



ISSN Print: 2085-2339
ISSN Online: 2654-7252

Perspektif Implementasi Prinsip Right to be Forgotten di Indonesia

Jurnal Surya Kencana Satu: Dinamika Masalah Hukum dan Keadilan

Editorial Office: Fakultas Hukum, Universitas Pamulang,
Jalan Surya Kencana No. 1, Pamulang Barat, Tangerang Selatan 15417, Indonesia.
Phone/ Fax: +6221-7412566
E-mail: dinamikahukum_fh@unpam.ac.id
Website: <http://openjournal.unpam.ac.id/index.php/sks>

Perlindungan Data Pribadi Dalam Penegakan Hukum Pidana di Era Digital Ditinjau dari Perspektif Implementasi Prinsip Right to be Forgotten di Indonesia

Nopit Ernasari^a

^a *Fakultas Hukum, Universitas Pamulang, Tangsel. E-mail: nopiternasari94@gmail.com*

Article	Abstract
	<p>Perlindungan data pribadi dalam penegakan hukum pidana di era digital merupakan isu krusial yang semakin relevan di Indonesia. Dengan pesatnya perkembangan teknologi informasi, data pribadi individu sering kali terancam kebocoran dan penyalahgunaan, terutama dalam konteks proses hukum. Penelitian ini mengkaji implementasi prinsip "right to be forgotten" (hak untuk dilupakan) di Indonesia sebagai langkah untuk melindungi privasi individu dan mengatur penggunaan data pribadi dalam penegakan hukum. Dalam masyarakat yang semakin terhubung secara digital, tantangan terkait privasi dan pengelolaan data pribadi menjadi sangat signifikan, terutama dalam proses hukum. Saat ini Indonesia telah memasukkan klausula hak untuk dilupakan di beberapa aturan perundang-undangan yang sudah disahkan, bahkan sudah diatur pula system pelaksanaannya. Namun masih terdapat banyak permasalahan yang membuat hak tersebut sedikit sulit untuk menegakkan penerapannya, mengingat Indonesia juga memiliki hak untuk berpendapat dan hak untuk mengetahui informasi publik sehingga implementasi dari hak untuk dilupakan ini masih sering mengalami kritik dan kesenjangan dengan hak untuk diingat/hak untuk mengetahui.</p> <p>Kata kunci: Perlindungan Data Pribadi; Right to be Forgotten; Penegakan Hukum; Era Digital</p> <p><i>Personal data protection in criminal law enforcement in the digital era is a crucial issue that is increasingly relevant in Indonesia. With the rapid development of information technology, individual personal data is often threatened with leakage and misuse, especially in the context of legal proceedings. This research examines the implementation of the "right to be forgotten" principle in Indonesia as a measure to protect individual privacy and regulate the use of personal data in law enforcement. In an increasingly digitally connected society, challenges related to privacy and personal data management have become very significant, especially in legal proceedings. Currently, Indonesia has included the right to be forgotten clause in several laws and regulations that have been passed, and the implementation system has also been regulated. However, there are still many problems that make</i></p>

this right a little difficult to enforce, considering that Indonesia also has the right to freedom of expression and the right to know public information so that the implementation of the right to be forgotten is still often criticized and the gap with the right to be remembered / the right to know is not clear.

Keywords: *Personal Data Protection; Right to be Forgotten; Law Enforcement; Digital Era*

PENDAHULUAN

Peranan teknologi informasi dan komunikasi di era globalisasi telah menempatkannya pada posisi yang sangat strategis karena merepresentasikan dunia tanpa batas, jarak, ruang dan waktu yang berdampak pada peningkatan produktivitas dan efisiensi. Pengaruh globalisasi dengan pemanfaatan teknologi informasi dan komunikasi telah mengubah pola kehidupan masyarakat dan membawa tatanan kehidupan baru serta mendorong terjadinya perubahan di bidang sosial, ekonomi, budaya, pertahanan, keamanan dan penegakan hukum. (Siswanto, 2009)

Manusia kerap panik ketika sebuah informasi terlupakan, dalam menghadapi keterbatasan kemampuan dalam mengingat, manusia terkadang menyiasatinya dengan menggunakan catatan, perekam digital, atau upaya lainnya. Namun, perkembangan internet saat ini justru menimbulkan kepanikan yang baru. Internet merupakan suatu jaringan yang bercabang-cabang tidak terputus. Pengguna internet dihubungkan dengan ribuan komputer yang masing-masing menyimpan informasi sehingga informasi yang terdapat dalam komputer lain tersebut dapat masyarakat baca pada layar komputer masyarakat sendiri. (Lubis, 2020)

Ketika suatu informasi telah terpublikasi di internet, maka kemungkinan besar informasi itu akan bertahan lama untuk tersimpan. Menyalin dan berbagi informasi semakin mudah dilakukan. Internet memiliki kemampuan yang nyaris tak terbatas dalam hal menyimpan dan mencari. David Lindsay menggambarkan fenomena ini sebagai the problem of digital eternity. (Lindsay, 2015)

Dengan adanya keabadian digital, privasi menjadi sangatlah penting. Privasi tidak hanya sederhana tentang kerahasiaan data seseorang tetapi menyangkut kerahasiaan hubungan seseorang dengan informasi atau orang lain. Selain itu, yang paling penting adalah pengguna internet tidak hanya membagikan informasi tentang diri mereka tetapi juga informasi tentang orang lain juga.

Hak untuk dilupakan (right to be forgotten) merupakan hak yang memiliki kaitan erat dengan hak privasi dalam pemakaian teknologi informasi (Christianto, 2002). Undang-Undang Dasar Negara Republik Indonesia Tahun 1945 yang selanjutnya akan ditulis dengan UUD 1945, pemahaman terkait hak untuk dilupakan (right to be forgotten) berkaitan erat dengan perlindungan hukum, perlindungan data pribadi dan pengakuan diri dalam hak asasi manusia yang dijamin dalam UUD 1945 yaitu Pasal 28G Ayat (1), yang memberikan ketentuan bahwa:

Setiap orang berhak atas perlindungan data diri pribadi, keluarga, kehormatan, martabat, dan harta benda yang di bawah kekuasaannya, serta berhak atas rasa aman

dan perlindungan dari ancaman ketakutan untuk berbuat atau tidak berbuat sesuatu yang merupakan hak asasi.

Kejahatan siber (cybercrime) terdiri dari cyber harassment, cyber hacking, malicious distribution, online defamation, impersonation/cloning, surveillance/tracking/cyber stalking, revenge porn/non-consecual pornography, sexting, online grooming, dan seluruh bentuk kejahatan beserta dengan modus operandinya yang dilakukan akibat dampak negatif dari keberadaan internet.

Mesin pencarian Di Google dapat memudahkan manusia untuk mendapatkan informasi serta membantu dalam mengingat. Akan tetapi, di sisi lain dapat berpotensi membebani proses mental seseorang jika orang tersebut menginginkan “hak untuk dilupakan” atau “Right To Be Forgotten” atas jejak digital masa lalu yang berisikan data pribadi dengan asumsi informasi elektronik atau jejak digital tersebut sudah tidak relevan. Implementasi Right To Be Forgotten di Indonesia nantinya tidak hanya pada mesin pencari (search engine). Penghapusan konten yang dianggap tidak relevan berdasarkan penetapan pengadilan langsung dilakukan oleh penyelenggara sistem elektronik yang memegang kendali langsung atas suatu konten tertentu. Hal tersebut tegas disebut dalam Pasal 26 ayat (3) revisi UU ITE.

Mengingat, bagaimana menakutkannya ketika sebuah data mulai terpublikasi di internet, kemungkinan besar data tersebut akan tersimpan lama atau bahkan abadi selamanya di internet. Data tersebut tidak hanya akan tersebar dalam satu platform digital karena kemudahan menyalin dan berbagi informasi yang dapat dilakukan di internet membuat data yang terpublish itu dapat tersebar keseluruh platform digital dengan sangat mudah. Internet sendiri memiliki kemampuan yang nyaris tidak terkontrol dalam hal mencari dan menyimpan, yang oleh David Linsay digambarkan sebagai fenomena the problem of digital eternity. (Jamaludin, 2020)

Setelah disahkannya Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi, hal ini menjadi bagian dari pengaturan dari hak untuk dilupakan melalui penghapusan data informasi (right to be forgotten). Pengaturan ini diakui lebih baik dibandingkan dengan Undang-Undang Nomor 1 Tahun 2024 tentang Informasi dan Transaksi Elektronik, sebab ketentuan penghapusan data lebih dipersempit untuk data pribadi, bukan informasi. Berdasarkan Pasal 43 ayat (1) Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi, diatur syarat penghapusan data, yakni data pribadi yang tidak diperlukan lagi, ditarik datanya oleh subjek data, permintaan subjek data, dan data yang diperoleh melalui perbuatan melawan hukum.

Pengaturan Undang-Undang ini dibuat guna mengatur penggunaan teknologi informasi, agar para pengguna mampu menggunakan teknologi informasi tersebut berdasarkan moral dan etika. Apalagi, pesatnya arus globalisasi juga berpengaruh pada penggunaan internet yang semakin tidak bisa dilepaskan pada hampir keseluruhan aspek kehidupan. Sehingga, kontrol terkait penggunaan internet tersebut juga sangat sulit dilakukan. Berkembangnya teknologi informasi memang memberikan banyak kontribusi terhadap peningkatan kemajuan, kesejahteraan dan peradaban manusia.

PERMASALAHAN

Metode penelitian yang digunakan untuk menulis penelitian ini adalah dengan metode penelitian yuridis-normatif. Penelitian yuridis normatif merupakan penelitian hukum yang dilakukan dengan cara menelisik bahan pustaka dan bahan sekunder belaka melalui penelaahan atas peraturan perundang-undangan serta berbagai literatur yang berkaitan dengan permasalahan yang diteliti. (Mamuji, 2013) Pendekatan yang dimaksud dilakukan dengan menggunakan metode penelitian kepustakaan dan pendekatan komparatif. Metode konseptual yang di perlukan untuk penelitian ini dengan menggunakan pemahaman melalui literatur yang diperoleh dari buku, jurnal, dan hasil penelitian sebelumnya, sehingga pengumpulan sumber data melalui buku atau media cetak/online yang dihimpun untuk dapat memberikan suatu gambaran mengenai hasil yang nantinya akan menjadi rujukan dalam penulisan ini?

PEMBAHASAN

Implementasi Prinsip Right To Be Forgotten Di Indonesia Dalam Penegakan Hukum Pidana Di Era Digital

Kejahatan kerap diartikan sebagai tindakan melanggar aturan hukum yang mengakibatkan orang tersebut dapat diberikan hukuman. Kejahatan merupakan bagian dari kehidupan masyarakat dan merupakan peristiwa sehari-hari. Seorang Filsuf bernama Cicero mengatakan *Ubi Societas, Ibi Ius, Ibi Crime* yang artinya ada masyarakat, ada hukum dan ada kejahatan. Masyarakat saling menilai, berkomunikasi dan menjalin interaksi, sehingga tidak jarang menimbulkan konflik atau perikatan. Satu kelompok akan menganggap kelompok lainnya memiliki perilaku yang menyimpang apabila perilaku kelompok lain tersebut tidak sesuai dengan perilaku kelompoknya. Perilaku menyimpang ini seringkali dianggap sebagai perilaku yang jahat. Batasan kejahatan dari sudut pandang masyarakat adalah setiap perbuatan yang melanggar kaidah- kaidah yang hidup di dalam masyarakat. (Alam, 2010)

Berkembangnya teknologi masa kini menjadikan banyaknya kejahatan melalui dunia maya yang biasa disebut *cybercrime*. Kejahatan ini dilakukan oleh pelaku untuk mendapatkan informasi secara ilegal, penyalahgunaan data sebagai keuntungan pelaku. *Cybercrime* memiliki arti yakni bentuk kejahatan dunia maya dengan memanfaatkan komputer yang memiliki jejaring sosial sebagai media kejahatan.

Kejahatan cyber (*cybercrime*) adalah bentuk ancaman baru yang belum pernah ada sebelumnya pada masyarakat dunia. *Hacking, cracking, defacing, sniffing, carding, phishing, spamming, ataupun scam* adalah sederet kejahatan internet yang cukup berisiko dan banyak menimbulkan kerugian pada banyak pihak. Tindak pidana *cybercrime* sangat tidak sesederhana seperti yang kita ketahui khususnya dalam proses penegakan hukumnya, mulai dari undang-undang yang mengatur mengenai kejahatan *cybercrime*, hingga Pengadilan Negeri mana yang berwenang untuk mengadili perkara tersebut. Tindak pidana *cybercrime* selain diatur dalam KUHP, Undang- Undang nomor 1 Tahun 2024 Tentang Perubahan kedua atas Undang-Undang Nomor 1 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik dan Undang-Undang Nomor 27 Tahun 2022 Tentang Pelindungan Data Pribadi.

Upaya penanggulangan cybercrime dalam perspektif hukum pidana dapat dilihat dari segala aspek, yaitu antara lain dari aspek kebijakan kriminalisasi (formulasi tindak pidana), aspek pertanggung jawaban pidana atau pemidanaan (termasuk aspek alat bukti/pembuktian), dan aspek yurisdiksi yang mana hal tersebut dapat membantu dalam hal penanggulangan cybercrime.

Kegiatan siber tidak lagi sederhana, karena kegiatannya ini tidak lagi dibatasi oleh teritorial suatu negara, yang mudah diakses kapanpun, dan dimanapun. Kerugian dapat terjadi, baik pada pelaku transaksi, maupun pada orang lain yang tidak melakukan transaksi di internet. Pembuktian merupakan hal yang sangat penting, mengingat informasi elektronik belum terakomodasi dalam sistem hukum acara di Indonesia secara komprehensif, dan ternyata juga sangat rentan untuk diubah, disadap, dipalsukan, dan dikirim ke berbagai penjuru dunia dalam waktu yang sangat singkat, dengan demikian dampak yang diakibatkannya bisa sangat kompleks dan rumit. (Prasetyo, 2020)

Adapun yang dimaksud dengan hak untuk dilupakan (right to be forgotten) yaitu Hak yang dimana berlaku untuk semua orang warga negara Indonesia yang meminta penghapusan informasi maupun dokumen elektronik terkait data dirinya yang sudah tak relevan lagi di dunia internet. Sehingga untuk mencapai dilupakan tersebut harus dilakukannya sistem penghapusan atau pemusnahan data/dokumen elektronik, walaupun tidak semua kasus dapat dimintakan penghapusannya sebab ada ketentuan lain yang harus diketahui dan dikonsumsi oleh publik mengenai dokumen tersebut.

Konsep right to be forgotten di Indonesia merupakan sebuah konsep yang sedang berkembang dalam bidang hukum siber. Konsep ini hadir sebagai bentuk kegiatan untuk mengembalikan fungsi kontrol atas informasi pribadi yang beredar di internet kepada masing-masing pribadi. Penerapan konsep right to be forgotten di Indonesia tidak menitikberatkan pada search engine, melainkan penghapusan konten yang dianggap tidak relevan didasarkan atas penetapan pengadilan langsung. Proses tersebut dilakukan oleh penyelenggara sistem elektronik yang memegang kendali langsung atas suatu konten tertentu dengan didasarkan atas penetapan pengadilan. (syahroni, 2021)

Hak untuk dilupakan merupakan bagian dari hak asasi manusia yang pada intinya mengenai hak untuk memperoleh perlindungan hukum akan gangguan atau pelanggaran terkait urusan individual, hubungan surat-menyurat, kehormatan maupun nama baik yang dimiliki oleh orang tersebut yang tidak boleh diganggu dengan sewenang-wenang. Dalam hak untuk dilupakan, data pribadi yang disebarkan hingga menimbulkan jejak digital, tanpa persetujuan orang yang memiliki atau berkaitan dengan data pribadi tersebut dapat dihapus atau dihilangkan rekam digitalnya. Namun hak untuk dilupakan ini juga mengalami beberapa kendala dan keterbatasan dalam penerapannya di berbagai negara, mengingat bahwa realitanya hak digital bersifat lintas negara, sebab website yang resmi di blokir oleh pemerintah Indonesia belum tentu mengalami pemblokiran pada negara lain sehingga hal ini dapat menyebabkan dokumen elektronik tersebut tetap dapat diakses ketika berada diluar negeri, untuk itu diperlukannya sebuah peraturan yang berlaku untuk seluruh website di dunia atas tindak pidana cybercrime.

Kemampuan internet yang nyaris sempurna itu tentu akan berdampak negatif bagi mereka yang kemudian data pribadinya disebar tanpa ada persetujuan darinya. Namun, sangat

disayangkan desain pengaturan dalam Undang-Undang Informasim Transaksi Elektronik terhadap hak untuk dilupakan ini masih belum memadai. Konsep pengaturannya masih terlalu umum atau dalam artian lain belum spesifik, masih ada pula bunyi pasal yang multitafsir sehingga mengakibatkan kekaburan norma, dan meskipun sudah terdapat rujukan pengaturan terkait perlindungan data pribadi seseorang, batasan data pribadi yang dapat dihapuskan dalam pengaturan hak untuk dilupakan ini masih terlalu luas, sehingga dapat menjadikan pengaturan hak untuk dilupakan tersebut bertabrakan dengan peraturan perundang-undangan terkait hak publik atas informasi dan kebebasan berekspresi, hal tersebut tentu menjadi problematika tersendiri dalam pengimplementasian hak untuk dilupakan yang kaitannya erat dengan Hak Asasi Manusia yang dijamin dalam Undang-Undang Dasar 1945, yakni perlindungan terhadap diri pribadi dalam kaitannya dengan perlindungan terhadap hak-hak pribadi atau hak privat sebagaimana yang diatur dalam Pasal 28 G Ayat (1) serta perlindungan hukum dan pengakuan diri dalam Hak Asasi Manusia.

Dalam perspektif Hak Asasi Manusia ini membuat adanya keterbatasan dalam mengakses informasi pribadi milik orang lain, alasannya adalah karena sesama warga negara Indonesia harus saling menghargai dan menghormati antar sesama privasi. Adanya hak untuk dilupakan ini juga membatasi adanya penyalahgunaan wewenang atas informasi data pribadi yang tersebar diinternet, sehingga perlu untuk terus di dorong penerapan dan pelaksanaannya.

Keberadaan hak atas informasi sendiri merupakan manifestasi dari hak fundamental untuk memperlihatkan apakah sebuah pemerintahan itu transparan dan partisipatoris atau justru sebaliknya. Salah satu sarana yang telah diberikan oleh pemerintah untuk penjaminan hak atas informasi itu sendiri adalah dengan produk hukum yang mengatur terkait kemerdekaan pers, yaitu Undang-Undang Nomor 40 Tahun 1999 tentang Pers. Dimana dalam Undang-Undang tersebut telah diberikan ketentuan terkait salah satu wujud masyarakat yang berdaulat adalah dengan adanya kemerdekaan pers itu sendiri. Dalam konsep pengaturan kemerdekaan pers ini, pendapat juga pikiran sesuai hati nurani serta kebebasan memperoleh informasi dijamin kemerdekaannya karena hak tersebut merupakan hak asasi manusia yang perlu ditegakkan dan dijamin pelaksanaannya.

Penjaminan terhadap kemerdekaan pers ini diperlukan guna mendapatkan penyampaian informasi yang benar; memperoleh sarana untuk bertukar pikir secara bebas; memperoleh instrument perubahan dan kemajuan dalam berbagai aspek kehidupan; memperoleh penjagaan ketertiban sosial karena dengan adanya kemerdekaan pers maka masyarakat memiliki tempat untuk menyalurkan pendapatnya ke meja pers tanpa adanya hambatan; memperoleh kekuasaan pemerintah yang dapat dikontrol, dalam artian lain sebagai alat pengawas untuk pemerintahan; memperoleh kesejahteraan dan kemakmuran atas dasar keadilan sosial bagi seluruh rakyat yang menjadi cita-cita bangsa; dan yang terakhir adalah untuk instrument penyebar nilai-nilai kemanusiaan, keterbukaan, toleransi dan nilai kemanusiaan yang lain. (Manan, 2018)

Rekam jejak digital dalam mesin pencari (search engine) memiliki banyak informasi apabila digunakan dengan tepat, karena dengan rekam jejak (track record) tersebut dapat diketahui bagaimana rekam jejak seseorang, apalagi jika berkaitan dengan rekam jejak seorang pejabat publik, mantan pejabat, calon pejabat, badan swasta maupun badan publik. Semisal adalah yang berkaitan dengan tindak korupsi, hak asasi manusia, lingkungan hidup dan informasi-informasi lain yang diperlukan untuk publik menilai kualitas dan integritas yang

bersangkutan. Sehingga, kemudian informasi tersebut dapat digunakan untuk hal-hal yang diperlukan, seperti pada halnya pemilihan umum. Ketentuan hak untuk dilupakan dapat disalahgunakan oleh pihak-pihak tertentu untuk menghapuskan informasi yang sifatnya menjadi hak publik untuk tau. Dalam artian lain, pihak-pihak yang menyalahgunakan hak untuk dilupakan tersebut dengan sengaja menghapus atau menyembunyikan informasi atau rekam jejak digital tentang dirinya yang buruk hingga tak dapat diketahui dan diakses oleh publik.

Problematika tentang pentingnya perlindungan data pribadi mulai menguat seiring dengan meningkatnya jumlah pengguna telepon seluler dan internet. Banyak kasus terjadi yang berkaitan dengan kasus penyalahgunaan dan kejahatan data pribadi seperti jual beli data pribadi, penggelapan rekening nasabah, kebocoran data pribadi seseorang yang berakhir dengan aksi penipuan atau tindak kriminal pornografi. Berkaca dari kejadian ini semakin menguatkan wacana pentingnya pembuatan aturan hukum untuk melindungi data pribadi. Perlindungan data pribadi berhubungan dengan konsep privasi. Konsep privasi sendiri adalah gagasan untuk menjaga integritas dan martabat pribadi. Hak privasi juga merupakan kemampuan individu untuk menentukan siapa yang memegang informasi tentang mereka dan bagaimana informasi tersebut digunakan. (Komarudin, Perlindungan Hak Atas Privasi di Internet-Beberapa Penjelasan Kunci, 2014)

Persoalan hak untuk dilupakan sesungguhnya mendasar secara konsep dan filsafat hukum. Ketika diturunkan menjadi kesenjangan antara hak untuk dilupakan versus hak kebebasan berekspresi, sehingga hak asasi manusia dapat menjadi pedang bermata dua. Kedua hak tersebut sama-sama merupakan hak asasi manusia. Tidak sedikit yang mengkritik adanya pelaksanaan klausul hak untuk dilupakan sebagai suatu bentuk penyensoran dan perlindungan diri atas dasar perbuatan masa lalu. Penyedia Jasa Aplikasi harus menghapus data yang diajukan oleh subjek data atas hak penghapusan informasi apabila memenuhi kondisi-kondisi yang disyaratkan yaitu data tidak lagi sesuai atau tidak lagi relevan dengan tujuan awal saat di kumpulkan, data tidak sah untuk di proses, data melanggar hukum dan aturan, dan data harus dihapus karena kewajiban. Apabila kondisi-kondisi tersebut sesuai dengan keadaan data dan subjek data dapat mengajukan penghapusan atas data tersebut, maka Penyedia Jasa Aplikasi wajib segera menghapus data tersebut tanpa menundanya lagi, serta bertanggung jawab atas semua biaya dan teknologi yang diperlukan untuk melakukan penghapusan tersebut. Namun, hak penghapusan informasi bukanlah hak absolut karena hak ini dibatasi pula dengan batasan-batasan dan pengecualian yaitu hak kebebasan berekspresi, untuk memenuhi kewajiban hukum, kepentingan umum kesehatan masyarakat, kepentingan umum, ilmiah, penelitian sejarah, serta pembentukan pertahanan dari tuntutan hukum. (sari, 2024)

Keberadaan hak untuk dilupakan (*right to be forgotten*) apabila tidak dipertimbangkan dengan sangat hati-hati, justru akan melangkahi batas garis yang ditetapkan oleh hak publik atas informasi dan hak media untuk berekspresi. Batasan terkait informasi yang layak untuk dihapuskan harus benar-benar diputuskan dengan hati-hati, cermat, dan obyektif melalui penetapan pengadilan. Karena dalam konteks hukum Indonesia, ada hak publik atas informasi dan kebebasan berekspresi sebagai hak atas kebebasan dan hak untuk dilupakan sebagai perlindungan hak di sisi lain. Pengaturan kedua hak tersebut harus benar-benar diseimbangkan agar dalam penerapannya tidak terjadi tumpang-tindih antara pengaturan hak yang satu dengan hak yang lain.

Perlindungan Data Pribadi Dalam Penegakan Hukum Pidana Di era Digital

Konstitusi negara Indonesia menjamin setiap orang berhak atas perlindungan, keluarga, kehormatan, martabat dan harta benda yang berada di bawah kendalinya dan mendapatkan hak atas rasa aman dan perlindungan dari ancaman ketakutan untuk berbuat atau tidak berbuat sesuatu yang merupakan bagian dari hak asasi manusia (HAM). Sedangkan, Pasal 29 Ayat (1) Undang-Undang Nomor 39 Tahun 1999 tentang HAM (UU Nomor 39 Tahun 1999), yang menyebutkan setiap orang berhak atas perlindungan diri pribadi, keluarga, kehormatan, martabat dan hak miliknya. Selain itu, Indonesia menjadi pihak yang meratifikasi ICCPR dan menjadi bagian hukum nasional dengan dibuatnya Undang-Undang Nomor 12 Tahun 2005 Tentang Pengesahan ICCPR (UU Nomor 12 Tahun 2005). Pastinya keberadaan aturan-aturan ini menjamin bahwa negara telah mencoba menjamin hak privasi menjadi bagian HAM.

Suatu data adalah data pribadi apabila data tersebut berhubungan dengan seseorang, sehingga dapat digunakan untuk mengidentifikasi orang tersebut, yaitu pemilik data. (Komarudin, 2014) Sementara itu, “data pribadi” adalah semua data yang berhubungan dengan orang-perorangan yang teridentifikasi dan dapat diidentifikasi. (Bernhard Ruben Fritz, 2016) Hak untuk dilupakan (right to be forgotten) adalah hak meminta penghapusan informasi dan data pribadi dari web yang hanya bisa dilakukan dalam kondisi tertentu. Hak untuk dilupakan merupakan hal yang sangat berkaitan erat dengan eksistensi diri. Hak untuk dilupakan dapat dikaitkan dengan hak asasi manusia terkait perlindungan hukum dan pengakuan diri. Pemikiran terhadap hak dilupakan tidak dapat dilepas dari hak privasi dalam penggunaan teknologi informasi.

Hak asasi manusia bahwa kemanusiaan manusia memiliki hak yang bersifat mendasar yang menyatu pada jati diri manusia, adanya hak tersebut berarti seseorang mempunyai suatu “keistimewaan” yang memungkinkan baginya diperlakukan sesuai kesitimewaan yang dimilikinya. Juga adanya suatu kewajiban yang harus dilaksanakan sesuai dengan “keistimewaan” yang ada pada orang lain. (El, 2009) Undang-Undang Dasar 1945 adalah fakta sejarah yang diyakini sebagai poin penting bagi penguatan demokrasi di Indonesia yang berbasiskan perlindungan terhadap HAM (Hak Asasi Manusia). (El, 2009) HAM tidak hanya berkembang seiring dengan perkembangan diri manusia itu sendiri yang cenderung dipengaruhi oleh lingkungan baik personal maupun masyarakat.

Perlindungan privasi dan data privasi tidak terlepas dari keberadaan hukum sebagai alat untuk melindungi hak konstitusional individu. Selain itu, ruang lingkup hukum dari perlindungan data pribadi sangat luas mulai dari jenis, prinsip, hak dan kewajiban subjek, kewajiban data controller dan juga data processor, transmisi data melewati jalur perbatasan negara lain, kedaulatan, data protection officer, data protection authority, serta bagaimana penyelesaian sengketa dan sanksinya bagi pelanggar hukum.

Adapun penjelasan terkait jenis data pribadi diatur dalam GDPR bahwa “*The following personal data is considered ‘sensitive’ and is subject to specific processing conditions:*

- a) *Personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs;*
- b) *Trade-union membership;*
- c) *Genetic data, biometric data processed solely to identify a human being;*

- d) *Health-related data*;
- e) *Data concerning a person's sex life or sexual orientation*".

Sedangkan, kategori data pribadi terdiri dari data pribadi yang bersifat umum dan data pribadi yang bersifat spesifik. "Uraian dari data pribadi yang bersifat umum meliputi:

- a) nama lengkap;
- b) jenis kelamin;
- c) kewarganegaraan;
- d) agama;
- e) kombinasi data pribadi guna dalam pengindentifikasian individu. Selain itu, data

Syarat vital dalam perlindungan data pribadi tidak hanya mengutamakan implementasi prinsip, tetapi juga pemenuhan hak subjek data dan kewajiban pengendali data. Faktanya, seorang pemilik data memiliki hak-hak yang terdiri dari: "hak untuk mendapatkan informasi; hak atas akses; hak untuk menyangkal; hak untuk memperbaiki, memblokir, dan menghapus; hak atas portabilitas data; hak pemrofilan dan pengambilan keputusan secara otomatis; hak pemulihan yang efektif, serta hak atas kompensasi dan pertanggungjawaban". Sedangkan, kewajiban pengendali data harus memberikan langkah-langkah organisasional dan teknis guna menunjukkan bahwa pengolahan data telah dilakukan sesuai dengan kaidah. (Nisa Nurfitri, 2022)

Beberapa ancaman keamanan siber seringkali berdampak langsung pada privasi, seperti kebocoran data, serangan phishing, dan malware. Misalnya, ketika sebuah perusahaan terkena serangan siber dan data pribadi pelanggan, seperti informasi keuangan atau kesehatan, dicuri, privasi mereka langsung terancam. Meski perusahaan sudah menerapkan berbagai perlindungan, seperti enkripsi atau firewall, kebocoran data tetap dapat terjadi, dan inilah yang bisa membahayakan privasi. Keamanan siber memang penting, tapi tidak cukup untuk melindungi privasi sepenuhnya. Organisasi harus memastikan bahwa data hanya digunakan untuk tujuan yang sah dan sesuai dengan persetujuan pemilik data. Contohnya, meskipun sistem sudah aman dari peretas, kalau data pelanggan digunakan tanpa sepengetahuan mereka, tetap saja privasi mereka dilanggar. Oleh karena itu, privasi membutuhkan pendekatan yang lebih menyeluruh, termasuk adanya kebijakan privasi yang jelas dan tata kelola yang baik.

Kontrol akses, yaitu cara kita membatasi siapa saja yang bisa mengakses data tertentu dalam suatu organisasi. Kontrol akses ini sangat penting, terutama jika menyangkut data sensitif, seperti informasi kesehatan atau keuangan. Contoh kontrol akses adalah Role-Based Access Control (RBAC), di mana seseorang hanya diberikan akses sesuai peran atau tanggung jawab mereka di perusahaan. Jadi, hanya mereka yang benar-benar perlu mengakses data tertentu yang bisa melihatnya, mengurangi risiko penyalahgunaan atau kebocoran data. Selain itu, enkripsi juga penting untuk menjaga privasi dan keamanan. Dengan mengenkripsi data, meskipun data tersebut berhasil dicuri, peretas tidak bisa membacanya tanpa kunci dekripsi yang tepat. Meskipun enkripsi membantu menjaga keamanan, organisasi juga harus berhati-hati dalam bagaimana mereka menggunakan dan membagikan data untuk memastikan tidak ada pelanggaran privasi.

Pentingnya pendekatan holistik dalam menggabungkan keamanan siber dan privasi. Artinya, organisasi harus memperlakukan kedua hal ini secara bersamaan, dari awal hingga akhir siklus hidup data mulai dari pengumpulan, penyimpanan, hingga pemusnahan data. Ini juga berarti kerjasama lintas tim, antara tim IT, hukum, dan tata kelola data, untuk memastikan semua langkah yang diambil mematuhi peraturan yang berlaku, seperti UU PDP, GDPR atau CCPA.

Konsep perlindungan diri pribadi juga memungkinkan seseorang untuk mengontrol sejumlah elemen kehidupan pribadinya, diantaranya mengenai informasi tentang diri pribadinya, kerahasiaan identitas pribadi, akses terhadap data pribadi yang dimiliki oleh pihak tertentu, intersepsi komunikasi, pilihan atau perubahan nama, kehidupan seksual, profesi atau domisili, perlindungan terhadap gangguan lingkungan, serta hak untuk membangun dan mengembangkan hubungan dengan orang lain. (RI, 2020)

Pada praktiknya, terdapat sejumlah kasus di mana aparat penegak hukum maupun masyarakat memanfaatkan lemahnya perlindungan data pribadi dengan bertindak sewenang-wenang. Minimnya regulasi ini, membuat data sensitif seseorang menjadi rentan terlebih saat seseorang sedang berhadapan dengan penegakan hukum. Hasil survei Komnas HAM RI pada 2020 menunjukkan bahwa 66% masyarakat Indonesia merasa takut terhadap keamanan data pribadinya di dunia maya. (Data, 2020)

Di Indonesia, prinsip *right to be forgotten* (hak untuk dilupakan) dapat ditemukan dalam beberapa ketentuan hukum, terutama dalam Undang-Undang No.27 Tahun 2022 tentang Perlindungan Data Pribadi dan Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik. Undang-Undang Data Pribadi yang disahkan pada tahun 2022 mengatur tentang hak-hak subjek data, termasuk hak untuk menghapus data pribadi didalam Pasal 26 dan Pasal 27 Undang-Undang No.27 Tahun 2022 tentang Perlindungan Data Pribadi, dan terdapat ketentuan sanksi pidana di dalam Pasal 67 dan Pasal 68 Undang-Undang No.27 Tahun 2022 tentang Perlindungan Data Pribadi. Di dalam Pasal 26 Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, juga terdapat pasal yang mengaru mengenai prinsip *right to be forgotten*. Secara keseluruhan, meskipun prinsip "*right to be forgotten*" tidak diatur secara eksplisit dalam satu pasal tunggal dalam UU ITE, penerapannya dapat diintegrasikan dalam konteks perlindungan data pribadi melalui ketentuan di UU PDP. Implementasi dan pengawasan yang efektif terhadap regulasi ini sangat penting untuk memastikan hak privasi individu terlindungi di era digital.

PENUTUP

Implementasi prinsip "*right to be forgotten*" di Indonesia dalam konteks penegakan hukum pidana di era digital menghadirkan tantangan yang kompleks namun juga menawarkan peluang untuk meningkatkan perlindungan data pribadi. Persoalan hak untuk dilupakan sesungguhnya mendasar secara konsep dan filsafat hukum. Ketika diturunkan menjadi kesenjangan antara hak untuk dilupakan versus hak kebebasan berekspresi, sehingga hak asasi manusia dapat menjadi pedang bermata dua. Kedua hak tersebut sama-sama merupakan hak

asasi manusia. Tidak sedikit yang mengkritik adanya pelaksanaan klausul hak untuk di lupakan sebagai suatu bentuk penyensoran dan perlindungan diri atas dasar perbuatan masa lalu. Keberadaan hak untuk dilupakan (right to be forgotten) apabila tidak dipertimbangkan dengan sangat hati-hati, justru akan melangkahi batas garis yang ditetapkan oleh hak publik atas informasi dan hak media untuk berekspresi. Batasan terkait informasi yang layak untuk dihapuskan harus benar-benar diputuskan dengan hati-hati, cermat, dan obyektif melalui penetapan pengadilan.

Perlindungan data pribadi dalam penegakan hukum pidana di era digital menjadi sangat krusial mengingat pesatnya perkembangan teknologi dan akses informasi. Di satu sisi, teknologi memberikan kemudahan dalam pengumpulan dan analisis data yang dapat mendukung proses hukum, di sisi lain, hal ini juga menimbulkan risiko pelanggaran privasi dan penyalahgunaan data pribadi. Perlindungan data pribadi dalam penegakan hukum pidana di era digital harus menjadi prioritas, guna memastikan bahwa hak individu dihormati sambil tetap mendukung upaya penegakan hukum yang adil dan efektif. Dengan pendekatan yang tepat, diharapkan akan tercipta keseimbangan antara perlindungan privasi dan kebutuhan untuk keadilan dalam masyarakat.

DAFTAR PUSTAKA

- Siswanto, S. (2009). *Hukum Informasi dan Transaksi Elektronik, Studi Kasus Prita Mulyasari*. Jakarta: PT. Rineke Cipta.
- Lubis, M. S. (2020). *Pengenalan Teknologi Informasi*. Yayasan Kita Menulis.
- Lindasay, D. (2015). *Questioning the Right to Be Forgotten Alternative Law*. 40(2), 109.
- Undang-Undang Dasar Negara Republik Indonesia 1945 Dengan Penjelasan dan Amandemennya Beserta Susunan Kabiner Baru. (t.thn.). Surabaya: Penerbit Anugerah.
- Christianto. (2002). *Konsep Hak Untuk Dilupakan Sebagai Pemenuhan Hak Korban Revenge Porn*. *Jurnal Berkala Fakultas Hukum Universitas Gajah Mada*, 184.
- Anggraini, E. (t.thn.). Diambil kembali dari www.cnnindonesia.com/teknologi
- Jamaludin, S. M. (2020, September). *Menimbang Kembali Kehadiran Hak Untuk Dilupakan: Penerapan dan Potensi Ancaman*. *Jurnal Legislasi Indonesia*, 17(3), 367.
- Alam, A. (2010). *Pengantar Kriminologi*. 2010, Makasar: Penerbit Pustaka Refleksi.
- Prasetyo, M. Z. (2020). *Penegakan hukum oleh aparat penyidik cybercrime dalam kejahatan dunia maya (cybercrime) di wilayah polda DIY*. *juornal UMY*, 1(2), 2.
- Mamuji, S. S. (2013). *Penelitian Hukum Normatif: Suatu Tinjauan Singkat*. Jakarta: Raja Grafindo Persada.

- Komarudin, W. D. (2014). *Perlindungan Hak Atas Privasi di Internet; Beberapa Penjelasan Kunci*. ELSAM.
- Bernhard Ruben Fritz, W. D. (2016). *PerlindunganData Pribadi; Usulan Pelebagaan Kebijakan dari Perspektif Hak Asasi Manusia*. ELSAM.
- El, M. M. (2009). *Dimensi-Dimensi HAM: Mengurangi Hak Ekonomi, sosial dan Budaya*. Jakarta: PT. Rajagarfindo Persada.
- syahroni, I. (2021, Februari 3). *Heylaw*. (heylaw) Dipetik Oktober 2024, dari Heylaw: <https://heylaw.id/blog/yuk-kenalan-dengan-konsep-right-to-be-forgotten-di-Indonesia>
- Manan, B. (2018). *Menjaga Kemerdekaan Pers di Pusaran Hukum*. Dewan Pers.
- sari, i. (2024). *Konten Ilegal (Illegal Content): Sebuah Tindak Pidana Menurut Undang-Undang Informasi Dan Transaksi Elektronik (UU ITE)*. *Jurnal sistem informasi*, 11(1), 84.
- Nisa Nurfitri, L. S. (2022). *Tiktok Phenomenon: Exoneration Clause Vs. Personal Data Protection*,”. *Jurnal Pendidikan Kewarganegaraan Undiksha*, 10(1), 441–53.
- RI, K. H. (2020). *Standar Norma dan Pengaturan Nomor 5 tentang Hak atas Kebebasan Berpendapat dan Berekspresi*.
- Data, K. (2020). *Diambil kembali dari* <https://www.komnasham.go.id/index.php/laporan/2021/10/07/85/laporan-riset-kuantitatif-hak-kebebasan-berpendapat-amp-berekspresi-di-indonesia.html>
- Komarudin, W. D. (2014). *Perlindungan Hak Atas Privasi di Internet-Beberapa Penjelasan Kunci*. Jakarta: Elsam.