yang lebih menitikberatkan pada upaya preventif sebelum terjadinya kejahatan. Berbeda halnya dengan kebijakan penal yang baru bekerja setelah terjadinya suatu tindak pidana, maka kebijakan penanggulangan kejahatan melalui jalur "non penal" lebih bersifat tindakan pencegahan sebelum terjadinya kejahatan.

Di dalam Rancangan Kitab Undang-Undang Hukum Pidana (September 2019), kebijakan penanggulangan tindak pidana melalui upaya penal yang terkait dengan kejahatan di bidang teknologi telah dirumuskan dalam perluasan asas teritorial sebagaimana diatur dalam Pasal 4 huruf (c) RKUHP 2019 mengenai ketentuan pidana dalam Undang-Undang berlaku bagi setiap orang yang melakukan tindak pidana di bidang teknologi informasi atau tindak pidana lainnya yang akibatnya dialami atau terjadi di wilayah Negara Kesatuan Republik Indonesia atau di Kapal Indonesia dan di Pesawat Udara Indonesia. Dalam Buku II yang mengatur tentang Tindak Pidana telah dilakukan perumusan delik terkait dengan kemajuan teknologi untuk dapat menanggulangi tindak pidana yang terkait dengan bidang teknologi, diantaranya: Pasal 228 (penyerangan kehormatan atau harkat dan martabat terhadap kepala negara sahabat di di NKRI menggunakan sarana teknologi informasi); Pasal 243 (perasaan permusuhan melalui sarana teknologi informasi; Pasal 247 (hasutan agar melakukan Tindak Pidana atau melawan penguasa umum dengan Kekerasan melalui sarana teknologi informasi); Pasal 250 (penawaran untuk memberi keterangan, kesempatan atau sarana guna melakukan Tindak Pidana dengan menggunakan sarana teknologi informasi); Pasal 257 (Penyadapan); Pasal 258 (merekam gambar seseorang atau lebih yang berada di dalam suatu rumah atau ruangan yang tidak terbuka); Pasal 262, Pasal 263 (Penyiaran Berita Bohong); Pasal 337, 338, 339, Pasal 354 (Tanpa Hak Mengakses Komputer dan Sistem Elektronik).

Bentuk penanggulangan kejahatan di bidang teknologi melalui upaya penal sebagaimana telah dijabarkan sebelumnya sudah semestinya ditegakkan secara integral dengan penanggulangan kejahatan melalui jalur "non penal" yang lebih bersifat tindakan preventif dengan sasaran utama untuk menangani faktor-faktor kondusif penyebab terjadinya kejahatan yang berasal dari masalah-masalah atau kondisi-kondisi sosial penyebab kejahatan. Kebijakan *non penal* dapat ditempuh dengan beberapa macam cara, antara lain perbaikan ekonomi nasional, pendidikan budi pekerti terutama kepada pihak yang rentan melaksanakan kejahatan, perbaikan sistem kesehatan mental masyarakat, mengefektifkan kerjasama internasional dalam pemberantasan *cyber crime*, memperbaiki sistem pengamanan komputer, serta mengefektifkan hukum administrasi dan hukum perdata yang berhubungan dengan penyelenggaraan sistem dan jaringan internet (Alvionita et.al, 2013).

Dalam hal upaya pembatasan penyebaran konten negatif, kebijakan kriminal *non penal* yang digunakan dapat berupa pengembangan pola pencegahan primer (*primary prevention*) dengan sasaran korban potensial dan para pelaku kejahatan; pencegahan sekunder (*secondary prevention*) dan pencegahan tersier (*tertiary prevention*). Bentuk lainnya adalah pencegahan individual (*individual prevention*) dan pencegahan masyarakat (*societal prevention*) (Muladi dan Dyah Sulistyani, 2016: 161). Terkait dengan pembahasan mengenai kebijakan kriminal *non penal* berupa penggunaan *techno prevention* ini lebih berhubungan dengan adanya program pem-

batasan penggunaan konten dalam internet dan aplikasi yang membatasi akses konten negatif. Dalam pelaksanaan kebijakan kriminal *non penal* ini, Pemerintah bekerjasama dengan Kementerian Komunikasi dan Informatika.

Pendekatan teknologi guna mencegah kejahatan ini merupakan subsistem dalam sebuah sistem yang lebih besar, yaitu pendekatan budaya karena teknologi merupakan hasil dari kebudayaan. Pendekatan budaya ini perlu dilakukan karena untuk membangun atau membangkitkan kepekaan warga masyarakat dan aparat penegak hukum dan menyebarluaskan tentang etika penggunaan komputer melalui media pendidikan. Tujuan utama dari upaya-upaya *non penal* mempunyai pengaruh preventif terhadap kejahatan yang memiliki kedudukan strategis dalam memegang posisi kunci yang terus diefektifkan.

Kebijakan *non penal* merupakan bentuk upaya preventif yang bersifat pencegahan dalam penanggulangan tindak pidana, berbeda halnya dengan kebijakan penal yang bersifat represif (pemberantasan). Kebijakan *penal* menggunakan hukum pidana seringkali tidak efektif karena baru bekerja setelah terjadinya suatu tindak pidana. Untuk kasus tertentu semisal terkait dengan perkembangan teknologi yang sedemikian cepat, penyebaran konten negatif tidak dapat terbendung lagi, dapat diakses dalam sepersekian detik oleh siapapun dan dari belahan bumi manapun. Oleh karena itu, penyebaran konten negatif sudah seharusnya dicegah sejak awal supaya tidak menimbulkan dampak yang lebih luas misal terganggunya stabilitas keamanan suatu Negara, memecah belah persatuan bangsa sebagaimana kasus pilkada dan kerusuhan di Wamena, Papua. Sebagai langkah preventif, kebijakan *non penal* menjadi pilihan yang tepat untuk membatasi penyebaran konten negatif.

Kebijakan kriminal *non penal* diprakarsai demi terwujudnya sebuah kesejahteraan. Kesejahteraan yang dimaksud tidak hanya pada sisi korban atau masyarakat pada umumnya namun lebih dari itu sisi pelaku juga dipertimbangkan keberadaannya. Kebijakan kriminal *non penal* dapat hadir guna melindungi kepentingan pelaku *non penal*, dapat menjadikan masyarakat sebagai lingkungan sosial dan lingkungan hidup yang sehat (secara materiil dan immateriil) dari faktor-faktor kriminogen. Penanggulangan dengan menggunakan pendekatan teknologi (*techno prevention*) dimulai dengan menciptakan keamanan dalam sistem elektronik informasi dan komunikasi yang digunakan. Baik , laptop, telepon selular dan perangkat elektronik lainnya (Frensh et.al, 2017).

Kebijakan kriminal *non penal* untuk penanggulangan penyebaran konten negatif dilakukan melalui edukasi dan *techno prevention*. Kementerian Komunikasi dan Informatika sebagai regulator membuat beberapa program untuk pencegahan penyebaran konten negatif dengan penggunaan teknologi diantaranya: (Kompas, 2017)

1) Program edukasi bagi masyarakat guna meminimalisir dampak negatif dari perkembangan teknologi.
   a) Pada Tahun 2010, Kemenkominfo menginiasi program Internet Sehat dan Aman (INSAN). Program ini memberi pemahaman yang cukup tentang penggunaan internet secara bijak dengan mengetahui bahaya internet dan antisipasinya, serta menumbuhkan semangat berinternet secara sehat dan aman.
   b) Setelah dua tahun berjalan, program INSAN diubah menjadi program Internet Cerdas Kreatif dan Produktif (INCAKAP), yang berarti penggunaan internet secara cerdas kreatif dan produktif serta beretika. Terjadi perubahan pendekatan dari yang awalnya *infrastructure protective* menjadi *self protective*, dimana masyarakat harus lebih mandiri dalam memilih situs yang bermanfaat bagi dirinya. Keberadaan INCAKAP juga bertujuan agar generasi muda lebih produktif untuk meningkatkan kemampuan atau taraf hidupnya seperti Andrew Darwis, founder komunitas online terbesar di Indonesia, Kaskus.
2) Membangun sistem penangkalan konten negatif yaitu software Whitelist

Nusantara yang akan digunakan oleh institusi pendidikan di tingkat SD, SMP, SMA, dan pesantren untuk mengatur situs yang diperbolehkan untuk diakses oleh para pelajar. Sampai saat ini pun Kemenkominfo masih mengembangkan langkah-langkah untuk meminimalisir berkembangnya konten negatif.

Konten negatif di internet kerap menjadi perhatian orang tua di internet. Berdasarkan laporan Kementerian Komunikasi dan Informatika (Kemenkominfo) selama periode Januari 2018 hingga Juni 2019, terdapat 1.091.557 situs negatif yang diblokir. Hampir 90 persen situs yang diblokir merupakan situs pornografi (964.167 situs), disusul oleh situs perjudian (117.700). Pada peringkat ketiga ada situs penipuan (7.626). Untuk melindungi anak dari konten negatif ini sebagai bentuk dari kebijakan kriminal melalui upaya non penal dengan pendekatan techno prevention maka dibuatlah aplikasi agar orang tua bisa mengadopsi teknologi secara bijak dan aman dalam keluarga, meliputi: (Indonesia, 2019)

1) *Gunakan aplikasi Family Link*.

Family Link bisa digunakan untuk memahami aktivitas anak saat menjelajahi internet. Orang tua bisa membatasi anak-anak dengan menggunakan beberapa fitur di Family Link. Fitur-fitur tersebut adalah:

a. Mengawasi waktu penggunaan perangkat dan membatasi akses harian.
b. Mengunci perangkat anak dari jarak jauh.
c. Melihat aktivitas anak.
d. Melihat lokasi anak
e. Mengelola akun dan aplikasi yang digunakan.

Periksa rating dan batasan usia di Google Play dan App Store Orang tua disarankan membaca ulasan dan mencari ikon bintang keluarga di aplikasi atau game untuk menentukan konten yang cocok bagi anak. Ikon bintang menandakan bahwa konten telah ditinjau agar cocok untuk anak-anak. Aplikasi atau game tersebut dikembangkan agar layak digunakan oleh anak-anak. Ikon bintang ini juga menampilkan rentang usia yang disarankan untuk konten tersebut. Periksalah rating konten untuk memahami tingkat kedewasaan suatu aplikasi dan mengatur filter berdasarkan rating tersebut. Hal ini dilakukan untuk menentukan aplikasi yang tepat bagi anak.

2) *Aplikasi YouTube Kids*.

Google membuat aplikasi YouTube Kids agar YouTube cocok untuk dilihat anak-anak. Eksplorasi dalam konten video bisa disesuaikan bagi anak-anak. YouTube memang secara gamblang melarang konten negatif, tapi berlandaskan kebebasan berekspresi para digital natives ini, YouTube juga menjadi sarang konten yang tak layak dikonsumsi oleh anak. Misalnya saja ucapan kasar, baju minim, dan berbagai hal yang tidak mencerminkan adat ketimuran Indonesia. Orang tua bisa menyeleksi pengalaman menonton konten yang cocok untuk anak melalui fitur-fitur sebagai berikut:

a. Video dan kanal pilihan untuk anak - anak tersedia di aplikasi;
b. Pasang timer untuk membatasi waktu anak-anak menonton video;
c. Mengizinkan anak untuk menonton koleksi channel yang telah dipilihkan oleh penyedia konten pihak ketiga terpercaya atau oleh tim YouTube Kids;
d. Pantau dan ketahui video apa saja yang ditonton anak melalui fitur "Tonton lagi";
e. Nonaktifkan fitur penelusuran agar anak hanya dapat menonton channel-channel yang telah diverifikasi oleh tim YouTube Kids;
f. Blokir video atau channel supaya tidak muncul di aplikasi yang dipakai anak;
g. Tandai video agar ditinjau jika yakin bahwa video tersebut tidak boleh ditayangkan dalam aplikasi YouTube Kids.

3) *Aplikasi Dinner Time*.

Dalam aplikasi Dinner Time ini memungkinkan orang tua untuk langsung mengunci dan membuka kunci ponsel anak dari perangkat orang tua. Sayangnya aplikasi ini hanya bisa digunakan untuk mengontrol ponsel Android dengan menggunakan perangkat

iOS atau OS. Orang tua dapat memilih tiga mode pembatasan waktu. Pertama adalah "Waktu Makan Malam" yang bisa menjeda aktivitas apa pun hingga dua jam. Kedua "Take a Break" yang bisa menjeda aktivitas apa pun hingga 24 jam. Terakhir adalah "Waktu Tidur" yang bisa menjeda aktivitas sesuai dengan durasi yang telah ditentukan. Dalam fitur ini, anak masih bisa mengakses jam atau alarm mereka.

4) Aplikasi MamaBear.

Aplikasi ini memiliki banyak fitur yang berguna untuk pemantauan media sosial, pelacakan lokasi dan peringatan, dan banyak lagi. Dengan aplikasi ini, orang tua dapat memonitor aktivitas Instagram, Twitter, dan Facebook untuk mengetahui kapan mereka memiliki tag baru, log in, atau mengunggah foto. Orang juga dapat mengetahui kapan bahasa yang tidak pantas atau indikasi bullying dikirim ke profil anak dengan membuat daftar kata-kata yang dibatasi.

Routing ke fitur safe search dari Kementerian Komunikasi dan Informatika sehingga per tanggal 10 Agustus 2019 lalu konten-konten negatif sudah tidak bisa diakses lagi di Google. Berdasarkan pada Siaran Pers No. 209/HM/KOMINFO/08/2018 Tanggal 31 Agustus 2018 Tentang Negara Melindungi Masa Depan Anak dari Konten Negatif, terdapat ketentuan batasan penggunaan alat teknologi atau gawai bagi anak-anak**.** Bentuk perlindungan dari pemerintah kepada anak-anak, salah satunya yaitu hak untuk memperoleh pengetahuan positif dalam kondisi pesatnya perkembangan bidang teknologi Informasi.Kementerian Kominfo telah sejak lama berupaya melindungi anak-anak dari pengaruh terpaparnya konten negatif, terutama dari internet (Setu, 2018).

5) *Bandwidth throttling*

Bandwidth throttling adalah proses melambatkan kecepatan/bandwidth internet dengan sengaja. Bandwidth throttling dapat terjadi saat transfer data antar perangkat maupun antara perangkat dengan website di internet yang sedang dibuka. Bandwidth throttling dilakukan oleh operator pada saat lalu-lintas data sedang sangat padat, mengurangi jumlah data yang harus diproses dari tiap sumber dalam satu waktu, sehingga kemacetan lalu-lintas data dapat berkurang dan lalu-lintas data tetap lancar. Operator juga kadang-kadang melakukan bandwidth throttling hanya terhadap lalu-lintas data ke atau dari sumber tertentu. Contohnya adalah pembatasan akses ke facebook. Akan tetapi pengguna akan "mengakali" bandwidth throttling dengan memasang Virtual Private Network (VPN) untuk mem-bypass pembatasan ini. Pemerintah dirugikan dengan penggunaan VPN karena tidak dapat melakukan pembatasan penggunaan konten negatif (Indotelko, 2019).

6) *Fanpage dan Grup Diskusi*

Penggunaan sejumlah fanpage dan grup diskusi anti hoax yang telah tersedia di facebook, misalnya Forum Anti Fitnah, Hasut, dan Hoax (FAFHH), Fanpage & Group Indonesian Hoax Buster, Fanpage Indonesian Hoaxes, dan Grup Sekoci. Di sejumlah fanpage dan grup diskusi anti hoax, netizen bisa ikut bertanya apakah suatu informasi merupakan hoax atau bukan, sekaligus melihat klarifikasi yang sudah diberikan oleh orang lain. Semua anggota bisa ikut berkontribusi sehingga grup berfungsi layaknya crowdsourcing yang memanfaatkan tenaga banyak orang (Yunita, 2017).

Kebijakan kriminal *non penal* untuk penanggulangan penyebaran konten negatif dilakukan melalui edukasi dan *techno prevention*. Kementerian Komunikasi dan Informatika sebagai regulator membuat beberapa program untuk pencegahan penyebaran konten negatif dan 6 (enam) aplikasi agar orang tua bisa mengadopsi teknologi secara bijak dan aman dalam keluarga. Selain upaya penanggulangan penyebaran konten negatif, berikut adalah empat aplikasi dan/ atau program perangkat lunak yang dirancang untuk membantu memerangi penindasan maya terkait dengan pencegahan terjadinya *cyberbullying*: (Mufid, 2018)

1) *Trend Micro Online Guardian* yang berisi kontrol komputer yang luas untuk melacak situs jejaring sosial

populer seperti *Twitter, Facebook dan YouTube*. Perangkat lunak ini juga menawarkan manajemen pesan instan dan per-lindungan *malware*.

2) *YouDiligence* untuk memantau halaman jejaring sosial anak mereka sementara secara khusus melacak kata kunci yang terkait dengan intimidasi, ejekan rasial, alkohol, kata-kata kotor dan banyak lagi. Dengan daftar lebih dari 500 kata dan frase peringatan yang dapat diedit oleh orang tua berdasarkan spesifikasinya, *You Diligence* dapat mengirimkan lansiran email kepada orang tua bila ada aktivitas yang meragukan. Pembaruan ini kemudian dapat dikirim melalui email ke orang tua dan dilihat melalui dasbord online agar mudah dilacak.
3) Perlindungan Jaringan Sosial Avira atau *Avira Social Network Protection* adalah program perangkat lunak lain yang diciptakan sebagai hasil dari orang tua yang menyaksikan anak mereka mengalami *cyberbullying*. *Avira Social Network Protection*, yang sebelumnya dikenal dengan Social Shield, membedakan dirinya dari program anti-*cyberbullying* lainnya dengan memantau situs jejaring sosial agar tidak hanya melindungi dari intimidasi, namun juga menjaga reputasi anak. Perangkat lunak ini menggunakan perangkat lunak berbasis awan, sehingga dapat diakses hampir di manapun melalui komputer atau telepon.
4) *STOPit*: Saat ini, hanya satu dari sepuluh korban *cyberbullying* yang menginformasikan orang dewasa tentang situasi mereka. Dengan aplikasi STOP, pengembang dan orang tua mencoba memberi anak tingkat kebebasan dan pemberdayaan yang lebih besar dengan memberi mereka alat untuk menghentikan penghentian penindasan di dunia maya itu sendiri. STOPit memungkinkan anak-anak mengambil tangkapan layar (*screenshot*) dari pelaku online berbahaya dan mengirimkannya ke pilihan orang dewasa yang disesuaikan, seperti guru dan orang tua. Sebagai contoh predator online yang lebih tua, anak-anak yang melaporkan masalah tetap anonim, dan aplikasinya menawarkan peringatan penegakan hukum lokal dan akses mudah ke jalur bantuan.

Kebijakan kriminal melalui upaya *non penal* ini diharapkan menjadi upaya yang efektif dan preventif dalam penanggulangan penyebaran konten negatif di internet. Terkait dengan pembahasan dalam artikel ini, penggunaan *techno prevention* ini sebagai suatu upaya pencegahan terjadinya penyebaran konten negatif oleh individu-individu yang tidak bertanggungjawab menggunakan internet sesuai dengan batas dan ruang lingkup yang telah ditentukan.

Dalam hal penyebaran konten negatif melalui internet, hukum pidana tidak akan mampu bekerja sendiri. Sebagaimana telah dijelaskan sebelumnya, bahwa penyebaran konten negatif sangat berpengaruh tidak hanya secara individu semata tetapi bahkan pada keamanan suatu bangsa dan negara terkait dengan persatuan dan kesatuan. Penyebaran konten negatif ini tentu saja tidak terlepas dari penggunaan teknologi maju sebagai sarana dan prasarana. Oleh karena itu, upaya yang paling rasional dalam menghadapi penyebaran konten negatif tersebut adalah mengutamakan pendekatan teknologi (*techno prevention*).

Model prevensi ini menjadi aktual karena keterbatasan hukum pidana itu sendiri yang bersifat *post factum*. Maksudnya, respon hukum pidana lahir ketika kejahatan sudah terjadi. Model pendekatan ini tidak lagi strategis dan efektif untuk menjawab munculnya persoalan kejahatan yang relatif baru karena pengaruh langsung dari kemajuan teknologi (Ufran, 2014). Untuk menjawab tuntutan itu maka kedepan perlu dipikirkan beberapa upaya alternatif untuk melakukan kontrol terhadap penyebaran konten negatif. Salah satunya adalah pendekatan yang berbasis teknologi yaitu penggunaan *techno prevention***.**

Seiring dengan perkembangan tekno-

logi dan adanya penyebaran konten negatif yang seringkali tidak dapat terbendung lagi, terdapat beberapa perangkat lunak (*software*) yang digunakan untuk memberikan perlindungan bagi anak ketika menggunakan *internet* dan terhubung di dalam dunia maya. Penggunaan berbagai program dan aplikasi internet yang telah diciptakan oleh Kementerian Komunikasi dan Informatika menjadi salah satu bentuk kebijakan kriminal *non penal* melalui upaya penggunaan *techno prevention* dalam penanggungan penyebaran konten negatif.

4. Simpulan

Pencegahan dan penanggulangan kejahatan harus dilakukan dengan pendekatan kebijakan yang integral, ada keseimbangan sarana *penal* dan *non penal*. Kebijakan kriminal *non penal* lebih menitikberatkan pada sifat "preventif" yang bersifat pencegahan sebelum kejahatan terjadi. Bentuk kebijakan kriminal *non penal* sebagai upaya penanggulangan penyebaran konten negatif dilakukan melalui edukasi dan *techno prevention*. Kementerian Komunikasi dan Informatika sebagai regulator membuat beberapa program untuk pencegahan penyebaran konten negatif diantaranya: program Internet Sehat dan Aman (INSAN) yang kemudian diubah menjadi program Internet Cerdas Kreatif dan Produktif (INCAKAP) dan membangun sistem penangkalan konten negatif yaitu *software Whitelist Nusantara* yang akan digunakan oleh institusi pendidikan. Untuk melindungi anak dari konten negatif ini sebagai bentuk dari kebijakan kriminal melalui upaya *non penal* dengan pendekatan t*echno prevention* maka dibuat aplikasi agar orang tua bisa mengadopsi teknologi secara bijak dan aman dalam keluarga, meliputi: aplikasi *Family Link, YouTube Kids, Dinner Time, MamaBear, Bandwidth throttling,* dan sejumlah *fanpage* dan grup diskusi anti *hoax* yang telah tersedia di *facebook*, misalnya *Forum Anti Fitnah, Hasut, dan Hoax (FAFHH), Fanpage & Group Indonesian Hoax Buster, Fanpage Indonesian Hoaxes, dan Grup Sekoci*. Selain upaya penanggulangan penyebaran konten negatif, berikut adalah empat aplikasi dan/ atau program perangkat lunak yang dirancang untuk membantu memerangi penindasan maya terkait dengan pencegahan terjadinya *cyberbullying,* meliputi: *Trend Micro Online Guardian*, *YouDiligence, Avira Social Network Protection* dan *STOPit*.

Meskipun upaya penanggulangan kejahatan melalui kebijakan *non penal* berupa *techno prevention* dianggap cukup efektif dikarenakan dilakukan sebelum terjadinya suatu tindak pidana dan bersifat preventif (mencegah terjadinya suatu tindak pidana). Akan tetapi penggunaan *techno prevention* ini belum mendapat perhatian lebih di Indonesia sehingga perlu kiranya untuk diperkenalkan lebih lanjut dengan cara mengintegrasikan dalam sistem hukum nasional yang terkait dengan upaya penanggulangan kejahatan melalui upaya *non penal* menggunakan pendekatan *techno prevention*. Dalam penanggulangan kejahatan diperlukan adanya upaya integral sebagai bentuk harmonisasi antara kebijakan *penal* dan *non penal*, berjalan secara beriringan dan sinergis.

5. Daftar Pustaka

Abdullah, S. (2012). *Kebijakan Hukum Pidana (Penal) dan Non Hukum Pidana (Non Penal) dalam Menanggulangi Aliran Sesat*.

Alvionita et.al, R. K. (2013). Kajian Yuridis Terhadap Prostitusi Online (Cyber Prostitution) Di Indonesia. *Jurnal Recidive*, *2*(3), 312.

Arief, B. . (2010). *Masalah Penegakan Hukum dan Kebijakan Hukum Pidana dalam Penanggulangan Kejahatan*. Jakarta: Kencana Prenada Media Group.

Asshiddiqie, J. (2005). *Hukum Tata Negara dan Pilar-Pilar Demokrasi*. Jakarta: Kompas.

Bayamlıoğlu, E. dan R. L. (2018). The 'rule of law' implications of data-driven decision-making: a techno-regulatory perspective. *Law, Innovation and Technology Journal*, *10*(2), 303–304.

Chiappetta, M. (2017). The Technostress: definition, symptoms and risk prevention. *Senses Sci Journal*, *4*(1), 358–361.

Frensh et.al, W. (2017). Kebijakan Kriminal Penanggulangan Cyber Bullying Terhadap Anak Sebagai Korban. *USU Law Journal*, *Vol. 5*(No.2), 38.

Ganesh et.al, J. (2019). Kebijakan Kriminal dalam Menanggulangi Tindak Pidana Makar di Indonesia. *Diponegoro Law Journal*, *8*(3), 2076–2095.

Hamdan. (1997). *Politik Hukum Pidana*. Jakarta: Raja Grafindo Persada.

Hasibuan, Z. A. (2007). Langkah-Langkah Strategis dan Taktis Pengembangan E-Government untuk Pemda. *Jurnal Sistem Informasi*, *3*(1), 1.

Indonesia, C. (2019). *5 Langkah Lindungi Anak Saat Berinternet*. Cnnindonesia.Com.

Indotelko. (2019). *Teknologi dibalik pembatasan akses ke medsos*. Indotelko.Com.

Jaya. (2017). *Pembaharuan Hukum Pidana*. Semarang: Pustaka Rizki Putra.

Kartono, K. (2005). *Patologi Sosial*. Jakarta: Raja Grafindo.

Kompas. (2017). *Begini Upaya Kominfo Atasi Maraknya Konten Negatif Di Internet*. Kompas.Com.

Makarim, E. (2003). *Kompilasi Hukum Telematika*. Jakarta: RajaGrafindo Persada.

Makarim, E. (2009). *Tanggung Jawab Penyelenggara terhadap Tata Kelola Yang Baik dalam Penyelenggaraan Sistem Elektronik*. Jakarta: Universitas Indonesia.

Makarim, E. (2015). Penyelenggaraan Community Certification Authority untuk Pengamanan Sumber Daya Internet oleh Komunitas untuk Kesiapan ASEAN Regional e-commerce. *Jurnal Hukum Dan Pembangunan*, *45*(1), 38.

Melvina. (2020). *Betrand Peto Korban Cyber Bullying: Pelaku Masih di Bawah Umur dan Tim Ruben Onsu Diperiksa*. Kompas.Com.

Miller, Gerri Sinclair, David Sutherland, Julie Zilber, G. (2009). *Regulation of The Internet. A Technological Perspective*.

Mufid, F. L. (2018). Kebijakan Integral Hukum Pidana dengan Technology Prevention dalam Upaya Pencegahan Kejahatan Cyberbullying. *Jurnal Rechtens*, *7*(2), 242.

Muladi. (1995). *Kapita Selekta Sistem Peradilan Pidana*. Semarang : Badan penerbit UNDIP.

Muladi dan Barda Nawawi Arief. (2007). *Bunga Rampai Hukum Pidana*. Bandung: Alumni.

Muladi dan Dyah Sulistyani. (2016). *Kompleksitas Perkembangan Tindak Pidana dan Kebijakan Kriminal*. Bandung: Alumni.

Munir. (2017). *Pengantar Hukum Siber Indonesia*. Depok: RajaGrafindo Persada.

Musyafak et al, N. (2017). Implementasi Peraturan Menteri Komunikasi dan Informatika Nomor 19 Tahun 2014 dalam Penanganan Situs Internet Bermuatan Negatif (Studi Kasus Pemblokiran terhadap Situs Radikal oleh Kemenkominfo Tahun 2015). *Islamic Communication Journal*, *Vol. 02*(No. 01), 81.

Pujiono. (2012). *Rekonstruksi Sistem Peradilan Pidana Indonesia*. Semarang: Pustaka Magister.

Republika. (2017). *Kominfo Blokir 6 ribu Situs Penyebar Hoax dan Ujaran Kebencian*. www.Nasional.Republika.co.id.

Setiyanti et al, L. (2017). Tata Kelola Konten Internet di Indonesia: Kebijakan, Praktik, dan Permasalahannya. *Http://Internetsehat.Id*.

Setu, F. (2018). *Negara Melindungi Masa Depan Anak dari Konten Negatif*. Kominfo.Go.Id.

Subrata. (2004). *Hukum Telematika*. Jakarta: BPHN.

Sudarto. (1996). *Hukum dan Hukum Pidana*. Bandung: Alumni.

Suteki,. & Taufani, G. (2018). *Metodologi Penelitian Hukum (Filsafat, Teori Dan Praktek)*. Depok: Raja Grafindo Persada.

Tran, D. (2018). The Law of Attribution: Rules for Attributing the Source of a Cyber Attack. *The Yale Journal of Law and Technology*, *20*, 376–441.

Ufran. (2014). Kebijakan Antisipatif Hukum Pidana untuk Penanggulangan Cyberterrorism. *Jurnal Masalah-Masalah Hukum*, *43*(4), 533.

Wulandari, C. (2013). Kebijakan Nonpenal dalam Penanggulangan Tindak Pidana Perbankan. *Jurnal Pandecta*, *8*(2), 171.

Yunita. (2017). *Ini Cara Mengatasi Berita "Hoax" di Dunia Maya*. Kominfo.Go.Id.

Peraturan perundang-undangan

Rancangan Kitab Undang-Undang Hukum Pidana (September 2019)