LAPORAN HASIL PENELITIAN

PENEGAKAN HUKUM PRIVASI PADA AKTIVITAS PERDAGANGAN ELEKTRONIK

Disusun Oleh :
Alivia Regista Pratiwi
Maslihati Nur Hidayati

PROGAM STUDI MAGISTER ILMU HUKUM
UNIVERSITAS AL AZHAR INDONESIA
2021/2022

KATA PENGANTAR

Bismillahirrahmanirrahim,

Assalamu'alaikum Wr.Wb

Segala puji Allah SWT yang tidak berhenti memberikan kasih dan cinta-Nya untuk semesta. Dengan pertolongan Allah YME, penulis dapat menyelesaikan laporan hasil penelitian yang berjudul "Penegakan Hukum Privasi Pada Perdagangan Elektronik". Penyusunan laporan ini, penulis menyadari keterbatasan, kemampuan, dan pengetahuan penulis dalam penyusunan. Namun kesulitan ini dapat dibantu oleh beberapa pihak. Oleh karenanya penulis mengucapkan banyak terima kasih untuk berbagai pihak yang memberikan bantuan berupa doa dan usaha.

Penulis menyadari, dalam penyusunan laporan ini masih banyak kekurangan, walaupun penulis sudah berusaha dengan sebaik-baiknya. Oleh karenanya kritik dan saran yang bersifat membangun sangat penulis harapkan guna penyempurnaan penyusunan dan penulisan mini skripsi. Penulis berharap supaya mini skripsi ini bermanfaat dan dapat memperluas serta menambah pengetahuan bagi kita semua.

Wasalamu'alaikum Wr.Wb

Jakarta, Juli 2022

Penulis

DAFTAR ISI

BAB I

PENDAHULUAN

1. Latar Belakang

Ketika teknologi informasi dan komunikasi berkembang, ada kekhawatiran yang berkembang tentang sejauh mana mereka mengizinkan pelanggaran privasi pengguna Internet dan penyalahgunaan informasi pribadi mereka. Banyak teknologi terkait internet memiliki implikasi privasi aktual atau potensial. Survei secara konsisten menunjukkan bahwa individu lebih memperhatikan privasi mereka saat menggunakan Internet daripada saat terlibat dalam aktivitas lain. Pentingnya membangun kepercayaan dan keyakinan dalam transaksi online telah lama menjadi tema berulang yang terkait dengan e-commerce.

Kemampuan teknologi digital untuk mengumpulkan, menyimpan, dan mengakses data dalam jumlah besar dengan cepat, mudah, dan murah telah menyebabkan berbagai cara penggunaan informasi pribadi. Migrasi arsip dari kertas ke bentuk digital telah memperluas penggunaan dan dengan demikian memfasilitasi transfer arsip. Perkembangan lain yang dapat berdampak signifikan pada privasi pribadi adalah meluasnya penggunaan kamera digital dan telepon kamera, semakin populernya situs konten buatan pengguna, mesin pencari yang ditingkatkan, dan konten internet yang diindeks. Tidak hanya lebih mudah untuk menangkap lebih banyak informasi pribadi dalam bentuk digital, tetapi informasi itu dapat dengan mudah diunggah ke situs Internet, dan bahkan materi yang tidak jelas dapat diambil oleh mesin pencari yang kuat.

Teknologi Internet yang banyak digunakan, seperti cookie, kesalahan jaringan, Hypertext Transfer Protocol (HTTP), dan spyware, memungkinkan pengumpulan, pencocokan, analisis, penyalinan, dan distribusi dalam jumlah besar. informasi tentang pengguna Internet dan dapat berdampak signifikan pada privasi online . Teknologi manajemen hak digital, geolokasi, dan komputasi awan juga menghadirkan tantangan baru terhadap privasi informasi pribadi. Serangkaian insiden yang melibatkan pengungkapan informasi pribadi seperti nama, alamat, rincian kartu kredit dan nomor jaminan sosial telah menimbulkan kekhawatiran tentang privasi online. Ada banyak contoh pelanggaran keamanan serius yang mengakibatkan pengungkapan sejumlah besar informasi pribadi. Perkembangan strategi e-government telah membuat

pemerintah semakin sadar akan pentingnya melindungi privasi dan memastikan keamanan informasi, tidak hanya untuk pegawai pemerintah tetapi juga untuk pegawai pemerintah, untuk warga dan memastikan keamanan informasi, tidak hanya untuk pegawai pemerintah tetapi juga untuk warga dan bisnis untuk berinteraksi dengan pemerintah secara online.

Sebagai hasil dari perkembangan ini, ada seruan untuk meninjau dan mereformasi undang-undang untuk perlindungan yang lebih baik di lingkungan online. Pertumbuhan Internet dan teknologi online telah menyebabkan perubahan dalam undang-undang privasi untuk melindungi pengguna Internet, seperti di masa lalu ketika teknologi baru diperkenalkan, seperti telepon - memungkinkan orang lain melacak atau mengakses perilaku atau informasi pribadi - ini menimbulkan kekhawatiran. mirip dengan apa yang saat ini muncul dengan internet.[1]

A. Sejarah Pekembangan Lahirnya Privasi

Ketika teknologi informasi dan komunikasi berkembang, ada kekhawatiran yang berkembang tentang sejauh mana mereka mengizinkan pelanggaran privasi pengguna Internet dan penyalahgunaan informasi pribadi mereka. Banyak teknologi terkait internet memiliki implikasi privasi aktual atau potensial. Survei secara konsisten menunjukkan bahwa individu lebih memperhatikan privasi mereka saat menggunakan Internet daripada saat terlibat dalam aktivitas lain. Pentingnya membangun kepercayaan dan keyakinan dalam transaksi online telah lama menjadi tema berulang yang terkait dengan e-commerce.

Kemampuan teknologi digital untuk mengumpulkan, menyimpan, dan mengakses data dalam jumlah besar dengan cepat, mudah, dan murah telah menyebabkan berbagai cara penggunaan informasi pribadi. Migrasi arsip dari kertas ke bentuk digital telah memperluas penggunaan dan dengan demikian memfasilitasi transfer arsip. Perkembangan lain yang dapat berdampak signifikan pada privasi individu adalah meluasnya penyebaran kamera digital, serta ponsel fotografi, semakin populernya situs web konten buatan pengguna, peningkatan mesin pencari dan pengindeksan situs web. Internet halaman web isi.[1]

1 B Fitzgerald,A Fitzgerald, E Clark, G Middleton, Y F Lim, Internet and E-Commerce Law, 2011, Thomson Reuters

Tidak hanya memudahkan untuk menangkap informasi pribadi dalam bentuk digital, tetapi juga dapat dengan mudah diunduh dari situs Internet dari yang bahkan informasi yang tidak jelas dapat diambil oleh mesin pencari yang kuat.

Teknologi Internet yang banyak digunakan seperti cookie, bug web, Hypertext Transfer Protocol (HTTP) dan spyware, yang mengumpulkan, membandingkan, membuat profil, menyalin, dan mendistribusikan sejumlah besar informasi tentang pengguna Internet, dapat berdampak signifikan pada privasi online. Tantangan baru terhadap privasi informasi pribadi juga dihadirkan oleh manajemen hak digital dan teknologi geolokasi dan komputasi awan. Kekhawatiran privasi online telah berkembang dengan serangkaian insiden yang melibatkan pengungkapan informasi pribadi, seperti nama, alamat, detail kartu kredit, dan nomor jaminan sosial.

Ada banyak contoh pelanggaran keamanan serius yang mengakibatkan pengungkapan informasi pribadi sejumlah besar individu. Pengembangan strategi e-government telah membuat pemerintah lebih sadar akan pentingnya melindungi privasi dan memastikan keamanan informasi, tidak hanya untuk pegawai pemerintah tetapi juga pegawai pemerintah, untuk semua bisnis untuk berinteraksi dengan e-government. Sebagai hasil dari perkembangan ini, seruan telah dibuat untuk UU untuk ditinjau dan direformasi untuk meningkatkan perlindungan online.

Pertumbuhan Internet dan teknologi online telah menyebabkan amandemen undang-undang privasi untuk melindungi pengguna Internet, seperti yang terjadi sebelumnya ketika teknologi baru, seperti telepon, dapat memantau atau mengakses perilaku seseorang atau informasi pribadi pengguna. lainnya - angkat kekhawatiran serupa tentang Internet yang sekarang muncul bersama Internet Secara historis, privasi telah menjadi konsep umum dan diakui di banyak negara berbeda, baik secara hukum maupun moralitas. dienkripsi. Untuk memerintah. Sebagai contoh, hak atas privasi di negara-negara tunduk pada hukum perdata, tampaknya di Belanda disebut dignitas yang berarti hak individu, di Jerman disebut personlichkeitsrecht yang berarti hak individu sebagai perwujudan ekspresi kepribadian sedangkan di Swiss istilah Geheimssphare . mengacu pada kehidupan pribadi orang yang dikenal). Padahal, tahap awal privasi telah dikenal sejak lama, terutama sejak zaman

Yunani ketika orang mulai membedakan antara kepentingan publik dan pribadi. Pemikiran ini dilanjutkan oleh Socrates dan Aristoteles, yang berpendapat bahwa harus ada garis antara pemerintah dan individu.

Pendapat Socrates dan Aristoteles tersebut kemudian menjadi dasar bagi filsafat pada masa Stoic untuk lebih mempertajam pemisahan antara publik dan privat tersebut. Menurut Raymond Wacks, pemisahan antara kepentingan publik dan privat berkembang pada abad ke 16 dan 17 berkaitan dengan lahirnya teori kedaulatan negara yang mulai mengatur pemisahan antara kepentingan negara dan kepentingan perorangan. Baru awal abad 19, di Inggris kemudian pemisahan ini diatur secara rinci. Contoh lahirnya hukum publik, hukum privat, *tort law*, hukum kontrak dan hukum kebendaan dan hukum dagang.

Kemudian pemikiran lain yang mempengaruhi lahirnya konsep privasi padaa abad modern adalah pemikiran yang dikemukakan oleh John Locke dalam bukunya *Second Treatise of Civil Goverment* menyatakan *"But we know God hath no left one Man so to the Mercy of another, that he may have him if he please..... every man has a property in his own person."*

Menurut Turkiington, pandangan John Locke tentang manusianya sendiri dapat dipahami bahwa manusia dipandang sebagai individu yang mandiri dengan kehidupannya sendiri, sehingga mereka mulai membedakan antara manusia sebagai masyarakat dan makhluk hidupnya sendiri. Selain itu, Warren dan Brandheis, yang menulis artikel di Journal of Science Harvard Law School dengan judul "The Right Way to Privacy", menyatakan bahwa "Privasi adalah hak untuk menikmati hidup dan hak untuk menyendiri dan evolusinya Warren dan Brandheis, dengan perkembangan dan kemajuan teknologi, ada persepsi publik bahwa telah terjadi persepsi bahwa seseorang memiliki hak untuk hidup yang didefinisikan sebagai hak seseorang untuk bebas dari gangguan dalam kehidupan pribadinya atau milik orang lain atau oleh undang-undang untuk mengakui dan melindungi hak atas privasi, untuk dilindungi sebagai berikut: pertama, dalam hubungan dengan orang lain, seseorang harus menutupi sebagian dari kehidupan pribadinya untuk mempertahankan posisinya, akalnya untuk Gelar Kedua, seseorang dalam hidupnya membutuhkan waktu untuk menyendiri (menyendiri) sehingga privasi diperlukan bagi seseorang Ketiga, privasi adalah hak yang melekat terlepas dari

hak-hak lain, tetapi hak itu hilang jika orang tersebut mengungkapkan hal-hal pribadi. Keempat, hak privasi juga mencakup hak atas hubungan keluarga, termasuk bagaimana seseorang membangun pernikahan, membangun keluarga, dan orang lain mungkin tidak menyadari hubungan individu, karena itu Warren menyebutnya benar melawan dunia. Kelima, alasan lain mengapa privasi layak mendapat perlindungan hukum adalah karena kerugian yang ditimbulkannya sulit untuk dinilai. Kerugian ini jauh lebih besar daripada kerugian materil, karena mengganggu kehidupan pribadinya, jika ada kerugian, korban harus diberi ganti rugi.

Menurut Berzanson, pendapat Warren dan Brandheis penting karena untuk pertama kalinya privasi dihadirkan sebagai konsep hukum yang mewajibkan Negara, dalam hal ini pengadilan, untuk menghormati hak seseorang, sehingga mereka dapat lebih menikmati hidupnya.

Menurut Grisworld, konsep hak untuk dibiarkan sendiri sebenarnya tersirat dalam Proposisi sebagai cerminan dari hak atas kebebasan individu, yang isinya adalah sebagai berikut: *"The Makers of our Constitution undertook to secure conditions favourable to the pursuit of happiness. They recognized the significance of man's spiritual nature. Of his feeling and of his intellect... They conferred, as against the Government, the right to be let alone.. the most comprehensive of rights and the right most valued by the civilized men."*

1. Memperkenalkan konsepnya, Warren juga mengatakan bahwa privasi tidak mutlak, tetapi memiliki batasan, yaitu:
2. Kemungkinan mengungkapkan informasi pribadi seseorang untuk kebaikan bersama tidak dikecualikan
3. Tidak ada perlindungan privasi jika tidak ada kerugian
4. Tidak ada hak privasi jika subjek data telah menyatakan persetujuan untuk informasi pribadi mereka untuk dipublikasikan
5. Persetujuan dan privasi dilindungi oleh hukum karena kerusakan sulit untuk dinilai. Karena melibatkan psikologi seseorang, kerugian kognitif jauh lebih besar daripada kerugian fisik ketika mengganggu kehidupan pribadi seseorang.

Menurut Turkiington, Warren dan Brandheis, pendapat memiliki dampak signifikan terhadap privasi , menghasilkan banyak tanggapan, setuju

dan tidak setuju. Faktanya, sejak penulisan artikel tersebut, ide perlindungan privasi telah berkembang tidak hanya di Amerika Serikat tetapi juga di negara lain. Padahal, di negara-negara yang menganut sistem common law, seperti Inggris dan Amerika Serikat, privasi bukanlah hukum asing, karena tort law sebenarnya memiliki perlindungan lain.

Dalam perkembangannya, privasi mengacu pada misalnya tentang pelanggaran (masuk ke rumah orang lain tanpa izin). Mode intrusi mirip dengan mode privasi karena memiliki properti yang sama dengan intrusi. Dengan kata lain, ada area (ruang) yang tidak boleh dimasuki oleh orang lain tanpa seizin orang yang dituju. Hanya mode intrusi yang memiliki makna material, dan mode privat memiliki makna spiritual. Wellington setuju dengan Warren dan Brandyce, mengklaim: *"this articles an extraordinary essay by many tests, especially for its attempt to fashion a legal principle from changes in moral perception"*

Oleh karena itu, menurut Wellington, pandangan Warren dan Bradhayes sangat penting karena menandai awal dari konsep etika dan diakui sebagai prinsip hukum dan dasar hak asasi manusia. .. Mempengaruhi keputusan pengadilan yang mulai menegakkan rahasia. Misalnya, Pavesichv, Georgia. Kehidupan di Inggris Baru. Konten perusahaan tahun 1995 menyatakan bahwa hak atas privasi berakar pada prinsip-prinsip etika yang berakar pada filosofi hukum alam dalam kerangka hukum umum. Kemudian lainnya seperti Alabama, Alaska, Arizona, California, Connecticut, Columbia Special Zone, Florida, Illinois, Indiana, Iowa, Kansas, Kentucky, Louisiana, Michigan.

B. Pengertian Privasi

Definisi yang tepat dari "privasi" membingungkan karena konsepnya memiliki beberapa arti, yang bervariasi tergantung pada konteksnya. Konsep ini telah menjadi bahan diskusi akademis selama lebih dari satu abad, sejak makalah penting Samuel Warren dan Louis Brandeis, "Privasi," diterbitkan dalam Harvard Law Review pada tahun 2014. 1890 (kami bersikeras):

"Perlindungan lengkap individu dan properti mereka adalah prinsip setua hukum umum; tetapi dari waktu ke waktu perlu untuk mendefinisikan

kembali sifat dan ketepatan dari perlindungan ini. Perubahan politik, sosial dan ekonomi membutuhkan pengakuan hak-hak baru, dan hukum umum, di masa mudanya yang abadi, dikembangkan sebagai tanggapan terhadap tuntutan baru masyarakat. Oleh karena itu, sejak awal undang-undang hanya memberikan ganti rugi atas gangguan fisik terhadap jiwa dan harta benda untuk pelanggaran administratif. Oleh karena itu, "hak untuk hidup" hanya berfungsi untuk melindungi subjek dari baterai dalam berbagai bentuknya; kebebasan berarti tidak ada paksaan yang nyata; dan menjamin hak milik individu atas tanah dan ternak mereka. Kemudian orang-orang menyadari sifat spiritual manusia, kasih sayang dan kecerdasannya. Secara bertahap, ruang lingkup hak-hak hukum ini melebar; dan sekarang hak untuk hidup berarti hak untuk menikmati hidup - hak untuk menyendiri; kebebasan menjamin pelaksanaan hak-hak sipil yang luas, dan istilah "properti" telah berkembang untuk mencakup semua bentuk properti, baik tidak berwujud atau berwujud."

Baru-baru ini, Westin telah mendefinisikan "privasi" sebagai persyaratan bagi individu, kelompok, atau organisasi untuk menentukan kapan, bagaimana, dan sejauh mana informasi tentang mereka dapat dibagikan dengan orang lain. Jelas, ada banyak konsep yang tidak bisa dikatakan tentang privasi. Sebaliknya, privasi "pada dasarnya bergantung secara politis dan sensitif terhadap perubahan sosial dan teknologi."

Klasifikasi yang berguna dari berbagai bentuk keamanan yang berbeda, tetapi terkait disediakan oleh Pusat Internasional untuk Privasi Elektronik dan Informasi Privasi tentang Privasi dan Hak Asasi Manusia 2000: Sebuah Survei Pemantauan Internasional tentang Hukum Privasi dan Pembangunan.

1. Informasi keamanan. Ini termasuk menetapkan aturan mengenai pengumpulan dan pemrosesan informasi pribadi seperti informasi kredit, catatan medis, dan data pemerintah. Ini juga dikenal sebagai "privasi":
2. privasi fisik. Ini termasuk perlindungan fisik dari prosedur invasif seperti pengujian genetik, pengujian obat dan deteksi karies. Bentuk komunikasi lain; lainnya;

3. Kerahasiaan komunikasi, termasuk keamanan dan privasi telepon, surat, email, dan bentuk komunikasi lainnya
4. privasi teritorial. Ini termasuk pengaturan pembatasan akses ke rumah dan lingkungan lain seperti kerja dan ruang publik. Ini termasuk investigasi, pengawasan video, dan verifikasi identitas.

Royal Academy of Engineering menawarkan daftar yang lebih luas dari berbagai bentuk keamanan: Privasi datang dalam berbagai bentuk, tentang apa yang ingin kita rahasiakan:

1. Keamanan adalah informasi sensitif. Anda mungkin ingin menyimpan informasi tertentu tentang saya atau hal-hal lain, hal-hal tertentu yang kami rahasiakan dari orang lain atau orang-orang tertentu.
2. Privasi Anonim: Kami mungkin tidak ingin beberapa tindakan kami (termasuk tindakan yang dilakukan di depan umum) dapat diakses sebagai individu atau agen tertentu.
3. Anda juga dapat mengharapkan kerahasiaan. Hak untuk merahasiakan identitas seseorang karena alasan tertentu, seperti memisahkannya dari kepribadian atau peran sebagai pegawai negeri.
4. Privasi sebagai penentuan nasib sendiri: kita mungkin menganggap beberapa perilaku kita bersifat pribadi dalam arti "kebebasan kepada kami" dan tidak ada urusan orang lain (di mana "orang lain" itu dapat berkisar dari negara bagian hingga kepada privacy karyawan kami);
5. Demikian pula, kita dapat memahami hak atas privasi sebagai kebebasan untuk “dibiarkan sendiri”; melakukan urusan kita tanpa pengawasan: ini termasuk kebebasan berbicara, karena kita mungkin ingin mengungkapkan pendapat yang mungkin tidak ingin saya dengar dari pemerintah, majikan, atau tetangga kita;
6. Privasi sebagai pengelolaan data pribadi: Kami mungkin ingin mengelola informasi tentang kami – di mana ia disimpan, siapa yang melihatnya, siapa yang mengonfirmasi bahwa itu benar, dll. Fokusnya adalah pada "informasi rahasia" atau "privasi". Artinya, kemampuan seseorang untuk mencegah orang lain menerima informasi pribadi tentang dirinya dan untuk mengontrol bagaimana informasi itu

digunakan. Paterson menjelaskan "privasi" dan membedakannya dari privasi dan keamanan informasi sebagai berikut:

Perlindungan data terutama tentang otonomi pribadi dan kemampuan individu untuk mengelola data pribadi. Oleh karena itu, "bukan hanya kurangnya informasi tentang kita di benak orang lain. Kita mengelola informasi tentang diri kita sendiri." [Fn: C. Fried, "Privacy" (1968) 77 Yale LJ 475 at 482] Dalam pengertian ini , ini sangat berbeda dari dua konsep privasi dan keamanan informasi lainnya yang sering membingungkan.[2]

Undang-undang privasi informasi umumnya berusaha untuk mencapai tujuan ini dengan mewajibkan kepatuhan terhadap prinsip-prinsip penanganan informasi yang adil. Secara khusus, mereka mensyaratkan bahwa individu harus diberi tahu tentang tujuan penggunaan data mereka pada saat pengumpulan dan bahwa penggunaan dan pengungkapan selanjutnya harus konsisten dengan tujuan tersebut kecuali jika disetujui sebaliknya. Mereka juga berisi prosedur yang memungkinkan individu untuk memeriksa apa yang telah dikumpulkan dan meminta perubahan informasi yang ditemukan tidak benar atau menyesatkan, serta kewajiban untuk menerapkan pengamanan keamanan dan untuk memastikan bahwa informasi disimpan akurat dan tidak lebih dari cukup yg dibutuhkan.

Kerahasiaan berbeda dari privasi karena pada dasarnya melibatkan kewajiban hukum dan etika untuk menjaga kerahasiaan. Ini muncul dari konteks di mana informasi ditransmisikan dan memiliki efek membatasi pengungkapan informasi yang tidak sah kepada pihak lain. Efek meningkatkan keamanan, tetapi hanya meningkatkan koefisien kontrol yang terkait dengan keterbukaan informasi.

Keamanan informasi, di sisi lain, menyangkut metode yang digunakan untuk menyimpan dan mengirimkan data. Oleh karena itu, 4044 menekankan penggunaan langkah-langkah teknis dan lainnya untuk menjaga kerahasiaan data, dan 4044 untuk memastikan integritas dan keaslian data. Sementara

2 B Fitzgerald,A Fitzgerald, E Clark, G Middleton, Y F Lim, Internet and E-Commerce Law, 2011, Thomson Reuters

kerahasiaan tidak dapat dijamin tanpa keamanan, dimungkinkan untuk memiliki sistem yang aman tetapi tidak memungkinkan individu untuk mengontrol penggunaan atau pengungkapan informasi mereka.

Akhirnya, hak atas privasi diakui oleh hukum sebagai hak yang harus dilindungi dalam rezim hak asasi manusia dasar, sebagaimana diakui dalam Deklarasi Universal Hak Asasi Manusia, 1948 dan Kovenan Internasional tentang hak asasi manusia, pertanyaan sipil dan politik, 1966 dan dalam banyak kasus perjanjian internasional dan regional lainnya. lainnya. Privasi mendasari martabat manusia dan nilai-nilai lain, seperti kebebasan berserikat dan berekspresi. Ini telah menjadi salah satu masalah hak asasi manusia yang paling penting di zaman modern.

Hampir setiap negara di dunia mengakui hak atas privasi dalam konstitusi mereka, secara tegas atau implisit, dan kesepakatan negara-negara tersebut sangat bervariasi, tergantung pada tingkat perlindungan privasi yang diharapkan di suatu negara. Paling tidak, ketentuan privasi adalah hak individu atas rumah mereka yang tidak dapat diganggu gugat dan privasi komunikasi pribadi. Ada juga negara-negara yang memiliki privasi dalam konstitusi mereka, seperti Afrika Selatan dan Hungaria, yang mencakup hak khusus untuk mengakses dan mengontrol informasi pribadi seseorang.

Di banyak negara di mana privasi tidak diakui secara eksplisit dalam konstitusi, seperti Amerika Serikat (AS), Irlandia, dan India. Di banyak negara, perjanjian internasional yang mengakui hak seperti kerahasiaan "Deklarasi Universal Hak Asasi Manusia, Kovenan Internasional tentang Hak Sipil dan Politik atau Konvensi Eropa tentang Hak Asasi Manusia" telah diadopsi dalam undang-undang nasional mereka, termasuk ratifikasi ICCPR di Indonesia pada tahun Undang-undang No. 12. Pada awal 1970-an, negara-negara mulai mengesahkan undang-undang umum untuk melindungi privasi individu. Di seluruh dunia, ada kecenderungan yang meningkat untuk memberlakukan undang-undang data pribadi yang komprehensif, yang mengatur sektor publik dan swasta, yang dipengaruhi oleh model peraturan Uni Eropa.

Privasi adalah hak asasi manusia yang mendasar, penting karena berkaitan dengan otonomi atau hak asasi manusia dan dilindungi oleh hukum internasional, regional dan nasional dan telah diklasifikasikan menurut

peraturan tentang hak asasi manusia. Privasi dalam konsep perlindungan asli disebut hak untuk tidak diganggu oleh orang lain "hak untuk dibiarkan sendiri", jadi hak ini mengakui bahwa orang menetapkan batas dan melindungi diri dari gangguan. intrusi yang tidak diinginkan ke dalam hidup kita, pengaturan privasi akan memberikan individu kemampuan untuk bernegosiasi dengan siapa dan bagaimana kita akan berinteraksi dengan orang-orang di sekitar kita.

Privasi membantu kami menentukan siapa yang memiliki akses ke tubuh, lokasi, informasi kontak, dan informasi seseorang. Aturan Privasi memberi kita kesempatan untuk menegaskan hak kita dalam menghadapi ketidakseimbangan kekuatan yang besar. Oleh karena itu, hak atas privasi merupakan sarana penting untuk melindungi diri kita sendiri dan masyarakat dari penggunaan kekuasaan yang sewenang-wenang dan tidak beralasan, dengan mengurangi apa yang dapat diketahui tentang kita dan orang lain, apa yang kita ketahui, apa yang dapat mereka lakukan dengan kita, pada saat yang sama.

dari mereka mencoba untuk memaksakan kontrol. Privasi penting bagi kita sebagai makhluk hidup dan ruang untuk menjadi diri kita sendiri tanpa penilaian, memungkinkan kita untuk berpikir bebas tanpa diskriminasi, dan menjadi bagian penting dari hidup kita, penting dalam hidup kita, penting dalam hidup kita. Ini membantu kita mengontrol siapa yang mengenal kita.

Dalam masyarakat modern, debat privasi adalah debat modern tentang kebebasan. Sama seperti kami berusaha untuk menetapkan dan melindungi batasan di sekitar individu dan kemampuan mereka untuk memilih apa yang terjadi pada mereka, kami juga berusaha untuk memutuskan:

1. Etika kehidupan modern
2. Aturan yang mengatur tindakan komersial
3. Batasan yang kita tempatkan pada kekuasaan

C. Privasi Dalam *Cyber Law*

Cyber law erat kaitannya dengan pencegahan tindak pidana dan penanggulangan tindak pidana. Hukum siber adalah aspek hukum yang ruang lingkupnya meliputi aspek individu atau badan hukum yang menggunakan dan menggunakan teknologi internet sejak masuk ke dunia maya. Setiap negara

memfasilitasi kehidupan bernegara melalui penggunaan sistem elektronik canggih dan internet, secara tidak langsung perkembangan cyber law juga berkembang di sana. Ruang lingkup hukum siber meliputi hak cipta, hak merek dagang, pencemaran nama baik, penistaan, penghinaan, peretasan, perdagangan elektronik, manajemen sumber daya Internet, keselamatan pribadi, kehati-hatian, kejahatan komputer, dengan bukti, investigasi, pencurian internet, perlindungan konsumen, dan penggunaan internet sehari-hari. Karena erat kaitannya dengan pencegahan kejahatan dan penanganan kejahatan, maka cyber law menjadi landasan hukum bagi proses penegakan hukum terhadap kejahatan elektronik, termasuk pencucian uang dan kejahatan teroris.

Kehadiran cyber law di Indonesia sudah ada sebelum tahun 1999. Saat itu, cyber law merupakan instrumen hukum yang menjadi dasar dan pengaturan transaksi elektronik. Pendekatan terhadap instrumen hukum ini dimaksudkan untuk memberikan dasar bagi hukum dan peraturan lain yang dapat digunakan. Berbagai macam kejahatan dan pelanggaran dalam penggunaan teknologi diatur dalam undang-undang sebagai dasar hukum bagi semua kejahatan dan pelanggaran yang terjadi.

Warga harus memiliki hak untuk privasi online dalam hal ini kaitannya dengan *Cyber Law* dengan pemerintah kewajiban untuk menjaga warganya aman. Menemukan keseimbangan yang tepat antara privasi dan keamanan adalah tindakan penyeimbangan halus. Pengalaman baru-baru ini di Eropa dengan retensi data memegang pelajaran yang menarik bagi semua orang yang peduli dengan keseimbangan ini.

Teknologi selalu dikaitkan dengan hak ini. Misalnya, kemampuan kami untuk melindungi privasi sekarang lebih besar dari sebelumnya, tetapi kemampuan pengawasan yang ada berkembang tidak seperti sebelumnya, kami sekarang dapat mengidentifikasi individu inti secara unik. inti antara aliran dan aliran data besar, dan membuat keputusan tentang orang berdasarkan kumpulan data besar.

Bisnis dan pemerintah kini dapat memantau setiap percakapan yang kita lakukan, setiap transaksi bisnis yang kita lakukan, dan ke mana pun kita pergi.

Kemampuan ini dapat berdampak negatif pada individu, kelompok dan bahkan masyarakat karena mencegah tindakan, pengucilan dan diskriminasi. Ini juga memengaruhi cara kita berpikir tentang individu, pasar, masyarakat, dan negara. Jika situasi muncul di mana institusi yang kita andalkan mungkin mengenal kita sejauh mereka dapat memeriksa sejarah kita, melacak semua tindakan kita, dan memprediksi tindakan kita sendiri, dinamika masa depan 4.444 dan ketidakseimbangan kekuatan besar akan muncul, yang mengarah pada penilaian diri pribadi. kepercayaan. dalam manajemen dengan perusahaan, kelompok dan pemerintah dihentikan dan setiap pelanggaran yang dianggap menyimpang akan diidentifikasi, dideportasi atau bahkan dihancurkan. Mungkin tantangan terbesar terhadap privasi adalah bahwa hal itu dapat dilanggar tanpa disadari oleh individu tersebut.

Dengan hak-hak lain, Anda mengetahui pelanggaran - penahanan, penyensoran atau pembatasan. Dengan kata lain, Anda tahu siapa yang melakukannya: petugas penahanan, sensor atau polisi. Semakin, tidak ada yang menyadari kegiatan pengawasan yang melacak kami, dan kami tidak dilengkapi dengan keterampilan atau kesempatan untuk menginterogasi mereka. Di masa lalu, pengawasan terselubung, karena sifatnya yang mengganggu, kurangnya akuntabilitas, dan risiko spesifik yang ditimbulkannya terhadap kehidupan demokrasi, telah tersebar luas. Saat ini, banyak agen semakin memantau orang dan karena itu tidak pernah mengungkapkan prosedur pengawasan mereka, bagaimana kita diperlakukan, pemeriksaan fisik kita, pemeriksaan properti kita. Jika individu dapat berpartisipasi dalam dunia modern, perkembangan hukum dan teknologi akan meningkatkan, bukan melemahkan, kemampuan mereka untuk menikmati hak-hak ini secara bebas.

D. Pengertian Perdagangan Elektronik atau *E-Commerce*

Munculnya e-commerce kembali ke tahun 1960-an ketika bisnis menggunakan EDI (pertukaran data elektronik) secara populer. Kemudian pada tahun 1979, “American Standards Institute mengembangkan ASC X12. ASC X12 umumnya digunakan untuk berbagi dokumen menggunakan perangkat elektronik dan terus berkembang pada 1980-an dan 1990-an hingga salah satu

perusahaan terbesar, eBay dan Amazon, merevolusi dunia perdagangan.e-commerce."

Lahir dan berkembangnya undang-undang teknologi informasi didorong oleh konvergensi telekomunikasi dan teknologi informasi dan salah satunya mendorong diperkenalkannya alternatif penyedia jasa yang dikenal dengan kegiatan komersial yaitu e-commerce (selanjutnya disebut e-commerce). perdagangan untuk jangka pendek). E-commerce adalah kegiatan komersial barang dan jasa dengan partisipasi pihak-pihak, yaitu:

1. B2B (bisnis ke bisnis)
2. B2C (bisnis ke konsumen)
3. B2E (Bisnis untuk Karyawan)

Ditinjau dari jenis transaksinya, e-commerce sebenarnya terbagi menjadi dua jenis, yaitu sebagai berikut:

1. Transaksi elektronik tidak langsung, yaitu hubungan hukum antara pembeli dan penjual, adalah penyelesaian kontrak melalui Internet, tetapi pengiriman barang terjadi dengan cara biasa dalam penjualan barang.
2. Transaksi elektronik langsung, khususnya hubungan hukum yang dilakukan melalui Internet, baik kontrak atau pengiriman, umumnya merupakan bagian dari perdagangan jasa, seperti penjualan perangkat lunak, film, dan film. , musik atau informasi yang dapat diunduh.

Dilihat dari latar belakang perkembangannya, sejak tahun 1960-an, e-commerce telah terjadi antara perusahaan-perusahaan besar yang sudah memiliki jaringan sendiri, dan ketika internet mulai digunakan, e-commerce menjadi populer. Pada pertengahan tahun 1990-an, e-commerce mulai digunakan dalam perdagangan internasional dan mulai menjalin hubungan dengan negara di Uni Eropa dan Asia, dimulai dengan Amerika Serikat yang mengembangkan perkembangan e-commerce global melalui Kementerian Perdagangan. Pangsa e-commerce dalam perdagangan internasional telah berkembang pesat. E-commerce meliputi kegiatan mendistribusikan, membeli, menjual dan memasarkan barang dan jasa melalui sistem elektronik seperti internet atau jaringan komputer. Industri teknologi informasi juga mendefinisikan e-commerce sebagai e-commerce. Misalnya, transfer bank, pemasaran, EDI.

Pesan data, di sisi lain, adalah perangkat untuk mengirim, menerima atau menyimpan data secara elektronik atau optik atau dengan cara lain yang serupa seperti EDI, surat elektronik, telegram dan teleks. Untuk memperjelas ruang lingkup e-commerce, sejumlah definisi telah diusulkan oleh para sarjana dan organisasi internasional untuk mengatasi masalah-masalah berikut:

a. Menurut kamus elektronik Wikipedia

E-commerce meliputi kegiatan mendistribusikan, membeli, menjual dan memasarkan barang dan jasa melalui sistem elektronik seperti internet atau jaringan komputer. Industri teknologi informasi juga mendefinisikan e-commerce sebagai e-commerce. Misalnya, transfer bank, pemasaran, EDI.

Pesan data, di sisi lain, adalah perangkat untuk mengirim, menerima atau menyimpan data secara elektronik atau optik atau dengan cara lain yang serupa seperti EDI, surat elektronik, telegram dan teleks.

b. World Trade Organization (WTO)

WTO mendefinisikan perdagangan elektronik sebagai proses yang mencakup produksi, distribusi, pemasaran, penjualan dan penyediaan barang dan jasa melalui perangkat elektronik.

Dari definisi di atas, kami menyimpulkan bahwa perdagangan elektronik dapat didefinisikan sebagai perdagangan melalui jaringan komunikasi yang dapat berupa faks, surat elektronik, telegram, teleks, EDI (data interchange), komputer) dan sarana elektronik lainnya. Pertukaran informasi internet, periklanan, pemasaran, kontrak, bank (perbankan elektronik)

2. Rumusan Masalah

1. Bagaimana Penegakan Hukum Privasi Terhadap Perdangangan Elektronik?
2. Bagaimana Tantangan atau Kekhawatiran Data Privasi dalam Perdagangan Elektronik ?
3. Bagaimana Kasus Kebocoran Data Privasi Pada Perdagangan Elektronik di Indonesia ?
4. Bagaimana Teknologi dan Praktik Yang Mempengaruhi Privasi Online ?
5. Bagaimana Pengaruh Instrumen Internasional dan Regional terhadap Perlindungan Data Privasi ?

BAB II
PEMBAHASAN

1. Penegakan Hukum Privasi Pada Aktivitas Perdagangan Elektronik

A. Perkembangan Hukum Privasi

Pesatnya perkembangan teknologi informasi dan komunikasi telah menciptakan berbagai peluang dan tantangan. Salah satu bidang yang terkena dampak perkembangan teknologi informasi adalah interaksi aktif (hubungan) antara 4.444 individu. Informasi telah memperkenalkan etika baru bahwa siapa pun yang memiliki informasi selalu secara naluriah menyampaikannya kepada orang lain. Di sisi lain, keinginan untuk tidak berbagi informasi dengan orang lain dipandang tidak berasal dari komunitas informasi. Pertukaran informasi telah menjadi global saat ini, dengan komunitas informasi di banyak bagian dunia berkomunikasi satu sama lain secara intens.

Hubungan antar komunitas diwujudkan melalui teknologi informasi virtual atau dunia maya. Sistem informasi seperti perdagangan (e-commerce), pendidikan (e-literacy), kesehatan (telemedicine), transportasi, industri, pariwisata dan pemerintahan (e-Government) digunakan dalam berbagai bidang kehidupan. Cakupan dan sistem teknologi informasi, termasuk proses pengumpulan, penyimpanan, produksi, dan pengiriman. Cepat dan efisien dengan industri atau masyarakat.

Teknologi informasi menjanjikan bahwa masyarakat akan memiliki jaringan komunikasi dan teknologi multimedia sebagai tulang punggungnya di abad ke-21. Janji-janji yang mengubah tatanan baru kehidupan sosial, atau sebaliknya, dapat menimbulkan masalah yang tidak pernah terbayangkan sebelumnya. Perubahan yang sangat penting ini terjadi bersamaan dengan berakhirnya globalisasi. Dunia menjadi masyarakat global yang mengambil tindakan baru yang berbeda dari masa lalu, dengan hubungan yang tidak sadar akan batas negara. Institusi baru yang lahir dari integrasi komunitas komputasi melalui jaringan virtual membawa implikasi baru. Artinya, interaksi sosial

orang-orang dalam komunitas komputasi dari berbagai ras, etnis, warga negara, tingkat kehidupan ekonomi di masyarakat, dan tingkat pendidikan. Dalam dunia yang mengglobal, akan muncul perilaku dan model karakter dari berbagai jenis dari masa lalu.

Privasi dalam komunitas informasi global sangat bervariasi antara pengaturan yang sebenarnya. Privasi dalam konteks data dan informasi pribadi hanya terjadi di komunitas komputer. Begitu pula dengan manfaat perlindungan data dan informasi yang cukup besar seiring dengan meningkatnya antusias pihak-pihak yang memiliki data dan informasi pribadi dalam menjaga kerahasiaan. Kebutuhan untuk menjaga kerahasiaan data dan informasi pribadi muncul sebagai prioritas untuk membangun kepercayaan dalam jaringan media interaktif. Ini adalah informasi yang harus diungkapkan secara naluriah, tetapi kami menyadari bahwa kami perlu melindungi data dan informasi pribadi tertentu tentangnya. Komunitas TI mempertimbangkan kebutuhan keamanan data dan informasi pribadi tertentu. Keinginan untuk melindungi data dan informasi erat kaitannya dengan tingkat kepercayaan, dan ada korelasi antara tingkat kepercayaan dan perlindungan data dan informasi tertentu yang terkait dengan kehidupan pribadi.

Mengingat perkembangan di atas, beberapa jenis pelanggaran data, atau perlindungan data, telah berevolusi untuk melindungi individu ketika informasi pribadi diakses tanpa izin. Perlindungan Informasi Pribadi Konsumen Online dalam Kebijakan Privasi E-Commerce Indonesia adalah gambaran lengkap tentang tanggung jawab dan pelaksanaan peraturan ini untuk melindungi hak privasi individu yang mengungkapkan informasi privasi dalam kegiatan e-commerce.

Kebijakan privasi dari setiap transaksi e-commerce

sangat penting dalam e-commerce

sebagai kode etik yang dihormati dan mudah diakses oleh para pihak. Selain itu, integrasi standar perlindungan data dalam sistem pasar online 4244 berdasarkan Pasal 2 Undang-Undang Kontrak Kesenjangan telah dilakukan. Ini

memastikan keterlibatan dan kinerja penyedia layanan e-commerce dan konsumen online.

Perbaikan yang tersedia untuk konsumen online terkait dengan pelanggaran data yang terbukti dari Konferensi Perserikatan Bangsa-Bangsa tentang Perdagangan dan Pembangunan (UNCTAD) atau dua proses: proses arbitrase (sengketa dan arbitrase) dan proses konsensus (arbitrase dan negosiasi). Konferensi PBB tahun 2003 tentang Perdagangan dan Pembangunan E-Commerce dan Laporan Pembangunan menjelaskan elemen penyelesaian dan persetujuan yudisial. Secara khusus, PP No 28 Tahun 2008 tentang ITE dan Tahun 2012 tentang peraturan baru untuk pelaksanaan sistem dan transaksi elektronik (PSTE) dapat membawa tindakan perdata untuk kerusakan. Ini dimaksudkan sebagai mekanisme hukum bagi pengguna online.

Klaim Warga ada mekanisme bagi vendor e-commerce baru untuk menuntut ganti rugi warga. Realitas bisnis e-commerce menunjukkan bahwa konsumen adalah pihak yang paling lemah dalam setiap transaksi tersebut. Ringkasnya, aturan teknis terkait kode etik dalam kegiatan e-commerce dikatakan melindungi kepentingan konsumen melalui persetujuan perlindungan. Rincian kebijakan privasi yang berlaku untuk e-commerce dan aktivitas e-commerce disepakati bersama oleh kedua belah pihak untuk mencegah penyedia platform pasar online mengumpulkan data semata-mata untuk tujuan menghasilkan uang.

Dalam konteks ini, negara adalah “perantara”, adil, dan mengontrol pihak-pihak yang menyediakan/menjual layanan e-commerce, dan mengembangkan kebijakan privasi yang setuju dengan konsumen mengenai data privasi yang dilakukan secara online. Oleh karena itu, dalam konteks ini, ketentuan standar kebijakan privasi, yang memiliki banyak kekurangan, dapat dengan cepat diubah untuk mencegah pelanggaran hak-hak konsumen.

Pengaturan perlindungan hukum tersebut tertuang dalam “Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU Nomor 18 Tahun 2008 tentang ITE) dan Peraturan Pemerintah Nomor 28 Tahun 2012 tentang Penyelenggaraan Sistem dan Transaksi Elektronik.” Upaya

hukum yang diakses secara online dan dikelola mekanisme hukum internasional tersedia untuk melindungi dari pelanggaran hak perlindungan data oleh penyedia e-commerce atau penyedia sistem pasar online.

Indonesia memiliki dasar hukum untuk membuat undang-undang yang berlaku di tingkat nasional. Indonesia menandatangani pedoman "Organization for Economic Co-operation and Development (OECD) atau Organization for Economic Co-operation and Development (Organization for Economic Co-operation and Development)" pada tahun 2004 untuk mempelajari lebih lanjut tentang bagaimana Indonesia mengatur privasi dan perlindungan data pribadi. Pedoman ini. Bagian ini menjelaskan "undang-undang perbankan, undang-undang telekomunikasi, undang-undang perlindungan konsumen, undang-undang kependudukan, undang-undang hak asasi manusia, undang-undang manajemen kependudukan, undang-undang informasi transaksi elektronik (ITE), pengungkapan publik, undang-undang kesehatan masyarakat, dan undang-undang dan peraturan lainnya."

"Berikut peraturan di Indonesia terkait privasi dan perlindungan data pribadi :

1. Undang - Undang Nomor 10 Tahun 1998 Tentang Perbankan (UU Perbankan)
2. Undang – Undang Nomor 36 Tahun 1999 Tentang Telekomunikasi
3. Undang – Undang Republik Indonesia Nomor 8 Tahun 1999 Tentang Perlindungan Konsumen (Undang-Undang Perlindungan Konsumen)
4. Undang-Undang nomor 39 Tahun 1999 Tentang Hak Asasi Manusia (Undang-Undang HAM 1999)
5. Peraturan Bank Indonesia Nomor 7/6/PBI/2009 Tentang Transparansi Produk Bank dan Penggunaan Data Pribadi Nasabah (PBI NO. 7/6/PBI/2005)
6. Undang-Undang Nomor 23 Tahun 2006 Tentang Administrasi Kependudukan (Undang-Undang Administrasi Kependudukan 2006)
7. Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik (UU ITE 2008)

8. Undang-Undang Nomor 14 Tahun 2008 Tentang Keterbukaan Informasi Publik (Undang – Undang Keterbukaan Informasi Publik)

9. Undang –Undang Nomor 36 Tahun 2009 Tentang Kesehatan (Undang-Undang Kesehatan 2009)

10. Peraturan Presiden Republik Indonesia No 67 Tahun 2011 Tentang Penerapan Kartu Tanda Penduduk Berbasis Nomor Induk Kependudukan Secara Nasional (Perpres KTP 2011)

11. Peraturan Menteri Kominfo Nomor 20 Tahun 2016 Tentang Perlindungan Data Pribadi Dalam Sistem Elektronik

12. Peraturan Pemerintah Nomor 71 Tahun 2019 Tentang Penyelenggaraan Sistem dan Transaksi Elektronik."

2. Tantangan atau Kekhawatiran Data Privasi dalam Perdagangan Elektronik

Kekhawatiran tentang privasi meningkat dalam konteks internet karena fakta bahwa aktivitas online pengguna internet - misalnya, mengirim email, mencari situs web, membeli atau menjual barang atau jasa - dapat dengan mudah dilacak dan banyak informasi pribadi informasi dapat dikumpulkan tanpa persetujuan atau sepengetahuan pengguna. Sebagian besar informasi pribadi dalam jumlah besar yang dikumpulkan adalah jaringan, sehingga memungkinkan untuk dibagikan di antara organisasi dan lintas batas negara dan digunakan untuk berbagai tujuan, termasuk penambangan data, pencocokan data, dan pemasaran langsung.

Ketika serangan kebocoran privasi terjadi, ancaman dari penjahat dunia maya semakin beragam dan dapat menyerang siapa saja. Menurut survei, 137,7 juta jenis malware ditemukan pada tahun 2020. Sementara itu, pada tahun 2021, 92,45 juta sampel malware ditemukan pada pertengahan Juni saja. Singkatnya, pertumbuhan serangan cyber semakin meluas dan dapat merugikan siapa saja. Jenis-jenis Cyber Crime atau Kejahatan Siber, berikut di antaranya:

1. Phishing

Phishing adalah contoh kejahatan dunia maya yang bertujuan mencuri informasi atau data pribadi dari email, panggilan telepon, pesan teks, atau tautan palsu yang menyamar sebagai agen atau pihak tertentu. Mekanisme phishing adalah mengelabui target dengan trik yang terlihat biasa saja, padahal mereka tidak menyadari bahwa informasi pribadi mereka telah dicuri. Penyerang phishing menargetkan data korban yang sensitif seperti kata sandi, informasi kartu kredit, alamat email, dan kata sandi satu kali (OTP). Data yang dicuri digunakan untuk kejahatan seperti pencurian, penyalahgunaan identitas pribadi, dan pemerasan.

3. Cracking

Cracking adalah upaya untuk meretas perangkat lunak atau sistem keamanan komputer untuk tujuan ilegal dan memaksanya masuk ke sistem komputer untuk menyebabkan kejahatan. Peretas mencuri, melihat, dan memanipulasi data untuk memperkenalkan malware. Ada banyak jenis crack yang umum: password crack, software crack, network crack, dll. Misalnya, Anda dapat membuat kombinasi kata sandi yang unik, menggunakan VPN, mengunjungi situs web yang sudah menggunakan HTTPS, atau menghindari mengklik tautan atau iklan di Internet. Anda dapat menghindari berbagai jenis serangan jailbreak. Jika Anda memiliki situs web perusahaan, terutama yang menyimpan data pelanggan, kami menyarankan Anda untuk melakukan uji penetrasi untuk memeriksa keamanan Anda terhadap peretasan.

4. Serangan Ransomware

Ransomware adalah jenis malware yang menargetkan perangkat keras untuk mengekstrak informasi berharga dari target dan mengenkripsi dan mengunci file. Saat membuka atau mengakses kembali data , penjahat menuntut korban tebusan. Jika korban tidak menanggapi permintaan tersebut, pelaku tidak segan-segan mengancam akan memblokir data tersebut. Jenis kejahatan dunia maya ini sering menargetkan teknisi rumahan dengan sedikit pengetahuan teknis. Tujuan akhir dari serangan ransomware adalah memaksa korban untuk membayar sejumlah tertentu untuk mengakses file terenkripsi.

5. Serangan DDoS

Distributed Denial of Service (DDoS) adalah contoh kejahatan dunia maya di mana lalu lintas server sangat padat sehingga tidak dapat menerima koneksi atau kelebihan beban oleh pengguna lain. Serangan normal dari peretas ini dilakukan dengan terus mengirimkan permintaan ke server menggunakan sejumlah besar transaksi data. Teknik serangan DDoS biasanya dilakukan dengan berbagai cara. Kumpulan bot yang disematkan pada virus dan malware yang disebut botnet.

6. Injeksi SQL

Injeksi SQL adalah teknik serangan yang menyuntikkan kode yang mengeksploitasi kerentanan di lapisan basis data aplikasi. Contoh penjahat dunia maya adalah ancaman terbesar bagi keamanan aplikasi web. Ini biasanya berarti bahwa pengembang aplikasi tidak menerapkan filter ke beberapa karakter wildcard yang digunakan dalam sintaks SQL, dan penyerang dapat menyuntikkan wildcard ini ke dalam instruksi aplikasi untuk mengakses database.

Terjadi karena. Serangan SQL juga dapat terjadi jika back-end melanggar Web Application Firewall (WAF) atau jika sistem pencegahan intrusi ini terintegrasi dengan baik ke dalam arsitektur jaringan untuk menemukan kerentanan, memiliki akses langsung ke database.

7. Carding

Carding adalah kejahatan yang mencuri informasi kartu kredit orang lain. Data ini digunakan oleh penjahat untuk melakukan transaksi dan menghapus pembatasan kartu dari akun mereka.

Ada dua kategori dari kartu. Salah satunya adalah keberadaan peta. Artinya proses pencurian data akan dilakukan pada POS/Merchant menggunakan skimmer kartu EDC. Yang kedua tidak memiliki kartu. Ini adalah pencurian data melalui akses internet, biasanya menggunakan email phishing atau peretasan untuk mengambil informasi pemilik kartu kredit.

8. Peretasan Situs dan Email

Seperti namanya, kejahatan dunia maya yang paling umum ini melibatkan peretasan ke situs web atau alamat email korban dan memodifikasi

penampilan mereka. Tanda yang Anda lihat ketika sebuah website diretas adalah perubahan tampilan yang tiba-tiba. Misalnya, halaman web yang tidak pantas dapat ditampilkan, iklan samar mungkin ditampilkan, atau bahkan data situs mungkin tidak diketahui dan dicuri.

Ada beberapa cara untuk mencegah website Anda diretas: hal ini bisa dilakukan, seperti dengan melakukan backup secara rutin, menggunakan SSL, dan memilih layanan cloud hosting yang handal seperti Dewaweb ISO 270001 bersertifikat untuk keamanan internasional.

9. Penipuan OTP

OTP atau One-Time Password adalah kode sementara seperti One-Time Password untuk melakukan proses otentikasi pada aplikasi smartphone. Seiring meningkatnya popularitas, begitu pula ancaman penjahat dunia maya yang ingin mencuri OTP. Penipuan OTP digunakan untuk berbagai kejahatan, termasuk pembobolan akun dan penipuan dalam pelaksanaan transaksi keuangan. Untuk menghindari penipuan kode OTP, jangan pernah memberikan kode OTP kepada orang yang dikenal atau tidak dikenal. Aktifkan juga autentikasi dua faktor dan selalu waspada terhadap tautan yang meragukan.

10. Data Forgery atau Pemalsuan Data

Data tampering adalah perusakan data dokumen penting yang disimpan sebagai dokumen tidak tertulis di Internet. Catatan-catatan ini biasanya milik suatu organisasi atau instansi yang memiliki database website.

Data korupsi sering e-commerce dengan memperlakukannya sebagai "salah ketik" yang pada akhirnya menguntungkan pelaku sebagai korban memasukkan informasi pribadi atau nomor kartu kredit yang dapat disalahgunakan.

11. Cyber Espionage

Cyber spionage adalah penjahat dunia maya yang menggunakan internet dengan membobol jaringan komputer dan memata-matai target tertentu. Penjahat ini sering menargetkan pesaing, lawan politik atau pejabat pemerintah yang dokumen dan data penting disimpan di sistem komputer. Cyber spionase sering dilakukan dengan menggunakan spyware, perangkat lunak yang diam-

diam diinstal oleh peretas untuk melacak perilaku online korban. Dengan cara ini, semua aktivitas dan data penting dapat dilihat tanpa diketahui.

12. Spoofing

Spoofing adalah contoh kejahatan dunia maya yang harus diwaspadai. Penjahat secara ilegal menggunakan ID palsu untuk melayani tujuan kriminal mereka.

13. Cyber Terrorism

Cyberterrorism adalah jenis kejahatan dunia maya yang merugikan negara dan mengancam keselamatan warga negara dan pemangku kepentingan yang mengarahkan kegiatan pemerintah. Cyberterrorism adalah serangan terhadap komputer, jaringan, dan sistem informasi yang dirancang untuk mengancam, menekan, atau memberikan kepentingan politik tertentu.

Penambangan data dan teknologi pencocokan data memungkinkan sejumlah besar informasi pribadi diatur dan dianalisis, menghasilkan profil yang mengumpulkan banyak informasi tentang individu dan aktivitasnya, biasanya tanpa persetujuan atau sepengetahuan individu tersebut. Masalahnya dijelaskan oleh ALRC dalam Laporan mereka, “For your information : Australian Privacy Law and Practice (2006):” *“Saat ini, sejumlah besar data dikumpulkan tentang pengguna internet, seringkali tanpa sepengetahuan atau persetujuan mereka. Misalnya, data sering dikumpulkan tentang istilah pencarian yang dimasukkan pengguna internet ke mesin pencari online; situs web yang dikunjungi pengguna internet; dan barang atau jasa yang telah dibeli atau ditanyakan oleh pengguna internet secara online. Data juga dikumpulkan tentang pengguna internet yang menggunakan alat yang disediakan oleh mesin pencari online, seperti email gratis dan layanan peta. Data ini berpotensi mengungkapkan sejumlah besar informasi tentang pengguna internet, termasuk "informasi tentang kesehatan, pendidikan, riwayat kredit, dan orientasi seksual atau politik".*

Informasi yang dikumpulkan tentang pengguna internet biasanya tidak terhubung langsung ke individu, melainkan ke komputer tertentu. Ini karena setiap komputer yang terhubung ke internet dialokasikan alamat Internet Protocol (IP) yang unik selama durasi setiap sesi internet . Beberapa informasi

yang dikumpulkan tentang pengguna internet mungkin tunduk pada model Prinsip Privasi Terpadu atau Unified Privacy Principles (UPPs).
Informasi yang dikumpulkan tentang pengguna internet dapat digunakan untuk berbagai tujuan, seperti membuat profil individu untuk tujuan pemasaran. “

Kekhawatiran tentang dampak perkembangan teknologi telah dipertimbangkan di beberapa tinjauan yang dilakukan oleh Komite Parlemen, Komisaris Privasi federal dan Negara Bagian dan Komisi Reformasi Hukum. Ini termasuk:

1. Komite Pemilihan Senat untuk Teknologi Informasi: Privasi di Masyarakat Informasi (2000);
2. Kantor Komisaris Privasi federal. Masuk dalam Undang-Undang - Tinjauan Ketentuan Sektor Swasta dari Undang-Undang Privasi 1988 (2005):
3. Komisi Reformasi Hukum Victoria: Privasi Tempat Kerja: Laporan Akhir (2005);
4. Komite Referensi Hukum dan Konstitusi Dewan: The Real Big Brother: Penyelidikan Undang-Undang Privasi 1988 (2005);
5. Komisi Reformasi Hukum New South Wales: Invasi Privasi (2009), Privasi Prinsip (2009) dan Akses ke Informasi Pribadi (2010);
6. Komisi Reformasi Hukum Australia: Untuk Informasi Anda: Hukum Privasi Australia dan Praktek (2008); dan
7. Komite Dewan Tetap untuk Lingkungan dan Komunikasi: Kecukupan Perlindungan untuk Privasi Warga Australia Online (2011)

a) Privacy Act 1998 (Undang-Undang Privasi 1988)

Pemberlakuan Undang-Undang Privasi 1988 adalah hasil dari upaya Pemerintah Buruh Hawke pada tahun 1986 untuk memperkenalkan skema identifikasi nasional, yang intinya adalah Kartu Australia. Dua RUU diperkenalkan ke Parlemen pada tahun 1986 - RUU Privasi dan RUU Kartu Australia. Namun, kedua RUU tersebut berakhir ketika Parlemen dibubarkan pada tahun 1987 dan, dalam menghadapi ketidaksetujuan publik yang luar biasa terhadap Kartu Australia, pemerintah membatalkan kartu dan nomor identitas nasional yang diusulkan. Namun demikian, penerapan nomor arsip pajak

ditingkatkan untuk memungkinkan pendapatan dari sumber yang berbeda dicocokkan dan Undang-Undang Privasi 1988 diperkenalkan untuk memberikan beberapa perlindungan.

Dalam bentuk aslinya, Privacy Act 1988 menciptakan seperangkat 11 IPP, berdasarkan Pedoman Organisasi untuk Kerjasama Ekonomi dan Pembangunan (OECD) tentang Perlindungan Privasi dan Arus Lintas Batas Data Pribadi (1980), yang mengatur penanganan data pribadi oleh departemen dan lembaga Pemerintah Persemakmuran. Ini juga memberikan pedoman untuk pengumpulan, penanganan dan penggunaan informasi nomor arsip pajak oleh organisasi sektor publik dan swasta. Undang-undang tersebut diubah pada tahun 1990 menyusul protes publik tentang niat industri kredit untuk memperkenalkan sistem pelaporan kredit positif untuk melindungi individu dalam kaitannya dengan pelaporan kredit konsumen. Bagian IIIA Undang-undang mengatur penanganan laporan kredit dan informasi kelayakan kredit lainnya oleh lembaga pelaporan kredit dan penyedia kredit.

Terlepas dari meningkatnya dukungan komunitas selama tahun 1990-an untuk perluasan peraturan privasi ke sektor swasta, pada tahun 1997 Perdana Menteri (saat itu) John Howard mengumumkan bahwa Pemerintah Federal, bertentangan dengan niat yang dinyatakan sebelumnya, tidak akan menerapkan undang-undang privasi untuk swasta. sektor. Mengingat penentangan Pemerintah Federal terhadap pengenalan undang-undang privasi yang berlaku untuk sektor swasta, pada tahun 1997 dan 1998, Komisaris Privasi Australia saat itu, Moira Scollay, mengembangkan Prinsip Nasional untuk Penanganan Informasi Pribadi yang Adil. Sepuluh prinsip yang dikeluarkan oleh Komisaris Privasi pada bulan Februari 1998 didasarkan pada Pedoman OECD dan dimaksudkan untuk digunakan dalam konteks sektor swasta sebagai pengganti peraturan mandiri untuk undang-undang.

Di sebuah pembalikan kebijakan yang signifikan, pada bulan Desember 1998 Pemerintah Federal mengumumkan bahwa mereka akan memperluas perlindungan privasi ke sektor swasta dengan memberlakukan undang-undang berdasarkan Prinsip Nasional Komisaris Privasi. Amandemen Privasi (Sektor Swasta) Act 2000, yang disahkan pada April 2001 dan mulai berlaku pada 21 Desember 2001, memperkenalkan standar nasional untuk penanganan informasi pribadi oleh sektor swasta. Dalam memberlakukan Undang-Undang

Amandemen Privasi (Sektor Swasta) 2000, Pemerintah Federal menggambarkan undang-undang tersebut sebagai "rejim legislatif sentuhan ringan" yang menetapkan perlindungan privasi minimum. Pemerintah Australia berharap, antara lain, amandemen sektor swasta akan memfasilitasi perdagangan dengan Uni Eropa dengan memperkenalkan standar perlindungan data untuk melindungi privasi orang Eropa ketika informasi pribadi mereka ditransfer. Namun, Uni Eropa saat ini tidak menganggap standar perlindungan data dalam Privacy Act 1988 sebagai standar yang memadai untuk tujuan Petunjuk Perlindungan Data Uni Eropa

3. Kasus Kebocoran Data Privasi Pada Perdagangan Elektronik di Indonesia

Konsep perlindungan data berarti bahwa seorang individu memiliki hak untuk memutuskan apakah akan berbagi atau bertukar data pribadi. Selain itu, orang tersebut berhak untuk menentukan kondisi di mana transfer data pribadi akan dilakukan. Selain itu, proteksi data

Juga dikaitkan dengan konsep proteksi data. Data pribadi telah berkembang untuk digunakan untuk mengembangkan hak untuk melindungi data pribadi. Privasi adalah elemen penting dari kebebasan dan martabat individu, dan privasi adalah pendorong kuat kebebasan politik, spiritual, agama, dan bahkan seksual. Hak atas penentuan nasib sendiri individu, kebebasan berekspresi, dan privasi adalah hak esensial yang menjadikan kita manusia. Potensi pelanggaran privasi terkait data pribadi tidak hanya terjadi secara online tetapi juga offline. Pelanggaran data pribadi secara online dapat terjadi, misalnya pengumpulan data pribadi secara masif (komputasi digital), pemasaran langsung (direct sales), media sosial, pengembangan penerapan program e-KTP, pelaksanaan program kesehatan elektronik dan kegiatan komputasi awan.

Banyaknya kasus pelanggaran privasi terkait data pribadi di Indonesia secara khusus menunjukkan bahwa perlu dilakukan tindakan pencegahan khusus untuk melindungi data pribadi. Menurut data Yayasan Lembaga Konsumen Indonesia (YKLI) tahun 2019, seiring dengan bertambahnya jumlah

masyarakat Indonesia yang terkoneksi ke Internet, maka semua aktivitas di Internet akan meningkat secara signifikan, terutama dalam kasus pembobolan data di bank, kredit online, asuransi, dll. Telekomunikasi, e-niaga.

Kementerian Komunikasi dan Informatika Johnny G. Plate mengungkapkan 29 instansi dan perusahaan mengalami pembobolan data dalam tiga tahun terakhir (2019-2021). Peningkatan terbesar terjadi pada tahun 2020. Berikut adalah beberapa contoh penutupan dan urgensi privasi di Indonesia:

1. Bukalapak

Pada tahun 2019, peretas Pakistan mengklaim telah menggunakan nama samaran "Gnostic Player" untuk meretas basis data yang berisi catatan dari 13 juta pengguna Bukalapak dan menjualnya di web gelap. Data tersebut mencakup informasi seperti alamat email pengguna, nomor telepon, dan tanggal lahir. Setelah pelanggaran data, Bukalapak menyelidiki pelanggaran dan mengkonfirmasi pelanggaran tersebut. Namun, Bukalapak menyatakan bahwa pelanggaran data tidak memengaruhi informasi sensitif seperti nama pengguna, alamat, dan informasi keuangan.

2. Tokopedia

Pada awal Mei 2020, “Tokopedia mengalami peretasan yang berdampak pada data 44,491 juta pengguna Tokopedia. Laporan peretasan dan pelanggaran data pertama kali ditemukan oleh perusahaan keamanan siber Israel Under the Breach. Temuan itu berdasarkan unggahan peretas yang membagikan database 15 juta pengguna Tokopedia di Internet Raid Forum. Segera setelah insiden itu diumumkan, Tokopedia melakukan penyelidikan dan memberi tahu semua pengguna, memastikan bahwa akun dan informasi keuangan mereka tidak terpengaruh oleh peretasan ini. Pelanggaran data segera diselidiki oleh Kementerian Informasi dan Komunikasi. Setelah melalui proses yang panjang, Tokopedia akhirnya mendapat persetujuan tertulis dari Kementerian Komunikasi dan Informatika.”

3. Bhinneka.com

Tak lama setelah kasus kebocoran Tokopedia terungkap, pada Mei 2020, sebanyak 1,2 juta data pribadi konsumen Bhinneka.com dijual bersamaan

dengan data pengguna 9 perusahaan lain di RaidForums seharga US$ 1.200 atau setara Rp18 juta oleh peretas bernama ShinyHunters. Menanggapi kabar itu, Bhinneka.com tidak membenarkan secara tegas adanya kebocoran data di server mereka. Mereka hanya mengatakan password pengguna aman karena dilindungi enkripsi. Sedangkan untuk informasi keuangan pengguna, mereka tidak menyimpannya sama sekali. Setelah kasus kebocoran data ini terungkap, Bhinneka.com langsung melakukan investigasi internal dan melakukan koordinasi dengan Badan Siber dan Sandi Negara (BSSN). Hingga saat ini, hasil penyelidikan dari kasus kebocoran data ini masih belum diungkap secara jelas.

4. Data Pemilih KPU

Pada akhir Mei 2020, konsultan keamanan siber asal Israel, Under the Breach, mengungkapkan bocornya data dari 2,3 juta penduduk indonesia milik KPU bocor dan ditawarkan di salah satu forum peretasan. Dalam file PDF yang diunggah, data ini berisi informasi seperti, nama, alamat, Nomor Induk Kependudukan (NIK),Nomor Kartu Kartu Keluarga, dan lainnya. Setelah ditelusuri, data tersebut merupakan data pemilih pada 2013. KPU RI membenarkan jika data yang bocor tersebut adalah Daftar Pemilih Tetap (DPT) pada tahun 2013. KPU menegaskan, data DPT tersebut telah sesuai dengan regulasi yang ada saat itu, dimana data pemilih bersifat terbuka. Namun hingga kini kasus kebocoran data ini masih belum jelas penyelesaiannya.

5. Data Covid-19

Pada Juni 2020, "pengguna Raid Forums Database Shopping mengklaim dan menjual basis data yang berisi data 230 ribu warga Indonesia terkait dengan Covid-19. Pelaku mengatakan data tersebut berhasil dibobol pada 20 Mei 2020. Namun, tidak disebutkan dari mana asalnya dan mulai ditawarkan pada 18 Juni 2020."

Berdasarkan penulusuran Cyberthreat.id, contoh data yang ditawarkan berisi tanggal laporan, nama, kewarganegaraan, kelamin, umur, telepon, alamat tinggal, jenis kontak, hubungan kasus, tanggal awal risiko, tanggal akhir risiko, tanggal mulai sakit, tanggal rawat jalan, faskes rawat jalan, tanggal rawat inap, keluhan sakit, tanggal ambil sampel, jenis periksa, tanggal kirim sampel, tanggal ambil hasil, status akhir, tanggal rapid test, hasil rapid test, tanggal PCR

test, dan hasil PCR test. Tak hanya itu, ada juga sejumlah nama yang telah menjalani pemeriksaan. Sebagian besar yang dimunculkan di sampel adalah data dari Bali, yang beberapa di antaranya adalah warga negara asing.

6. Kreditplus

Pada awal Juli 2020, perusahaan keamanan siber yang berbasis di Atlanta, Cyble Inc. menemukan 896.170 data pelanggan CreditPlus untuk dijual di Forum Internet. Vendor data dengan akun Megadimarus (memiliki reputasi terpercaya dalam status GOD) memiliki database yang berisi nama, alamat email, kata sandi, alamat, nomor telepon, informasi pekerjaan, informasi perusahaan, dan informasi keluarga. Data nasabah Kreditplus ini telah diberikan melalui Raid Forum sejak 27 Juni 2020. Kemudian, pada 16 Juli, data tersebut kembali disediakan oleh akun ShinyHunters. Sayangnya, sejauh ini tidak ada informasi dari Kredit Plus, dan pelanggaran data ini hilang begitu saja.

7. Basis Data Polri

Pada Juni 2020, Teguh Aprianto, pendiri komunitas peretas etis Indonesia, mengungkap dugaan pelanggaran data oleh anggota Polri di forum internet melalui Twitter-nya. “Dia mengunggah tangkapan layar yang berisi informasi pribadi tentang petugas polisi, mulai dari foto hingga karier, pangkat, dan lainnya. Akun Hojatking mengklaim berhasil membobol database Polri pada 31 Mei 2020. Hojatking menjual akses penuh ke database seharga US $ 1.200 (setara dengan Rs 17 juta). Sementara itu, dijual seharga $ 2.000 (Rs 28,5 juta) untuk informasi tentang bug aplikasi (kerentanan keamanan). Meski dikenal sebagai hoax, pembobolan data ini diperparah dengan video yang diunggah oleh pelaku pembobolan database Polri dan memperlihatkan cara mengakses dan mengakses database SDM Polri layaknya seorang administrator. Basis data tersebut berisi 14.785 pegawai aktif, 909 pegawai di luar Satker, 31 pegawai sedang mengikuti pelatihan, 1.594 pegawai pensiun, 515 pegawai meninggal dunia, dan 9.081. Berisi data jabatan aktif dan beberapa data lainnya.”

8. BPJS Kesehatan

Pada Mei 2021, seorang pengguna Forum Raid bernama Kotz menjual database informasi pribadi tentang penduduk Indonesia. Data yang dijual antara lain NIK KTP, gaji, nomor handphone, alamat, dan email. Kotz mengaku mendapatkan data dari website bpjs-kesehatan.go.id dan menjual database tersebut seharga 0,15 BTC (setara dengan Rp 84,3 juta atau sekitar US$ 6.000). Basis data terdiri dari 279 juta, di mana 20 juta di antaranya memiliki foto pribadi. Kots mengklaim bahwa data tersebut juga mencakup daftar orang yang meninggal. Kasus pembobolan informasi ini awalnya ditangani oleh Kementerian Komunikasi dan Informatika dan BSSN, namun akhirnya dirujuk ke polisi dan tidak ada informasi terkini terkait kasus tersebut.

9. BRILife Syariah

Pada Juli 2021, seorang pengguna bernama "Reckt" memberikan data di Forum Hacker yang diduga milik 2 juta nasabah asuransi jiwa BRI. Namun segera thread yang menyediakan data pelanggan menghilang. Sebelumnya, perusahaan cybersecurity Israel Hudson Rock menemukan peretasan pada beberapa komputer milik karyawan BRI Life dan Bankrayat Indonesia (BRI).

Diyakini bahwa peretasan ini memberi peretas akses awal ke perusahaan. Data nasabah BRI Life saat ini dijual di forum hacking seharga US$ 7.000 atau Rp 100 juta. Vendor data juga melampirkan beberapa sampel data yang direkam dalam format video 250GB selama 30 menit. Basis data tidak hanya berisi data pribadi 2 juta pelanggan. Namun, itu juga berisi 463.000 dokumen, termasuk rincian bank, salinan KTP, hasil tes, dan data wajib pajak.

10. eHAC

Pada Agustus 2021, tim peneliti vpnMentor menemukan sekitar 1,3 juta data pengguna aplikasi Indonesian Electronic Health Alert Card (eHAC) yang dikembangkan oleh Kementerian Kesehatan RI yang dipublikasikan di Internet. Hasil dilaporkan dua kali ke Kementerian Kesehatan pada Juli 2021 dan ke BSSN pada Agustus 2021, tetapi tidak ada tanggapan. Database dapat diakses melalui web dan berisi data tes kesehatan Covid-19, termasuk identitas dan jenis penumpang, identitas rumah sakit, alamat dan waktu kunjungan rumah, jenis

tes, hasil tes, dll. Kasus ini diselidiki, tetapi akhirnya ditarik karena tidak ada pencurian data yang terdeteksi.

11. KPAI

Pada Oktober 2021, pengguna RaidForums "C77" memberikan data KPAI eksklusif. Ini memberikan sampel data untuk menarik pembeli. Setiap data bernilai 8 sks. KPAI juga mengaku mengalami pelanggaran data yang mengakibatkan terungkapnya data klaim online di website KPAI. Namun, mereka memastikan bahwa peretasan dan pencurian data tidak memengaruhi layanan di situs web KPAI.

Dari data sampel yang tersebar , database disusun dalam bentuk tabel dalam format file .csv, yang berisi id, nama, nomor KTP/KTP, kebangsaan, telepon, hp laptop, pendidikan agama, pekerjaan, pendidikan, alamat, email, tanggal. . kelahiran, jenis kelamin, provinsi, kota dan umur. Kepolisian Negara Republik Indonesia sedang menyelidiki pelanggaran data KPAI dan tidak ada perkembangan terbaru dalam penyelidikan.

4. Teknologi dan Praktik Yang Mempengaruhi Privasi Online.

Banyak teknologi internet standar dapat berdampak signifikan pada privasi orang yang terlibat dalam aktivitas online. Teknologi ini memungkinkan banyak informasi (benar atau salah) untuk dikumpulkan, dicocokkan dan diprofilkan, direplikasi, didistribusikan dan dijual. Jenis data yang dikumpulkan dapat mencakup lokasi geografis, nama, tanggal lahir, dan sebagainya. Potensi pelanggaran privasi terjadi melalui penggunaan teknologi ini meningkat karena mereka dapat diinstal dan dioperasikan tanpa sepengetahuan pengguna internet. Teknologi lain yang berpotensi berdampak buruk pada privasi termasuk manajemen hak digital atau Digital Rights Management (DRM), Cloud computing, dan teknologi geo-lokasi.

A. Cookies

Cookie adalah file teks kecil yang dihasilkan oleh server web, yang disimpan di hard drive komputer pengguna internet saat situs web diakses.

Cookie mengaktifkan web server dan server lain untuk mengakses dan memanggil kembali, di kemudian hari, informasi tentang komputer yang telah mengakses situs web. Mereka pertama kali diperkenalkan di browser Netscape pada tahun 1994 sehingga isi keranjang belanja web akan diingat. Jenis informasi yang dikumpulkan oleh cookie termasuk nama pengguna, kata sandi, ulang tahun, situs web yang dikunjungi, dan daftar barang yang dibeli secara online.

Informasi yang dikumpulkan biasanya tidak ditampilkan kepada pengguna dan banyak pengguna tidak menyadari bahwa cookie diinstal pada komputer mereka. Cookie dapat bertahan untuk waktu yang cukup lama - dalam beberapa kasus, selama beberapa tahun. Jika pengguna kembali ke situs web di kemudian hari, browser web pengguna akan mengirimkan informasi yang disimpan sebelumnya ke situs web. Lewat sini. cookie dapat menginformasikan situs web bahwa itu adalah komputer yang sama yang dikunjungi beberapa waktu lalu, sehingga melacak aktivitas pengguna komputer tertentu selama periode waktu tertentu. Informasi yang terkandung dalam cookie dapat diperbarui setiap kali komputer kembali ke situs web.

Karena cookie berisi kode atau data yang secara unik mengidentifikasi komputer pengguna web, sering kali diklaim bahwa cookie hanya menyampaikan informasi yang tidak mengidentifikasi pengguna web secara pribadi. Namun, meskipun cookie itu sendiri mungkin tidak berisi informasi pengenal pribadi, situs web juga dapat mengumpulkan informasi tentang identitas pengguna situs web. Contohnya adalah situs web yang mengumpulkan nama atau alamat email pengguna dari pertanyaan online, pendaftaran, atau transaksi e-niaga. Profil perilaku online pengguna web dapat dibangun dengan menerapkan pencocokan data dan teknologi penambangan data untuk mengumpulkan aliran klik dan bentuk data lain yang disimpan dalam basis data yang luas.

B. Web Bugs and Beacons

Web bugs - juga dikenal sebagai beacon dan pixels - kecil, grafik tak terlihat tertanam di halaman web dan pesan email, yang dapat digunakan untuk

melacak siapa yang mengunjungi situs web, berapa banyak orang yang mengunjungi situs web itu, dan berapa kali email telah diteruskan dan dibaca. Sebagai gambar yang jelas tanpa konten yang terlihat, gambar tersebut dapat disertakan dalam tag gambar dari kode HTML halaman web dan dalam pesan email yang mendukung HTML. Ketika halaman web yang berisi bug diakses, berbagai informasi dikirim ke server web, termasuk alamat IP komputer, URL halaman web, jenis browser yang digunakan untuk mengaksesnya, waktu dilihat dan nilai cookie yang ditetapkan sebelumnya.

Web bugs dapat digunakan untuk berbagai tujuan. Ketika dilampirkan ke email, mereka dapat mengirim informasi kembali ke pengirim pesan bahwa email telah dibuka dan waktu pembukaan. Web bugs yang disertakan pada halaman web dapat membantu mengumpulkan informasi tentang situs yang dikunjungi oleh pengguna web tertentu. Jaringan periklanan dapat menempatkan web bugs mereka di situs perusahaan lain untuk memungkinkan mereka merekam situs dan halaman mana yang dikunjungi pengguna dan kemudian menambahkan informasi ke profil pengguna. Beberapa atau semua informasi tersebut kemudian diteruskan, baik ke situs yang dilihat, atau ke perusahaan lain atau orang lain. Teknologi ini biasanya digunakan dalam iklan spanduk di mana web bugs dapat melacak pergerakan pengguna melalui situs web yang ditautkan. Segera setelah pengguna mengklik spanduk, jejak informasi dimulai. Informasi yang dikumpulkan diberikan ke situs web host dan pengiklan, sehingga pada saat orang yang sama masuk lagi, iklan dapat ditargetkan ke pengguna berdasarkan iklan yang sebelumnya telah mereka tarik.

Investigasi oleh Wall Street Journal pada pertengahan 2010 menemukan bahwa 50 situs web paling populer di Amerika Serikat (menyumbang 40% dari tampilan halaman di Amerika Serikat) diinstal hampir 3.200 file pelacakan di komputer uji. Sementara hanya satu situs, Wikipedia.org, yang tidak memasang file pelacakan sama sekali, 50 situs web teratas memasang rata-rata 64 buah teknologi pelacakan dan beberapa (termasuk Dictionary.com dan Microsoft's MSN.com) masing-masing memasang lebih dari 100. Jumlah alat pelacak terbanyak ditempatkan oleh perusahaan (seperti Google dan Microsoft) yang bergerak dalam bisnis mengikuti pengguna internet untuk membuat basis data profil pengguna yang dapat dijual. Alat pelacak yang lebih baru memindai secara real time apa yang dilakukan pengguna web, termasuk apa yang mereka

ketik dan ke mana mouse bergerak, dan dapat membuat penilaian cepat terhadap lokasi, pendapatan, dan minat belanja.

C. Hypertext Transfer Protocol (HTTP)

Hypertext Transfer Protocol (HTTP) dikembangkan untuk memungkinkan informasi diminta dan dikirim melalui internet. Selain mengirimkan informasi tentang URL halaman web yang ingin diakses oleh pengguna web, setiap kali halaman web diakses, perangkat lunak browser pengguna mengirimkan informasi ke situs server tanpa sepengetahuan pengguna. Informasi yang dapat dikirimkan antara lain:

1. Variabel alamat jarak jauh dan variabel host jarak jauh, yang dapat memberikan informasi tentang lokasi pengguna;
2. Variabel "HTTP From" dan "remote user", yang dapat meneruskan alamat email pengguna atau indikasi identitas lainnya; dan
3. “Perujuk HTTP", yang mengungkapkan halaman web yang dilihat pengguna sebelum mengakses halaman saat ini. Jika halaman sebelumnya adalah mesin pencari, seluruh kueri dalam pencarian (istilah pencarian) diteruskan. Jika URL diklik atau merupakan file pribadi di hard disk, maka nama file akan diteruskan ke situs. Jika file adalah pesan email yang dilihat dalam program email, informasi yang diteruskan mungkin sangat rinci untuk menyertakan nama pengguna, alamat email, program yang digunakan, dan bahkan direktori file dan ruang file.

Sementara bagian-bagian individual dari data yang dikumpulkan mungkin tampak tidak signifikan, ketika data tersebut dicocokkan dengan data lain dan diprofilkan, sejumlah besar informasi rinci dapat dikumpulkan.

D. Digital Rights Management (DRM)

Laporan ALRC, “for your information: Australian Privacy Law and Practice (2008), mengidentifikasi ancaman terhadap privasi yang disajikan oleh penggunaan teknologi manajemen hak digital (DRM) sebagai berikut:

“Teknologi DRM memungkinkan pemilik hak cipta untuk melindungi materi digital dengan mengontrol cara materi diakses, digunakan, disalin, dan didistribusikan. Telah dicatat bahwa hampir semua teknologi DRM memerlukan pengumpulan informasi pribadi tentang konsumen materi hak

cipta. Oleh karena itu, mereka membatasi kemampuan konsumen ini untuk mengakses materi secara anonim. Selanjutnya, teknologi DRM dapat digunakan untuk memantau aktivitas konsumen dengan mengumpulkan informasi tentang "konten yang digunakan, waktu penggunaan, frekuensi penggunaan, dan lokasi penggunaan.

E. Search Engines and Targeted Advertising

Mesin pencari internet seperti Google mengumpulkan sejumlah besar informasi tentang pengguna melalui penggunaan teknologi seperti cookie dan cache, dan layanan bernilai tambah seperti alat pencarian orang. Informasi (termasuk istilah pencarian yang digunakan dan alamat IP yang dikunjungi) dapat dikorelasikan untuk membuat profil individu dan preferensi mereka. Masalahnya telah dijelaskan secara ringkas Tene, yang menjelaskan: *"Google adalah penjaga gerbang informasi yang menyimpan kekayaan data pribadi yang tak terbayangkan sebelumnya. Miliaran kueri penelusuran mengalir di seluruh server Google setiap bulan, kumpulan pemikiran umat manusia, online. Google mengkompilasi log pencarian individu, yang berisi informasi tentang ketakutan dan harapan pengguna, minat dan gairah, dan lengkap dengan informasi yang bersifat keuangan, medis, seksual, politik, singkatnya - pribadi."*

Praktik privasi dari mesin pencari terkemuka telah dikritik. Misalnya, pada bulan Mei 2007, badan penasihat Uni Eropa yang terdiri dari perwakilan dari otoritas perlindungan privasi dari masing-masing negara anggota Uni Eropa, yang dikenal sebagai Article 29 Working Party (WP29), memberi tahu Google bahwa praktiknya tidak sesuai dengan data Uni Eropa standar perlindungan. Karena Google adalah penyedia mesin telusur yang dominan di hampir setiap negara bagian Uni Eropa, menguasai hingga 95% pasar di beberapa negara, WP29 menganggap bahwa kurangnya fokus Google pada privasi pengguna web menjadi alasan untuk dikhawatirkan. WP29 mengidentifikasi penggunaan cookie oleh Google, data yang dapat diidentifikasi secara pribadi (sebagai lawan dari data yang dianonimkan), periode penyimpanan untuk log server dan penyimpanan data pribadi untuk berbagai tujuan, termasuk keamanan, sebagai area di mana praktik yang ditingkatkan diperlukan. Pada tahun 2008, WP29 menerbitkan Opininya tentang

Masalah Perlindungan Data Terkait dengan Mesin Pencari, menekankan sensitivitas data pribadi yang terkait dengan permintaan pencarian yang "berisi jejak minat, hubungan, dan niat orang itu dan harus diperlakukan sebagai pribadi yang sangat rahasia. data". Opini WP29 membahas persyaratan perlindungan data Uni Eropa bahwa periode penyimpanan tidak boleh lebih lama dari yang diperlukan untuk tujuan pemrosesan tertentu, setelah itu data harus dihapus, dan pentingnya anonimisasi lengkap untuk mencegah identifikasi individu dengan menghubungkan kueri penelusuran yang disimpan.

WP29 telah bekerja dengan Google (serta Microsoft dan Yahoo!) untuk membuat mesin pencari mereka mematuhi prinsip-prinsip perlindungan data Uni Eropa, menghasilkan pengumuman oleh Google bahwa itu akan memperkenalkan langkah-langkah untuk mempersulit permintaan pencarian online untuk dikaitkan dengan orang yang membuatnya. Untuk mencegah identifikasi dari individu yang telah melakukan pencarian, setelah periode 9 bulan Google sekarang menganonimkan alamat IP dalam file log permintaan pencarian dengan menghapus delapan bit terakhir (oktet) dari alamat IP komputer tempat pencarian berasal. Sementara menyambut ini sebagai langkah ke arah yang benar, WP29 tidak menganggapnya sebagai langkah yang cukup jauh dan telah mendesak Google untuk lebih mengurangi periode retensi hingga maksimum enam bulan dan untuk mengadopsi proses anonimisasi yang lebih baik yang diverifikasi oleh pihak eksternal dan audit independen. WP29 tidak menganggap langkah-langkah ini cukup untuk membuat Google mematuhi arahan perlindungan data Uni Eropa karena penghapusan sebagian alamat IP tidak menjamin anonimisasi yang memadai atau mencegah identifikasi subjek data. Praktik Google dalam mempertahankan cookie selama 18 bulan berarti bahwa kueri penelusuran individual dapat dikorelasikan dan alamat IP dapat dengan mudah diambil setiap kali pengguna membuat kueri baru dalam periode 18 bulan tersebut.

Di Amerika Serikat, ada dukungan yang berkembang untuk pengenalan undang-undang yang mengharuskan mesin pencari untuk menyediakan mekanisme jangan-lacak yang akan memungkinkan pengguna internet untuk memilih keluar dari pemantauan aktivitas online mereka. Komisi Perdagangan Federal (FTC) mengeluarkan laporan pada bulan Desember 2010 yang mengusulkan bahwa pengaturan jangan-lacak harus dimasukkan dalam browser

web konsumen sehingga mereka memiliki pilihan apakah akan mengizinkan pengumpulan data tentang pencarian dan penjelajahan online mereka. kegiatan. Pada bulan Maret 2011, Gedung Putih mendesak Kongres untuk menyetujui Bill of Rights privasi konsumen yang akan mengatur pengumpulan dan penggunaan informasi pribadi di internet dan memberikan perlindungan privasi data konsumen dasar.

F. Social Networking Platforms

Fokus perhatian baru-baru ini adalah informasi yang diungkapkan oleh pengguna layanan jejaring sosial populer seperti Facebook, Twitter, dan MySpace. Situs-situs ini mendorong pengguna untuk mengembangkan lingkaran kontak melalui alat perpesanan dan halaman profil pribadi. Ini berarti bahwa pengguna layanan tersebut memposting banyak informasi tentang diri mereka sendiri dan orang lain secara online. Meskipun sebagian besar informasi ini tidak berbahaya dan bersifat sementara, seperti pesan tidak formal dan updates, informasi tentang acara sosial dan tautan ke teman dan kontak, sedikit informasi individual ini dapat dikumpulkan dan disusun kembali oleh komputer untuk membuat gambar individu dan identitas mereka yang semakin akurat. Teknik penambangan data yang kuat yang menggunakan korelasi statistik untuk membangun profil individu dapat "menghilangkan anonim" informasi tentang individu dan memprediksi karakteristik dan preferensi mereka.

Sebuah studi oleh Profesor Vitaly Shmatikov dari University of Texas, dan pascasarjana Universitas Stanford, Arvind Narayanan, menemukan bahwa dengan memeriksa korelasi antara akun online, mereka dapat mengidentifikasi lebih dari 30% pengguna Twitter dan Flickr meskipun mengidentifikasi informasi seperti akun nama dan alamat email telah dihapus. Pengguna jejaring sosial dapat memilih untuk menerapkan kontrol privasi yang ketat pada informasi pribadi mereka (misalnya, di bawah pengaturan privasi Facebook), tetapi teman dan kontak online mereka dapat mengungkapkan informasi tentang mereka dengan merujuk ke sekolah, jenis kelamin, majikan, lokasi, dan minat mereka. Dalam tinjauan undang-undang privasi 2006-08, ALRC menemukan bahwa perhatian utama tentang individu yang menangani informasi pribadi terkait dengan publikasi konten (foto, video, komentar) di jejaring sosial dan situs konten buatan pengguna (seperti Facebook dan YouTube) yang dapat

mengganggu privasi orang lain. Pada tahun 2007, lokakarya konsultasi yang diselenggarakan oleh ALRC dengan kaum muda berusia 12-25 tahun, mengangkat privasi di ruang jejaring sosial seperti YouTube dan MySpace sebagai isu yang sangat penting.

G. Cloud Computing and Application Service Providers

Penyedia layanan aplikasi memungkinkan pelanggan mereka mengakses aplikasi perangkat lunak melalui internet, tetapi sejumlah besar data pelanggan biasanya disimpan dari jarak jauh dan di luar kendali pelanggan. Meningkatnya penggunaan komputasi awan dengan jumlah data yang lebih besar yang dikumpulkan dan disimpan untuk jangka waktu yang lebih lama, menimbulkan masalah tentang privasi dan keamanan data yang disimpan dari jarak jauh. Dalam survei tahun 2009 yang dilakukan oleh Microsoft, 90% responden menyatakan keprihatinan tentang keamanan data di cloud. Dengan tidak adanya perlindungan legislatif yang efektif atas privasi dan penguatan kerja sama internasional untuk memastikan keamanan data yang melintasi batas negara, cloud cornputing tidak mungkin mencapai potensinya. Meskipun implikasi privasi komputasi awan tidak dipertimbangkan oleh ALRC dalam tinjauan privasi 2006-08, dalam draft “Australian Government Information Management Office (AGIMO)’s Cloud Computing Strategic Direction Paper (2011),” Pemerintah Federal mengidentifikasi panduan praktik yang baik tentang privasi sebagai komponen penting dari Cloud Framework.

H. Spyware

Spyware adalah segala jenis teknologi yang membantu mengumpulkan informasi tentang seseorang atau organisasi tanpa sepengetahuan atau persetujuan mereka. Ini biasanya disebut sebagai "snoopware" atau "trespassware" karena program mengintai atau masuk tanpa izin ke dalam kehidupan pribadi pengguna. Dalam laporannya, “Outcome of the Review of the Legislative Framework on Spyware (2005),” Commonwealth Department of Communications, Information Technology and the Arts (DCITA) mendefinisikan "spyware" sebagai:

“aplikasi perangkat lunak apa pun yang umumnya diinstal tanpa sepengetahuan atau persetujuan pengguna, untuk mendapatkan, menggunakan,

atau mengganggu informasi atau sumber daya pribadi, konten, atau pengaturan untuk tujuan jahat atau tidak diinginkan."

Definisi ini mencakup "grayware" - aplikasi yang dibuat oleh badan hukum untuk tujuan komersial - dan "malware" - aplikasi berbahaya yang dibuat dengan tujuan kriminal. Seorang pengguna internet dapat secara tidak sadar dan tidak sengaja memasang spyware dengan mengunduh lampiran email pembawa mata-mata atau perangkat lunak "gratis". Lebih sering, bagaimanapun, hanya dengan menggunakan internet dapat mengakibatkan spyware ditempatkan pada komputer pengguna karena spyware mengeksploitasi kerentanan dalam sistem operasi pengguna.

Beberapa contoh perangkat lunak bebas yang diketahui disertai dengan spyware antara lain bilah alat dan modifikasi browser, protokol transfer file, UnZip, PC clocks, personal organizer, dan Kazaa. Spyware dapat memfasilitasi pencurian informasi rahasia, seperti detail rekening bank dan kata sandi, yang dapat mengarah pada pencurian identitas dan bentuk kegiatan kriminal lainnya. Penggunaan spyware yang paling serius dan berbahaya akan dianggap sebagai pelanggaran komputer di bawah KUHP.

I. Location Data

Teknologi geo-identifikasi, yang memungkinkan lokasi perangkat - dan individu yang menggunakannya - untuk ditentukan secara real time dan untuk menghasilkan catatan pergerakan fisik individu, berpotensi berdampak signifikan pada privasi. Dengan teknologi pendeteksi lokasi seperti GPS (Global Positioning System) yang kini menjadi fitur standar di berbagai perangkat, lokasi spasial pengguna ponsel, laptop, konsol game, dan sebagainya dapat dengan mudah dipastikan. Identifikasi geografis tidak hanya dapat mengurangi tingkat anonimitas yang diberikan kepada pengguna internet, tetapi kombinasi lapisan informasi spasial dengan informasi lain dapat memungkinkan identitas individu untuk ditentukan. Dalam Laporan mereka, Untuk Informasi Anda: Undang-Undang Privasi Australia dan Praktek (2008), ALRC menunjukkan bahwa:

"Dengan menganalisis informasi tentang lokasi individu, pihak ketiga dapat memperoleh atau menyimpulkan informasi pribadi tentang individu, seperti informasi tentang preferensi konsumen individu atau aktivitas sosial."

Dalam audiensi di depan Kongres Amerika Serikat pada pertengahan tahun 2010, Apple Inc mengonfirmasi bahwa mereka mengumpulkan dan menyimpan kumpulan data lokasi "berkelompok" dari perangkat pengguna (seperti Apple iPhone dan komputer) setiap 12 jam sekali. Informasi yang dikumpulkan dan disimpan oleh Apple tidak secara langsung terkait dengan identitas atau perangkat tertentu dan pengguna dapat memilih keluar dari pengumpulan data. Untuk iPhone dengan chip GPS, posisi dihitung menggunakan sinyal satelit, sementara perangkat lain melakukan triangulasi posisinya menggunakan data tentang menara ponsel dan titik akses Wi-Fi. Aplikasi seperti Google Maps dapat mengakses dan menggunakan data lokasi yang dikumpulkan.

Arahan Uni Eropa tentang privasi dan komunikasi elektronik melarang pemrosesan "data lokasi" yang menunjukkan posisi geografis pengguna layanan komunikasi elektronik yang tersedia untuk umum tanpa persetujuan individu, kecuali data tersebut telah dianonimkan.

J. Privacy Enhancing Technologies and Practices

Pengguna internet dapat menggunakan berbagai teknologi yang tersedia yang disebut "Privacy-Enhanced Technologies" (PETS) - untuk meningkatkan privasi dan keamanan komunikasi online mereka. Contoh teknologi ini termasuk Platform for Privacy Preferences (P3P), standar teknologi yang dikembangkan oleh World Wide Web Consortium (W3C), yang memungkinkan pengguna Internet untuk menentukan informasi apa yang ingin mereka simpan secara online dan informasi yang mereka inginkan. dapat diakses. Teknologi lain, seperti Pretty Good Privacy (PGP) dan tanda tangan digital, yang mengenkripsi komunikasi online sehingga hanya orang dengan "kunci" yang dapat membacanya, juga dapat digunakan untuk melindungi informasi pribadi. Banyak contoh dan hyperlink ke program perangkat lunak yang dapat digunakan untuk mengamankan komunikasi online tercantum di situs web Federal Privacy Commissioner.

Pengguna web semakin memberi pengguna fitur yang dapat disesuaikan yang dapat digunakan untuk mengontrol dan melindungi informasi yang mengalir antara pengguna web dan pihak serta situs yang berinteraksi dengan

mereka secara online. Mengambil saran dari Komisi Perdagangan Federal Amerika Serikat pada bulan Desember 2010, pada awal 2011 Microsoft dan Mozilla telah mengumumkan bahwa versi berikutnya dari browser web mereka (Internet Explorer 9 dan Mozilla 4) akan menyertakan alat do-not-track, sehingga memungkinkan pengguna untuk memilih apakah mereka ingin dilacak secara online atau tidak. Dengan mengaktifkan fungsi jangan-lacak, pengguna dapat memilih keluar dari pelacakan perilaku dengan menghentikan file, seperti cookie dan bug web, agar tidak diunduh ke komputer mereka. Pengenalan kemampuan teknis untuk meningkatkan privasi online telah menanggapi permintaan pengguna, meskipun tampaknya ada peningkatan dukungan untuk pengenalan undang-undang untuk mendukung langkah-langkah tersebut.

Pengguna internet juga dapat mengadopsi praktik yang meningkatkan privasi online mereka. Seperti yang ditunjukkan Edwards, "pertimbangan keamanan pribadi dan ancaman privasi terhadap konsumen [tidak dapat] secara berguna dipisahkan dari praktik keamanan rumah dari individu yang sama". Dr Antony Bendall, Deputi Komisaris Privasi Victoria, juga menekankan peran internet individu pengguna dalam memahami dan mengelola risiko online:
"Di atas segalanya, memastikan bahwa individu sepenuhnya mendapat informasi dan mampu memahami kedua manfaatnya dan risiko yang melekat dalam interaksi dan keterlibatan online, sejauh ini, akan menjadi yang paling efektif dan metode yang efisien untuk melindungi privasi online, baik individu terlibat dalam sosial jaringan atau bertransaksi online."

Risiko terlibat dalam transaksi online dapat dikurangi dengan menggunakan situs web yang menampilkan segel persetujuan yang dikeluarkan oleh program akreditasi keamanan online, seperti TRUST, 64 yang mengeluarkan segel Privasi Web dan Privasi Email.

Meskipun segel privasi tidak memiliki efek hukum, mereka menunjukkan kepada pengguna internet bahwa operator situs web mengklaim sebagai entitas online yang dapat dipercaya karena mematuhi standar praktik terbaik yang ditetapkan oleh organisasi akreditasi.

Komisioner Privasi Federal merekomendasikan agar pengguna Internet mengambil langkah-langkah berikut untuk melindungi informasi pribadi mereka secara online: Hanya menjalankan bisnis, mengunjungi situs web, atau

berinteraksi dengan situs web dengan kebijakan privasi yang memadai yang mencakup, minimal:

1. Dengan siapa informasi Anda akan dibagikan, mengapa dikumpulkan, bagaimana akan digunakan, dan bagaimana Anda akan mengakses informasi yang dimiliki organisasi Anda tentang Anda?
2. Instal dan gunakan perangkat lunak peningkatan privasi, seperti firewall, pembersih cookie, pembersih kesalahan, penjelajahan web anonim, email terenkripsi, filter iklan, alat antispam, dan antispyware.
3. Saat mengisi formulir, mohon untuk tidak melakukan kontak lebih lanjut dengan organisasi tersebut kecuali Anda mengetahui bahwa Anda ingin melakukan kontak lebih lanjut dengan organisasi tersebut.
4. Berikan informasi pribadi sebanyak yang diperlukan.
5. Gunakan layanan email dan ID online gratis untuk mencegah spammer memberikan informasi.[3]

Carnivore adalah program perangkat lunak berpemilik yang sebelumnya digunakan oleh Biro Investigasi Federal AS (FBI) untuk secara diam-diam mencegat email dan lalu lintas Internet.Tujuannya dinyatakan secara publik adalah untuk mengumpulkan bukti memberatkan terhadap pornografi anak, tersangka teroris, penipuan online dan kejahatan lainnya.Pada tahun 2005, dilaporkan secara luas bahwa Carnivore digantikan oleh perangkat lunak yang tersedia secara komersial.Carnivore konon digunakan untuk memantau lalu lintas di beberapaserverPenyedia Layanan Internet(ISP) antara akhir 1990-an dan 2005. Meskipun pemerintah enggan membahas rincian Carnivore, beberapa fakta telah cukup mapan.

Perangkat lunak karnivora digunakan oleh FBI untuk mencegat email dan lalu lintas Internet. Karnivora adalah “pengendus paket” yang dirancang untuk membaca header pada paket informasi yang lewat.Header menyertakan informasi pengirim/penerima, di antara detail lainnya.Dengan memindai semua paket yang lewat di server ISP, Carnivore dapat menggunakan sistem penyaringan untuk secara otomatis menyalin dan mencatat paket apa pun yang cocok dengan kriteria tertentu.Kriteria, berdasarkan identifikasi, dapat

3 B Fitzgerald,A Fitzgerald, E Clark, G Middleton, Y F Lim, Internet and E-Commerce Law, 2011, Thomson Reuters

menargetkan beberapa atau semua komunikasi online subjek.Paket data yang tidak memicu filter hanya akan melewati yang belum diproses.

Berita Karnivora akhirnya bocor untuk memenuhi tanggapan publik yang negatif.Dalam pernyataan kepada pers, Donald Kerr, Asisten Direktur FBI, menekankan bahwa FBI mengikuti protokol yang terlebih dahulu memerlukan panggilan pengadilan atau surat perintah berdasarkan kecurigaan yang masuk akal, sebelum menjebak komunikasi online seseorang.Meski begitu, surat perintah mungkin terbatas pada email tertentu atau situs web tertentu.Namun, jaminan tidak banyak meredakan kekhawatiran publik, terutama para pendukung privasi.

Kritikus Carnivore berpendapat bahwa implementasinya dalam memantau semua paket lalu lintas di server atau jaringan dapat dengan mudah disalahgunakan atau disalahgunakan untuk melanggar hak privasi warga negara yang taat hukum.Ditambah dengan kurangnya pengawasan terhadap program Carnivora, karena sifat dasar FBI menghalangi pengawasan independen.Kekhawatiran ini tetap ada hari ini.

Karnivora adalah program generasi ketiga, dengan inkarnasi sebelumnya (1997-1999) yang disebutOmnivora.Setelah Carnivore menerima pers negatif seperti itu, FBI mengubah nama program penyadapan kawat elektronik sekali lagi menjadiDSC-1000 yangtidak terlalu mengancam.Akronim tersebut dilaporkan merupakan singkatan dari “Digital Collection System.

DSC-1000 sebenarnya adalah rangkaian dari tiga program, di mana Carnivore adalah salah satunya.Dua program lainnya adalahPacketeerdanCoolMiner.Meskipun tidak pernah ada kata resmi tentang fungsi Packeteer atau CoolMiner, secara umum diyakini bahwa Carnivore menjebak paket data, Packateer memasangnya kembali, dan CoolMiner menjalankan analisis pada informasi yang dihasilkan.Suite ini secara kolektif dikenal sebagaiDragonWare Suite.

Jika beberapa pembuat undang-undang memiliki keinginan mereka, packet sniffer mungkin akan segera menjadi tidak diperlukan untuk penegakan

hukum.Pemerintah AS bergerak ke arah yang secara hukum mewajibkan ISP untuk menyimpansemua datapadasemuaindividu hingga dua tahun.Proposal ini, yang secara resmi dikenal sebagai "retensi data", juga sering disebut sebagaipengintaian ISP.Jikapengintaian ISPmenjadi hukum, aktivitas online setiap pengguna, termasuk email, situs web yang dikunjungi, program yang diunduh, dan komunikasi lainnya, akan menjadi bagian tak terpisahkan dari basis data besar untuk penggunaan penegakan hukum.

Sementara para pendukung privasi menentang penyimpanan data dengan berbagai alasan, Uni Eropa mengesahkan undang-undang serupa pada bulan Desember 2005, yang diharapkan mulai berlaku pada tahun 2008. Dengan prospek memiliki basis data yang begitu besar dengan informasi terperinci tentang setiap dan setiap sejarah online warga negara, potensi untuk pelanggaran keamanan dan pelanggaran yang mengejutkan.Beberapa bahkan berpendapat bahwa jika ada sesuatu yang positif untuk dikatakan tentang penyimpanan data, itu mungkin hanya membuat Karnivora terlihat jinak

5. Pengaruh Instrumen Internasional dan Regional terhadap Perlindungan Data Privasi

"Beberapa instrumen yang mempengaruhi perlindungan data privasi dalam lingkup internasional dan regional yakni :

1. Deklarasi Universal tentang Hak Asasi Manusia 1948 (UDHR)
2. Kovenan Internasional tentang Hak-Hak Sipil dan Politik (ICCPR) 1996
3. Konvensi Eropa tentang Hak Asasi (ECHR) 1950
4. Konvensi Amerika tentang Hak Asasi Manusia 1969
5. Deklarasi Kairo tentang Hak Asasi Manusia Islam 1990
6. Perlindungan Data Privasi di Uni Eropa
7. Peran Lembaga Pengawas (Data Protection Authority)

8. Resolusi Madrid dalam *International Conference of Data Protection and Privacy Commissioners*[4]"

Pada intinya, privasi adalah kualitas dasar hak asasi manusia. Privasi diabadikan dalam semua instrumen hak asasi manusia utama, baik internasional maupun regional, termasuk:

1. Deklarasi Universal Hak Asasi Manusia Perserikatan Bangsa-Bangsa (UDHR) 1948, Pasal 12 "Jangan sewenang-wenang mengganggu urusan pribadinya, keluarga, rumah, komunikasi, atau merusak kehormatan atau reputasinya. Setiap orang. Anda berhak atas perlindungan hukum terhadap campur tangan atau pelanggaran tersebut . "

2. Kovenan Internasional tentang Hak Sipil dan Politik (ICCPR) 1966, Pasal 17: "1. Secara sewenang-wenang atau melawan hukum mengganggu individu, keluarga, urusan rumah tangga, telekomunikasi, atau secara tidak sah menyerang kehormatan atau nama baik.

3. Setiap orang berhak atas perlindungan hukum terhadap gangguan atau serangan tersebut.

"Hak atas privasi juga tercantum dalam :

1. Pasal 14 dari Konvensi PBB tentang Buruh Migran
2. Pasal 16 dari Konvensi PBB tentang Hak-Hak Anak
3. Pasal 10 dari Piagam Afrika tentagn Hak dan Kesejahteraan Anak
4. Pasal 4 dari Prinsip Uni Afrika tentang Kebebasan Berekspresi (hak mengakses informasi)
5. Pasal 11 dari Konvensi Hak Asasi Manusia Amerika
6. Pasal 5 dari Deklarasi Amerika tentang Hak dan Kewajiban Manusia

[4] Aspek Data Privasi menurut hukum internasional, regional dan nasional, Dr. Sinta Dewi Rosadi, SH, LL.M, Refika, bandung, 2022

7. Pasal 16 dan 21 dari Piagam Arab tentang Hak Asasi Manusia
8. Pasal 21 dari Deklarassi Hak Asasasi Manusia ASEAN, serta:
9. Pasal 8 Konvensi Hak Asasi Manusia Eropa"

Di lebih dari 130 negara, terdapat deklarasi konstitusional yang melindungi privasi di seluruh dunia. Elemen penting dari privasi adalah perlindungan data pribadi. Hak atas perlindungan data secara umum dapat diturunkan dari perlindungan privasi, namun beberapa media internasional dan regional juga telah menetapkan hak yang lebih spesifik mengenai perlindungan data pribadi.

1. "Pedoman OECD untuk perlindungan Privasi dan Aliran Lintas Batas Pribadi.
2. Konvensi 108 Dewan Eropa tentang Perlindungan Individu terkait Pemrosesan Otomatis Data Pribadi
3. Sejumlah Direktif Uni Eropa dan peraturannya yang masih tertunda, serta Piagam Hak-Hak Dasar Uni Eropa
4. Kerja Sama Ekonomi Asia Pasifik (APEC) Kerangka Kerja Privasi 2004, dan
5. Komunitas Ekonomi Negara-Negara Afrika Barat memiliki undang-undang tambahan perlindungan data sejak 2010."

Saat ini, hampir 100 negara memiliki beberapa bentuk undang-undang perlindungan data. Namun, hari ini sangat umum untuk menggunakan pengawasan tanpa menghormati perlindungan ini. Ini adalah salah satu alasan mengapa Privacy International ada untuk mencegah agen kuat seperti pemerintah dan bisnis menyalahgunakan atau menipu hukum untuk menyerang privasi Anda.

Globalisasi dan komunikasi elektronik tanpa batas telah lama membawa manfaat besar bagi individu. Pada saat yang sama, peningkatan eksploitasi data privasi oleh sektor swasta dan pengumpulan data privasi yang dilaporkan

melalui internet telah menyebabkan kekhawatiran internasional yang meluas. Penunjukkan baru-baru ini oleh Dewan Hak Asasi Manusia PBB dari pelapor khusus tentang hak atas privasi pada musim panas 2015 dan adopsi pada 18 Desember 2013 oleh Majelis Umum PBB atas sebuah resolusi tentang "Hak atas privasi di era digital", menunjukkan minat internasional yang berkembang dalam hak perlindungan data. Ada kebutuhan yang berkembang akan aturan hukum yang melindungi pemrosesan data yang dapat diidentifikasi secara pribadi, yang dikenal sebagai perlindungan data, untuk ditambatkan lebih kuat dalam hukum internasional publik.

Meningkatnya jumlah konflik regulasi yang disebabkan oleh perbedaan konsepsi perlindungan data nasional dan regional, seperti yang digambarkan oleh putusan Pengadilan Kehakiman Uni Eropa pada tanggal 6 Oktober 2015 di Maximillian Schrems, seharusnya menjadi peringatan bagi komunitas internasional tetap terfragmentasi dan lemah, menciptakan risiko bagi individu dan masalah bagi organisasi internasional (seperti entitas PBB dan organisasi kemanusiaan internasional), yang banyak di antaranya memproses data privasi dalam jumlah besar. Isu-isu di bawah hukum internasional publik

Undang-Undang Perlindungan Data tunduk pada pemrosesan data privasi pada aturan hukum yang ditetapkan, untuk melindungi hak-hak individu dan kepentingan masyarakat. Ini terkait erat dengan hak atas privasi dan bersinggungan dengannya dalam banyak hal, tetapi memiliki indentitasnya sendiri. Misalnya, beberapa data yang dicakup oleh Undang-Undang Perlindungan Data mungkin tidak dengan sendirinya menjadi "pribadi", tetapi ketika digabungkan dapat berfungsi untuk mengidentifikasikan individu, dengan dampak yang dihasilkan pada privasinya, kehidupan keluarga, kebebasan berekspresi, dan hal penting lainnya. Minat hukum perlindungan data berakar pada instrumen hak asasi manusia internasional, seperti "Deklarasi Universal Hak Asasi Manusia (UDHR) dan Kovenan Internasional Hak Sipil dan Politik (ICCPR) yang melindungi hak atas kehidupan pribadi, kehidupan keluarga, rumah, dan korespondensi." Secara khusus, ICCPR telah ditafsirkan oleh Komisi Hak Asassi Manusia PBB (Komentar Umum 16) untuk memasukkkan jaminan perlindungan data tertentu. Satu – satunya instrumen

PBB yang secara khusus menangani perlindungan data adalah seperangkat Pedoman PBB yang tidak mengingat untuk pengaturan file data privasi yang terkomputerisasi, sejak tahun 1990. Perjanjian internasional di bidang ini dengan sebagian besar negara pihak adalah Konvensi Dewan Eropa 108, sedangkan sejumlah organisasi internasional lainnya (seperti APEC, OECD, ECOWAS dan Organisasi Negara-Negara Amerika) telah mengadopsi instrumen perlindungan data, yang sebagian besar tidak mengikat lebih dari 100 negara kini telah memberlakukan Undang-Undang Perlindungan Data, banyak diantaranya telah dipengaruhi oleh EU Directive 95/46 (Petunjuk Perlindungan Data, secara resmi Petunjuk 95/46/EC, yang diberlakukan pada Oktober 1995, adalah petunjuk Uni Eropa yang mengatur pemrosesan data pribadi di dalam Uni Eropa dan pergerakan bebas data tersebut) .

Undang – undang Uni Eropa (UE) juga mencangkup hak atas perlindungan data di tingkat konstitusional (misalnya, dalam Piagam Hak – Hak Fundamental UE) dan Pengadilan Hak Asasi Manusia Eropa telah menafsirkan "Pasal 8 Konvensi Eropa tentang Hak Asasi Manusia untuk memasukkan perlindungan data." Terlepas dari semua ini, status perlindungan data dalam hukum internasional publik tetap tidak pasti karena sejumlah faktor :

i. Perjanjian hak asasi manusia internasional seperti ICCPR tidak secara khusus menyebutkan perlindungan data, dan ketentuannya tentang perlindungan kehidupan pribadi dirumuskan secara luas sehingga tidak memberikan banyak panduan dalam menentukan rincian hak perlindungan data.
ii. Sebagai besar instrumen internasional lainnya yang secara khusus menangani perlindungan data bersifat regional daripada global, atau tidak mengikat secara hukum.
iii. Perbedaan dalam persepsi budaya dan hukum tentang privasi berartu kurangnya konsensus internasional tentang pertanyaan dasar, seperti perbedaan antara privasi (yaitu perlindungan ruang pribadi individu) dan perlindungan data (yaitu pembatasan pemrosesan data yang berkaitan dengan individu yang dapat diidentifikasi) dan maksud dan tujuan akhir dari perlindungan

data (misalnya, memastikan keadilan dalam pemrosesan data, kontrol atau penentuan nasib sendiri berdasarkan informasi, melindungi kebebasan individu, memperbaiki ketidakseimbangan kekuatan dalam pemrosesan data dan lain-lain)

Terdapat fragmentasi yang cukup besar mengenai perlindungan data dalam sistem hukum nasional dan regional. Hal ini dapat dilihat, misalnya, dalam perbedaan antara pendekatan hak-hak dasar dalam hukum Uni Eropa dan pendekatan perlindungan konsumen di Amerika Serikat. Selain itu, beberapa negara setuju dengan posisi Amerika Serikat bahwa hukum internasional tidak melarang "aktivitas pengumpulan intelijen pasif" yang tidak sah untuk menyalin data, selama aktivitas terebut tidak melibatkan spionase komersial atau industri atau perusakan atau manipulasi data kerangka hukum internasional yang terfragmentasi untuk proteksi data.

Perlindungan data privasi dalam beberapa tahun sangat berpengaruh, baik dalam sektor publik maupun swasta, karena pengaruh perkembangan industri TIK yang sangat pesatmenurut laporan tahunan "*International Telecommunication Union* ITU (Persatuan Telekomunikasi Internasional adalah sebuah organisasi internasional yang didirikan untuk membakukan dan meregulasi radio internasional dan telekomunikasi)." Teknologi informasi dan komunikasi atau industri TIK adalah istilah luas yang mencakup semua perangkat teknis yang mampu memproses dan mengirimkan informasi penting, dan semakin banyak orang menggunakan Internet yang terhubung ke Internet untuk mengakses aplikasi dan layanan baru. Komunitas global dapat berjejaring secara online, membawa banyak perspektif menarik. Pesatnya pertumbuhan teknologi informasi dan komunikasi (TIK) berdampak besar baik bagi pelaku bisnis maupun pengguna. Alhasil, hampir semua kebutuhan manusia, seperti informasi, komunikasi, perdagangan, dan hiburan, bisa tersampaikan secara online, dan semua konsumen kini mengandalkannya.

ITU memperkirakan bahwa pada akhir tahun 2013, jumlah fixed-broadband langganan akan naik ke lebih dari 688.000.000, sesuai dengan penetrasi dunia sebesar 9,8%. Pada saat yang sama, jumlah pelanggan mobile

broadband aktif akan tumbuh sebesar 21% antara tahun 2010 dan 2013 dengan perkiraan 2,1 Miliar pada akhir tahun 2013; mewakili hampir tiga kali jumlah langganan seluler, yang akan mencapai sekitar 6.840.000 pada akhir tahun 2013. Melihat perkembangan tersebut diatas, maka data dapat diakses secara cepat dan dalam jumlah yang banyak terutama melalui generasi 4G, sehingga sangat berpotensial terjadinya akses, pengelolaan, serta diseminasi data, khususnya data privasi secara berlebih tanpa sepengetahuan pemilik data yang dilakukan oleh badan pemerintah melalui program e-government maupun oleh pelaku usaha melalui e-commerce, dan melihat perkembangan ini secara global, negara-negara menyuarakan keprihatinan dan menginginkan masyarakat internasional melalui hukum internasional untuk lebih berperan aktif untuk mengatur pelanggaran-pelanggaran yang telah terjadi. Beberapa dokumen hukum internasional telah meletakkan dasar bagi hukum perlindungan data domestik modern. Beberapa alat ini dikembangkan dengan pengaturan privasi tertentu, sementara yang lain mengelola aturan umum yang mencakup berbagai aspek, termasuk privasi.

a) Tinjauan ALRC tentang undang-undang privasi (2006-2008)

Tinjauan undang-undang privasi yang dilakukan oleh Komite Senat pada tahun 2000 dan 2005 merekomendasikan agar tinjauan yang lebih luas terhadap undang-undang privasi harus diluncurkan untuk memastikan apakah ketentuan Undang-Undang Privasi 1988 saat ini memadai dan efektif dalam konteks keadaan teknologi saat ini. Hal ini menyebabkan Pemerintah Federal mengeluarkan permintaan pada tahun 2006 kepada Komisi Reformasi Hukum Australia untuk melakukan tinjauan terhadap Undang-Undang Privasi 1988 dan membuat rekomendasi untuk perbaikan Undang-Undang tersebut. Di antara hal-hal yang diminta untuk dipertimbangkan oleh ALRC adalah dampak dari "kemajuan teknologi yang cepat yang memengaruhi cara informasi dikumpulkan, disimpan, dan dikomunikasikan". Selama penyelidikannya dari tahun 2006 hingga 2008, ALRC mengidentifikasi beberapa masalah yang muncul yang memerlukan penyelidikan, termasuk penyebaran informasi publik secara online, pelanggaran data yang mengakibatkan pengungkapan informasi pribadi dan arus informasi lintas batas.

Laporan akhir ALRC, “For Your Information: Australian Privacy Law and Practice,” dirilis pada Agustus 2008. Laporan tersebut membahas, di antara berbagai masalah lainnya, dampak perkembangan teknologi terhadap kelayakan Undang-Undang Privasi 1988 untuk melindungi informasi pribadi dalam lingkungan teknologi saat ini. Ini berisi 295 rekomendasi, yang paling relevan untuk tujuan saat ini adalah:

1. Undang-Undang Privasi 1988 harus diubah untuk mendefinisikan "informasi pribadi" sebagai "informasi atau pendapat, apakah benar atau tidak, dan apakah dicatat dalam bentuk materi atau tidak, tentang individu yang diidentifikasi atau dapat diidentifikasi secara wajar" dan bahwa Komisaris Privasi harus menerbitkan pedoman tentang arti "diidentifikasi atau dapat diidentifikasi secara wajar" dan "tidak cukup dapat diidentifikasi”

2. Untuk mempromosikan keseragaman yang lebih besar dari undang-undang privasi di Australia, Undang-Undang Privasi 1988 harus diperluas untuk diterapkan pada informasi pribadi yang dipegang oleh Pemerintah Federal dan organisasi sektor swasta (dengan undang-undang Negara Bagian dan Wilayah yang saat ini berlaku untuk organisasi sektor swasta sedang diamandemen sehingga tidak berlaku lagi)

3. Nomor Pendaftaran Perusahaan (NPP) dan Informasi Pengenal Pribadi (IPP) yang ada dalam Privacy Act 1988 harus digabungkan dan diganti dengan satu set prinsip privasi, Unified Privacy Principles (UPP):

4. Pemerintah Federal, Negara Bagian dan Teritori harus mengadopsi kebijakan antar pemerintah kesepakatan, membentuk skema kerja sama yang mengatur berlakunya undang-undang dengan Negara Bagian dan Wilayah yang mengatur penanganan informasi pribadi di tempat umum mereka sektor. Undang-undang Negara Bagian dan Wilayah tersebut harus konsisten dengan Undang-Undang Privasi 1988 dan mengadopsi Prinsip Privasi Terpadu.

5. Undang-Undang Privasi 1988 harus diamandemen untuk memasukkan Bagian baru tentang pemberitahuan pelanggaran data, di mana lembaga atau organisasi berkewajiban untuk memberi tahu Komisaris Privasi dan individu yang terpengaruh ketika informasi pribadi tertentu telah diperoleh oleh orang

yang tidak berwenang, mengarah ke risiko nyata dari bahaya serius untuk setiap individu yang terkena dampak. Kegagalan untuk memberi tahu Komisaris Privasi tentang pelanggaran data akan dikenakan hukuman perdata

6. Komisaris Privasi harus mengembangkan panduan tentang publikasi dalam bentuk elektronik informasi pribadi yang terkandung dalam publikasi yang tersedia secara umum, menetapkan faktor-faktor yang harus dipertimbangkan dalam menerbitkan informasi tersebut dan mengklarifikasi penerapan UPPS untuk pengumpulan informasi pribadi dari umumnya publikasi yang tersedia. Pemerintah Federal harus memastikan bahwa instrumen legislatif yang membuat daftar publik yang berisi informasi pribadi menetapkan batasan apa pun atas publikasi elektronik dari informasi tersebut.

7. Komisaris Privasi harus memiliki wewenang untuk mengarahkan lembaga Pemerintah Federal untuk memberikan Penilaian Dampak Privasi dari proyek atau pengembangan baru yang menurut Komisaris Privasi dapat berdampak signifikan pada penanganan informasi pribadi

8. Komisaris Privasi harus memiliki wewenang untuk mengeluarkan pemberitahuan kepatuhan kepada badan atau organisasi Pemerintah Federal, yang menentukan tindakan yang harus diambil oleh badan atau organisasi dan untuk dapat memulai proses penegakan hukum di Pengadilan Federal atau Pengadilan Magistrat Federal untuk menegakkan pemberitahuan tersebut. Komisaris Privasi harus dapat meminta hukuman perdata dalam kasus gangguan serius atau berulang terhadap privasi individu.

BAB III

KESIMPULAN

Pertukaran informasi telah menjadi global saat ini, dan komunitas informasi di seluruh dunia berkomunikasi satu sama lain dengan cara yang kuat. Hubungan antar komunitas diwujudkan melalui komputasi virtual atau dunia maya. Sistem informasi seperti perdagangan (e-commerce), pendidikan (e-writing), kesehatan (telemedicine), transportasi, industri, pariwisata dan pemerintahan (e-Government) digunakan di semua bidang kehidupan. Cakupan dan sistem teknologi informasi, termasuk proses pengumpulan, penyimpanan, produksi, dan distribusi. Cepat dan efisien untuk industri atau masyarakat. Banyaknya pelanggaran privasi yang melibatkan data pribadi di Indonesia merupakan indikasi khusus bahwa tindakan pencegahan khusus harus diambil untuk melindungi data pribadi. Menurut data dari Yayasan Lembaga Konsumen Indonesia (YKLI) pada tahun 2019, seiring dengan semakin banyaknya masyarakat Indonesia yang terkoneksi ke Internet, maka semua aktivitas di Internet akan meningkat secara signifikan, terutama dalam kasus pembobolan data perbankan. , kredit online, asuransi. , dan lain-lain. Telekomunikasi, perdagangan elektronik. Johnny G. Plate, Menteri Komunikasi dan Informatika, mengumumkan bahwa 29 organisasi dan perusahaan mengalami pelanggaran data dalam tiga tahun terakhir (2019-2021). Peningkatan terbesar terjadi pada tahun 2020.

Penegakan hukum yang dapat dilakukan konsumen online jika terjadi pelanggaran data dapat dilakukan melalui dua proses yaitu proses arbitrase (sengketa dan arbitrase) dan proses konsensus (mediasi dan negosiasi). United Nations Conference on Trade and Development (UNCTAD) atau United Nations Conference on Trade and Development (E-commerce and Development Report 2003) telah menyatakan bahwa para korban pelanggaran data permintaan UU ITE no. 18 2008, serta sistem klaim perdata dan hak transaksi elektronik yang tersedia berdasarkan Hukum Indonesia berdasarkan Keputusan No. 28 2012 tentang peraturan pelaksana baru (PSTE), khususnya kompensasi pengguna online untuk operator e-commerce baru, sebagaimana disyaratkan oleh mekanisme regulasi. Hal ini diharapkan dapat membantu korban peretasan data privasi pengguna e-commerce mengubah mekanisme pencarian ganti rugi perdata.

DAFTAR PUSTAKA

Dr. Sinta Dewi Rosadi, SH, LLM, *Cyber Law : Aspek Data Privasi Menurut Hukum Internasional, Regional dan Nasional,* Refika Aditama, 2022.

Dr. Shinta Dewi, SH, LLM, *Cyber Law : Perlindungan Privasi atas Informasi Pribadi Dalam E-commerce Menurut Hukum Internasional*, Widya Padjajaran, 2009.

B Fitzgerald, A Fitzgerald, E Clark, G Middleton, Y F Lim, *Internet and E-Commerce Law: Business and Policy*, Thomson Reuters.