Triwikrama: Jurnal Ilmu Sosial
Volume 01, Number 03, 2023 pp. 23-40
E-ISSN: 2988-1986
Open Access:

TINJAUAN YURIDIS TERADAP PERLINDUNGAN HAK ASASI MANUSIA DALAM KASUS CYBERCRIME

Anandhia Salsa
UIN Walisongo Semarang

ARTICLE INFO

Article history:
Received September 2023
Revised September 2023
Accepted September 2023
Available online September 2023

Kata Kunci:
Perlindungan, Cybercrime, HAM, Yuridis

ABSTRAK

Kejahatan dunia maya merupakan ancaman serius terhadap hak asasi manusia di era digital saat ini. Oleh karena itu, perlindungan hak asasi manusia dalam kasus cybercrime perlu mendapat perhatian serius. Tinjauan materi terhadap perlindungan hak asasi manusia dalam kasus kejahatan dunia maya dapat memberikan pandangan yang jelas dan komprehensif mengenai upaya yang dapat dilakukan untuk mencegah dan menangani kasus kejahatan dunia maya yang melanggar hak asasi manusia. Beberapa faktor yang mempengaruhi terjadinya cybercrime yang melanggar hak asasi manusia antara lain ketidakjelasan peraturan hukum, kurangnya kesadaran masyarakat, dan kurangnya kualitas aparat penegak hukum. Upaya pencegahan dan penanganan cybercrime yang melanggar hak asasi manusia antara lain dengan meningkatkan kesadaran masyarakat, meningkatkan kualitas aparat penegak hukum, dan menegakkan peraturan hukum yang tegas. Kebijakan legislatif yang dapat diterapkan pemerintah untuk mencegah cybercrime yang melanggar hak asasi manusia antara lain Undang-Undang Informasi dan Transaksi Elektronik (UU ITE), Undang-Undang Perlindungan Data Pribadi (UU PDP), dan Undang-undang Telekomunikasi. Dengan demikian, peninjauan kembali terhadap perlindungan hak asasi manusia dalam kasus kejahatan dunia maya dapat memberikan pedoman dan arahan yang jelas bagi pemerintah dan aparat penegak hukum dalam menangani kasus cybercrime yang melanggar hak asasi manusia.

Keywords: Perlindungan, Cybercrime, HAM, Yuridis

Pendahuluan

Hak Asasi Manusia (HAM) adalah hak yang dianugerahkan Tuhan Yang Maha Esa kepada setiap individu di muka bumi. Setiap orang wajib menjaga, melindungi dan menghormati hak setiap orang. Salah satu tantangan dalam melindungi hak asasi manusia di era digital adalah privasi. Di era digital, data pribadi seperti nama, alamat, nomor telepon dan informasi lainnya dapat dengan mudah dikumpulkan dan dibagikan tanpa persetujuan pemilik data. Hal ini dapat mengakibatkan penggunaan data yang tidak diinginkan seperti identitas palsu, penipuan, atau pelecehan.

Teknologi di era globalisasi saat ini berkembang pesat dan sangat mempengaruhi sikap serta kondisi hidup manusia, terutama di bidang teknologi informasi dan komunikasi. Salah satu bukti perkembangan teknologi di era teknologi dan komunikasi ini adalah di bidangan

Triwikrama: Jurnal Ilmu Sosial
Volume 01, Number 03, 2023 pp. 23-40
E-ISSN: 2988-1986
Open Access:

sosial media. Namun dalam perkembangannya tidak hanya menimbulkan dampak positif tetapi juga dampak negatif yang bisa disebut juga dengan *cybercrime*. *Cybercrime* adalah tindakan ilegal yang dilakukan dengan menggunakan teknologi komputer dan jaringan internet untuk menyerang sistem informasi korban. Kejahatan ini terjadi karena banyak pihal-pihak yang menyalah gunakan fungsi dari media sosial ini. Beberapa individu yang tidak bertanggung jawab memanfaatkan media sosial untuk menyebarkan aib, melakukan penipuan, mencuri identitas, *cyberbullying,* penyebaran berita hoaks, dan lain sebagainya.

Dalam rangka melindungi hak asasi manusia di era digital, perlu adanya kerangka hukum yang mengatur perlindungan hak asasi digital, pendidikan, regulasi, kesadaran, dan edukasi. Pemerintah telah mengeluarkan Undang-undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik dan Undang-undang Nomor 19 Tahun 2016 tentang Perubahan atas Undang-undang Nomor 11 Tahun 2008 yang menjadi landasan dalam penanganan *cybercrime*.[1] Perlindungan hukum terhadap korban *cybercrime* dapat dilakukan melalui tindakan atau cara untuk melindungi individu dan masyarakat dari tindakan sewenang-wenang pelaku kejahatan *cybercrime*. Edukasi dan kesadaran masyarakat juga sangat penting untuk melindungi korban *cybercrime*. Dengan meningkatkan kesadaran masyarakat akan bahaya *cybercrime*, maka masyarakat akan lebih waspada dan dapat menghindari tindakan-tindakan yang dapat memicu *cybercrime.*

Metode Penelitian

Metode yang digunakan dalam membuat artikel ini yaitu Metode yuridis normatif: Metode pendekatan yuridis normatif dapat digunakan untuk menganalisis tindak pidana *cybercrime* dalam perspektif hukum pidana, perlindungan hukum bagi korban *cybercrime*, dan pemidanaan *cybercrime* dalam perspektif hukum pidana positif. Metode yuridis normatif dapat digunakan untuk menganalisis tindak pidana *cybercrime* dari perspektif hukum pidana, perlindungan hukum bagi korban *cybercrime*, dan pemidanaan *cybercrime* dari perspektif hukum pidana positif.

Hasil Penelitian dan Pembahasan

Definisi Hak Asasi Manusia

Hak asasi manusia adalah seperangkat hak yang melekat pada hakikat dan keberadaan manusia sebagai makhluk Tuhan Yang Maha Esa dan merupakan anugerah-Nya yang wajib dihormati, dijunjung tinggi, dan dilindungi oleh negara, hukum, pemerintah, dan setiap orang demi kehormatan serta perlindungan harkat dan martabat manusia.[2] Hak Asasi Manusia juga telah diatur dalam Undang-Undang Nomor 39 Tahun 1999, menjelaskan bahwa Hak Asasi Manusia adalah seperangkat hak yang melekat pada setiap individu sebagai makhluk Tuhan

[1] Wahyudi, D. (2013). Perlindungan Hukum Terhadap Korban Kejahatan Cyber Crime Di Indonesia. *Jurnal Ilmu Hukum Jambi*, *4*(1), 43295.
[2] https://umsu.ac.id/hak-asasi-manusia/

Triwikrama: Jurnal Ilmu Sosial
Volume 01, Number 03, 2023 pp. 23-40
E-ISSN: 2988-1986
Open Access:

Yang Maha Esa dan wajib dijunjung tinggi, dihormati, dan dilindungi oleh negara, hukum, pemerintah, dan setiap orang.

Hak-hak tersebut mencakup hak untuk hidup, keamanan, kebebasan dari pelecehan, kebebasan dari perbudakan dan penyiksaan. Apabila seseorang atau sekelompok orang tidak memberikan hak yang memadai kepada seseorang atau sekelompok orang, maka ia diancam dengan pidana penjara sementara atau paling lama seumur hidup.

Definisi *Cybercrime*

Cybercrime merupakan kejahatan yang berkaitan dengan komputer atau perangkat jaringan, biasanya kejahatan ini dilakukan secara online. Faktanya, kejahatan siber ini bisa menyasar siapa saja. Jika Anda menjadi salah satu korbannya tentu akan menimbulkan banyak kerugian. Bahkan berdampak pada kondisi mental Anda bahkan kerugian finansial. Salah satu contoh kejahatan cyber yang sangat berbahaya adalah Doxing, yang mengarah pada *cyberbullying*, pengambilan data pribadi dan menyebarkannya di internet. Tujuan dari tindakan ini sangat beragam, mulai dari ancaman, pemerasan, mempermalukan seseorang dan memanfaatkan orang lain.

Seiring berkembangnya teknologi komputer dan internet, penjahat juga mengembangkan cara untuk mencuri data perusahaan dan individu. Oleh karena itu, tidak heran jika saat ini keamanan siber data bisnis harus dijaga dengan teknologi terkini. Berikut jenis-jenis *cybecrime* :

1. *Pishing*
   Phising adalah salah satu kejahatan elektronik dalam bentuk penipuan. Dimana proses phising ini bermaksud untuk menangkap informasi yang sangat sensitif seperti username, password dan detil kartu kredit dalam bentuk meniru sebagai sebuah entitas yang dapat dipercaya/legitimate organization dan biasanya berkomunikasi secara elektronik. [3]
2. *Ransomware*
   Ransomware adalah perangkat lunak berbahaya yang mengandung virus, worm, trojan, horse dan program lain yang dapat membahayakan perangkat keras (PC) atau pencurian data pribadi. *Ransomware* atau *Malware* adalah singkatan dari "Malicious Software" yang berarti perangkat lunak mencurigakan. Perangkat lunak perusak ini dapat berdampak negatif pada komputer dan pengguna komputer. Program-programnya dapat memodifikasi, merusak, menemukan celah, dan mencuri data pribadi seseorang yang tentunya sangat merugikan. *ransomware* dapat diinstal saat mengunduh data melalui email, pesan,dan situs web. Salah satu perangkat yang paling banyak digunakan saat ini adalah smartphone sebagai perangkat untuk mengakses website.
3. *Carding*
   Carding adalah kejahatan siber yang memanfaatkan data kartu kredit orang lain untuk bertransaksi. Data kartu kredit tersebut dapat diperoleh dengan berbagai

[3] Dian Rachmawati, "Phising Sebagai Salah Satu Bentuk Ancaman dalam Dunia Cyber," Jurnal Saintkom, Vol. 13, No. 3, 2014, hlm. 211.

Triwikrama: Jurnal Ilmu Sosial
Volume 01, Number 03, 2023 pp. 23-40
E-ISSN: 2988-1986
Open Access:

cara, misalnya meretas situs tempat Anda menggunakan nomor kartu kredit untuk berlangganan dan menanamkan *hardware* khusus di balik mesin EDC yang Anda gunakan untuk membayar di supermarket. *Hardware* khusus ini digunakan untuk merekam data kartu yang telah Anda gesek dan mengirimkannya kepada oknum penipu terkait.

4. *Cyberbullying*
   Cyberbullying adalah penindasan yang menggunakan teknologi digital. Hal ini dapat terjadi di media sosial, platform chat, platform game, dan ponsel. *Cyberbullying* adalah perilaku berulang yang bertujuan untuk menakut-nakuti, mengecewakan, atau mempermalukan orang-orang yang menjadi sasarannya.
5. Kejahatan Konten
   Konten ilegal dilakukan pelaku dengan memberikan informasi yang tidak benar, bahkan melanggar hukum. Contohnya seperti berita bohong atau hoax, pornografi, informasi yang bersifat SARA, dan informasi negara yang sangat rahasia.
6. Pemalsuan Identitas
   Pemalsuan identitas adalah tindak pidana berupa pemalsuan identitas seseorang atau suatu badan yang meliputi nama palsu, alamat palsu, jabatan palsu dan identitas lainnya dengan tujuan agar korbannya percaya seolah-olah identitas atau badan tersebut benar.
7. OTP *Fraud*
   One-time password atau OTP adalah serangkaian kode sekali pakai yang dikirimkan oleh sistem ke nomor ponsel atau email yang terdaftar di sistem. Tujuan pengiriman kode OTP ini adalah untuk keamanan ganda. Namun sayangnya, saat ini banyak juga penipu yang menggunakan kode tersebut untuk melakukan kejahatan.

Di era digital yang semakin maju, *cybercrime* semakin sering terjadi dan jenisnya pun semakin beragam. Oleh karena itu, penting bagi pengguna internet untuk mewaspadai dan mengenali jenis-jenis kejahatan dunia maya yang sering terjadi demi melindungi diri dan data pribadinya.

Analisis yuridis terhadap kasus *cybercrime* yang melanggar hak asasi manusia

Berdasarkan beberapa sumber, analisis yuridis terhadap kasus *cybercrime* yang melanggar hak asasi manusia dapat dilakukan dengan memperhatikan hal-hal sebagai berikut:

1. Perlindungan hak asasi manusia dalam kasus kejahatan dunia maya harus menjadi prioritas utama dalam pembuatan undang-undang dan kebijakan terkait *cybercrime*. Hal ini penting untuk memastikan bahwa upaya pencegahan dan penanganan *cybercrime* maya tidak mengorbankan hak asasi manusia.
2. Undang-undang dan kebijakan terkait *cybercrime* harus mempertimbangkan prinsip-prinsip hak asasi manusia, seperti kebebasan berekspresi, privasi, dan perlindungan terhadap diskriminasi.
3. Dalam penanganan kasus *cybercrime* yang melanggar hak asasi manusia, perlu dilakukan investigasi yang profesional dan transparan untuk memastikan hak-hak korban tidak dilanggar.

Triwikrama: Jurnal Ilmu Sosial
Volume 01, Number 03, 2023 pp. 23-40
E-ISSN: 2988-1986
Open Access:

4. Dalam penanganan kasus *cybercrime* yang melanggar hak asasi manusia, perlu dilakukan penegakan hukum yang adil dan proporsional, serta memperhatikan hak-hak terdakwa.
5. Perlu adanya kerja sama internasional dalam penanganan kasus *cybercrime* yang melanggar hak asasi manusia, mengingat kejahatan tersebut bersifat transnasional

Dengan memperhatikan analisis yuridis terhadap kasus-kasus *cybercrime* yang melanggar hak asasi manusia, diharapkan upaya pencegahan dan penanganan *cybercrime* dapat dilakukan dengan memperhatikan hak asasi manusia dan memastikan hak-hak korban dan terdakwa tetap terlindungi.

Tinjauan yuridis terhadap *cybercrime*

Hasil penelitian menunjukkan bahwa tinjauan yuridis kejahatan *cybercrime* dalam hukum pidana di Indonesia mempunyai berbagai dampak positif dan negatif, baik dari KUHP maupun di luar KUHP, sesuai dengan peraturan pidana konvensional, serta upaya yang dapat dilakukan. digunakan untuk mengatasi kejahatan dunia maya. Beberapa delik atau tindak pidana yang dapat dikenakan dalam kasus kejahatan siber yang melanggar hak asasi manusia antara lain:

1. Penyalahgunaan data pribadi
   Penyalahgunaan data pribadi dikenakan hukuman dalam Pasal 68 Undang-Undang Pelindungan Data Pribadi (UU PDP) di Indonesia. Pasal ini menyatakan bahwa setiap orang yang dengan sengaja membuat data pribadi palsu untuk menggunakan diri sendiri atau orang lain yang dapat merugikan pihak lain akan dikenai hukuman pidana penjara mulai dari 4 tahun hingga denda miliaran rupiah. Selain itu, dalam Pasal 67 dan Pasal 68 UU PDP, pelaku juga dapat dijatuhi pidana tambahan berupa perampasan keuntungan dan atau harta kekayaan yang diperoleh atau hasil dari tindak pidana, serta pembayaran ganti kerugian.
2. Penyadapan informasi
   Penyadapan informasi merupakan perbuatan yang dilarang oleh hukum pidana. Berdasarkan Pasal 40 Undang-Undang Telekomunikasi, setiap orang dilarang melakukan penyadapan atas informasi yang disalurkan melalui jaringan telekomunikasi dalam bentuk apa pun. Pelanggaran ini dapat dikenakan sanksi pidana penjara paling lama 15 tahun[4]. Selain itu, Pasal 31 Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) juga melarang penyadapan dan dapat dikenakan sanksi pidana penjara maksimal 10 tahun[5]. Namun, penyadapan dapat dilakukan oleh para penegak hukum untuk kepentingan penyelesaian kasus hukum, dengan syarat mendapat izin dari pihak pengadilan dan hanya dapat dilakukan oleh penyidik atas perintah tertulis atasan penyidik setempat[6]. Oleh karena itu, penyadapan informasi yang dilakukan tanpa izin atau tidak sesuai dengan ketentuan hukum dapat dikenakan sanksi pidana yang tegas.

[4] https://antikorupsi.org/id/article/penyadapan-dalam-hukum-pidana
[5]https://www.kominfo.go.id/content/detail/3436/gatot-dewa-broto-penyadapan-langgar-uu-telekomunikasi-dan-uu-ite/0/berita_satker
[6] https://indonesiabaik.id/infografis/siapa-berhak-melakukan-penyadapan

Triwikrama: Jurnal Ilmu Sosial
Volume 01, Number 03, 2023 pp. 23-40
E-ISSN: 2988-1986
Open Access:

3. Penyebaran berita palsu (hoax)
   Penyebaran berita palsu atau hoax juga dikenal sebagai tindak pidana dalam hukum pidana Indonesia. Pelaku penyebaran hoax dapat dikenakan sanksi pidana sesuai dengan Pasal 28 ayat 1 Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) yang menyatakan bahwa setiap orang dengan sengaja dan tanpa hak menyebarkan berita bohong dan menyesatkan yang mengakibatkan kerugian konsumen dalam transaksi elektronik dapat dikenakan sanksi pidana penjara maksimal 6 tahun dan atau denda maksimal Rp 1 miliar[7]. Selain itu, Pasal 14 UU ITE juga mengatur bahwa setiap orang yang dengan sengaja dan tanpa hak menyebarkan informasi yang ditujukan untuk menimbulkan rasa kebencian atau permusuhan individu atau kelompok masyarakat tertentu berdasarkan atas suku, agama, ras, dan antargolongan (SARA) dapat dikenakan sanksi pidana penjara maksimal 6 tahun dan/atau denda maksimal Rp 1 miliar[8]. Oleh karena itu, penyebaran berita palsu atau hoax dapat dikenakan sanksi pidana yang tegas sesuai dengan ketentuan hukum yang berlaku.
4. Konten ilegal
   Konten ilegal adalah salah satu bentuk tindak pidana *cybercrime* yang dapat dikenakan sanksi pidana. Berikut adalah beberapa jenis konten ilegal yang dapat dikenakan sanksi pidana:
   a. Konten pornografi: Konten pornografi adalah konten yang melanggar kesusilaan dan dapat merusak moral dan nilai-nilai agama. Pelanggaran ini dapat dikenakan sanksi pidana sesuai dengan Pasal 27 ayat (1) Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) yang menyatakan bahwa setiap orang dilarang mentransmisikan dan mendistribusikan konten yang melanggar kesusilaan dalam konteks pornografi..
   b. Konten perjudian: Konten perjudian adalah konten yang berisi informasi atau tawaran perjudian yang melanggar ketentuan hukum. Pelanggaran ini dapat dikenakan sanksi pidana sesuai dengan Pasal 27 ayat (2) UU ITE yang menyatakan bahwa setiap orang dilarang menyebar konten perjudian.
   c. Penghinaan dan pencemaran nama baik: Penghinaan dan pencemaran nama baik adalah tindakan yang merugikan dan merusak reputasi seseorang atau kelompok tertentu. Pelanggaran ini dapat dikenakan sanksi pidana sesuai dengan Pasal 27 ayat (3) UU ITE yang menyatakan bahwa setiap orang dilarang melakukan penghinaan dan pencemaran nama baik.
   d. Konten negatif: Konten negatif adalah konten yang melanggar peraturan perundang-undangan, seperti pornografi anak, kekerasan, pemerasan, penipuan, dan pelanggaran hak kekayaan intelektual. Pelanggaran ini dapat dikenakan sanksi pidana sesuai dengan Pasal 40 ayat (2a) UU ITE yang menyatakan bahwa setiap orang dilarang membuat dapat diaksesnya konten negatif yang terblokir.

[7] https://fahum.umsu.ac.id/bahaya-hoax-pidana-sanksi/
[8] https://fahum.umsu.ac.id/hati-hati-bahaya-penyebaran-berita-hoax/

Triwikrama: Jurnal Ilmu Sosial
Volume 01, Number 03, 2023 pp. 23-40
E-ISSN: 2988-1986
Open Access:

Dengan mengetahui jenis-jenis konten ilegal yang dapat dikenakan sanksi pidana, masyarakat dapat lebih berhati-hati dalam menggunakan teknologi informasi dan komunikasi serta mematuhi ketentuan hukum yang berlaku.

Korban kejahatan dunia maya dapat mengambil tindakan hukum dengan melaporkan kejadian tersebut kepada aparat penegak hukum, mengumpulkan bukti, mengajukan gugatan perdata, dan mengikuti proses hukum. Dengan mengetahui pelanggaran atau tindak pidana yang dapat dikenakan dalam kasus *cybercrime* yang melanggar hak asasi manusia, maka aparat penegak hukum dapat mengambil tindakan yang tepat untuk menangani kasus tersebut dan memberikan perlindungan hukum bagi para korbannya.

Faktor penyebab terjadinya *cybercrime* yang melanggar hak asasi manusia

Berikut faktor-faktor yang mempengaruhi terjadinya *cybercrime* yang melanggar hak asasi manusia berdasarkan ulasan dari beberapa sumber:

1. Penyalahgunaan teknologi: Penggunaan teknologi yang tidak bertanggung jawab dapat memicu kejahatan dunia maya yang melanggar hak asasi manusia. Contohnya adalah ujaran kebencian di dunia maya yang dapat merugikan individu atau kelompok tertentu.
2. Kurangnya tindakan tegas aparat penegak hukum: Tidak adanya tindakan tegas aparat penegak hukum dalam menangani kasus *cybercrime* yang melanggar HAM dapat memperburuk keadaan dan memberikan peluang bagi pelaku untuk melakukan tindak pidana serupa di kemudian hari.
3. Sikap egois : Sikap egois individu atau kelompok tertentu dapat memicu kejahatan dunia maya yang melanggar hak asasi manusia. Contohnya adalah tindakan pencurian data pribadi yang dilakukan untuk kepentingan pribadi atau kelompok tertentu.
4. Rendahnya kesadaran akan hak asasi manusia: Rendahnya kesadaran akan hak asasi manusia dapat memicu *cybercrime* yang melanggar hak asasi manusia. Individu atau kelompok yang tidak memahami pentingnya hak asasi manusia dapat melakukan tindakan kriminal yang merugikan orang lain.

Dari faktor-faktor tersebut dapat disimpulkan bahwa terjadinya *cybercrime* yang melanggar hak asasi manusia dipengaruhi oleh faktor internal dan eksternal. Faktor internal berupa sikap egois dan rendahnya kesadaran akan hak asasi manusia, sedangkan faktor eksternal berupa penyalahgunaan teknologi dan kurangnya ketegasan aparat penegak hukum. Oleh karena itu, diperlukan upaya peningkatan kesadaran terhadap hak asasi manusia dan tindakan tegas aparat penegak hukum dalam menangani kasus *cybercrime* yang melanggar hak asasi manusia.

Upaya pencegahan dan penanganan *cybercrime* yang melanggar hak asasi manusia

Berikut upaya pencegahan dan penanganan *cybercrime* yang melanggar hak asasi manusia berdasarkan ulasan dari beberapa sumber:

1. Peraturan hukum yang jelas dan tegas: Peraturan hukum yang jelas dan tegas diperlukan untuk mencegah dan menangani kejahatan siber yang melanggar hak asasi manusia.

Peraturan ini harus memuat sanksi tegas bagi pelaku kejahatan siber dan perlindungan hak asasi manusia bagi korbannya.

2. Meningkatkan kesadaran masyarakat: Meningkatkan kesadaran masyarakat tentang bahaya kejahatan dunia maya dan pentingnya hak asasi manusia dapat membantu mencegah kejahatan dunia maya yang melanggar hak asasi manusia. Meningkatkan kesadaran ini dapat dilakukan melalui kampanye sosialisasi dan pendidikan.
3. Kerjasama antar negara: Kerja sama antar negara dalam menangani kejahatan siber yang melanggar hak asasi manusia dapat membantu memperkuat penanganan kasus-kasus tersebut. Kolaborasi ini dapat dilakukan melalui pertukaran informasi dan pengembangan teknologi.
4. Peningkatan kualitas aparat penegak hukum: Peningkatan kualitas aparat penegak hukum dalam menangani kasus-kasus kejahatan siber yang melanggar hak asasi manusia dapat membantu memperkuat penanganan kasus-kasus tersebut. Peningkatan kualitas ini dapat dilakukan melalui pelatihan dan pengembangan teknologi.

Dari upaya tersebut dapat disimpulkan bahwa pencegahan dan penanganan *cybercrime* yang melanggar hak asasi manusia memerlukan kerja sama antar negara, peraturan hukum yang jelas dan tegas, peningkatan kesadaran masyarakat, dan peningkatan kualitas aparat penegak hukum. Upaya tersebut harus dilakukan secara terpadu dan berkelanjutan untuk memperkuat perlindungan hak asasi manusia di era digital saat ini.

kebijakan hukum untuk mencegah *cybercrime* yang melanggar hak asasi manusia

Berikut adalah beberapa kebijakan perundang-undangan yang dapat diterapkan oleh pemerintah untuk mencegah terjadinya *cybercrime* yang melanggar hak asasi manusia:

1. Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (ITE): Undang-undang ini mengatur tentang tindakan pidana dalam dunia maya, termasuk pengancaman, pemerasan, dan penyebaran konten yang melanggar hak asasi manusia[9].
2. Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (ITE): Undang-undang ini mengatur tentang perlindungan data pribadi dan privasi pengguna internet[10].
3. Undang-Undang Nomor 36 Tahun 1999 tentang Telekomunikasi: Undang-undang ini melarang setiap orang melakukan perbuatan tanpa hak, tidak sah, atau melawan hukum dalam bidang telekomunikasi, termasuk dalam konteks cybercrime.
4. Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi: Undang-undang ini mengatur tentang perlindungan data pribadi dan privasi pengguna internet[11].

[9] Bunga, D. (2019). Politik hukum pidana terhadap penanggulangan cybercrime. *Jurnal Legislasi Indonesia*, *16*(1), 1-15.
[10] Firdaus, I. (2022). Upaya Perlindungan Hukum Hak Privasi Terhadap Data Pribadi dari Kejahatan Peretasan. *Jurnal Rechten: Riset Hukum Dan Hak Asasi Manusia*, *4*(2), 23-31.
[11] Firdaus, I. (2022). Upaya Perlindungan Hukum Hak Privasi Terhadap Data Pribadi dari Kejahatan Peretasan. *Jurnal Rechten: Riset Hukum Dan Hak Asasi Manusia*, *4*(2), 23-31.

5. Undang-Undang Nomor 19 Tahun 2016 tentang Hak Asasi Manusia**: Undang-undang ini mengatur tentang perlindungan hak asasi manusia dalam konteks teknologi informasi dan komunikasi[12].
6. Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (ITE)**: Undang-undang ini mengatur tentang perlindungan data pribadi dan privasi pengguna internet.

Dengan menerapkan kebijakan hukum yang jelas dan tegas, pemerintah dapat memberikan perlindungan hak asasi manusia yang lebih baik dalam kasus *cybercrime*. Selain itu, pemerintah juga perlu melakukan sosialisasi dan edukasi kepada masyarakat tentang pentingnya memahami dan menaati peraturan perundang-undangan yang ada.

Simpulan

Berdasarkan tinjauan yuridis terhadap perlindungan hak asasi manusia dalam kasus cybercrime, dapat disimpulkan bahwa perlindungan hak asasi manusia dalam kasus *cybercrime* harus menjadi prioritas utama dalam pembuatan undang-undang dan kebijakan terkait kejahatan siber. Undang-undang dan kebijakan terkait *cybercrime* harus mempertimbangkan prinsip-prinsip hak asasi manusia, seperti kebebasan berekspresi, privasi, dan perlindungan terhadap diskriminasi. Dalam penanganan kasus *cybercrime* yang melanggar hak asasi manusia, perlu dilakukan investigasi yang profesional dan transparan untuk memastikan hak-hak korban tidak dilanggar. Dalam penanganan perkara *cybercrime* yang melanggar hak asasi manusia, perlu dilakukan penegakan hukum yang adil dan proporsional, serta memperhatikan hak-hak terdakwa. Dengan memperhatikan perlindungan hak asasi manusia dalam kasus kejahatan siber, diharapkan upaya pencegahan dan penanganan *cybercrime* dapat dilakukan dengan memperhatikan hak asasi manusia dan memastikan hak-hak korban dan terdakwa tetap terlindungi.

Saran

Saran untuk penelitian selanjutnya adalah melakukan penelitian yang lebih mendalam mengenai perlindungan hak asasi manusia dalam kasus *cybercrime* dan memperhatikan perkembangan teknologi yang terus berkembang. Selain itu, beberapa hal yang harus dilakukan ialah dengan menyempurnakan undang-undang yang masih belum secara benar melindungi para korban *cybercrime*. Dalam upaya penegakan ini, diharuskan adanya harmonisasi yang baik antara masyarakat, penegak hukum dan negara sehingga *cybercrime* bisa diatasi dengan baik.

[12] Sari, U. I. P. (2021). Kebijakan Penegakan Hukum Dalam Upaya Penanganan Cyber Crime Yang Dilakukan Oleh Virtual Police Di Indonesia. *Jurnal Studia Legalia*, *2*(01), 58-77.

Triwikrama: Jurnal Ilmu Sosial
Volume 01, Number 03, 2023 pp. 23-40
E-ISSN: 2988-1986
Open Access:

Daftar Pustaka

Firdaus, I. (2022). Upaya Perlindungan Hukum Hak Privasi Terhadap Data Pribadi dari Kejahatan Peretasan. *Jurnal Rechten: Riset Hukum Dan Hak Asasi Manusia*, *4*(2), 23-31.

Sari, U. I. P. (2021). Kebijakan Penegakan Hukum Dalam Upaya Penanganan Cyber Crime Yang Dilakukan Oleh Virtual Police Di Indonesia. *Jurnal Studia Legalia*, *2*(01), 58-77.

Bunga, D. (2019). Politik hukum pidana terhadap penanggulangan cybercrime. *Jurnal Legislasi Indonesia*, *16*(1), 1-15.

Dian Rachmawati, ”Phising Sebagai Salah Satu Bentuk Ancaman dalam Dunia Cyber,” Jurnal Saintkom, Vol. 13, No. 3, 2014, hlm. 211.

Wahyudi, D. (2013). Perlindungan Hukum Terhadap Korban Kejahatan Cyber Crime Di Indonesia. *Jurnal Ilmu Hukum Jambi*, *4*(1), 43295.

Engla, A. D., Dean, L., Rilandi, N. R., & Raihana, R. (2023). Tinjauan Yuridis Tindak Pidana Cybercrime Berdasarkan Hukum Pidana. *Jurnal Hukum dan Sosial Politik*, *1*(2), 36-47.

Hertianto, M. R. (2021). Tinjauan yuridis terhadap perlindungan anak dalam ruang siber di Indonesia. *Jurnal Hukum & Pembangunan*, *51*(3), 555-573.

Hertianto, M. R. (2021). Tinjauan yuridis terhadap perlindungan anak dalam ruang siber di Indonesia. *Jurnal Hukum & Pembangunan*, *51*(3), 555-573.

Rumlus, M. H., & Hartadi, H. (2020). Kebijakan penanggulangan pencurian data pribadi dalam media elektronik. *Jurnal Ham*, *11*(2), 285-299.