P ISSN 0853-6422 E-ISSN 2621-3737
KERTHA WICAKSANA
Sarana Komunikasi Dosen dan Mahasiswa
Available Online At:https://ejournal.warmadewa.ac.id/index.php/kertawicaksana e-mail: info.kerthawicaksana@gmail.com

Analisis Potensi Kejahatan di Dalam Dunia Maya Terkait Data

Ni Putu Suci Meinarni dan Happy Budyana Sari
STMIK STIKOM Indonesia
rahmatfauzi24oke@gmail.com

Published: 01/02/2020

How To Cite:
Meinarni, N, P, S., Sari, H, B**. (**2020). Analisis Potensi Kejahatan di Dalam Dunia Maya Terkait Data. *KERTHA WICAKSANA: Sarana Komunikasi Dosen dan Mahasiswa*. 14 (1). Pp 9 - 15. https://doi.org/10.22225/kw.14.1.1530.9-15

Abstrak

Penelitian ini bertujuan untuk mengungkapkan bagaimana konsep etika pada dunia maya dan menganalisis kejahatan yang terjadi di dunia maya terkait pemakaian data. Penelitian ini merupakan salah satu jenis penelitian yang bersifat normative empiris dengan menggunakan pendekatan metode diagnostic dan preskiptif. Hasil analisis menunjukan bahwa pertama peredaran data yang terdapat dalam dunia maya memiliki potensi kejahatan karena dapat digunakan tanpa seijin pemilik data dan perolehan data tersebut dapat dilakukan melalui berbagai cara dengan sambungan internet. Kedua, data digital yang terdapat pada gadget seseorang tidak akan pernah aman selama data tersebut terhubung dengan internet. Oleh karena itu, masyarakat harus memiliki kesiagaan terhadap data digital yang mereka miliki dengan tidak sembarang menyimpan data rahasia di dalam gadget.

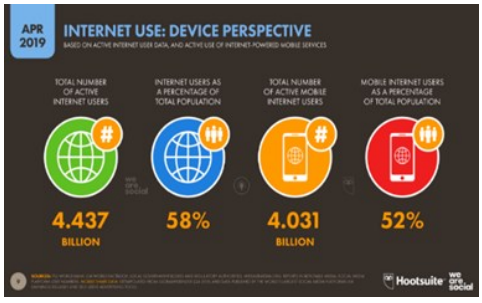
Kata kunci: Etika dunia maya; Hukum Siber; Kejahatan siber; Proteksi Data

Abstract

This study aims to reveal how the concept of ethics in cyberspace and analyze crimes that occur in cyberspace related to data usage. This research is a type of empirical normative research using diagnostic and prescriptive method approaches. The analysis shows that the first circulation of data contained in cyberspace has the potential for crime because it can be used without the permission of the owner of the data and the acquisition of that data

I. PENDAHULUAN

Salah satu survei yang dilakukan oleh lembaga survei independen Wearesocial, rata-rata hampir 1 juta orang diseluruh dunia per harinya menggunakn internet pada waktu yang bersamaan. Data ini berdasarkan atas survei yang dilakukan 1 tahun belakangan. Hasil survei penggunaan internet diseluruh dunia per bulan April 2019 dapat dilihat pada gambar berikut (Wearesocial, 2019)



Sumber: Survei Penggunaan Internet per Bulan April 2019, www.wearesocial.com

Cara mendata tingginya tingkat penggunaan internet diseluruh dunia adalah dengan mengintegerasikan data yang dimiliki oleh beberapa penyelenggara sistem elektronik yang bersedia membagikan informasi atas data yang dibutuhkan. Pemberian data tersebut sebenarnya patut dipertanyakan apakah terdapat hal-hal yang diluar ijin dari pemiliki data untuk bersedia dimanfaatkan datanya. Dalam prinsip umum, untuk kepentingan Pendidikan biasanya, data dapat diberikan tanpa seijin pemilik namun penyelenggara sistem informasi harus memastikan bahwa data tersebut tidak bersifat rahasia dan tidak berpotensi merugikan pemilik data.

Pada kondisi yang lain, masyarakat tidak lagi asing dengan telepon, bahkan mereka dapat menjadi pelaku bisnis telemarketing seperti lembaga penyedia jasa keuangan yang bergerak dalam bidang kredit dan asuransi. Hal ini tentunya menjadi pertanyaan bagi sebagian orang, bagaimana perusahaan-perusahaan tersebut mendapatkan data yang belum pernah dibagikan oleh pemilik data. Hal ini mungkin tidak disadari oleh sebagian orang bahkan tidak peduli, namun sebagian lainya tentu merasa terganggu haknya dan bertanya-tanya, apakah kondisi tersebut dapat diadukan pada aparat penegak hukum?

Term and condition, adalah sebuah klausul didalam beberapa penyelenggara sistem informasi yang mensyaratkan beberapa hal terkait dengan hak dan kewajiban dari pengguna jasa sistem informasi tersebut. Pada umumnya syarat dan ketentuan yang termaktub disana mengharuskan pengguna untuk memberikan informasi/data pribadinya. Dengan terpaksa, maka pengguna tersebut bersedia melakukan apa yang menjadi syarat untuk dapat menggunakan jasa dari penyelenggara sistem informasi tersebut. Pertanyaanmnya adalah, apakah data tersebut dapat dipastikan akan aman?

Potensi kejahatan terkait data sangatlah mungkin untuk terjadi. Beberapa negara telah sejak lama memiliki perhatian yang lebih untuk keamanan data yang ada didalam dunia maya. Implementasi dari perhatian tersebut tertuang dalam regulasi-regulasi nasional terkait teknologi informasi. Indonesia menuangkan segala hak dan kewajiban terkait hukum siber didalam Undang-Undang Nomor 19 tahun 2016 tentang Informasi dan Transaksi Elektronik yang disingkat dengan UU ITE.

Di Negara India, pengaturan mengenai cybercrime dan e-commerce diatur didalam Information Technology Act, 2000 (Indian Ministry of law, 2000). Beberapa pasal yang berfokus pada penggunaan data diantaranya terkait dengan, source documents, hacking, using password of another person, cheating using computer resource, dan private image denda sampai dengan 500.000 rupee.

Di Indonesia sendiri di tahun 2013 hingga 2014 telah terjadi kenaikkan pelaporan kasus di. Sekitar 53 persen (41 kasus dari 72 kasus UU ITE) terjadi di tahun 2014. Angka rata-rata kasus UU ITE sampai Oktober 2014 menunjukkan bahwa terdapat empat kasus yang dilaporkan per bulan. Sedangkan wilayah persebaran pelaporan kasus terjadi merata dari Aceh sampai ke Makassar (Techinasia, 2014). Pada tahun tersebut tingkat penggunaan internet masih rendah dan kompleksitas kepentingan setiap orang belum seberagam sekarang. Dapat dibayangkan bagaimana signifikannya perubahan kuantitas maupun kualitas dari pelaporan kasus dalam ranah dunia maya.

Beberapa hal yang patut dikaji berkaitan dengan munculnya aplikasi (software) yang semakin hari semakin canggih adalah terkait privasi di dalam dunia maya diantaranya, perlindungan dari spy, perlindungan atas data pribadi serta privasi posisi. Padahal setiap persetujuan terkait download secara otomatis telah memberi celah bagi pemilik aplikasi untuk meretas data pribadi maupun melacak keberadaan pengunduh aplikasi. Peraturan hukum nasional, perjanjian bilateral serta peraturan hukum internasional terkait dengan data diharapkan mampu mengatasi permasalahan-permasalahan berkaitan dengan aspek privasi tersebut. Oleh karena itu, penelitian ini bertujuan untuk mengungkapkan bagaimana konsep etika pada dunia maya dan menganalisis kejahatan yang terjadi di dunia maya terkait pemakaian data.

II. METODE

Penelitian ini merupakan salah satu jenis penelitian yang bersifat normative empiris dengan menggunakan pendekatan metode diagnostic dan preskiptif supaya analisis data dalam penelitian lebih terperinci. Ditinjau dari tujuan penelitian hukum itu sendiri terdapat jenis penelitian normatif (kepustakaan) dan penelitian empiris (lapangan). Penelitian normatif (kepustakaan) adalah penelitian hukum yang dilakukan dengan cara meneliti bahan pustaka atau data sekunder (Mamudji, 2003).

III.HASIL DAN PEMBAHASAN

Konsep Etika di Dunia Maya

Secara etimologi, etika berasal dari bahasa Yunani, yaitu *Ethikos* yang memiliki arti "timbul dari kebiasaan". Etika merupakan sebuah cabang utama filsafat yang mempelajari nilai atau kualitas yang menjadi studi mengenai standard dan penilaian moral. Etika mencakup analisis dan penerapan konsep seperti benar, salah, baik, buruk dan tanggung jawab. (Wikipedia, 2017a). Dalam kehidupan manusia etika merupakan sebuah alat ukur atau panduan hidup dalam berinteraksi sebagai mahluk sosial pada lingkungannya. Etika mengatur tingkah polah manusia sehingga apa yang dianggap baik atau benar merupakan hal yang patut dilakukan secara konsisten di dalam sebuah interaksi sosial.

Interaksi sosial merupakan suatu fondasi dari hubungan yang berupa tindakan yang berdasarkan norma dan nilai sosial yang berlaku dan diterapkan di dalam masyarakat. Dengan adanya nilai dan norma yang berlaku, interaksi sosial itu sendiri dapat berlangsung dengan baik jika aturan - aturan dan nilai – nilai yang ada dapat dilakukan dengan baik. Jika tidak adanya kesadaran atas pribadi masing – masing, maka proses sosial itu sendiri tidak dapat berjalan sesuai dengan yang kita harapkan (Wikipedia, 2017b).

Beberapa organisasi serta komunitas didalam dunia maya telah mengatur dan menyepakati untuk menerapkan beberapa hal terkait etika didalam lingkup mereka. Menurut (Tavani, 2016), salah satu contoh, anggota profesi IT, The Association for Computing Machinery (ACM) memiliki kode etik untuk mengatur para anggotanya bertanggung jawab secara moral untuk:

Contribute to society and human well being (Berkontribusi pada masyarakat dan manusia lainnya)

Avoid harm to others (Menghindari penyerangan)

Be honest and trustworthy (Bersikap jujur dan dapat dipercaya)

Be fair and take action not to discriminate (Adil dan tidak diskriminatif)

Honor property copyrights and patents (Menghormati kekayaan hak cipta dan hak paten)

Give proper credit for intellectual property (Memberikan imbalan yang layak pada kekayaan intelektual)

Respect the privacy of others (Menghargai privasi orang lain)

Honor confidentiality (Menghormati hal yang dianggap rahasia)

Terkait dengan privasi, bangsa barat telah menyadari sejak lama mengenai hak dasar yang dimiliki oleh manusia. Seperti contoh, pakar hukum dari *Harvard University* telah menuliskan didalam sebuah jurnal terbitan tahun 1890 yang berjudul: *The Right to Privacy*.

"It could be done only on principles of private justice, moral fitness, and public convenience, which, when applied to a new subject, make common law without a precedent; much more when received and approved by usage".

Yang mengandung arti privasi dijunjung tinggi atas prinsip keadilan dan atas dasar kesehatan moral dengan mengedepankan kenyamanan umum. Jadi, selama hal-hal yang berkaitan dengan privasi dapat diterima di dalam masyarakat maka ketentuan atas hukum terkait privasi dapat diberlakukan.

Kemudian istilah *"The Right To Be Let Alone",* jadi hak ini mengakui bahwa terdapat batasan-batasan terkait atas perlindungan dari gangguan yang tidak diinginkan dalam kehidupan. Pengaturan mengenai privasi akan memberikan kewenangan perorangan untuk menegosiasikan dengan siapa dan bagaimana akan berinteraksi dengan orang lain.

Dalam penjelasan lain yaitu pada Pasal 1 dari United Nation Declaration on Human Rights (Nation, 1948) berbunyi :

"All human beings are born free and equal in dignity and rights. They are endowed with reason and conscience and should act towards one another in a spirit of brotherhood."

Yang berarti bahwa semua orang dilahirkan merdeka dan mempunyai martabat dan hak-hak yang sama. Mereka dikaruniai akal dan hati nurani dan hendaknya bergaul satu sama lain dalam semangat persaudaraan. Terkait dengan hak pribadi seseorang, tertuang di dalam Pasal 12 yaitu:

"No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour

and reputation. Everyone has the right to the protection of the law against such interference or attacks."

Tidak seorang pun dapat diganggu dengan sewenang-wenang urusan pribadinya, keluarganya, rumah-tangganya atau hubungan surat-menyuratnya, juga tak diperkenankan pelanggaran atas kehormatan dan nama baiknya. Setiap orang berhak mendapat perlindungan hukum terhadap gangguan atau pelanggaran seperti itu.

Undang-Undang Republik Indonesia Nomor 39 Tahun 1999 tentang Hak Asasi Manusia (Indonesia, 1999)

Dalam Undang-undang ini yang dimaksud dengan:

Hak Asasi Manusia adalah seperangkat hak yang melekat pada hakikat dan keberadaan manusia sebagai mahluk Tugas Yang Mha Esa dan merupakan anugrah-Nya yang wajib dihormati, dijunjung tinggi dan dilindungi oleh negara hukun, Pemerintahan, dan setiap orang demi kehormatan serta perlindungan harkat dan martabat manusia.

Kewajiban dasar manusia adalah seperangkat kewajiban yang apabila tidak dilaksanakan, tidak memungkinkan terlaksana dan tegaknya hak asasi manusia.

Diskriminasi adalah setiap pembatasan, pelecehan, atau pengucilan yang langsung ataupun tak langsung didasarkan pada pembedaan manusia atas dasar agama, suku, ras, etnik, kelompok, golongan, status sosial, status ekonomi, jenis kelamin, bahasa, keyakinan politik, yang berakibat pengurangan, penyimpangan atau penghapusan pengakuan, pelaksanaan atau penggunaan hak asasi manusia dan kebebasan dasar dalam kehidupan baik individu maupun kolektif dalam bidang politik, ekonomi, hukum, social, budaya, dan aspek kehidupan lainnya.

Penyiksaan adalah setiap perbuatan yang dilakukan dengan sengaja, sehingga menimbulkan rasa sakit atau penderitaan yang hebat, baik jasmani maupun rohani pada seseorang untuk memperoleh pengakuan atau keterangan dari seseorang atau dari orang ketiga, dengan menghukumnya atas suatu perbuatan yang telah dilakukan atau diduga telah dilakukan oleh seseorang atau orang ketiga, atau mengancam atau memaksa seseorang atau orang ketiga, atau untuk suatu alasan yang didasarkan pada setiap bentuk diskriminasi, apabila rasa sakit atau penderitaan tersebut ditimbulkan oleh, atas hasutan dari, dengan persetujuan, atau sepengetahuan siapapun dan atau pejabat publik.

Anak adalah setiap manusia yang berusia di bawah 18 (delapan belas) tahun dan belum menikah, termasuk anak yang masih dalam kandungan apabila hal tersebut adalah demi kepentingannya.

Pelanggaran hak asasi manusia adalah setiap perbuatan seseorang atau kelompok orang termasuk aparat negara baik disengaja maupun tidak disengaja atau kelalaian yang secara melawan hukum mengurangi, menghalangi, membatasi, dan atau mencabut hak asasi manusia seseorang atau kelompok orang yang dijamin oleh Undangundang ini, dan tidak mendapatkan, atau dikhawatirkan tidak memperoleh penyelesaian hukum yang adil dan benar, berdasarkan mekanisme hukum yang berlaku.

Komisi Nasional Hak Asasi yang selanjutnya disebut Komnas HAM adalah lembaga mandiri yang berkedudukan setingkat dalam negara lainya yang berfungsi melaksanakan pengkajian, penelitian, penyaluran, pemantauan, dan mediasi hak asasi manusia.

Dari ke-7 poin diatas, terdapat unsur-unsur yang patut untuk digaris bawahi yaitu hak dan kewajiban manusia, diskriminasi dan pelanggaran serta lembaga negara yang bertugas untuk memberikan pelayanan HAM.

Undang-Undang Nomor 11 Tahun 2008 jo. Undang-Undang Nomor 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik (Indonesia, 2016)

Pengaturan mengenai perlindungan data pribadi didalam Undang-Undang Informasi dan Transaksi Elektronik (UU ITE)

Setiap orang dengan sengaja dan tanpa hak atau melawan hukum melakukan intersepsi atau penyadapan atas informasi Elektronik dan/ atau Dokumen Elektronik dalam suatu komputer dan/atau Sistem Elektronik tertentu milik Orang lain.

Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum melakukan intersepsi atas transmisi Informasi Elektronik dan/atau Dokumen Elektronik yang tidak bersifat publik dari, ke, dan di dalam suatu Komputer dan/atau Sistem Elektronik tertentu milik Orang lain, baik yang

tidak menyebabkan perubahan apa pun maupun yang menyebabkan adanya perubahan, penghilangan, dan/atau penghentian Informasi Elektronik dan/atau Dokumen Elektronik yang sedang ditransmisikan.

Kecuali intersepsi sebagaimana dimaksud pada ayat (1) dan ayat (2), intersepsi yang dilakukan dalam rangka penegakan hukum atas permintaan kepolisian, kejaksaan, dan/atau institusi penegak hukum lainnya yang ditetapkan berdasarkan undang-undang.

Ketentuan lebih lanjut mengenai tata cara intersepsi sebagaimana dimaksud pada ayat (3) diatur denganPeraturan Pemerintah.

Kejahatan Siber Terkait Data

Pengertian data pribadi menurut Peraturan Menteri Komunikasi Dan Informatika Republik Indonesia Nomor 20 Tahun 2016 Tentang Perlindungan Data Pribadi Dalam Sistem Elektronik adalah data perseorangan tertentu yang disimpan, dirawat, dan dijaga kebenaran serta dilindungi kerahasiaannya (Kominfo, 2016). Berdasarkan Peraturan Menteri tersebut, maka timbul hak dan kewajiban antara pemilik data pribadi, pengguna data serta penyelenggaran sistem elektronik. Ketiga entitas tersebut memiliki hak dan kewajiban untuk melindungi data pribadi termasuk dalam proses, perolehan dan pengumpulan, pengolahan dan penganalisisan, penyimpanan, penampilan, pengumuman, pengiriman, penyebarluasan, dan/ atau pembukaan akses dan pemusnahan data. Penggunaan/pengelolaan data tersebut harus dilakukan dengan berhati-hati dan penuh tanggung jawab guna menghindari terjadinya pemanfaatan data yang mengarah pada tindakan kejahatan siber.

Kejahatan siber adalah tindak kriminal yang dilakukan dengan menggunakan teknologi computer sebagai alat kejahatan utama. Kejahatan siber merupakan kejahatan yang memanfaatkan perkembangan teknologi computer khusunya internet. Kejahatan siber didefinisikan sebagai perbuatan melanggar hukum yang memanfaatkan teknologi computer yang berbasis pada kecanggihan perkembangan teknologi internet (Silalahi, 2012). Kejahatan siber merupakan salah satu bentuk atau dimensi baru dari kejahatan masa kini yang mendapat perhatian luas di dunia internasional. Volodymyr Golubev menyebutnya sebagai the new form anti-social behavior. Beberapa julukan/sebutan lainnya yang cukup keren diberikan kepada jenis kejahatan baru ini dalam berbagai tulisan, antara lain, sebagai kejahatan dunia maya (cyber space/virtual space offence), dimensi baru dari high tech crime, dimensi baru dari transnational crime, dan dimensi baru dari white collar crime. Kejahatan siber merupakan salah satu sisi gelap dari kemajuan teknologi yang mempunyai dampak negatif sangat luas bagi seluruh bidang kehidupan modern saat ini (Arief, 2006).

Dalam background paper lokakarya Kongres PBB X pada tahun 2000 juga memberikan definisi kejahatan siber, akan tetapi membagi definisi tersebut dalam narrow sense (arti sempit) dan broader sense (arti Luas), dimana :(Nations, 2000)

"Cybercrime in narrow sense is any illegal behavior directed by means of elctronic operations that targets the security of computer systems and the data processed by them." "Cybercrime as a broader sense adalah any illegal behavior commited by means of, or in relation to, a computer system or network, including such crimes is illegal possession, offering or distributing information by means of a computer system or network."

Kejahatan bersaranakan teknologi informasi, menurut Barda Nawawi Arief meliputi: (Arief, 2006)

Economic Cyber Crime

EFT (Electronic Funds Transfer) Crime

Cybank Crime, Internet Banking Crime, Online Business Crime

Cyber/Electronic Money Laundering

Hitech WCC (White Collar Crime)

Internet Fraud (Bank Fraud, Credit Card Fraud, Online Fraud)

Cyber Terorism

Cyber Stalking

Cyber sex, Cyber (child) Pornography, Cyber Defamation, Cyber- Criminals

Pada tahun 2017, terdapat sebuah kasus cybercrime yang menimpa Rumah Sakit Harapan Kita dan Dharmais. Kejahatan tersebut dilakukan oleh hacker dengan menyerang data dengan malware (program jahat) yang bernama Wannacry. Pelaku kejahatan meminta tebusan sejumlah uang dengan penebusan melalui Bitcoin.

Virus tersebut menyerang dengan cara mengunci komputer korban atau mengenkripsi semua file yang ada sehingga tidak bisa diakses kembali, dan ini tentunya menyulitkan dan merugikan pihak rumah sakit.

Dari kasus diatas dapat kita ketahui, bahwa kecanggihan teknologi dapat digunakan dalam membantu proses administratif sebuah rumah sakit. Namun kecanggihan teknologi juga memiliki dampak yang negatif. Sistem komputerisasi administratif yang canggih ternyata masih memiliki kelemahan terutama dalam hal menangkal virus. Virus ini dapat berbahaya bagi perangkat yang terpapar. Virus dapat menjalar pada sebuah perangkat salah satunya adalah ketika perangkat tersebut terhubung dengan internet. Internet mengambil porsi yang penting dalam konektivitas tersebut. Hal inilah yang menjadi keraguan atas penerapan konsep Internet of Things dalam kehidupan manusia.

Internet of Things (IoT) merupakan sebuah paradigma inovatif yang membuat bumi dalam pengaturan telekomunikasi nirkabel modern dengan cepat. Kesan dasar dari konsep ini adalah perluasan internet ke dunia nyata dengan mengambil benda-benda sehari-hari. Agen fisik tidak lagi terpisah dari dunia virtual tetapi dikendalikan dari jarak jauh bertindak sebagai titik kontak fisik ke layanan Internet (Talari dkk., 2017) “things” yang dimaksud disni adalah benda -benda yang dalam kehidupan sehari-hari dapat ditingkatkan daya guna atau pengawasannya, sehingga kinerja benda tersebut dapat berlaku efektif dan efisien. Efisiensi daya kerja yang dimaksud adalah si pemilik dapat melakukan sistem kontrol jarak jauh hanya dengan melalui koneksi internet.

IoT adalah sistem komputasi dengan perangkat yang terhubung ke internet dan saling terhubung ke perangkat lain, dengan komponen-komponen sebagai berikut:(Technology, 2019)

Sensors/devices: Sensor atau divais berfungsi untuk mengumpulkan data dari lingkungan.

Connectivity: Data yang didapat kemudian akan dikirim ke suatu cloud penyimpanan menggunakan perangkat konektivitas.

Data Processing: Setelah data sampai ke cloud, akan diproses menggunakan perangkat lunak tertentu.

User interface: Hasil informasi ditampilkan dengan cara tertentu agar bermanfaat bagi pengguna.

Dalam merespon kecanggihan teknologi kita seharusnya tetap waspada. Seluruh data yang terekam melalui device tidak dapat diseleksi dan semuanya akan masuk ke dalam sebuah server. Sebagai gambaran bagaimana alur data diproses dengan konsep IoT adalah pada sebuah proses kerja CCTV yang disambungkan dengan perangkat Smart Phone:

Kamera pada CCTV menangkap gambar pada lokasi tertentu dalam jangka waktu tertentu.

Disuatu tempat tertentu lainnya pemilik CCTV ingin mengetahui situasi dan kondisi lokasi daerah pemasangan CCTV tersebut.

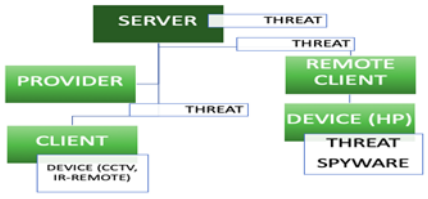
Dengan sistem kendali jarak jauh (remoting) pemilik tersebut dapat mengetahui situasi dan kondisi tempat tertentu dengan melihat tampilan gambar yang terekam melalui CCTV hanya dengan menggunakan smartphone miliknya.

Untuk dapat mengoperasikan smartphone serta CCTV tersebut agar dapat bekerja, kedua perangkat harus saling terhubung. Yang digunakan untuk menghubungkan satu sama lain adalah jaringan internet yang disediakan oleh penyedia jasa khusus yang kita umum kita kenal dengan istilah provider.

Gambar hasil tangkapan dari CCTV kita sebut dengan data. Data ini kemudian dikirimkan oleh CCTV ke smartphone pemilik melalui server. Karena tanpa adanya server, data tidak akan dapat terkirim ke smartphone.

Dalam proses transmisi data, terdapat beberapa titik dimana potensi serangan (threat) terhadap data yang mungkin terjadi.

Alur tersebut dapat diilustrasikan pada gambar dibawah.



Sumber: Diolah oleh peneliti, 2019.

Dari gambaran ilustrasi diatas, kekhawatiran yang muncul adalah ketika terdapat aktivitas pribadi yang tidak ingin dipublikasikan ke ranah publik. Dan ketika data digital dicuri melalui serangan digital maka sudah dapat dipastikan

keamanan data tersebut tidak akan pernah terjamin. Entitas terpenting dari transmisi ini adalah penghubung, yaitu jaringan internet. Sehingga setiap kali sebuah perangkat terkoneksi dengan internet maka saat itulah ancaman terhadap data sedang terjadi. Data berupa foto, video, berkas, atau berupa sandi tertentu yang beredar di dunia maya tidak pernah aman.

IV. KESIMPULAN

Berdasarkan penelitian yang dilakukan dapat disimpulkan bahwa peredaran data yang terdapat dalam dunia maya memiliki potensi kejahatan karena dapat digunakan tanpa seijin pemilik data dan perolehan data tersebut dapat dilakukan melalui berbagai cara dengan sambungan internet. Data digital yang terdapat pada gadget seseorang tidak akan pernah aman selama data tersebut terhubung dengan internet. Oleh karena itu masyarakat harus menyadari dan memiliki kesiagaan terhadap data digital yang mereka miliki dengan tidak sembarangan menyimpan data rahasia di dalam gadget masing-masing, misalnya tidak mencatat password kartu kredit di handphone, lebih baik dicatat secara manual di dalam buku. Selain itu, masyarakat patut meningkatkan kewaspadaan mengenai potensi-potensi kejahatan yang muncul melalui dunia maya, sehingga kewaspadaan tersebut dapat menghindarkan masyarakat dari model kejahatan baru dunia maya.

DAFTAR PUSTAKA

Arief, B. N. (2006). *Tindak Pidana Mayantara Perkembangan Kajian Cyber Crime di Indonesia*. Jakarta: PT Raja Grafindo Persada.

Mamudji., S. S. S. (2003). *Penelitian Hukum Normatif; Suatu Tinjauan Singkat*. Jakarta: PT. Rajagrafindo Persada.

Silalahi, H. R. (2012). Analisis Yuridis Kejahatan Cyber Crime Dalam Pembobolan Mesin ATM Bank (Universitas Pembangunan Nasional "Veteran" Jawa Timur). Retrieved from http://eprints.upnjatim.ac.id/5264/1/file1.pdf

Talari, S., Shafie-khah, M., Siano, P., Loia, V., Tommasetti, A., & Catalão, J. (2017). A Review of Smart Cities Based on the Internet of Things Concept. *Energies*, *10*(4), 421. https://doi.org/10.3390/en10040421

Tavani, H. T. (2016). *Ethics and Technology*. Retrieved from https://www.researchgate.net/publication/271826911_Ethics_and_Information_Technologies_History_and_Themes_of_a_Research_Field

Indian Ministry of Law, J. and C. A. (Legislative D. *Information Technology Act*. , (2000).

Indonesia, R. *Undang-Undang tentang Hak Asasi Manusia*. , (1999).

Indonesia, R. *UU Informasi dan Transaksi Elektronik*. , Pub. L. No. Undang-Undang Nomor 19 Tahun 2016 perubahan atas Undang-Undang Nomor 11 Tahun 2008 (2016).

Kominfo. *Peraturan Menteri Komunikasi Dan Informatika Republik Indonesia Nomor 20 Tahun 2016 Tentang Perlindungan Data Pribadi Dalam Sistem Elektronik*. , (2016).

Nation, U. (1948). Universal Declaration on Human Rights.

Nations, U. *Workshop on Crimes Related to The Computer Network,*. , (2000).

Techinasia. (2014). Laporan kasus Undang-Undang ITE selama tahun 2008 hingga 2014 (INFOGRAFIS).

Technology, Dt. (2019). Internet of Things.

Wearesocial. (2019). The State of Digital in April 2019: All The Numbers You Need To Know.

Wikipedia. (2017a). Etika.

Wikipedia. (2017b). Interaksi Sosial.