TOMALEBBI
Volume 11 Nomor 1, Maret 2024
Jurnal Pemikiran, Penelitian Hukum, Pendidikan Pancasila dan Kewarganegaraaan
p-ISSN 2355-6439. e-ISSN 2962-3685
Halaman 12-16

KEAMANAN SIBERNETIKA DAN TANTANGAN GEOPOLITIK DI ERA DIGITAL

Anindia Dwi Maharani[1], Aulia Ryndha Luthfitasari[2], Bagas Alif Rachman[3], Aditya Rahman[4], Suryo Ediyono[5]

Jurusan D4-Keselamatan dan Kesehatan Kerja, Sekolah Vokasi Universitas Sebelas Maret,
Dosen Pendidikan dan Kewarganegaraan, Fakultas Ilmu Budaya Universitas Sebelas Maret.
Jl. Ir Sutami No.36, Kec. Jebres, Kota Surakarta, Jawa Tengah
Email: [1]anindiadwimaharani@student.uns.ac.id, [2]auliaryndha@student.uns.ac.id,
[3]ladityarh@student.uns.ac.id, [4]alifattaf@student.uns.ac.id, [5]ediyonosuryo@staff.uns.ac.id[5]

Abstract: *Human life is always experiencing changes and improvements due to the progress of civilization which occurs due to the emergence of discoveries by scientists. The internet is one of the biggest invention made in the history of human civilization that has provided both convenience and a challenge. But, if not dealt well, it would have brought negative effects especially towards national defense. The government's involvements towards eradicating cybercrime is very much needed so that there would be no data leaks like the BPJS data leak to happen again. The purpose of this article is to investigate the dynamics of cybercrime towards the circumstances of the country itself. It also proposes a few recommendations that could be done for Indonesia's national security to respond towards the threat of cybercrime.*

Keywords*: Security, Cybernetics, Geopolitical Challenges, Digital*

Abstrak, Kehidupan manusia senantiasa mengalami perubahan dan peningkatan akibat kemajuan peradaban yang terjadi akibat munculnya penemuan-penemuan oleh para ilmuwan. internet merupakan salah satu penemuan terbesar dalam sejarah peradaban manusia yang memberikan banyak kemudahan sekaligus tantangan. Hal tersebut harus disikapi secara bijaksana sehingga perubahan yang ada dapat membawa kemajuan bangsa. Namun apabila tidak dapat disikapi dengan baik akan membawa dampak negatif khususnya bagi pertahanan negara. Salah satu dampak perubahan tersebut adalah saat ini siber dianggap sebagai salah satu masalah penting yang menjadi fokus pemerintah. Peran pemerintah dalam memberantas kejahatan siber ini sangat diperlukan supaya tidak ada lagi kebocoran data seperti kebocoran data BPJS. Artikel ini bertujuan menyelidiki dinamika serangan siber terhadap sekitar. Artikel ini juga mengusulkan beberapa rekomendasi yang dapat dilakukan untuk keamanan nasional Indonesia dalam menanggapi ancaman *cybercrime*.

Kata Kunci: Keamanan, Sibernetika, Tantangan Geopolitik, Era Digital

PENDAHULUAN

Saat ini kemajuan globalisasi membawa perubahan besar untuk kehidupan manusia khususnya di bidang teknologi informasi. Teknologi informasi membuat komunikasi antara manusia dan negara menjadi lebih mudah dan cepat, tanpa memandang ruang dan waktu.

Menurut Sajidiman, Srijanthi (2014:278), “Globalisasi adalah masuk atau meluasnya pengaruh dari suatu

wilayah/negara ke wilayah/negara lain dan/atau proses masuknya suatu negara ke dalam pergaulan dunia. Proses membawa segala sesuatu yang dapat mempengaruhi suatu negara ke dalam negaranya dari luar negeri.

Globalisasi dalam arti teknologi informasi tidak dapat dipisahkan dari dunia *cyber*. *Cyber* merupakan awalan yang berhubungan dengan teknologi informasi. Menurut Norbert Wiener, pada akhir tahun 1940-an, sibernetika dipahami sebagai studi tentang sistem kendali dan komunikasi antara manusia dan mesin. Weiner menggunakan kata Yunani *cyber*, yang mempunyai arti serupa dengan kepemimpinan.

Globalisasi di bidang teknologi informasi tentunya membawa tantangan geopolitik, khususnya di era digital saat ini. Tantangan-tantangan ini akan selalu ada seiring berjalannya waktu kecuali era globalisasi hilang. Misalnya serangan melalui media sosial atau biasa disebut cybercrime. Bahaya terbesar berpotensi timbul jika informasi sensitif yang bernilai strategis jatuh ke tangan pihak-pihak yang tidak bertanggung jawab, sehingga dapat mempengaruhi kedaulatan nasional dan keutuhan wilayah NKRI.

Biro Sandi Siber Nasional (BSSN) mengumumkan jumlah kejahatan siber pada tahun 2020 meningkat empat kali lipat dibandingkan tahun 2019 yang mencapai 39 juta jiwa. Hal ini tentu menunjukkan bahwa mekanisme perlindungan data di Indonesia belum memadai. Pemerintah Indonesia telah menetapkan Undang-Undang Kejahatan Dunia Maya yaitu Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik. Undang-undang ini mengatur bahwa siapa pun dilarang melakukan perbuatan tersebut.

Akses yang disengaja ke komputer atau sistem elektronik yang diakibatkan oleh pelanggaran, pelanggaran, pelampauan, atau pelanggaran terhadap sistem keamanan dapat mengakibatkan sanksi. Peristiwa kebocoran informasi ini termasuk dalam kejahatan siber yang merupakan kejahatan tanpa batas. Oleh karena itu, diperlukan upaya yang saling terintegrasi dan berkelanjutan untuk mengatasi hal ini.

Salah satu kasus pelanggaran data adalah hilangnya data BPJS. Seiring dengan semakin nyatanya ancaman kejahatan siber, Indonesia perlu bersiap membendung dampak ancaman kejahatan siber yang dapat menimbulkan kerugian besar dan mengancam keamanan nasional. Penelitian ini bertujuan untuk mengetahui (a) bentuk-bentuk kejahatan siber, (b) potensi dampak kejahatan siber terhadap keamanan Indonesia, (c) besarnya ancaman kejahatan siber, dan (d) peran dan komitmen masyarakat Indonesia. Mengerjakan. Pemerintah perlu mendeteksi dan meminimalkan kejahatan dunia maya global.

METODE PENELITIAN

Penulisan ini disusun menggunakan metode kepustakaan (*library research*). *Library research* ini dilakukan dengan mengumpulkan berbagai referensi bacaan yang relevan dengan permasalahan yang diteliti, kemudian dilakukan pemahaman cara teliti dan *careful* sehingga mendapatkan sebuah temuan-temuan penelitian (Zed, 2003: 3). Penulis melakukan *literature study* secara mendalam untuk mendukung penelitian ini.

HASIL DAN PEMBAHASAN

Pengertian sibernetika telah dikemukakan oleh Louis Couffignal pada tahun 1956, beliau adalah salah satu pelopor sibernetika, yang mengkarakterisasi sibernetika sebagai "seni untuk memastikan keberhasilan dalam suatu tindakan". *"Cybernetics is a theory of control systems based on communication (transfer of information) between systems and environment and within the system, and control (feedback) of the system's function in regard to environment*". Sibernetika

adalah teori sistem pengontrol yang didasarkan pada komunikasi (penyampaian informasi) antara sistem dan lingkungan, dan antar sistem, pengontrol (*feedback*) dari sistem berfungsi dengan memperhatikan lingkungan. Jadi, antara unsur satu dengan unsur lainnya harus saling mempengaruhi agar tidak terjadi konflik.

Proses digitalisasi menjadi salah satu kunci berkembangnya revolusi industri 4.0 yang ditandai dengan eratnya keterhubungan kehidupan masyarakat dengan internet. Tidak mengherankan jika kemajuan teknologi telah menyebabkan hilangnya batas antara media fisik dan digital. Hal ini tentunya berdampak pada berbagai bidang kehidupan, salah satunya adalah bidang kesehatan. Proses digitalisasi sektor kesehatan berdampak positif dalam menjaga *database* kesehatan lebih bersih, terorganisir, sederhana, efisien dan efektif. Namun, proses digitalisasi tidak selalu memberikan dampak positif terhadap keberlanjutan mekanisme layanan kesehatan. Tjdrawinata (2011) mengatakan bahwa sektor kesehatan berpotensi menjadi sektor yang paling rentan akibat perkembangan teknologi yang senantiasa mengalami perubahan yang signifikan dan tiba-tiba.

Banyak kejadian yang terjadi di Indonesia, salah satunya adalah bocornya 18,5 juta data pengguna BPJS Ketenagakerjaan yang dijual di forum gelap seharga Rp 153 juta. Dalam postingan di forum hacker, penjahat siber Bjorka membocorkan 19,5 juta data dengan nama "BPJS Ketenagakerjaan Indonesia 19 Juta". Pelaku kejahatan siber menyebarkan 100 ribu sampel yang berisi NIK, nama lengkap, tanggal lahir, alamat, nomor ponsel, alamat email, jenis pekerjaan, dan nama perusahaan. Asisten Komunikasi BPJS, Oni Marbun mengaku pihaknya melakukan penyelidikan bersama dengan Biro Siber dan Sandi Negara (BSSN) dan Kementerian Komunikasi dan Informatika (Kominfo). Kasus kebocoran data ini jelas melanggar prinsip keamanan data, perlindungan data, dan etika. Keamanan data adalah mekanisme yang melindungi sekumpulan database dari berbagai ancaman yang disengaja maupun tidak disengaja.

Motif pencurian data akan mengakibatkan hilangnya kerahasiaan, privasi, ketersediaan dan integritas BPJS Kesehatan. Aliran data ini tentunya akan menimbulkan kerugian baik materiil maupun nonmateriil terhadap kelangsungan pelayanan kesehatan di Indonesia. Hal ini juga membuat masyarakat Indonesia kehilangan kredibilitas atau kepercayaan. Selain itu, kasus ini juga melanggar aspek terkait perlindungan data. Menurut *Privacy, Trust and Disclosure Online*, privasi dibagi menjadi tiga bagian: privasi data, privasi aksesibilitas, dan privasi ekspresif. Jika kasus kebocoran data ini melanggar aspek privasi informasi, karena pengguna tidak mengetahui informasi yang diberikan dan hilangnya informasi terkait penggunaan informasi yang dikirimkan. Selain itu, hal ini melanggar aspek privasi eksplisit dari ketidakamanan informasi yang ditransfer bahkan ke lembaga pemerintah melalui paksaan tidak langsung.

Kebocoran data pribadi membawa dampak yang signifikan bagi banyak orang yang data pribadinya tersebar luas. Selain membahayakan privasi mereka, mereka juga dapat menjadi korban kejahatan dunia maya seperti pemalsuan, penipuan, pemerasan atau doxing, pengungkapan yang ditargetkan, dan pembagian informasi oleh pihak yang tidak berwenang. Arus data bahkan dapat mengganggu stabilitas suatu negara. Kebocoran data demografi memudahkan partai politik mana pun di seluruh dunia untuk melancarkan upaya propaganda yang diperhitungkan. Itu sebabnya para aktivis dark web selalu menunggu bocoran dari beberapa lembaga, menurut Yudi Prayud, direktur Pusat Kajian Digital Forensik Universitas Islam Indonesia (UII). Berdasarkan

uraian sebelumnya dapat dikatakan bahwa jika terjadi kebocoran data pribadi yang berkaitan dengan privasi seseorang atau bersifat pribadi, maka dapat dikatakan bahwa permasalahan kebocoran data pribadi merupakan permasalahan yang cukup krusial. karena masalah ini dapat menimbulkan dampak yang sangat serius yang dapat mengganggu hak privasi seseorang. Akibat dari kebocoran informasi pribadi peserta BPJS antara lain kerugian materiil 279 juta BPJS atau kebocoran informasi tenaga kesehatan BPJS hingga Rp 600 triliun, dan juga dapat memicu potensi penyalahgunaan KTP palsu untuk menggunakan informasi orang lain untuk peminjaman. Tentang layanan pinjaman online dan lain-lain.

Direktorat Tindak Pidana Siber (Dittipidsiber) Badan Reserse Kriminal Kepolisian Republik Indonesia (Bareskrim Polri) sudah membentuk tim untuk menyelidiki kasus dugaan bocornya data ini yang didukung satuan lain termasuk dari Polda Metro Jaya. Dittipidsiber juga telah melayangkan panggilan pemeriksaan kepada Direktur Utama BPJS Kesehatan, Ali Ghufron Mukti untuk diminta klarifikasi terhadap kasus kebocoran. Data pribadi BPJS Kesehatan. Upaya menelusuri kebocoran data pribadi juga telah dilakukan oleh Kementerian Komunikasi dan Informatika (Kemenkominfo), BPJS Kesehatan, serta Direktorat Jenderal Kependudukan dan Pencatatan Sipil (Ditjen Dukcapil) Ke-menterian Dalam Negeri (Kemendagri).

Secara khusus, ketentuan terkait privasi dan data pribadi dalam sistem elektronik dapat ditemukan dalam Undang-Undang Informasi dan Transaksi Elektronik Nomor 11 Tahun 2008 atau disingkat UU ITE, sebagaimana telah diubah dengan Perubahan Undang-Undang Nomor 19 Tahun 2016. Informasi dan Transaksi Elektronik- Undang-Undang Nomor 11 Tahun 2008.

KESIMPULAN

Berdasarkan hasil dan pembahasan yang telah penulis jelaskan sebelumnya, maka dapat disimpulkan bahwa teknologi informasi dapat menjadi sumber ancaman terhadap keamanan negara dalam segala hal, termasuk dalam memberikan informasi kepada warga negara. Pada contoh di atas, peretasan yang dilakukan oleh individu atau hacker merupakan ancaman terhadap keamanan informasi pribadi warga negara, yang dampaknya sangat berbahaya bagi seluruh warga negara Indonesia, yaitu merugikan berupa kebocoran informasi pribadi warga negara Indonesia. Kebocoran data demografi memudahkan pihak mana pun di seluruh dunia untuk melancarkan aktivitas propaganda yang diperhitungkan dan dapat mengganggu stabilitas suatu negara. Oleh karena itu, tidak ada kata terlambat bagi pemerintah Indonesia untuk menyikapi perkembangan ancaman siber dengan memetakan segala kemungkinan serangan dan memperbaiki sistem informasi masyarakat Indonesia. Selain itu, pemerintah juga harus memaksimalkan peran Badan Siber dan Kriptografi Nasional untuk melindungi seluruh sektor yang mungkin menjadi sasaran penyerang.

DAFTAR PUSTAKA

Amarullah, A. H., Simon, A. J., & Widiawan, B. (2021). Jurnal Kajian Stratejik Ketahanan Nasional - scholarhub.ui.ac.id. Jurnal Kajian Stratejik Ketahanan Nasional. https://scholarhub.ui.ac.id/cgi/viewcontent.cgi?article=1037&context=jkskn

Anggoro, K. (2020, August 15). Perubahan Geopolitik Dan Ketahanan nasional: Sebuah Penjelajahan Teoretikal. Jurnal Lemhannas RI. http://jurnal.lemhannas.go.id/index.php/jkl/article/view/130

Ilman, M. Z., Wijoyo, A., Hidayat, A. T., Gumelar, G., & Jepri, M. (2023, October 25). Evolusi Ancaman Terhadap Kemanan Komputer. JRIIN : Jurnal Riset Informatika dan Inovasi. https://jurnalmahasiswa.com/index.php/jriin/article/view/422

Ramadhan, I. (2021, August 2). Implikasi Ruang Siber Terhadap geopolitik negara the implication of... Implikasi Ruang Siber Terhadap Geopolitik Negara. https://www.researchgate.net/profile/Iqbal-Ramadhan-6/publication/35437-8711_The_Implication_of_Cyberspace_Towards_State_Geopolitics/links/61358047c69a4e487981430d/The-Implication-of-Cyberspace-Towards-State-Geopolitics.pdf

Rofii, M. S. (2018). Jurnal Kajian Stratejik Ketahanan Nasional - scholarhub.ui.ac.id. Jurnal Kajian Strtejik Ketahanan Nasional. https://scholarhub.ui.ac.id/cgi/viewcontent.cgi?article=1037&context=jkskn