TEKNOBIS : Teknologi, Bisnis Dan Pendidikan
Volume 3, No. 3, Tahun 2025
ISSN 3024-8256 (media online)
Hal 429-435

Kelemahan Keamanan Sistem Perpajakan Pemerintahan Indonesia Studi Kasus : Kasus Pembobolan Data Nomor Pokok Wajib Pajak (NPWP) Bjorka (2024)

Jevon Bryant Tanyones[1], Yazid Ilham[2], Abila Saputra[3], Isal Guntur Saputra [4], Annisa Elfina Augustia[5]

[1-5]Fakultas Teknik dan Ilmu Komputer, Teknik Informatika, Universitas Indraprasta PGRI, Jakarta ,Indonesia
Email :[1]jek777inmyside@gmail.com, [2]yazidilham174@gmail.com, [3]abilasaputra0407@gmail.com, [4]isalguntur.19@gmail.com, [5]annisa12elfina@gmail.com

Abstrak−Penelitian ini menganalisis sistem keamanan cyber di Indonesia yang dimana dalam pembahasan ini di bidang perpajakan. Kita mengambil studi kasus dari pencurian data Nomor Pokok Wajib Pajak (NPWP) oleh oknum Bjorka yang sedang hangat belakangan ini karena dapat mengungkapkan banyak rahasia - rahasia besar di instansi pemerintahan Indonesia ,pada september 2024 6 juta data penduduk Indonesia Nomor Pokok Wajib Pajak (Nomor Pokok Wajib Pajak (NPWP)) di curi dan dipublikasikan ke dalam situs ilegal. Hal ini sangat berbahaya dan bukan hanya penduduk biasa saja namun juga para pejabat tinggi sampai mantan Presiden Joko Widodo juga terkena waktu itu.Dengan menerapkan metode hukum normatif dan dievaluasi kasus empiris, penelitian ini mengungkap berbagai faktor utama, seperti kurangnya fasilitas teknologi, rendahnya tingkat ketahanan cyber secara menyeluruh (dengan nilai rata-rata global sekitar 65,7 dari 100, meskipun Indonesia mencapai nilai tinggi di beberapa aspek), dan kesalahan dalam faktor manusia (human error) juga membuka peluang baik besar maupun kecil bagi serangan luar. Temuan utama ini mengungkap bahwa kejadian tersebut mengakibatkan penurunan rasa percaya masyarakat, berkurangnya kesediaan mematuhi kewajiban pajak, dan ancaman stabilitas ekonomi akibat publikasi informasi rahasia yang luas. Melalui lensa akuntansi perilaku, konsep atribusi dan model kepercayaan institusional menggambarkan bagaimana kegagalan internal di Direktorat Jenderal Pajak (DJP) semakin memperlemah pandangan publik terhadap perlindungan data nasional. Untuk mengatasi hal ini, penelitian ini menyarankan langkah-langkah penanggulangan dan pencegahan seperti penegakan tegas Undang-Undang Perlindungan Data Pribadi, pemeriksaan keamanan berkala, serta kerjasama antarinstansi guna mengurangi potensi ancaman mendatang. Temuan-temuan ini menjadi arahan esensial bagi para pengambil keputusan untuk meningkatkan daya tahan infrastruktur digital negara ini.

Kata Kunci: Keamanan digital; perpajakan Indonesia; peretasan Bjorka; kebocoran data; keamanan Cyber; kepatuhan wajib pajak; *human error*.

Abstract−*This study analyzes the cyber security system in Indonesia, specifically in the field of taxation. We take a case study of the theft of Nomor Pokok Wajib Pajak or Taxpayer Identification Number (Nomor Pokok Wajib Pajak (NPWP)) by Bjorka, which has been a hot topic lately because it revealed many big secrets in Indonesian government agencies. In September 2024, 6 million Indonesian citizens' Nomor Pokok Wajib Pajak (NPWP) data was stolen and published on an illegal website. This was very dangerous and affected not only ordinary citizens but also high-ranking officials, including former President Joko Widodo. By applying normative legal methods and evaluating empirical cases, this study reveals several key factors, such as a lack of technological facilities, a low overall level of cyber resilience (with a global average score of around 65.7 out of 100, although Indonesia scored highly in some aspects), and human error, which opens up both large and small opportunities for external attacks. These key findings reveal that these incidents resulted in a decline in public trust, reduced willingness to comply with tax obligations, and threats to economic stability due to the widespread publication of confidential information. Through the lens of behavioral accounting, the concepts of attribution and institutional trust models illustrate how internal failures at the directorate Direktorat Jenderal Pajak or General of Taxes (DJP) has further weakened public confidence in national data protection. To address this, this study recommends mitigation and prevention measures such as strict enforcement of the Personal Data Protection Law, regular security checks, and inter-agency cooperation to reduce potential future threats. These findings provide essential guidance for decision makers to improve the resilience of the country's digital infrastructure.*

Keywords: *Digital security; Indonesian taxation; Bjorka hacking; data leaks; cyber security; taxpayer compliance; human error.*

1. PENDAHULUAN

Seperti yang kita tahu saat ini sudah memasuki era digital, banyak aspek dalam kehidupan yang selama ini kita tahu sudah berubah dengan pesat mulai dari sistem transaksi, komunikasi,

TEKNOBIS : Teknologi, Bisnis Dan Pendidikan
Volume 3, No. 3, Tahun 2025
ISSN 3024-8256 (media online)
Hal 429-435

transportasi, dan lain sebagainya. Perpajakan juga tidak luput dari hal ini seperti pembayaran pajak digital secara online maupun offline sudah menggunakan *smartphone* (gawai pintar) dan juga komputer.

Namun di Indonesia sistem keamanan dari perpajakan kita masih sangat kurang dalam bidang digitalnya karena masih minimnya kesadaran dan biaya yang disiapkan untuk hal ini. Lalu mayoritas masyarakat belum memahami tentang peraturan wajib pajak karena dari pemerintah sendiri kurang mensosialisasikan tentang wajib pajak itu sendiri. Padahal wajib pajak penting untuk menaikan taraf dan kualitas hidup suatu negara, pada era digitalisasi ini banyak orang dituntut untuk memahami teknologi dan juga akibat wabah Coronavirus Disease - 2019 (COVID-19), teknologi sangat berkembang pesat beberapa tahun ini.

Kita bisa lihat banyak sekali pekerjaan dibidang perpajakan digantikan oleh sistem otomatis ataupun komputer namun perkembangan tersebut tidak diimbangi dengan sosialisai yang benar maka masyarakat justru mengalami kesulitan ketika melakukan pembayaran wajib pajak. Karena itu banyak ancaman negara baru muncul dan penanggulangannya belum terencana, pada kasus ini Nomor Pokok Wajib Pajak (NPWP) warga negara menjadi sasaran para pelaku tindak kriminalitas di bidang siber.

Pada sistem perpajakan ada istilah *official assessment*, ini merupakan salah satu sistem yang meletakan wajib pajak ke posisi yang lemah dan pasif dimana semua mengikuti perintah dan ketentuan dari fiskus (pejabat atau pegawai pemerintah). Hal ini menyebabkan penyelewengan dana pajak sehingga tidak terbuka dan transparansinya kurang, karena hal itu anggaran untuk mengamankan data secara digital tidak maksimal, banyak sekali kelemahan yang timbul dalam sistem digital yang ada di dunia perpajakan yang bisa dimanfaatkan para tindak pelaku kriminalitas siber untuk membobol, lalu tim khusus pengamanan juga tidak dibuat guna menanggulangi dan mencegah hal ini.

2. METODE PENELITIAN

2.1. Pendekatan dan Jenis Penelitian

Metode yang dipakai dalam kasus ini adalah kualitatif deskriptif karena penelitian ini bertujuan menggambarkan dan menjelaskan suatu fenomena kasus yang ada di dalam pembobolan data Nomor Pokok Wajib Pajak (NPWP) di perpajakan. Metode ini dipilih karena fokus penelitian ini terjadi pada kisah nyata, lalu kita ingin melihat bagaimana respon pemerintahan terhadap kejadian ini serta penanggulangan apa yang disiapkan untuk hal ini, selain itu data numerik yang digunakan dalam penelitian ini tidak banyak dan rumit. Kualitatif deskriptif berfokus pada proses pemaknaan realitas, bukan pengujian hipotesis atau generalisasi statistik (Creswell, 2016).

2.2. Objek dan Sumber Data

Pengumpulan data yang dilakukan dalam penelitian ini menggunakan metode observasi non-partisipatif dan dokumen yang ada digital. Peneliti mencari jurnal, artikel, dan berita yang ada serta media berupa video pada sosial media tentang wawancara dengan pakar dan pegawai pajak, dokumen dan video yang dianalisis memiliki kualifikasi sebagai berikut :

a. Memiliki sumber dan penulisan yang jelas.
b. Narasumber yang menguasai bidangnya.
c. Video yang diterbitkan dari pihak terverifikasi.
d. Video yang memiliki 100.000 sampai 500.000 penonton.
e. Terdapat tanggapan rakyat yang jelas di dalam video atau artikel tersebut.
f. Terdapat instansi yang bersangkutan dalam kasus tersebut.
g. Terdapat dampak dan akibat dari kasus tersebut.

Semua data tersebut disimpan dalam bentuk pdf, video unduhan guna menghindari hilang atau terhapusnya artikel tersebut dari jejak digital.

2.3. Uji Keabsahan Data

Uji keabsahan data dalam hal ini menggunakan empat poin yang penting menurut Lincoln & Guba (1985), kredibilitas, transferabilitas, dependabilitas, dan konfirmabilitas. Kredibilitas ini dibuktikan melalui triangulasi sumber data, lalu transferabilitas dibuktikan dengan mendeskripsikan

TEKNOBIS : Teknologi, Bisnis Dan Pendidikan
Volume 3, No. 3, Tahun 2025
ISSN 3024-8256 (media online)
Hal 429-435

penelitian secara terperinci, dependabilitas dan konfirmabilitas dibuktikan dengan menjaga konsistensi dalam prosedur penelitian yang ada serta memberikan bukti konkrit terkait sumber-sumber yang dipakai.

3. ANALISA DAN PEMBAHASAN

Dalam penelitian ini mendapatkan banyak sekali fakta dan pembahasan-pembahasan yang sangat penting dalam penelitian ini, mulai dari tanggapan presiden kita pada waktu itu yaitu Jokowi mengatakan, "Saya sudah perintahkan Kementerian Komunikasi dan Digital (Komdigi) maupun Menteri Keuangan untuk mitigasi secepatnya, termasuk Badan Siber dan Sandi Negara (BSSN). dan peristiwa ini juga terjadi di negara - negara lainnya. Semua data itu mungkin karena keteledoran password atau karena penyimpanan data yang banyak di tempat-tempat yang berbeda yang bisa menjadi ruang untuk diretas atau disusupi oleh hacker yang ada" KOMPAS TV (2024), hal tersebut juga langsung ditanggapi oleh menteri keuangan pada saat itu yaitu Sri Mulyani, "Saya sudah minta Pak Dirjen Pajak dan seluruh pihak di Kementerian Keuangan untuk melakukan evaluasi terhadap persoalan ini" CNN INDONESIA (2024).

Namun dari tanggapan ini belum ada yang mengusulkan tindakan kepada masyarakat yang terdampak dalam 6 juta data bocor tersebut. Hal ini kita bahas lebih dalam lagi pada poin-poin pembahasan yang ada serta penanggulangan dan respon dari banyak pihak yang terkait dalam kasus tersebut serta dampak dan bagaimana nasib data tersebut.

3.1. Kurangnya Kesadaran Pemerintahan dalam Perlindungan Data

Dalam poin ini analisis yang didapatkan adalah pemerintahan sangat kurang dalam menyadari perkembangan digital dalam beberapa tahun ini, melihat kasus sebelum perpajakan juga terdapat kasus instansi pemerintah lainnya yang disusupi oleh *malware* yang mengakibatkan data sebagian pemerintahan rusak dan tidak dapat dipakai lagi. Namun hal ini belum juga menjadikan pelajaran yang sangat perlu dievaluasikan dalam ancaman negara, jika kita lihat pemerintah hanya fokus pada fasilitas non digital sedangkan fasilitas digital cenderung tidak diperhatikan dan dinomor duakan oleh sebagian orang.

Namun sikap kesadaran pemerintahan akan perlindungan data secara digital adalah salah satu dari banyak nya faktor-faktor lain terjadinya pencurian data. Menurut ketua dari Lembaga Riset Keamanan Siber dan dan Komunikasi Communication and Information System Security Research Centre (CISSReC), keamanan siber indonesia sangatlah jauh dari kata aman karena pada serangan pertama kali di institusi pusat data nasional yang diserang secara habis-habisan oleh *hacker* dari pihak pemerintah nampak belum sungguh-sungguh menanggapi ancaman tersebut sehingga timbul serangan-serangan baru secara serentak.

Dibandingkan dengan instansi swasta, sistem yang ada di lembaga pemerintahan cukup mudah diretas bahkan dari salah satu pendiri Ethical Hacker Indonesia yang bernama Teguh Aprianto mengatakan, "Website pemerintah itu memang website yang paling buruk. Kaya ngebobol mereka itu butuh sekian menit doang," ujar Teguh (CNN Indonesia, 2021). Hal ini membuktikan bahwa keamanan sistem indonesia sangatlah rentan. Bahkan lebih parahnya lagi terdapat kasus penangkapan seorang pemuda berinisial MAA yang ditangkap karena adanya dugaan ilegal siber yang dilakukan oleh pemuda tersebut, namun orang tuanya membantah dan menghubungi pihak kompas.com untuk meminta dan mengeluarkan pernyataan yaitu, "Dia bukan orang jahat. Dia tidak berniat menghancurkan atau merusak website Komisi Pemilihan Umum (KPU) tersebut. Sebelumnya dia sudah memberitahukan kelemahan website itu kepada pemerintah" ujar Nila (Kompas, 2019).

Ini merupakan salah satu contoh mengapa sikap pemerintahan menjadi tidak acuh / peduli terhadap sistem keamanan siber yang ada di indonesia hingga saat ini belum ada kelanjutan mengenai fasilitas dan bentuk nyata yang ditunjukan oleh pemerintahan dalam mencegah atau menanggulangi hal ini.

3.2. Lemahnya Sistem pada Keamanan Digital Perpajakan

Poin ini berfokus pada sistem keamanan Digital Perpajakan itu sendiri dimana kita melihat dan menganalisis kekurangan sistem pada keamanan digitalisasi perpajakan serta langkah apa yang

TEKNOBIS : Teknologi, Bisnis Dan Pendidikan
Volume 3, No. 3, Tahun 2025
ISSN 3024-8256 (media online)
Hal 429-435

diambil pada saat terjadi serangan tersebut oleh *hacker* berinisial Bjorka yang sudah lama menjadi dalang peretasan dari mulai tahun 2022 hingga sekarang.

Namun kita berfokus pada serangan yang terjadi di tahun 2024 dimana data Nomor Pokok Wajib Pajak (NPWP) Direktorat Jenderal Pajak (DJP) bocor ke tangan Bjorka dan tidak hanya masyarakat biasa saja, sekelas pejabat dan presiden ikut menjadi korban pada saat serangan ini terjadi. Kita perlu tahu bahwa pada saat serangan itu terjadi apa dan dalam bentuk apa sistem keamanan website tersebut. Dari sumber CPO Magazine mengatakan bahwa keamanan pada saat serangan belum terdapat autentifikasi, dan kontrol akses sangatlah lemah, hal ini menyebabkan *hacker* bisa masuk dengan mudah melalui celah ini lalu merusak dan mengambil alih situs secara penuh. Selain hal tersebut ada data sensitif belum terenkripsi yang menyebabkan para *hacker* dapat membaca data-data tersebut dengan mudah (Antara News, 2024), perlu kita ketahui enkripsi adalah hal yang sangat penting dalam menyimpan data-data krusial (sensitif), dengan adanya enkripsi proses pencurian data bisa menjadi sangat sulit atau bahkan menggagalkan pencurian tersebut. Namun keamanan Direktorat Jenderal Pajak (DJP) belum menggunakan enkripsi pada saat itu sehingga data yang tercuri dengan mudahnya dibaca oleh *hacker*.

Selain enkripsi komunikasi antar lembaga sangatlah kurang, hal ini dapat menyebabkan koordinasi pengamanan data dari Badan Siber dan Sandi Negara (BSSN) menjadi tidak maksimal menurut penelitian ini bisa menjadi hal yang sangat krusial bagi keamanan data tersebut bahkan backup data yang dilakukan oleh mereka juga tidak sepenuhnya bisa mengembalikan atau memulihkan data yang sudah dicuri atau dirusak oleh *hacker*. Namun tidak semua kekurangan pengamanan dari pihak Direktorat Jenderal Pajak (DJP) kurang maksimal ada juga tindakan yang menurut peneliti sudah cukup awal pengamanan walaupun tidak seratus persen aman yaitu memisahkan data ke banyak tempat penyimpanan walaupun ini juga bisa menyulitkan *user* itu sendiri namun langkah tersebut bisa dibilang cukup sebagai langkah awal pengamanan data.

Namun itu merupakan faktor internal dari pihak perpajakan ada juga faktor dimana masyarakat kurang mendapatkan edukasi tentang digitalisasi perpajakan tentang aplikasi yang seharusnya memudahkan masyarakat dalam membayar pajak justru membuat rakyat merasa kesulitan kita akan bahas hal ini lebih lanjut dalam poin ketiga penelitian jurnal ini.

3.3. Dampak Kepercayaan Masyarakat Terhadap Instansi Pemerintahan

Seperti di poin sebelumnya kita akan membahas tentang dampak dari kasus tersebut ke masyarakat terhadap instansi pemerintahan, kepercayaan masyarakat terhadap pemerintahan suatu negara merupakan suatu hal yang krusial atau penting maka dari itu pemerintah juga harus menjaga rasa percaya tersebut dengan segala upaya dan juga meningkatkan rasa percaya masyarakat akan keamanan berwarga negara di suatu negara. Tanpa adanya rasa percaya suatu negara bisa hancur bahkan dijajah karena rakyatnya sendiri bisa memberontak atau mempunyai kemungkinan saling mengkhianati demi kepentingannya sendiri, pemerintahan sebagai lembaga yang mengatur jalannya suatu negara harus bisa memberikan itu semua kepada rakyatnya demi berjalannya sistem pemerintahan suatu negara.

Kasus ini membuat banyak sekali penurunan rasa kepercayaan masyarakat kepada instansi pemerintahan karena dianggap kurang kompeten dalam menjaga data diri setiap warga negara, dari kasus Bjorka warga juga bisa melihat kelemahan dan tidak kesiapan negara tidak bisa mengikuti era digitalisasi yang sedang berjalan dengan cepat. Pada tahun 2020 merupakan titik balik dari era digitalisasi dengan cepat hingga tahun 2025 sekarang, teknologi berkembang dengan cepat sekali dimulai dengan munculnya teknologi bernama *artificial Intelligence (AI)* di tahun 2022 yang merupakan awal rilisnya *chat GPT* ini menjadi sangat heboh dimana ia bisa menjawab banyak hal meskipun tidak secanggih tahun 2025 sekarang.

Dengan ada nya teknologi ini pemerintah seharusnya bisa lebih memanfaatkan nya namun pemerintah justru hanya memandang hal tersebut sebelah mata. Menurut Teguh Aprianto situs pemerintahan kerap kali menjadi tempat bermain *hacker* pemula karena dinilai sangat mudah untuk diretas. Dari pernyataan tersebut masyarakat menjadi turun kepercayaannya kepada pemerintahan yang ada, karena berulang kali data kita bocor oleh satu oknum yang berinisial Bjorka dan dijual belikan secara bebas di situs ilegal dengan harga yang sangat kecil.

Masyarakat juga meminta jawaban dan kepastian pemerintahan indonesia terkait hal-hal yang ada, namun dari pihak pemerintah hanya memberikan pernyataan bias dan terkesan kurang

TEKNOBIS : Teknologi, Bisnis Dan Pendidikan
Volume 3, No. 3, Tahun 2025
ISSN 3024-8256 (media online)
Hal 429-435

menanggapi hal ini dengan serius. Dimana pada waktu data Nomor Pokok Wajib Pajak (NPWP) dan Nomor Induk Kependudukan (NIK) tercuri, yang langsung ditindak hanyalah milik mantan presiden yaitu Jokowi dan para pejabat yang memiliki kedudukan tinggi dalam pemerintahan, lalu nasib masyarakat hanya diminta jangan panik dan meminta agar akun Nomor Pokok Wajib Pajak (NPWP) mereka untuk dinonaktifkan secara mandiri (KOMPAS, 2024).

Hal ini sangatlah disayangkan karena seharusnya bisa dicegah dan ditanggulangi dengan baik namun menjadi sangat kurang dalam kedua hal tersebut, selain itu mengembalikan rasa percaya masyarakat cukup sulit dan tidak mudah kerana itu sampai hari ini masyarakat juga belum percaya pemerintahan secara penuh dan juga dilansir dari Tempo (2025) sosok yang diduga Bjorka sudah tertangkap namun hal tersebut sangatlah kurang benar karena pada waktu setelah penangkapan Bjorka masih aktif dalam akun sosial media yang biasanya digunakan dan sempat menyindir para polisi karena salah tangkap *hacker* tersebut, dari situ masyarakat mulai meragukan lebih lagi tentang kemampuan kinerja pemerintahan dan lembaga-lembaga yang ada.

3.4. Langkah dan Respon Penanggulangan Pemerintah Terhadap Data yang Bocor

Peneliti melakukan analisis ini terhadap hal apa saja yang dilakukan pemerintahan pada saat kasus tersebut terjadi, pada waktu kejadian tersebut terpublikasi pemerintah langsung dibanjiri oleh wartawan untuk memberi pernyataan resmi terkait kejadian tersebut karena kejadian tersebut cukup dekat pada kasus-kasus lainnya yang pada saat itu masih juga menjadi topik hangat dalam pembicaraan media massa dimana itu kasus instansi pemerintahan banyak dibanjiri oleh serangan-serangan *hacker* yang sangat mengancam keamanan negara.

Pemerintah langsung mengeluarkan pernyataan terkait kasus tersebut masih diselidiki oleh para Direktorat Jenderal Pajak (DJP) dan Badan Siber dan Sandi Negara (BSSN) terkait benar atau tidaknya kasus tersebut (Kompas, 2024), lalu Presiden Jokowi pada saat itu langsung wartawan dari kompas menanyakan hal tersebut kepada Jokowi lalu beliau mengatakan bahwa tindakan yang dilakukan ialah meminta Badan Siber dan Sandi Negara (BSSN) dan Direktorat Jenderal Pajak (DJP) untuk segera memitigasi data-data yang ada serta meminta menteri keuangan pada saat itu Sri Mulyani untuk mengevaluasi kejadian ini (Kompas, 2024).

Lalu Sri Mulyani mengeluarkan pernyataan pada jumpa pers yaitu beliau meminta para Direktorat Jenderal Pajak (DJP) untuk mengevaluasi kejadian ini dan segera berkomunikasi dengan pihak Badan Siber dan Sandi Negara (BSSN). Namun menurut Dr. Pratama Dahlian Persadha pemerintah kurang berpartisipasi dalam kasus kejadian ini karena sudah banyak kejadian *hacker* yang menyerang situs lembaga pemerintahan dan mencuri data bahkan merusak situs atau data tersebut (Kompas, 2024). Dan juga pada saat kasus itu terjadi akun Nomor Pokok Wajib Pajak (NPWP) presiden dan pejabat langsung dinonaktifkan oleh pihak Direktorat Jenderal Pajak (DJP) namun dari masyarakat hanya diberikan himbauan untuk tidak termakan penipuan yang mengaku dari pihak perpajakan indonesia. Hal ini sangatlah disayangkan karena masyarakat terlihat justru menjadi opsi yang tidak diutamakan oleh pemerintahan. Selain itu Dr. Pratama Dahlian Persadha mengatakan bahwa seharusnya pemerintah menetapkan undang-undang resmi terkait perlindungan data namun undang-undang tersebut lebih condong tajam ke pihak swasta saja tidak ke instansi negara yang dimana seharusnya lebih bisa menjaga data diri kita.dan pemerintah juga melakukan hal yang terkesan tidak masuk akal yaitu mengeluarkan pernyataan terbuka yang sangat kontroversial dari lembaga Kementerian Komunikasi dan Digital (Komdigi) dimana pada saat itu situasi sedang genting, pernyataan tersebut ialah “kalo bisa *hacker*, jangan menyerang” hal ini diucapkan oleh Semuel Abrijani Pangerapan (SUARA.COM).

Dari hal ini kita bisa membuat poin-poin utama hal apa saja yang dilakukan oleh pemerintahan pada saat kejadian tersebut ada.

1. Pemerintah langsung meminta para lembaga Direktorat Jenderal Pajak (DJP) dan Badan Siber dan Sandi Negara (BSSN) untuk mengevaluasi kebenaran kasus tersebut.
2. Pemerintahan langsung meminta Direktorat Jenderal Pajak (DJP) dan Badan Siber dan Sandi Negara (BSSN) mengevaluasi kinerja mereka.
3. Pemerintahan langsung meminta Direktorat Jenderal Pajak (DJP) dan Badan Siber dan Sandi Negara (BSSN) memitigasi data yang ada.
4. Badan Direktorat Jenderal Pajak (DJP) dan Badan Siber dan Sandi Negara (BSSN) menonaktifkan Nomor Pokok Wajib Pajak (NPWP) presiden dan pejabat negara.

TEKNOBIS : Teknologi, Bisnis Dan Pendidikan
Volume 3, No. 3, Tahun 2025
ISSN 3024-8256 (media online)
Hal 429-435

5. Badan Direktorat Jenderal Pajak (DJP) dan Badan Siber dan Sandi Negara (BSSN) meminta masyarakat untuk tidak panik dan memberikan himbauan agar tidak terjerat penipuan oleh oknum yang mengaku dari pihak Direktorat Jenderal Pajak (DJP).
6. Kementerian Komunikasi dan Digital (Komdigi) mengeluarkan pernyataan yang kontroversial di depan publik.

3.5. Pencegahan Pemerintah Terhadap Keamanan Digital Perpajakkan

Pemerintah Indonesia telah melakukan berbagai langkah strategis dalam memperkuat keamanan digital, khususnya pada sistem perpajakan yang menjadi tulang punggung pendapatan negara. Pencegahan terhadap potensi kebocoran dan serangan siber dilakukan melalui kombinasi kebijakan regulatif, peningkatan infrastruktur digital, serta penerapan prinsip keamanan berlapis *(multi-layer security*).

Secara regulatif, sejumlah payung hukum telah diterbitkan sebagai dasar penguatan keamanan digital nasional. Di antaranya adalah Undang-Undang Nomor 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik (ITE), Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik, serta Peraturan Presiden Nomor 82 Tahun 2022 mengenai Perlindungan Infrastruktur Informasi Vital. Kebijakan ini diperkuat dengan Peraturan Presiden Nomor 47 Tahun 2023 tentang Strategi Keamanan Siber Nasional yang diinisiasi oleh Badan Siber dan Sandi Negara (Badan Siber dan Sandi Negara (BSSN)). Melalui regulasi tersebut, pemerintah berupaya memastikan bahwa sistem digital, termasuk milik Direktorat Jenderal Pajak (DJP), memenuhi standar keamanan dan mitigasi risiko kebocoran data.

Pada tataran teknis, pemerintah menerapkan prinsip *Zero Trust Architecture* yang direkomendasikan Badan Siber dan Sandi Negara (BSSN). Pendekatan ini menekankan bahwa setiap akses pengguna, baik internal maupun eksternal, harus diverifikasi secara ketat tanpa mengandalkan kepercayaan otomatis. Penerapan *multi-factor authentication (MFA)*, enkripsi data wajib pajak, serta audit log akses sistem menjadi langkah konkret untuk mencegah kebocoran akibat pencurian kredensial atau penyalahgunaan akses administratif.

Selain itu, transformasi digital perpajakan yang dilakukan melalui proyek *Core Tax Administration System (CTAS)* juga menjadi bagian penting dalam penguatan keamanan. Sistem ini didesain dengan integrasi basis data yang lebih aman, mekanisme backup otomatis, serta sistem monitoring untuk mendeteksi aktivitas mencurigakan secara real-time. Tujuan akhirnya bukan hanya efisiensi layanan, tetapi juga memastikan bahwa informasi wajib pajak terlindungi dari ancaman siber.

Pemerintah juga mengedepankan pendekatan Sumber Daya Manusia (SDM) melalui pelatihan keamanan siber untuk pegawai pajak dan ASN terkait. Kesadaran keamanan *(security awareness)* menjadi faktor penting karena sebagian besar serangan siber justru memanfaatkan kelalaian manusia. Dalam konteks ini, pelatihan berkala dan pembentukan tim tanggap insiden *(Computer Security Incident Response Team/CSIRT)* di bawah koordinasi Badan Siber dan Sandi Negara (BSSN) menjadi langkah preventif yang signifikan.

Dengan langkah-langkah tersebut, dapat disimpulkan bahwa pencegahan pemerintah terhadap ancaman keamanan digital perpajakan mencakup tiga dimensi utama, yaitu:

1. Dimensi Regulatif: Pembentukan kerangka hukum dan kebijakan nasional keamanan siber.
2. Dimensi Teknis: Implementasi sistem keamanan berlapis, autentikasi kuat, dan pemantauan real-time.
3. Dimensi Manajerial: Peningkatan kompetensi Sumber Daya Manusia (SDM) dan pembentukan tim khusus tanggap insiden.

Namun demikian, efektivitas upaya pencegahan ini masih menghadapi tantangan seperti keterbatasan koordinasi antar-lembaga, infrastruktur digital yang belum seragam, serta masih rendahnya kesadaran keamanan di tingkat operasional. Oleh karena itu, langkah berkelanjutan berupa audit keamanan independen, peningkatan literasi digital, dan kolaborasi lintas sektor menjadi sangat penting untuk memperkuat kepercayaan masyarakat terhadap keamanan digital sistem perpajakan Indonesia.

TEKNOBIS : Teknologi, Bisnis Dan Pendidikan
Volume 3, No. 3, Tahun 2025
ISSN 3024-8256 (media online)
Hal 429-435

4. KESIMPULAN

Dari penelitian ini banyak yang bisa menjadi kesimpulan yang sangat menarik dimana melihat dari kinerja dan pencegahan, lalu apa saja dampak dari terjadinya kasus tersebut. Kesimpulan dari hal ini dimana kinerja pemerintah dalam mengamankan data-data yang krusial kerap kali kurang bisa menjaga dan tidak tidak bisa mengembalikan datanya,lalu banyak hal juga menjadi pembelajaran yang sangat penting seperti serangan-serangan yang bertubi-tubi di situs pemerintahan lalu juga kritikan - kritikan yang ada dalam wawancara oleh para ahli dimana situs pemerintah yang kemananannya cukup minim dan sangat mudah untuk diretas bahkan oleh peretas pemula sekalipun. Hal ini cukup menjadikan bukti bahwa pemerintah harus membuat kebijakan khusus demi keamanan data negara yang ada di digital. Lalu bagaimana juga kita bisa melihat kepercayaan masyarakat kepada pemerintahan cukup menurut drastis karena kasus - kasus ini, dimana ini sangatlah susah untuk pemerintah menaikan rasa percaya mereka kembali.data yang kita punya seringkali tidak terenkripsi dengan aman sehingga pemerintah perlu membenahi hal tersebut untuk dijadikan bahan evaluasi demi menjaga keamanan data negara kita. Dari kesimpulan ini bisa menjadikan acuan atau dasar kita untuk saling paham dan menjaga data diri kita di tengah pesatnya perkembangan era digitalisasi sehingga kita bisa aman lalu terhindar dari bahaya atau tindak kriminalitas, semoga kita semua lebih sadar akan kondisi kita dan bersikap kritis diera ini.

UCAPAN TERIMA KASIH

Penulis dan segenap peneliti mengucapkan rasa terima kasih sebesar-besarnya terhadap para jurnalis yang ada karena sudah meliput hal-hal yang diperlukan dalam melakukan penelitian ini dan juga para narasumber yang terdapat pada video yang ada karena memberikan informasi yang jelas dan rinci serta tidak melibatkan perasaan pribadi dalam pernyataan kepada publik. Lalu juga untuk para pejabat yang sudah berusaha semaksimal mungkin untuk memberikan keamanan kepada data negara. Dan juga tidak lupa kepada institusi yang memberikan fasilitas dan ruang akademik yang kondusif serta arahan yang jelas dalam penyelesaian penulisan karya ini. Semoga jurnal ini dapat menjadi acuan dan memberikan kontribusi secara ilmiah kepada para teknik informatika yang lainnya.

REFERENCES

Alshammari, R., & Alhassan, R. (2022). Zero trust architecture for cloud computing security: A systematic review. *Journal of Cloud Computing*, 11(1), 1–15. https://doi.org/10.1186/s13677-022-00300-7

ArsTechnica Indonesia. (2024, Maret 17). 6 juta data Nomor Pokok Wajib Pajak (NPWP) bocor termasuk milik Jokowi dan Sri Mulyani: Ini tanggapan Ditjen Pajak. Wantimpres. https://wantimpres.go.id/id/newsflows/6-juta-data-Nomor Pokok Wajib Pajak (NPWP)-bocor-termasuk-milik-jokowi-dan-sri-mulyani-ini-tanggapan-djpajak/

Badan Siber dan Sandi Negara. (2023, Mei 8). Penerapan Zero Trust sebagai Upaya Perlindungan dari Ancaman Serangan Siber. Sekretariat Kabinet Republik Indonesia. https://setkab.go.id/penerapan-zero-trust-sebagai-upaya-pelindungan-dari-ancaman-serangan-siber/

CPO Magazine. (2024, Maret 19). Indonesia's Tax Agency Data Breach Impacts 6 Million, Including President Widodo and His Cabinet. https://www.cpomagazine.com/cyber-security/indonesias-tax-agency-data-breach-impacts-6-million-including-president-widodo-and-his-cabinet/

Nugroho, A., & Pratama, Y. (2021). Analisis kebijakan perlindungan data pribadi di Indonesia: Tantangan dan peluang. *Jurnal Hukum & Pembangunan*, 51(3), 455–472. https://doi.org/10.21143/jhp.vol51.no3.3121

Putra, D. A., & Santoso, B. (2020). Cybersecurity readiness in Indonesian government institutions: A case study. *Proceedings of the 2020 International Conference on Information Technology Systems and Innovation (ICITSI)*, 1–6. IEEE. https://doi.org/10.1109/ICITSI50517.2020.9264942

Rahardjo, B., & Aprianto, T. (2023). Evaluating Indonesia's cybersecurity resilience against data breaches. *Indonesian Journal of Information Systems*, 8(2), 77–89. https://doi.org/10.24002/ijis.v8i2.5678

Susanto, H., & Chen, C. (2021). Cybersecurity policy implementation in Southeast Asia: Comparative study of Indonesia and Singapore. *Journal of Cyber Policy*, 6(2), 245–263. https://doi.org/10.1080/23738871.2021.1931234