TI 6A Reguler/3/Alvin Tandiardi/5/Resume Masalah Privasi

TI 6A Reguler/11/Harun/5/Resume Masalah Privasi

TI 6A Reguler/23/Nely Febrianita/5/Resume Masalah Privasi

**Tugas Resume**

* **Buat resume tentang masalah privasi yang disebabkan oleh layanan Google.**

Layanan google adalah salah satu penawaran yang diberikan oleh pihak google, yang bertujuan menjaga perangkat tetap berfungsi dan memudahkan dalam melakukan suatu aktivitas seperti login di suatu aplikasi. Untuk memakai layanan ini maka pengguna harus mengisi sejumlah form yang didalamnya terdapat data seseorang. Layanan google didesain untuk saling terhubung, sehingga memudahkan untuk berpindah dari satu aktivitas ke aktivitas berikutnya. Misalnya, Maps dapat mengingatkan untuk berangkat ke janji temu yang muncul di Google Kalender Anda.

Google menyediakan berbagai layanan yang mencakup privasi, yaitu:

* aplikasi dan situs (seperti Search dan Maps)
* platform (seperti Google Play)
* layanan terintegrasi (seperti Maps yang disematkan di aplikasi atau situs perusahaan lain)
* perangkat (seperti Google Home)

Layanan ini mencerminkan cara kerja bisnis google, hukum yang berlaku untuk perusahaan google, dan hal-hal tertentu yang diyakini benar. Oleh karena itu, Persyaratan layanan ini membantu menentukan hubungan google dengan seseorang saat berinteraksi dengan layanan google. Misalnya, persyaratan ini mencakup:

* Hal yang dapat pengguna harapkan dari google, yang menjelaskan cara google menyediakan dan mengembangkan layanan ini
* Hal yang google harapkan dari pengguna, yang menetapkan aturan tertentu untuk menggunakan layanan ini
* Konten di layanan Google, yang menjelaskan hak atas kekayaan intelektual pada konten yang pengguna temukan di layanan google apakah konten tersebut milik pengguna, Google, atau orang lain
* Jika terjadi masalah atau ketidaksetujuan, yang menjelaskan hak hukum lainnya yang pengguna miliki, dan apa yang diharapkan jika seseorang melanggar persyaratan ini.

Penting untuk memahami persyaratan ini karena, dengan menggunakan layanan google, berarti menyetujui persyaratan ini. Selain persyaratan ini, google juga memublikasikan kebijakan privasi. Google memberikan fitur untuk memperbarui, mengelola, mengekspor, dan menghapus informasi.

Era internet dengan segala inovasinya membuat banyak aktivitas masyarakat menjadi lebih mudah. Namun di sisi lain, digitalisasi juga diduga memudarkan batas privasi pengguna. Sebab data-data pengguna terekam dalam sistem yang tidak bisa dikontrol seluruhnya oleh pengguna. Sebuah penelitian mengungkapkan, Google lewat sistem operasi Android dan Chrome selama ini mengumpulkan data lebih agresif dari yang mungkin disadari pengguna.

Google saat ini berada di bawah pengawasan masalah privasi. Bulan lalu, Komisi Energi dan Perdagangan AS mengirim surat ke perusahaan induk Google, Alphabet, mempertanyakan bagaimana Google mengumpulkan data melalui layanan lokasi, menara seluler, hotspot Wifi dan koneksi bluetooth, terutama ketika perangkat sedang tidak aktif. Investigasi Associated Press menemukan bahwa layanan Google pada perangkat Android dan iPhone melacak dan menyimpan data lokasi, bahkan jika mematikan riwayat lokasi di pengaturan privasi.

* **Prinsip - prinsip cyberlaw dan kendala hukum positif dalam menanggulangi cybercrime.**

Cyberlaw adalah hukum yang digunakan di dunia cyber (dunia maya), yang umumnya diasosiasikan dengan Internet. Cyberlaw merupakan aspek hukum yang ruang lingkupnya meliputi setiap aspek yang berhubungan dengan orang perorangan atau subyek hukum yang menggunakan dan memanfaatkan teknologi internet yang dimulai pada saat mulai online dan memasuki dunia *cyber* atau maya.

Cyberlaw sendiri merupakan istilah yang berasal dari **Cyberspace Law**. Cyberlaw akan memainkan peranannya dalam dunia masa depan, karena nyaris tidak ada lagi segi kehidupan yang tidak tersentuh oleh keajaiban teknologi dewasa ini dimana kita perlu sebuah perangkat aturan main di dalamnya (*Virtual World*).

Prinsip - prinsip yang ditetapkan dan pengembangan teknologi informasi:

* Melibatkan unsur yang terkait (pemerintah, swasta, profesional)
* Menggunakan pendekatan moderat untuk mensintesiskan prinsip.
* Memperhatikan keunikan dari dunia maya.
* Mendorong adanya kerjasama internasional mengingat sifat Internet yang global.
* Menempatkan sektor swasta sebagai *leader* dalam persoalan yang menyangkut industri dan perdagangan.
* Pemerintah harus mengambil peran dan tanggung jawab yang jelas untuk persoalan yang menyangkut kepentingan publik.
* Aturan hukum yang akan dibentuk tidak bersifat restriktif melainkan harus direktif dan futuristik.
* Melakukan pengkajian terhadap perundangan nasional yang memiliki kaitan langsung maupun tidak langsung dengan munculnya persoalan hukum akibat transaksi di internet seperti: UU Hak Cipta, UU Merk, UU Perlindungan Konsumen, UU Penyiaran dan Telekomunikasi, UU Perseroan Terbatas, UU Penanaman Modal Asing, UU Perpajakan, Hukum Kontrak, Hukum Pidana, dll.

Cyberlaw tidak akan berhasil jika aspek yurisdiksi hukum diabaikan. Karena pemetaan yang mengatur Cyberspace menyangkut juga hubungan antar kawasan, antar wilayah, dan antar negara, sehingga penetapan yuridiksi yang jelas mutlak diperlukan. Ada tiga yurisdiksi yang dapat diterapkan dalam dunia Cyber :

* Yurisdiksi legislatif di bidang pengaturan,
* Yurisdiksi judicial, yakni kewenangan negara untuk mengadili atau menerapkan kewenangan hukumnya, Yurisdiksi eksekutif untuk melaksanakan aturan yang dibuatnya.

Dalam rangka menanggulangi Cybercrime, Resolusi Kongres PBB VIII/1990 mengenai Computer Related Crimes mengajukan beberapa kebijakan antara lain sebagai berikut:

1. Menghimbau negara anggota untuk mengintensifkan upaya-upaya penanggulangan penyalahgunaan komputer yang lebih efektif dengan mempertimbangkan.
2. Menghimbau negara anggota meningkatkan kegiatan internasional dalam upaya penanggulangan Cybercrime.
3. Merekomendasikan kepada Komite Pengendalian dan Pencegahan Kejahatan (Committee on Crime Prevention and Control) PBB.4

Walaupun Resolusi Kongres PBB VIII/1990 telah menghimbau negara anggota untuk menanggulangi Cybercrime dengan sarana penal, namun kenyataannya tidaklah mudah. Hal ini disebabkan oleh beberapa hal, yaitu:

1. Perbuatan jahat yang dilakukan berada dilingkungan elektronik. Oleh karena itu penanggulangan Cybercrime memerlukan keahlian khusus, prosedur investigasi dan kekuatan/dasar hukum yang mungkin tidak tersedia pada aparat penegak hukum di negara yang bersangkutan.
2. Cybercrime melampaui batas-batas negara, sedangkan upaya penyidikan dan penegakan hukum selama ini dibatasi dalam wilayah territorial negaranya sendiri.
3. Struktur terbuka dari jaringan komputer internasional memberi peluang kepada pengguna untuk memilih lingkungan hukum (negara) yang belum mengkriminalisasikan cybercrime.
4. Terjadinya data havens (negara tempat berlindung/singgahnya data, yaitu negara yang tidak memprioritaskan pencegahan penyalahgunaan jaringan komputer) dapat menghalangi usaha negara lain untuk memberantas kejahatan itu.

Mengenai upaya penanggulangan Cybercrime memerlukan suatu perhatian dan keahlian khusus dalam bidang teknologi, karena kejahatan ini mempergunakan sistem jaringan komputer yang dapat digunakan oleh siapapun juga tanpa mengenal batas teritorial dan waktu. Terkait dengan hal tersebut di Indonesia telah memiliki Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik dalam menindak kejahatan Cybercrime. Namun dalam pembuktian mengenai cybercrime Kitab Undang-Undang Hukum Acara Pidana belum mengatur mengenai informasi elektronik sebagai salah satu alat bukti. Sehingga diharapkan ketentuan mengenai informasi elektronik diatur secara tegas sehingga terdapat suatu kepastian hukum.

* **Virus >< Antivirus**

Virus adalah sebuah program kecil yang bisa menggandakan dirinya sendiri dalam media penyimpanan suatu perangkat (komputer, laptop, hp, dll). Virus umumnya dapat merusak perangkat lunak dan tidak dapat secara langsung merusak perangkat keras, tetapi dapat mengakibatkan kerusakan dengan cara memuat program yang memaksa over process ke perangkat tertentu. Efek negatifnya adalah virus dapat memperbanyak dirinya sendiri,, yang membuat sumber daya memori menjadi kurang signifikan. Hampir 95% virus komputer berbasis sistem operasi Windows, sisanya menyerang linux/GNU, Mac, FreeBSD,OS/2 IBM, dan Sun Operating System.

Antivirus adalah sebuah jenis [perangkat lunak](http://id.wikipedia.org/wiki/Perangkat_lunak) yang digunakan untuk mengamankan, mendeteksi, dan menghapus [virus komputer](http://id.wikipedia.org/wiki/Virus_komputer) dari sistem komputer. Antivirus disebut juga Virus Protection Software. Aplikasi ini dapat menentukan apakah sebuah sistem komputer telah terinfeksi dengan sebuah virus atau tidak. Umumnya, perangkat lunak ini berjalan di latar belakang (background) dan melakukan pemindaian terhadap semua berkas yang diakses (dibuka, dimodifikasi,atau ketika disimpan). Antivirus terbaru sekarang tidak hanya mendeteksi virus. Program antivirus sekarang juga telah dilengkapi dengan kemampuan untuk mendeteksi spyware, rootkits, dan malware - malware lainnya. Tidak hanya itu, antivirus sekarang dilengkapi firewall untuk melindungi komputer dari serangan hacker dan anti spam untuk mencegah masuknya email sampah dan/atau virus ke inbox pengguna.

Antivirus adalah sebuah program aplikasi yang berfungsi untuk mendeteksi dan membasmi program-program perusak, yang disebut malicious code pada perangkat komputer. Jika database antivirus tidak mampu membasmi suatu malicious code, maka biasanya antivirus akan mengkarantina program perusak tersebut. Durasi waktu pengkarantinaan akan ditentukan sampai antivirus menemukan formula untuk membasmi malicious code. Pengguna juga bisa langsung menghapus data yang diserang malicious code yang tersimpan pada folder karantina.

Untuk memudahkan para pengguna, program antivirus memberikan fasilitas penjadwalan yang bisa diatur sesuai keinginan pengguna. Penjadwalan yang dimaksud adalah jadwal untuk mendownload (mengunduh) database maupun versi, juga jadwal untuk scanning (mendeteksi) secara otomatis. Namun untuk jadwal men-download tentunya perangkat komputer harus tersambung ke jaringan internet. Proses peng-update-tan (pemutakhiran) database bisa juga dilakukan secara manual.

* **Invasi privasi ditinjau dari ITE**

Privasi berkaitan dengan hak individu untuk mempertahankan informasi pribadi dari pengaksesan oleh orang lain yang memang tidak diberi ijin untuk melakukannya. Contoh kasus Mr. X yang merupakan nasabah di bank A yang ditelepon dan ditawari kredit dan layanan lainnya dari penyedia jasa kredit padahal tidak pernah mendaftar layanan tersebut tetapi tidak sampai disitu, penelpon pun tahu data pribadi Mr. X seperti nama, tanggal lahir, bahkan nama ibu kandung . Contoh kasus lainnya adalah Mbak S yang mendapat teror melalui Whatsapp dan sms dari driver ojek online yang dinaikinya, bahkan driver tersebut juga membagikan nomor, nama, sampai alamat dari Mbak S ini ke driver lainnya, tentu saja ini sudah melanggar hak privasi dari Mbak S.

Secara umum, privasi adalah hak untuk sendiri dan hak untuk bebas terhadap gangguan orang lain. Privasi informasi adalah hak untuk menentukan informasi apa dan kapan informasi (diri sendiri ) tersebut dapat dikomunikasikan dengan orang lain. Hak ini berlaku untuk individu, kelompok maupun institusi.

Bagaimana permasalahan mengenai invasi privasi apabila dilihat dari kacamata Undang Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (ITE). Terkait perlindungan data pribadi dari penggunaan tanpa izin, Pasal 26 UU ITE mensyaratkan bahwa penggunaan setiap data pribadi dalam sebuah media elektronik harus mendapat persetujuan pemilik data bersangkutan. Setiap orang yang melanggar ketentuan ini dapat digugat atas kerugian yang ditimbulkan.

Bunyi Pasal 26 UU ITE adalah sebagai berikut:

* Penggunaan setiap informasi melalui media elektronik yang menyangkut data pribadi seseorang harus dilakukan atas persetujuan Orang yang bersangkutan.
* Setiap Orang yang dilanggar haknya sebagaimana di maksud pada ayat (1) dapat mengajukan gugatan atas kerugian yang ditimbulkan berdasarkan Undang-Undang ini

Pada bagian penjelasan Pasal 26 Undang-Undang Informasi dan Transaksi Elektronik menjelaskan lebih lanjut apa yang dimaksud dengan perlindungan data pribadi dalam kaitannya pemanfaatan teknologi informasi. Dijelaskan bahwa data pribadi adalah salah satu bagian dari hak pribadi (*privacy rights*) yang mengandung pengertian merupakan hak untuk menikmati kehidupan pribadi dan bebas dari segala macam gangguan, hak untuk dapat berkomunikasi dengan orang lain tanpa tindakan memata-matai dan hak untuk mengawasi akses informasi tentang kehidupan pribadi dan data seseorang.

Data pribadi merupakan seluruh informasi yang bersifat perseorangan dan sifatnya menjadi subjektif, sebagai contoh, mungkin bagi sebagian orang, berbagi informasi mengenai tanggal lahir adalah hal yang biasa, sementara bagi orang lainnya, informasi tanggal lahir sama pentingnya dengan informasi nomor kartu kredit. Perbedaan Perbedaan kebutuhan akan perlindungan data pribadi ini lah yang membuat saya berpendapat bahwa definisi data pribadi harus dibuat seluas mungkin dan bersifat subjektif.

Dalam Pasal 26 ayat (2) Undang-Undang Informasi dan Transaksi Elektronik dijelaskan bahwa bagi orang yang merasa hak atas perlindungan data pribadinya dilanggar, ia dapat mengajukan 36 gugatan atas kerugian yang ditimbulkan. Perlindungan data pribadi lebih diarahkan ke ranah hukum perdata dengan akhir penyelesaian adalah perolehan suatu bentuk ganti rugi yang dapat bersifat materil (dapat berupa kompensasi uang) maupun juga immaterial (dapat berupa permintaan permohonan maaf di surat kabar).

Definisi data pribadi sebagaimana pasal 26 UU ITE menurut kami belum cukup menjelaskan apa saja yang termasuk data perorangan. Oleh sebab itu, masih diperlukan referensi yang dimaksud data pribadi dalam peraturan perundangan lain. Sebagai contoh, Pasal 84 UU Adminduk menjelaskan data pribadi penduduk yang harus dilindungi meliputi:

* nomor KK (Kartu Keluarga);
* NIK (Nomor Induk Kependudukan);
* tanggal/bulan/tahun lahir;
* keterangan tentang kecacatan fisik dan/atau mental;
* NIK ibu kandung;
* NIK ayah; dan
* beberapa isi catatan Peristiwa Penting.

# **Refrensi**

Jannah, H. S., & Naufal, M. (2012, Februari-Agustus). PENEGAKAN HUKUM CYBER CRIME DITINJAU DARI HUKUM POSITIF DAN HUKUM ISLAM. *AL-MAWARID, XII*, 70-84.

Sari, S. W. (n.d.). *Virus dan Anti Virus.* Academia.edu.

UNPAS. (n.d.). TINJAUAN UMUM TENTANG PERLINDUNGAN HAK PRIVASI PENGGUNA SIM CARD BERDASARKAN PERMEN KOMINFO NOMO 14 TAHUN 2017 TENTANG REGISTRASI PELANGGAN JASA TELEKOMUNIKASI. *repository.unpas.ac.id*.

Windara, M. A., & Sukranatha, A. K. (2013, Juni 19). KENDALA DALAM PENANGGULANGAN CYBERCRIME SEBAGAI SUATU TINDAK PIDANA KHUSUS. *Bagian Hukum Pidana Fakultas Hukum Universitas Udayana*, pp. 1-10.

Yuda, H. S. (2013, Januari 02). Dasar Hukum Perlindungan Data Pribadi Pengguna Internet. *Indonesia Cyber Law Community*.

GOOGLE MENGHADAPI MASALAH PRIVASI PENGGUNA. Dikutip 28 Maret 2020 13.10 [Online]: <https://internasional.kontan.co.id/news/google-menghadapi-masalah-privasi-pengguna>

PRIVASI DAN PERSYARATAN GOOGLE. Dikutip 28 Maret 2020 14.00 [Online]: policies.google.com/terms/update?hl=id

BAB 2 INVASI PRIVASI. Dikutip 28 Maret 2020 09.25 [Online]: <https://slideplayer.info/slide/3070417/>

ETIKA PROVESI DAN KOMUNIKASI, DEFINISI CYBERLAW. Dikutip 28 Maret 2020 09.13[Online]: <http://etikaprofesitikbsi.blogspot.com/2013/05/cyberlaw.html>