JCIC: Jurnal CIC Lembaga Riset dan Konsultan Sosial – ISSN: 2746-5160 (e)
Vol. 5, no. 2 (September 2023), pp. 55-66, doi: 10.51486/jbo.v5i2.113

Kejahatan Siber dan Kebijakan Identitas Kependudukan Digital: Sebuah Studi Tentang Potensi Pencurian Data Online

Cybercrime and Digital Population Identity Policies: A Study on the Potential of Online Data Theft

Yedija Otniel Purba[1], Agus Mauluddin[2]

[1,2]Departemen Kriminologi, FISIP, Universitas Indonesia
Email: yedija.otniel@ui.ac.id

ABSTRACT

The rapid advancement of technology has significantly impacted the global way of life in a positive manner. However, it has also brought about negative consequences, particularly in the form of cybercrime. This article explores cybercrime, focusing specifically on cases of online data theft in Indonesia. Through a mixed research method, it can be identified that Indonesia is facing serious challenges related to cybersecurity, marked by a series of data leaks involving both government and private entities. The research also delves into the potential for online data theft in the policy transition from the National Identity Card (Kartu Tanda Penduduk or KTP) to the Digital Population Identity (Identitas Kependudukan Digital or IKD) in Indonesia. By detailing previous data leakage cases, this study indicates that the implementation of IKD in Indonesia needs to be reassessed. The conclusion drawn from the research is that efforts to enhance cybersecurity in Indonesia require concrete and collaborative measures, including the development of consistent regulations, the improvement of human resources in the field of cybersecurity, and better awareness among the public and government regarding the importance of protecting personal data. The study suggests further research to delve into the effectiveness of cybersecurity regulations in Indonesia and to understand the variables that influence public and governmental awareness regarding personal data protection.

Keywords*: cybercrime, online data theft, cybersecurity, digital population identity (IKD), personal data protection regulations*

ABSTRAK

Pesatnya teknologi berdampak positif bagi kehidupan dunia secara signifikan. Namun, bersamaan juga dengan dampak negatifnya, terutama dalam bentuk kejahatan siber atau cybercrime. Artikel ini mengeksplorasi cybercrime, khususnya pada kasus pencurian data online di Indonesia. Melalui metode penelitian campuran*, dapat teridentifikasi bahwa Indonesia menghadapi tantangan serius terkait keamanan siber. Ditandai dengan serangkaian kasus kebocoran data yang melibatkan entitas pemerintah dan swasta. Penelitian ini juga membahas potensi pencurian data online pada kebijakan penggantian Kartu Tanda Penduduk (KTP) dengan Identitas Kependudukan Digital (IKD) di Indonesia. Dengan merinci kasus kebocoran data sebelumnya, penelitian ini menunjukkan bahwa implementasi IKD di Indonesia perlu ditinjau ulang. Kesimpulan dari penelitian bahwa upaya meningkatkan keamanan siber di Indonesia memerlukan langkah-langkah konkret dan kolaboratif antar-pihak, termasuk pengembangan regulasi yang konsisten, peningkatan sumber daya manusia dalam bidang keamanan siber, dan kesadaran publik dan pemerintah yang lebih baik terhadap pentingnya melindungi data pribadi. Penelitian lanjutan juga diusulkan untuk mendalami efektivitas peraturan keamanan siber di Indonesia dan memahami variabel-variabel yang memengaruhi kesadaran masyarakat dan pemerintah terhadap perlindungan data pribadi.*

Kata Kunci: Kejahatan Siber, Pencurian Data Online, Keamanan Siber, Identitas Kependudukan Digital (IKD), Regulasi Perlindungan Data Pribadi

PENDAHULUAN

Dunia telah memasuki zaman di mana perkembangan teknologi menjadi sangat pesat. Teknologi memberikan dampak positif bagi kehidupan. Namun juga memiliki dampak negatif. Dampak negatif dari perkembangan teknologi adalah kejahatan siber. Kejahatan ini secara umum dapat dipahami sebagai kejahatan yang dilakukan berbasis online dengan memanfaatkan teknologi modern dengan berbagai perangkat teknologinya. Beberapa penelitian menjelaskan yang memiliki titik poin yang sama yaitu mengenai kejahatan dunia maya, misalnya (Gupta & Mata-Toledo, 2016) menjelaskan bahwa kejahatan siber adalah istilah yang digunakan untuk menggambarkan aktivitas yang melanggar hukum di mana seseorang atau kelompok melanggar atau meretas sistem atau jaringan komputer dengan maksud untuk mendapatkan data sensitif secara ilegal atau mendistribusikan perangkat lunak berbahaya. Sementara itu Broadhurst (2017) menjelaskan bahwa kejahatan siber dicirikan sebagai penyebaran perangkat lunak berbahaya, penipuan dalam penyalahgunaan komputer, dan pencurian identitas yang melibatkan kolaborasi publik dan swasta serta koordinasi internasional. Terminologi yang lebih sederhana dijelaskan oleh Chandra & Snowe (2020) bahwa kejahatan siber merupakan istilah untuk segala aktivitas kriminal yang dilakukan dengan menggunakan teknologi komputer. Dijelaskan juga oleh Mauluddin dan Royandi (2023) yang menitikberatkan pada kejahatan di era digital adanya bentuk kriminalitas yang menyusup ke ranah teknologi. Beberapa contohnya dalam konteks sosio-politik seperti Buzzer yang memecah belah persatuan bangsa melalu orkestrasinya di dunia maya. Berangkat dari pandangan-pandangan tersebut dapat ditarik sebuah penalaran bahwa kejahatan siber adalah segala jenis kegiatan yang melibatkan teknologi dengan tujuan kejahatan.

Dilihat dari penjelasan tentang kejahatan siber tersebut serta perkembangan teknologi saat ini yang sudah hampir memasuki era 5.0 maka dapat dikatakan bukan tidak mungkin kejahatan siber tersebut terus menjadi ancaman nyata bagi kehidupan dunia modern. Hal tersebut dapat dilihat dari berbagai kasus yang pernah terjadi seperti (Tendiyanto, Istiqamah, & Suwandoko, 2023) dalam penelitiannya menjelaskan bahwa adanya masalah ketika melakukan transaksi jual beli secara online. Terdapat masalah pada sistem pembayaran yang memengaruhi pelanggan dan pihak penjual. Tidak hanya itu dalam masalah kejahatan siber ada juga permasalah seperti upaya mencari dan menyebarkan informasi seseorang dengan tujuan intimidasi, serta ada masalah di mana seseorang menghina dengan teks melalui media online, kedua masalah tersebut biasanya dikenal sebagai *doxing dan cyberbullying.* Mengenai hal tersebut Saputra, Munifah, & Pramesty (2023) dalam penelitiannya menemukan bahwa terdapat masalah privasi yang diakibatkan oleh *cyberbullying* dan *doxing* dalam materi *reality show* investigasi polisi yang disiarkan di *platform* internet dan televisi. Berdasarkan hal ini dapat dilihat bahwa terdapat pelanggaran privasi serta terjadinya *bullying* berbasis online pada kejahatan dunia siber.

Kejahatan siber dapat dikatakan tindak kriminalitas yang kompleks. Sebab semua orang dapat menjadi korbannya, bahkan teknologi itu sendiri juga dapat menjadi korban. Sebagai contohnya kasus eksploitasi anak di media sosial di mana menurut Komisi Perlindungan Anak Indonesia (KPAI), media sosial digunakan dalam 60% kasus yang melibatkan pekerja anak dan eksploitasi seksual anak di bawah umur (Nua, 2021). Kasus lainnya yang melibatkan media online adalah kasus anak kelas 6 SD di Bandung yang menjadi korban pemerkosaan dan perdagangan manusia. Pada kasus ini korban yang masih anak-anak berteman dengan pelaku melalui media sosial dan diperkosa serta dijual di aplikasi kencan kepada beberapa orang (Jo, 2023). Dengan melihat kasus tersebut dapat dilihat bahwa teknologi media online juga berdampak negatif dan memiliki potensi yang berbahaya bagi berbagai kalangan, muda maupun dewasa, dalam kasus kejahatan siber yang melibatkan anak-anak yang menjadi korban maupun pelaku. Seperti pada contoh kasus tersebut peran orang tua menjadi sangat penting. Hal ini sejalan dengan apa yang dijelaskan oleh Haryono, Legiani, & Carolina (2023) bahwa orang tua mempunyai peran utama dalam membentuk kepribadian dan perilaku anak-anaknya. Peran orang tua dalam mendidik anak sangat berpengaruh bagi tumbuh kembang dan perilaku anak. Hal ini agar anak tidak melakukan kenakalan maupun menjadi korban dari kejahatan, dalam konteks ini adalah kejahatan siber.

Kasus lainnya yang masih berkaitan dengan kejahatan siber adalah kasus beredarnya informasi atau berita bohong di media sosial, yang sering disebut sebagai hoax. Penjelasannya

sangatlah beragam misalnya penelitian (Haeranah et al, 2022) mengatakan bahwa berita palsu (hoax) merupakan kejahatan material yang menimbulkan kerugian bagi konsumen, yang berupa pengguna barang produksi, penerima pesan iklan, dan pengguna jasa. Sementara itu (Finneman & Thomas, 2018) menjelaskan bahwa informasi palsu yang disebarkan oleh situs web, pejabat publik, dan media sosial dikenal sebagai berita palsu dan media hoax. Penjelasan lebih lengkap oleh (Salaverría et al, 2020) bahwa hoax adalah sebuah peristiwa misinformasi berita yang memiliki empat jenis seperti digunakan untuk lelucon, bersifat berlebihan, dekontekstualisasi, dan menipu. Berangkat dari penjelasan tersebut dapat ditarik sebuah tafsir bahwa hoax merupakan salah satu kejahatan siber yang berbasis penyebaran informasi palsu menggunakan media online. Hal ini tentunya sangat berbahaya apalagi jika dalam kondisi bencana dapat menimbulkan kepanikan moral bagi masyarakat dan membentuk persepsi negatif. Sejalan dengan hal ini (Dulkiah, 2023) dalam penelitiannya menyatakan bahwa di dunia digital saat ini, berita palsu adalah masalah yang dapat memengaruhi semua orang, termasuk individu yang berpendidikan tinggi dan anggota dari era milenial, terutama mahasiswa. Berdasarkan hal tersebut sekali lagi dapat dikatakan bahwa kejahatan siber dapat berdampak bagi siapa saja dan bagi kalangan apapun. Misalnya dalam kasus politik saat ini berita online dapat sangat memengaruhi persepsi masyarakat tentang pilihan mereka sebagai hak berdemokrasi. Berita palsu juga dapat membentuk persepsi negatif terkait dengan agama dan politik dan menciptakan perpecahan antar-masyarakat.

Masalah lain yang juga merupakan bagian dari kejahatan siber dan sudah umum terjadi adalah masalah pencurian data online. Secara sederhana pencurian data online dapat dipahami sebagai tindakan kejahatan siber yang menggunakan media teknologi untuk mengambil data publik ataupun data pribadi seseorang dengan tujuan menyebarkan, menjual dan atau menggunakannya untuk tujuan yang ilegal. Sejalan dengan hal ini (Lee, 2013) menjelaskan bahwa pencurian data online adalah ketika peretas mencuri informasi pribadi berharga dari seseorang melalui penggunaan serangan siber. Sementara itu penejelasan yang hampir sama oleh (Holt, 2013) yang mengatakan bahwa pencurian data online adalah tindakan peretas yang mendapatkan informasi pribadi pelanggan dan menjualnya kembali untuk mendapatkan keuntungan besar di forum internet. Penjelesan lebih kompleks tentang hal tersebut dijelaskan Banks (2015) yang mengatakan bahwa pencurian data online adalah kebocoran data yang tidak disengaja maupun pengumpulan informasi yang disengaja, melalui peretasan atau rekayasa sosial, dari database digital dan bentuk data sosioteknik. Dengan demikian pencurian data online dapat dipahami adalah tindakan peretasan secara ilegal untuk tujuan ilegal untuk mendapatkan keuntungan dari data yang dicuri secara online. Dari hal ini mengartikan bahwa potensi kebocoran data online sangat besar mengingat pesatnya teknologi saat ini, bagaimanapun keamanan siber ditingkatkan maka akan selalu ada potensi kebocoran data. Menurut temuan Azkiya Dihni (2022) menemukan bahwa Indonesia mengalami kenaikan kebocoran data pada kuartal II 2022, di mana terdapat 1,04 juta akun yang mengalami kebocoran data pengguna di Indonesia, menurut data perusahaan keamanan siber Surfshark. Jumlah ini melonjak 143% dari kuartal I 2022 yang sebanyak 430,1 ribu akun. Ini hanya satu data yang menunjukkan kenaikan kasus kebocoran data, kasus lainnya cukup banyak yang akan dijelaskan pada bagian pembahasan.

Berdasarkan apa yang sudah dijelaskan di atas, dapat dipahami bahwa kejahatan siber merupakan masalah kompleks pada masa modern saat ini. Namun, Dalam semua contoh kasus dan penjelasan tersebut tidak semuanya akan dibahas dalam kajian ini. Ruang lingkup kajian ini hanya berfokus pada kasus pencurian data online sebagai kejahatan siber serta mengkaji kebijakan penggantian Kartu Tanda Penduduk (KTP) menjadi Identitas Kependudukan Digital (IKD), di mana argumen awal ini adalah adanya potensi besar pencurian data online yang mengancam data masyarakat apabila kebijakan ini dilaksanakan. Hal ini didukung dengan kasus kebocoran data yang pernah dialami oleh pemerintah Indonesia dan data-data pendukung lainnya. Berdasarkan hal tersebut maka pertanyaan utama kajian ini adalah mengapa kebijakan IKD tersebut belum layak diterapkan di Indonesia serta bagaimana sebetulnya potensi pencurian data online di Indonesia.

METODE PENELITIAN

Metode penelitian yang digunakan dalam riset ini adalah metode campuran atau *mixed methods*, di mana pendekatan penelitian ini menggabungkan atau mengasosiasikan bentuk kualitatif dan kuantitatif. Untuk mengatasi keterbatasan masing-masing pendekatan, penelitian metode campuran dan tinjauan studi campuran mengintegrasikan metode kuantitatif dan kualitatif, sehingga memberikan pengetahuan yang lebih menyeluruh tentang temuan studi (Pluye & Hong, 2014). Penelitian kualitatif melibatkan dengan mempelajari sifat suatu fenomena dengan menggunakan metode seperti penelitian dokumen, observasi non-partisipan, wawancara mendalam dan kelompok fokus (Busetto, Wick, & Gumbinger, 2020). Dalam hal ini Sumber data kualitatifnya menggunakan studi dokumen dan studi kasus yaitu dengan menganalisis semua jurnal maupun dokumen yang berhubungan dengan topik penelitian. Sementara sumber data kuantitatifnya adalah dengan data yang diperoleh dari hasil laporan orang lain yaitu analisis data sekunder. Analisis data sekunder adalah analisis data yang sudah ada sebelumnya, yang dapat digunakan untuk pekerjaan eksplorasi, konfirmasi, atau korelasional (Weston et al, 2019). Data sekunder mengacu pada data yang dikumpulkan oleh orang lain selain pengguna atau digunakan untuk tujuan tambahan selain tujuan aslinya (Pederson et al, 2020). Secara sederhana studi-studi tersebut menunjukkan bahwa data sekunder dalam penelitian statistik mengacu pada data yang dikumpulkan oleh orang lain untuk tujuan lain dan digunakan untuk analisis lebih lanjut, menjawab pertanyaan baru atau menambah sumber data lain.

HASIL DAN PEMBAHASAN

Pencurian Data Online sebagai Masalah Nyata di Indonesia

Berdasarkan apa yang sudah dijelaskan sebelumnya maka dapat ditarik sebuah pemahaman umum bahwa pencurian data online sebagai salah satu kejahatan siber. Kejahatan ini merupakan masalah nyata yang dihadapi oleh masyarakat di era modern saat ini. Dalam konteks Indonesia berbagai kasus kebocoran data telah terjadi dari pihak pemerintah maupun dari pihak swasta. Hal tersebut tidak dapat dianggap sepele karena pihak-pihak yang tidak bertanggung jawab menyalahgunakan data pribadi atau privat. Hal itu dapat merugikan bagi korban maupun organisasi yang menjadi target pencurian data online tersebut. Penyalahgunaan data yang dicuri seringkali digunakan untuk penipuan. Misalnya penipuan berskala besar (seperti *phishing* dan pencurian identitas), tindakan ilegal (seperti membeli dan menjual barang terlarang menggunakan data orang lain), dan serangan permusuhan (seperti sabotase dan penindasan siber misalnya *revenge porn*). Semua hal tersebut menggunakan data yang diperoleh melalui kejahatan siber yaitu pencurian data online. Hal ini sejalan dengan apa yang dijelaskan oleh (Zeid et al 2020) yang dalam penelitiannya menyatakan bahwa kejahatan siber menggunakan data yang dicuri untuk tujuan-tujuan ilegal, seperti membeli dan menjual barang dan jasa ilegal hingga menggunakannya untuk akses ke data pribadi pemerintah. Masih sejalan dengan ini (McMahon et al, 2016) juga memberikan penjelasan bahwa penipuan, pencurian identitas, pencurian data atau uang, penyebaran data seksual, serangan siber menggunakan virus (sabotase), dan bahkan penindasan di dunia maya seperti *bullying* adalah beberapa penggunaan yang mungkin digunakan untuk informasi yang dicuri.

Selain itu kejahatan siber juga dapat mengeksploitasi data yang dicuri untuk kegiatan ilegal seperti penipuan keuangan, pencurian identitas, dan spionase (Dolzhenkov et al, 2020). Bahkan dalam data yang ditemukan dalam (Brand, 2011) mengatakan bahwa setidaknya $388 miliar per tahun dapat dihasilkan melalui penggunaan trojan perbankan yaitu alat yang digunakan oleh penjahat siber untuk menghasilkan, mendistribusikan, dan memanen data keuangan untuk kemudian diambil uang dari data-data keuangan tersebut. Dalam konteks Indonesia praktik penjualan data ilegal hasil pencurian data online telah terjadi cukup lama, seperti data dalam (Halim & Galih, 2019) menemukan bahwa sebuah kasus yang melibatkan pembelian dan penjualan data kependudukan di situs web yang berisi jutaan kartu kredit, nomor rekening, nomor ponsel, KK, dan informasi pribadi lainnya terungkap pada tahun 2019. Bukan hanya itu kasus serupa juga terjadi, di mana hingga 374 terabyte data pribadi, termasuk KTP dan NPWP direktur perusahaan, diduga bocor dan dijual di pasar gelap pada tahun 2022, data tersebut berasal dari 21.000 perusahaan di Indonesia (BBC News Indonesia, 2022).

Semua hal ini tentunya mencerminkan bahwa pencurian data online merupakan kejahatan siber yang benar-benar nyata terjadi pada era modern yang serba digital saat ini. Tidak hanya itu, penjelasan-penjelasan tersebut juga menggambarkan bahwa ada potensi besar terjadinya kejahatan dalam lingkup digital. Hal tersebut bukan hanya bualan semata, ini dapat dibuktikan seperti apa yang ditemukan (Nurhayati-Wolff, 2023) menjelaskan bahwa Indonesia berada di peringkat ke-5 di dunia dalam hal jumlah serangan siber pada tahun 2022, dengan 38,4 juta serangan. Hal serupa juga ditemukan dalam data yang ditemukan oleh (Azkiya Dihni, 2022) yang berdasarkan data yang ditemukannya dari SAFEnet menunjukkan bahwa ada sekitar 193 insiden serangan siber di Indonesia melalui WhatsApp dan Instagram pada tahun 2021 lalu. Hal tersebut dapat diinterpretasikan bahwa masalah ini membutuhkan penanganan dan regulasi yang tepat, cepat, serta serius untuk mengatasi ancaman ini. Beberapa tindakan sebenarnya sedang dilakukan oleh pihak pemerintah Indonesia untuk mengatasi penyalahgunaan data curian seperti penjualan data yang sudah dijelaskan sebelumnya. Contohnya Kementerian Komunikasi dan Informatika telah menegaskan bahwa tindakan menjual dan menyalahgunakan data pribadi adalah bentuk pelanggaran hukum, dan mereka sedang menyiapkan regulasi terkait hal tersebut (KOMINFO, 2019). Meski demikian hal tersebut masih belum cukup karena masalah ini merupakan masalah yang kompleks dan membutuhkan berbagai pihak untuk ikut serta dalam mengatasi dan penanganannya secara komprehensif.

Kasus-kasus Kebocoran Data di Indonesia Sebagai Refleksi Lemahnya Perlindungan Data

Beberapa contoh selain kasus pencurian data online yang sudah dijelaskan sebelumnya yaitu kasus terjadinya pembobolan 1,3 miliar informasi pribadi pemilik kartu SIM, termasuk NIK, alamat, nomor kartu keluarga, dan nomor ponsel. Data dari 105 juta orang diduga dicuri dari basis data Komisi Pemilihan Umum (KPU) pada awal September 2022 (Yuliastuti & Liman, 2022). Kasus lain yakni pada 6 September 2022, Bjorka disebut telah membuka informasi pribadi masyarakat Indonesia, antara lain NIK, nomor kartu keluarga (KK), nama lengkap, tempat dan tanggal lahir, jenis kelamin, tempat tinggal, dan usia (Alfarizi, 2022). Kasus lainnya yaitu Kominfo mengakui pada bulan Juli 2022 bahwa mereka telah mengetahui adanya kebocoran data paspor yang diduga melibatkan 34.900.867 warga negara Indonesia (Alfarizi, 2022). Kasus lainnya yang pernah dialami Indonesia adalah tiga kasus pembobolan data, satu melibatkan data PLN yang melibatkan 17 juta pelanggan, satu lagi melibatkan data Indihome, dan yang terbaru melibatkan 1,3 miliar data registrasi kartu SIM prabayar ini terjadi pada bulan Agustus 2022 (Anisah, 2022). Tidak hanya itu rupanya Indonesia adalah negara dengan kebocoran data tertinggi ke-13 di dunia. Ini dapat dilihat dari kebocoran data alamat email yang terjadi sejak 2004 dengan 143,7 juta akun di Indonesia. Jumlah ini juga meningkat 85% dalam dua kuartal terakhir (Pahlevi, 2023). Kemudian selain itu pihak polri juga mengatakan bahwa pada tahun 2022 periode 1 Januari sampai 22 Desember kejahatan siber meningkat, hal tersebut diperlihatkan dari data penindakan kasus kejahatan siber sebanyak 8.831 (Pusiknas Bareskrim Polri, 2022).

Bercermin dari data serta kasus-kasus di atas, menggambarkan bahwa masalah kejahatan siber dalam kasus pencurian data online adalah masalah bahkan pihak yang memiliki sumber daya besar yaitu pemerintah saja belum cukup mampu melindungi data-data masyarakat dengan baik. Hal tersebut sejalan dengan apa yang dijelaskan oleh (BBC News Indonesia, 2021) yang mengatakan bahwa para pakar siber menjelaskan situs-situs pemerintahan Indonesia tergolong sangat mudah dibobol, kemudian para pakar tersebut juga mengatakan bahwa ini mencerminkan bahwa infrastruktur keamanan digital Indonesia masih dalam kategori buruk dan hal tersebut diperlukan regulasi yang tepat seperti Undang-Undang Perlindungan Data Pribadi (UU PDP) dan turunannya guna kepastian hukum.

Lemahnya Perlindungan Data di Indonesia

Kasus-kasus kebocoran data yang banyak tersebut juga mencerminkan lemahnya perlindungan data di Indonesia (Christine, 2021). Berbagai kasus juga dapat mencerminkan bahwa masih ada kekurangan yang signifikan dalam keamanan siber di Indonesia, meskipun dalam data yang ditemukan dalam (BSSN.go.id, 2022) menjelaskan bahwa *International Telecommunication Union* (ITU) telah mengeluarkan *Global Cybersecurity Index* (GCI), yang menempatkan Indonesia di

posisi ke-24 dari 194 negara dalam hal keamanan siber. Indonesia memiliki skor indeks keamanan siber sebesar 94,88. Setelah Singapura dan Malaysia, Indonesia berada di peringkat ketiga di ASEAN dan peringkat keenam di Asia Pasifik dalam skala regional. Namun, semua hal tersebut tetap sia-sia karena tidak dapat dipungkiri dalam hal menangani permasalahan kejahatan siber dalam konteks ini khususnya pencurian data online Indonesia tetaplah belum mampu dan belum cukup memadai dalam melindungi diri dari ancaman serangan kejahatan siber.

Hal tersebut pun dijelaskan dan didukung oleh (Saputra & Ghifari 2023) yang mengatakan bahwa masyarakat tidak puas dengan kinerja Badan Siber dan Sandi Negara karena dianggap tidak mampu mengamankan informasi pribadi warga negara Indonesia. Masih sejalan dengan hal tersebut (Setiyawan, 2019) juga menjelaskan hal yang sama yaitu bahwa karena peraturan yang tidak memadai dan sudut pandang yang ketinggalan zaman tentang bahaya siber, Indonesia belum mampu merespons serangan siber secara efektif.

Faktor-Faktor Penyebab Ketidakmampuan Indonesia dalam Menangani Serangan Kejahatan Siber

Dapat ditarik sebuah penalaran umum bahwa ketidakmampuan Indonesia dalam menangani serangan kejahatan siber adalah karena kurangnya regulasi kebijakan hukum yang tepat yang mengatur hal tersebut. Kurangnya kolaborasi antar-instansi serta sumber daya manusia yang belum memadai. Hal tersebut diperkuat oleh penelitian (Mulyadi, & Rahayu, 2018) yang menjelaskan bahwa karena kurangnya rencana, tata kelola, hukum, dan peraturan, serta kurang-nya koordinasi antara entitas pemerintah, keamanan siber nasional Indonesia belum ditangani dengan baik. Pandangan yang sama juga disampaikan oleh (Saputra, 2016) yang menjelaskan bahwa ketiadaan kebijakan keamanan siber yang tepat di Indonesia membuat masalah ini menjadi serius. Berangkat dari penjelasan-penjelasan tersebut dapat diinterpretasi-kan bahwa permasalahan ini adalah masalah kompleks dan sangat dibutuhkan regulasi yang benar dalam mengatasi kegagalan yang terjadi.

Berangkat dari apa yang sudah dijelaskan sebelumnya terkait kasus-kasus dan penjelasan mengapa kejahatan siber dapat dikatakan belum dapat diatasi oleh Indonesia secara optimal karena masih belum efektifnya regulasi yang mengatur bidang tersebut. Selain itu, sumber daya manusia Indonesia masih kurang. Kemudian infrastruktur teknologi bidang tersebut di negara ini juga masih terbilang belum cukup memadai. Hal ini sejalan dengan apa yang dikatakan oleh (Candra et al, 2021) yang memberikan pandangan bahwa meskipun Indonesia telah mengambil langkah-langkah proaktif untuk melindungi kepentingan dan tujuannya dalam keamanan siber, Indonesia masih menghadapi berbagai kendala seperti kurangnya infrastruktur teknologi, sumber daya manusia, dan persiapan regulasi. Dalam hal SDM, salah satu yang membuat pencurian data dengan mudah terjadi juga adalah karena kurangnya kesadaran masyarakat awam akan pentingnya menjaga data pribadi tetap terjaga dengan baik.

Namun sayangnya masyarakat Indonesia dari data yang ditemukan masih kurang paham akan hal tersebut. Hal ini ditunjukkan oleh data yang diperoleh dalam (Saptoyo & Galih, 2022) yang menjelaskan bahwa Hampir setengah dari 1.014 responden di 34 provinsi di Indonesia yang berpartisipasi dalam penelitian Litbang Kompas pada akhir Januari 2022 tidak memahami pentingnya perlindungan data pribadi dalam aktivitas digital. Sebanyak 46,5% responden mengatakan bahwa mereka tidak menyadari pentingnya aktivitas online sebagai sumber data, termasuk jejaring sosial, belanja, dan browsing. 67,9% peserta mengatakan bahwa mereka tidak pernah memperbarui kata sandi di akun online mereka. 22,4% responden mengatakan bahwa ketika memasukkan informasi pribadi ke dalam sistem atau aplikasi digital, mereka tidak membaca syarat dan ketentuan yang berkaitan dengan keamanan data. Dari mereka yang disurvei, 59% mengatakan bahwa mereka tidak pernah memverifikasi keamanan aplikasi di ponsel mereka. Masih sejalan dengan data tersebut data lain yang oleh (Azkiya Dihni, 2022) juga turut mendukung hal tersebut di mana berdasarkan hasil temuannya bahwa jumlah korban serangan siber pada tahun 2021 warga biasa menduduki peringkat kedua sebanyak 34 orang terkena. Berdasarkan data-data ini mencerminkan bahwa kesadaran akan pentingnya menjaga data pribadi sendiri pun masih sangat rendah pada masyarakat Indonesia. Hal ini ditambah dengan tidak adanya regulasi kebijakan hukum yang tepat maka potensi pencurian data online Indonesia sangatlah besar. Hal tersebut selaras dengan apa yang dijelaskan dalam (Desiana & Prima, 2022) bahwa kerentanan Indonesia

terhadap serangan siber semakin meningkat, dikarenakan peraturan Keamanan Siber Maritim yang terbatas dan sosialisasi keamanan sosial di antara organisasi pemerintah masih sangat kurang. Tidak hanya itu dalam hal SDM yang memiliki keahlian dalam bidang keamanan siber pun masih terbilang sangat kurang. Hal ini diperkuat oleh data yang diambil dari (Tanujaya, 2023) yang menjelaskan bahwa Indonesia masih kekurangan sumber daya manusia di bidang keamanan siber, dengan hanya 0,4 orang per 100.000 penduduk yang memiliki sertifikat keamanan siber.

Relevansi Kasus terhadap Kebijakan IKD

Berbagai kasus kebocoran data dapat dilihat bahwa Indonesia masih dalam kategori negara yang memiliki penangkalan rendah terhadap kejahatan siber. Secara khusus terkait dengan kebocoran data termasuk pencurian data online. Berangkat dari data-data yang sudah dijabarkan dan kasus-kasus pencurian data online di Indonesia dapat ditarik sebuah pemahaman bahwa penerapan kebijakan penggantian Kartu Tanda Penduduk (KTP) menjadi Identitas Kependudukan Digital (IKD) di Indonesia adalah bukan langkah yang tepat. Perlu dikaji ulang. Hal tersebut dilihat dari kasus-kasus sebelumnya yang mencerminkan kegagalan pemerintah dalam melindungi data masyarakat Indonesia. Kemudian kegagalan-kegagalan dalam berbagai kasus juga membuat masyarakat kecewa akan perlindungan yang diberikan oleh negara terkhusus perlindungan data mereka. Sejalan dengan hal ini, data yang ditemukan dalam (Muhamad, 2023) mengatakan bahwa menurut penelitian Kurious-Katadata Insight Center (KIC), 62,6% partisipan mengatakan bahwa mereka memiliki keraguan terhadap keamanan siber dari fasilitas penyimpanan data yang dimiliki pemerintah Indonesia. Terkait dengan Identitas Kependudukan Digital (IKD) sebagai contoh bahwa masyarakat masih belum percaya pemerintah mampu melindungi data mereka. IKD di Jogja saat ini hanya 1,68% masyarakatnya sudah membuat, sisanya tidak, karena alasan kasus kebocoran data sebelumnya (Ramadhan, 2023).

Kekhawatiran masyarakat yang tercermin dari data tersebut memang wajar jika melihat dari kegagalan pihak pemerintah melindungi data masyarakat dari berbagai data kasus yang ada. Hal ini juga mencerminkan bahwa pemerintah Indonesia belum optimal dan belum sepenuhnya serius dalam menangani fenomena ini. Senada dengan hal tersebut (Stevani & Sudirman, 2021) menjelaskan hal serupa yaitu bahwa sulit bagi aparat penegak hukum untuk melakukan perlindungan data pribadi seefektif mungkin karena pemerintah Indonesia tidak sepenuhnya memahami relevansinya. Pandangan yang sama juga diberikan oleh (Wibowo, 2018) yang mengatakan bahwa keamanan siber di Indonesia secara umum dapat dikatakan masih kurang mendapat perhatian dari pemerintah dan penyedia layanan publik. Hal tersebut memang selaras dengan belum adanya regulasi hukum yang baik dari pihak pemerintah.

Tidak hanya itu jika kebijakan penggantian Kartu Tanda Penduduk (KTP) menjadi Identitas Kependudukan Digital (IKD) di Indonesia diterapkan sepenuhnya hal tersebut memerlukan berbagai pertimbangan, meskipun sekarang kebijakan tersebut tidak serta merta meng-hilangkan penggunaan KTP. Namun, tetaplah perlu mempertimbangkan berbagai hal seperti keterbatasan akses teknologi karena penggunaan IKD ini menggunakan basis teknologi smartphone penting memastikan bahwa semua masyarakat memiliki teknologi tersebut karena ada kemungkinan beberapa daerah terpencil tidak memilikinya. Menurut data (Badan Pusat Statistik, 2023) mengatakan berdasarkan statistik yang dikumpulkan oleh Survei Susenas pada tahun 2022, 66,48 persen orang Indonesia menggunakan internet pada tahun tersebut, naik dari 62,10 persen pada tahun 2021. Selanjutnya, pada tahun 2022 tercatat 67,88 persen orang Indonesia memiliki ponsel. Meskipun demikian pihak yang belum memiliki akses teknologi digital bukan berarti dibiarkan begitu saja, tentunya hal tersebut juga harus diperhatikan dan diberikan solusi yang baik apabila kebijakan IKD tersebut diterapkan secara menyeluruh. Menurut temuan data yang dilaporkan *We Are Social*, Indonesia adalah negara dengan jumlah penduduk terbesar ketujuh di dunia yang tidak memiliki akses internet. Hingga Oktober 2023 tercatat sebanyak 93,2 juta penduduk Indonesia tidak memiliki akses internet. Angka ini mewakili 33,5% dari keseluruhan populasi Indonesia (Mutia Annur, 2023).

Hal tersebut menggambarkan pesatnya teknologi di Indonesia memang sudah cukup tinggi, tetapi belum merata sepenuhnya. Hal ini tentunya penting diperhatikan jika kebijakan IKD tadi dilaksanakan. Kemudian penting pula memastikan keamanan data yang kuat untuk mencegah

terjadinya kebocoran data dan penyalahgunaan data karena data yang tersimpan dalam format digital tersebut. Jika kebijakan tersebut harus berjalan maka keamanan siber haruslah ditingkatkan karena jika dilihat dari kasus-kasus dan data yang sudah disedikan sebelumnya, seluruhnya menandakan bahwa keamanan siber dalam hal menjaga data tidak dicuri secara online. Seluruhnya mengarah pada kesimpulan bahwa hal tersebut masih sangat lemah dan sangat belum optimal dari segi regulasi maupun infrastruktur serta SDM yang belum mumpuni.

Dengan demikian kesadaran pendidikan digital bagi masyarakat terkait pentingnya keamanan data, dan ketersediaan infrastruktur yang merata seperti jaringan yang stabil serta penerimaan yang positif dari masyarakat menjadi sangat krusial. Tidak hanya itu jika kebijakan IKD ini harus berjalan, kolaborasi antar-berbagai pihak menjadi poin kunci yang perlu disegerakan, hal tersebut selaras dengan apa yang dijelaskan oleh (Marune & Hartanto, 2021) bahwa untuk mengamankan informasi pribadi dan menjaga ketahanan siber di Indonesia, kolaborasi antar kementerian, lembaga, institusi pemerintah, sektor komersial, dan pemangku kepentingan lainnya sangatlah penting. Dengan demikian jika bercermin dari kasus-kasus dan data terjadinya pencurian data online atau kebocoran data di Indonesia maka kebijakan pergantian Kartu Tanda Penduduk (KTP) menjadi Identitas Kependudukan Digital (IKD) di Indonesia bukanlah langkah yang tepat selama keamanan siber Indonesia masih rendah. Namun jika regulasi kebijakan tersebut harus dijalankan maka faktor-faktor yang sudah dijelaskan sebelumnya harus dipertimbangkan dan ditangani dengan solusi yang benar-benar konkret.

KESIMPULAN

Secara keseluruhan dari apa yang sudah dijelaskan sebelumnya, maka dapat ditarik sebuah kesimpulan bahwa kejahatan siber yang dalam konteks ini berfokus pada pencurian data di Indonesia masih membutuhkan peningkatan yang signifikan. Hal tersebut dapat dicapai salah satunya melalui pengembangan regulasi kebijakan hukum yang konsisten dan optimal serta berdaya guna. Kemudian untuk masyarakat dapat memahami pentingnya keamanan data dengan adanya sosialisasi mengenai langkah-langkah keamanan data untuk mengurangi risiko pencurian data online atau kebocoran data.

Pencurian data online menjadi masalah yang signifikan bagi Indonesia berdasarkan temuan dan perdebatan. Banyaknya kasus kebocoran data dari sumber swasta, pemerintahan maupun publik yang telah terjadi menunjukkan bahwa insiden-insiden ini mendeskripsikan kerentanan keamanan siber Indonesia masih ada. Jika dilihat melalui data dan banyak kasus yang sudah dijelaskan, dapat dikatakan bahwa keamanan siber Indonesia khususnya dalam hal pencurian data online masih sangat lemah. Dengan demikian penguatan berbagai faktor untuk menguatkan dan melindungi data sangat diperlukan dan perlu disegerakan, terutama yang berkaitan dengan hukum, sumber daya manusia, dan kesadaran masyarakat. Kemudian, perlu juga dipikirkan secara serius mengenai implementasi kebijakan yang akan menggantikan KTP dengan Identitas Kependudukan Digital (IKD). Sebab melihat dari yang sudah dijelaskan sebelumnya langkah kebijakan tersebut memiliki potensi besar terjadinya pencurian data online atau kebocoran data. Perlu mempertimbangkan berbagai hal serta mengerjakannya secara optimal seperti kerangka kerja keamanan data yang kuat, infrastruktur yang memadai, dan kesadaran publik yang luas, serta kolaborasi antar-berbagai pihak diperlukan untuk menerapkan pendekatan ini.

Berdasarkan penjelasan yang diberikan, sejumlah rekomendasi untuk penelitian selanjutnya yang dapat dibuat untuk memberikan masukan dan rekomendasi yang lebih rinci. Penelitian tentang keefektifan peraturan keamanan siber di Indonesia dan penelitian tentang variabel-variabel yang memengaruhi kesadaran masyarakat dan pemerintah akan pentingnya perlindungan data pribadi sangat diperlukan. Selanjutnya, penelitian tentang bagaimana kebijakan penggantian KTP menjadi Identitas Kependudukan Digital (IKD) memengaruhi keamanan informasi pribadi individu. Kemudian yang masih relevan dengan kejahatan siber adalah diperlukan penelitian tentang kebijakan rupiah digital yang memiliki potensi besar dalam terjadinya kejahatan siber.

DAFTAR PUSTAKA

Alfarizi, M. K. (2022). Cybersecurity Expert Confirms Validity of 105 Mln Leaked Indonesians Data. Tempo. https://en.tempo.co/read/1631831/cybersecurity-expert-confirms-validity-of-105-mln-leaked-indonesians-data

Alfarizi, M. K. (2022). Kominfo Clarifies Alleged Breach of 1.3 Million SIM Card Data. Tempo. https://en.tempo.co/read/1629410/kominfo-clarifies-alleged-breach-of-1-3-million-sim-card-data

Anisah, L. (2022). DPR Keluhkan Kebocoran Data Pribadi, Kominfo Mengaku Tak Bisa Bekerja Lebihi Wewenang. Kontan. https://nasional.kontan.co.id/news/dpr-keluhkan-kebocoran-data-pribadi-kominfo-mengaku-tak-bisa-bekerja-lebihi-wewenang

Azkiya Dihni, V. (2022). Kasus Kebocoran Data di Indonesia Melonjak 143% pada Kuartal II 2022. Databoks. https://databoks.katadata.co.id/datapublish/2022/08/09/kasus-kebocoran-data-di-indonesia-melonjak-143-pada-kuartal-ii-2022.

Azkiya Dihni, V. (2022). Serangan Digital di Indonesia Meningkat Sepanjang 2021, Siapa Saja Korbannya? Databoks Katadata. https://databoks.katadata.co.id/datapublish/2022/03/28/serangan-digital-di-indonesia-meningkat-sepanjang-2021-siapa-saja-korbannya

Banks, J. (2015). The Heartbleed bug: Insecurity repackaged, rebranded, and resold. *Crime, Media, Culture: An International Journal*, 11, 259 - 279. https://doi.org/10.1177/1741659015592792.

BBC News Indonesia. (2021). Data eHAC bocor, pakar siber sebut 'Infrastruktur keamanan digital pemerintah Indonesia sangat buruk'. https://www.bbc.com/indonesia/indonesia-58406164

BBC News Indonesia. (2022). Dokumen Rahasia dari 21.000 Perusahaan di Indonesia Dilaporkan Bocor, 'Ini Bisa Jadi Alat Penipuan'. https://www.bbc.com/indonesia/majalah-62603873

Badan Pusat Statistik. (2023). Statistik Telekomunikasi Indonesia 2022 (Nomor Katalog: 8305002; Nomor Publikasi: 06300.2313; ISSN/ISBN: 2476-9134). Tanggal Rilis: 31 Agustus 2023. Dapat diakses melalui https://www.bps.go.id/id/publication/2023/08/31/131385d0253c6aae7c7a59fa/statistik-telekomunikasi-indonesia-2022.html

Brand, M. (2011). FORENSIC RECOVERY AND ANALYSIS OF THE ARTEFACTS OF CRIMEWARE TOOLKITS. . https://doi.org/10.4225/75/57B2B94E40CE8.

Broadhurst, R. (2017). Cybercrime: Thieves, Swindlers, Bandits and Privateers in Cyberspace. *Legal Perspectives in Information Systems eJournal*. https://doi.org/10.2139/ssrn.3009574.

BSSN.go.id. (2022). Indeks Keamanan Siber Indonesia Peringkat Ke-24 dari 194 Negara di Dunia. https://www.bssn.go.id/indeks-keamanan-siber-indonesia-peringkat-ke-24-dari-194-negara-di-dunia/

Busetto, L., Wick, W., & Gumbinger, C. (2020). How to use and assess qualitative research methods. *Neurological Research and Practice*, 2. https://doi.org/10.1186/s42466-020-00059-z.

Candra, A., Suhardi, S., & Persadha, P. (2021). INDONESIA FACING THE THREAT OF CYBER WARFARE: A STRATEGY ANALYSIS. *Jurnal Pertahanan: Media Informasi ttg Kajian & Strategi Pertahanan yang Mengedepankan Identity, Nasionalism & Integrity*. https://doi.org/10.33172/jp.v7i3.1424.

Chandra, A., & Snowe, M. (2020). A taxonomy of cybercrime: Theory and design. *Int. J. Account. Inf. Syst.*, 38, 100467. https://doi.org/10.1016/j.accinf.2020.100467.

Christine, B. (2021). Mandate of Procurement of Independent Commission for Personal Data Protection In Indonesia Reviewed from International Legal Instruments. *International Journal of Social Service and Research*. https://doi.org/10.46799/ijssr.v1i2.21.

Desiana, R., & Prima, S. (2022). Cyber security policy in Indonesian shipping safety. *Journal of Maritime Studies and National Integration*. https://doi.org/10.14710/jmsni.v5i2.13673.

Dolzhenkova, E., Mokhorov, D., & Baranova, T. (2020). National and International Issues of Cyber Security. IOP Conference Series: Materials Science and Engineering, 940. https://doi.org/10.1088/1757-899X/940/1/012015.

Dulkiah, M. (2023). Social Trust and Fake News: Study Among College Students in West Java, Indonesia [Kepercayaan Sosial dan Berita Palsu: Studi di Kalangan Mahasiswa di Jawa Barat, Indonesia]. *JCIC: Jurnal CIC Lembaga Riset dan Konsultan Sosial,* 5(1), 1-12. https://doi.org/10.51486/jbo.v5i1.81

Finneman, T., & Thomas, R. (2018). A family of falsehoods: Deception, media hoaxes and fake news. *Newspaper Research Journal*, 39, 350 - 361. https://doi.org/10.1177/0739532918796228.

Gupta, P., & Mata-Toledo, R. (2016). Cybercrime: In Disguise Crimes. *Journal of Information Systems and Operations Management*, 10, 1-10.

Haeranah, M., Mirzana, H., Azisa, N., & Nurdin, A. (2022). REVIEW OF CRIMINAL PROVISIONS OF FAKE NEWS (HOAX) BASED ON LEGISLATION IN INDONESIA. *Awang Long Law Review*. https://doi.org/10.56301/awl.v5i1.538.

Halim, D., & Galih, B. (2019). "Ini 6 Fakta Terkait Kasus Jual-Beli Data Kependudukan di Situs Web". Kompas.com. https://nasional.kompas.com/read/2019/08/16/08291671/ini-6-fakta-terkait-kasus-jual-beli-data-kependudukan-di-situs-web

Haryono, W. H. Legiani, & M. Carolina. (2023). The Social Construction of Reality: Junior High School Students Brawl in Balaraja Tangerang [Konstruksi atas Realitas Sosial Tawuran Antar-Pelajar Sekolah Menengah Atas di Balaraja, Kabupaten Tangerang]. *JCIC: Jurnal CIC Lembaga Riset dan Konsultan Sosial,* 5(1), 13-20. https://doi.org/10.51486/jbo.v5i1.75

Holt, T. (2013). Exploring the social organisation and structure of stolen data markets. *Global Crime*, 14, 155 - 174. https://doi.org/10.1080/17440572.2013.787925.

Jo, B. (2023). Kisah Anak Kelas 6 SD Hilang, Dijual, dan Diperkosa di Bandung. tirto.id. https://tirto.id/gTCJ

KOMINFO. (2019). Pernyataan BRTI Mengenai Praktik Jual Beli Data Pribadi. Siaran Pers No. 102/HM/KOMINFO/05/2019. https://www.kominfo.go.id/content/detail/18778/siaran-pers-no-102hmkominfo052019-tentang-pernyataan-brti-mengenai-praktik-jual-beli-data-pribadi/0/siaran_pers

Lee, N. (2013). Personal Information Management. , 159-168. https://doi.org/10.1007/978-1-4614-5308-6_12.

Mauluddin, A., & Royandi E. (2023). Sosiologi Kriminalitas. Bandung: Widina Bhakti Persada.

Marune, A., & Hartanto, B. (2021). Strengthening Personal Data Protection, Cyber Security, and Improving Public Awareness in Indonesia: Progressive Legal Perspective. *International Journal of Business, Economics, and Social Development*. https://doi.org/10.46336/ijbesd.v2i4.170.

McMahon, R., Bressler, M., & Bressler, L. (2016). New Global Cybercrime Calls for High Tech Cyber-Cops. *Journal of Legal, Ethical and Regulatory Issues*, 19, 26.

Muhamad, N. (2023). Mayoritas Masyarakat Tidak Yakin dengan Tingkat Keamanan Siber di Indonesia. Databoks. https://databoks.katadata.co.id/datapublish/2023/08/10/mayoritas-masyarakat-tidak-yakin-dengan-tingkat-keamanan-siber-di-indonesia

Mulyadi, & Rahayu, D. (2018). Indonesia National Cybersecurity Review: Before and After Establishment National Cyber and Crypto Agency (BSSN). *2018 6th International Conference on Cyber and IT Service Management (CITSM)*, 1-6. https://doi.org/10.1109/CITSM.2018.8674265.

Mutia Annur, C. (2023). Indonesia Negara ke-7 dengan Populasi Terbanyak yang Tak Terhubung Internet. Databoks Katadata. Dapat diakses melalui https://databoks.katadata.co.id/datapublish/2023/11/24/indonesia-negara-ke-7-dengan-populasi-terbanyak-yang-tak-terhubung-internet

Nua, F. (2021). 60% Kasus Eksploitasi Anak Lewat Medsos, Pemerintah Harus Proaktif. Media Indonesia. https://mediaindonesia.com/humaniora/403223/60-kasus-eksploitasi-anak-lewat-medsos-pemerintah-harus-proaktif

Nurhayati-Wolff, H. (2023). Cybersecurity and Cybercrime in Indonesia - Statistics & Facts. Statista. https://www.statista.com/topics/11732/cybersecurity-and-cybercrime-in-indonesia/#topicOverview

Pahlevi, R. (2023). Cek Data: Gibran Singgung Pencurian Data, Indonesia Negara ke-13 dengan Kebocoran Tertinggi. Databoks. https://databoks.katadata.co.id/datapublish/2023/12/22/cek-data-gibran-singgung-pencurian-data-indonesia-negara-ke-13-dengan-kebocoran-tertinggi

Pederson, L., Vingilis, E., Wickens, C., Koval, J., & Mann, R. (2020). Use of secondary data analyses in research: Pros and Cons. , 6, 058-060. https://doi.org/10.17352/2455-3484.000039.

Pluye, P., & Hong, Q. (2014). Combining the power of stories and the power of numbers: mixed methods research and mixed studies reviews.. *Annual review of public health*, 35, 29-45 . https://doi.org/10.1146/annurev-publhealth-032013-182440.

Pusiknas Bareskrim Polri. (2022). Kejahatan Siber di Indonesia Naik Berkali-kali Lipat. https://pusiknas.polri.go.id/detail_artikel/kejahatan_siber_di_indonesia_naik_berkali-kali_lipat

Ramadhan, A. (2023). Capaian IKD di Kota Jogja Masih 1,68 Persen, Pemkot Yogyakarta Jamin Keamanan Data. Tribunnews. https://jogja.tribunnews.com/2023/09/20/capaian-ikd-di-kota-jogja-masih-168-persen-pemkot-yogyakarta-jamin-keamanan-data#:~:text=Septi%20mengungkapkan%2C%20standar%20keamanan%20data%20IKD%20dilengkapi%20dengan,oleh%20orang%20lain%20di%20samping%20si%20pemilik%20identitas.

Salaverría, R., Buslón, N., López-Pan, F., León, B., López-Goñi, I., & Erviti, M. (2020). Desinformación en tiempos de pandemia: tipología de los bulos sobre la Covid-19. *Profesional De La Informacion*, 29. https://doi.org/10.3145/epi.2020.may.15.

Saputra, D. D., Munifah, N. F., & Pramesty, L. A. (2023). Pelanggaran Privasi Dalam Program Realita Investigasi Polisi di Indonesia: Ancaman, Kebijakan, Dan Kebutuhan Pembaruan [Privacy Breach in Police Investigation Reality Program in Indonesia: Threats, Policy, and The Need For Reform]. *JCIC: Jurnal CIC Lembaga Riset dan Konsultan Sosial*, 5(1), 29-38. https://doi.org/10.51486/jbo.v5i1.85

Saputra, R., & Ghifari, W. (2023). STRATEGI HUMAS DALAM MEMPERTAHANKAN CITRA BSSN PASCA TERJADINYA KEBOCORAN DATA. *Paradigma: Jurnal Masalah Sosial, Politik, dan Kebijakan*. https://doi.org/10.31315/paradigma.v27i1.8619.

Saputra, R. (2016). A survey of cybercrime in Indonesia. *2016 International Conference on ICT For Smart Society (ICISS)*, 1-5. https://doi.org/10.1109/ICTSS.2016.7792846.

Saptoyo, R. D. A., & Galih, B. (2022). KABAR DATA: Kesadaran Keamanan Data Pribadi Masyarakat dalam Angka. Kompas.com. https://www.kompas.com/cekfakta/read/2022/02/10/090900082/kabar-data-kesadaran-keamanan-data-pribadi-masyarakat-dalam-angka

Setiyawan, A. (2019). The Urgency of Defining Indonesia's National Critical Infrastructure. , 6, 164. https://doi.org/10.25134/unifikasi.v6i2.1673.

Stevani, W., & Sudirman, L. (2021). Urgensi Perlindungan Data Pengguna Financial Technology terhadap Aksi Kejahatan Online di Indonesia. *Journal of Judicial Review*. https://doi.org/10.37253/JJR.V23I2.5028.

Tanujaya, A. (2023). Statistik Kejahatan Siber di Indonesia Selama 2023. Detik.com. https://inet.detik.com/security/d-7054249/statistik-kejahatan-siber-di-indonesia-selama-2023

Tendiyanto, T., Istiqamah, D. T., & Suwandoko. (2023). Perlindungan Pelaku Usaha Jual Beli Online dengan Sistem Pembayaran Cash on Delivery [Ecommerce Seller Protection with Cash on Delivery Payment System]. *JCIC: Jurnal CIC Lembaga Riset dan Konsultan Sosial*, 5(1), 39-44. https://doi.org/10.51486/jbo.v5i1.89

Weston, S., Ritchie, S., Rohrer, J., & Przybylski, A. (2019). Recommendations for Increasing the Transparency of Analysis of Preexisting Data Sets. *Advances in Methods and Practices in Psychological Science*, 2, 214 - 227. https://doi.org/10.1177/2515245919848684.

Wibowo, S. (2018). Enriching Digital Government Readiness Indicators of RKCI Assessment with Advance Https Assessment Method to Promote Cyber Security Awareness Among Smart

Cities in Indonesia. *2018 International Conference on ICT for Smart Society (ICISS)*, 1-4. https://doi.org/10.1109/ICTSS.2018.8549974.

Yuliastuti, N., & Liman, U. (2022). PDP Bill Ratification Urged Amid Rising Reports of Data Breach. Antara News. https://en.antaranews.com/news/249889/pdp-bill-ratification-urged-amid-rising-reports-of-data-breach

Zeid, R., Moubarak, J., & Bassil, C. (2020). Investigating The Darknet. *2020 International Wireless Communications and Mobile Computing (IWCMC)*, 727-732. https://doi.org/10.1109/IWCMC48107.2020.9148422.