REFORMULASI *PENETRATION STRESS TEST* SEBAGAI PERLINDUNGAN HUKUM DATA PRIBADI KONSUMEN DI ERA BISNIS DIGITAL

Abel Parvez*, Andi Vallian Superani, Muhammad Hasyim Anta Maulana*****
Fakultas Syariah dan Hukum, Universitas Islam Negeri Syarif Hidayatullah Jakarta
Jalan. Ir. H. Juanda No. 95, Tangerang Selatan, Banten, Indonesia

disampaikan Agustus 2022 – ditinjau April 2023 – diterima Juni 2023

Abstract

This research focus on consumer personal data protection as a part of invention from privacy right in digital era. The high number of consumer personal data utilization by electronic system operator not accompanied with decent penetration stress test (PST) regulation. The purpose of this research is to give solution to clear personal data protection problem through PST testing method. The method that used by this research is normative research through statutory approach and conceptual approach. The result from this research concludes that there are still many problematic PST regulation. The problem can be seen from personal data protection that shattered in 30 statutory from different sector with no one arrange PST comprehensively. This dispute culminates to emergence dissimilarity definition, overlapping authority between receiver of System Management Security Information certification annual report, and PST operator polemic. As the result, it causes rampant of personal data breach that inflict consumer by matter, along with specific data exploitation that lead to sluggish business and economic country. Therefore, PST testing reformulation is needed as prevention step to protect consumer personal data in digital business era.

***Keywords*:** *Digital Business; Penetration Stress Test; Personal Data Protection.*

Intisari

Penelitian ini fokus membahas perihal perlindungan hukum terhadap data pribadi konsumen sebagai bagian dari pemutakhiran hak privasi di era bisnis digital. Tingginya angka pemanfaatan data pribadi konsumen oleh penyelenggara sistem elektronik (PSE) tidak disertai dengan pengaturan pengujian *penetration stress test* (PST) yang baik. Tujuan penelitian ini adalah untuk memberikan solusi atas buruknya perlindungan

*Correspondence e-mail: abelparvezjustice@gmail.com
**Correspondence e-mail: andivallian@gmail.com
***Correspondence e-mail: maulanahasyim.31@gmail.com

data pribadi melalui metode pengujian PST. Metode penelitian yang digunakan adalah penelitian hukum normatif melalui pendekatan perundang-undangan dan pendekatan konseptual. Hasil penelitian menyimpulkan bahwa masih banyak problematika regulasi PST yang buruk. Salah satunya tampak pada pengaturan perlindungan data pribadi yang tersebar dalam 30 undang-undang di berbagai sektor, di mana tidak ada satu pun yang mengatur pengujian PST secara komprehensif. Persoalan tersebut, berujung pada munculnya ketidaksamaan definisi, tumpang tindih wewenang penerima laporan sertifikasi Sistem Manajemen Pengamanan Informasi (SMPI), dan polemik pihak penyelenggara PST. Akibatnya ialah maraknya kebocoran data pribadi yang merugikan konsumen secara materiil, serta eksploitasi data spesifik hingga bermuara pada lesunya bisnis dan perekonomian negara. Oleh karena itu, dibutuhkan reformulasi pengujian PST sebagai langkah preventif dalam melindungi data pribadi konsumen di era bisnis digital.

Kata Kunci: Bisnis Digital, *Penetration Stress Test*, Perlindungan Data Pribadi.

A. Latar Belakang Masalah

Hukum dalam perspektif *philosopica ratio* dengan sendirinya memuat nilai-nilai perlindungan Hak Asasi Manusia (selanjutnya disebut dengan HAM) sebagai *Conditio Sine Qua Non* (keadaan yang tidak bisa dipisahkan satu sama lain). Postulat tersebut selaras dengan pernyataan Jan Materson yang secara garis besarnya memaknai HAM sebagai nilai kodrati manusia yang tidak bisa diganggu gugat.[1] Selaras dengan pernyataan tersebut, terdapat salah satu turunan dari HAM yang harus dilindungi juga yaitu hak privasi. Hak privasi berfungsi membatasi intensitas interaksi panca indra seseorang,[2] di mana nilai dimilikinya juga berkaitan erat dengan hak milik pribadi[3] dan hak atas kebebasan individu.[4] Nilai fungsional yang memiliki keterikatan dengan hak-hak lainnya tersebut menjadi sangat vital, sehingga memerlukan perlindungan hukum (*rechtsbescherming*).

[1] Jan Materson, 2020, *Hukum dan Hak Asasi Manusia*, Mitra Wacana Media, Bogor, hlm. 62.
[2] Syafrizal, *et.al*., 2021 *Pengantar Ilmu Sosial*, Yayasan Kita Menulis, Medan,hlm. 180
[3] Russel Brown, "Rethinking Privacy", *Alberta Law Review*, Vol. 43, No. 589, 2006, hlm. 592
[4] Glenn Negley, "Philosophical Views on the Value of Privacy", *Law & Contemporary Problems Review*, Vol. 31, No. 319, 1966, hlm. 319.

Fungsi vital yang dimiliki hak privasi menjadi *ratio legis* perlindungan hukum secara langsung oleh negara sebagai pengemban tanggung jawab untuk penghormatan, perlindungan, dan pemajuan HAM. Konsekuensinya ialah negara tidak dapat lepas tangan pada pihak manapun.[5] Hal tersebut menjadi tanggung jawab konstitusional berdasarkan Pasal 28G Ayat 1 Undang-Undang Dasar Negara Republik Indonesia Tahun 1945 (selanjutnya disebut dengan UUD NRI Tahun 1945). Implikasi normatif dari pencantuman ini yaitu terlegitimasinya hak privasi sebagai hak konstitusional, sehingga menjadi mutlak insani sepanjang konstitusi mengaturnya.[6]

Pencantuman hak privasi dalam konstitusi menimbulkan kewajiban bagi negara untuk melindungi data pribadi sebagai hak privasi di era transformasi digital. Salah satu komponen yang terinternalisasi dalam transformasi digital adalah pengujian *Penetration Stress Test* (selanjutnya disebut dengan PST) sebagai tonggak perlindungan data pribadi (selanjutnya disebut dengan PDP). PST terdiri atas *penetration test* untuk uji kebobolan mencari kerentanan dalam sistem[7] dan *stress test* guna melihat ketahanan platform dari kegagalan sistem (*crash*).[8] Akan tetapi, formulasi regulasi PST yang berlaku sekarang tidak mencerminkan amanat Pasal 28G Ayat (1) UUD NRI Tahun 1945 sama sekali. Pasalnya, konstitusi mensyaratkan adanya perlindungan hukum guna mengarahkan pada ketertiban hidup manusia.[9]

Perlindungan hukum tidak terejawantahkan dalam regulasi yang berada di bawahnya secara paripurna. Hal itu disebabkan pengaturan PST yang masih parsial dan sektoral sehingga mengakibatkan tidak sistematis dan integral. Bentuk dari

[5] Sefriani dan Sri Wartini, "Corporate Social Responsibility Dan Tanggung Jawab Negara Terhadap Hak Ekonimi, Sosial, Dan Budaya Di Indonesia", *Jurnal Yustisia*, Vol. 4, No. 2, 2015, hlm. 284
[6] Osgar S Matompo, "Pembatasan Terhadap Hak Asasi Manusia Dalam Prespektif Keadaan Darurat", *Jurnal Media Hukum*, Vol. 21, No. 1, 2014, hlm. 64.
[7] Mohammed Chanine Ghanem and Thomas M Chen, "Reinforcement Learning for Efficient Network Penetration Testing", *Journal Information*, Vol. 11, No. 6, 2020, hlm. 1.
[8] Ni Luh Ayu Sonia Ginasari, kadek Suar Wibawa, dan Ni Kadek Ayu Wirdiani, "Pengujian Stress Testing API Sistem Pelayanan Dengan Apache JMeter," *Jurnal Ilmiah Teknologi Dan Komputer*, Vol. 2, No. 2, 2021, hlm. 2.
[9] Muchsin, 2003, *Perlindungan Dan Kepastian Hukum Bagi Investor*, Tesis, Magister Ilmu Hukum Program Pascasarjana Universitas Sebelas Maret, Surakarta, hlm. 14.

ketidaksistematisan tersebut meliputi ketidakjelasan pihak yang berhak menyelenggarakan PST dalam rangka sertifikasi, serta ketiadaan pengaturan pengujian keamanan platform Pasal 10 Ayat (1) Undang-Undang Nomor 19 Tahun 2016 perihal Informasi Transaksi Elektronik (selanjutnya disebut dengan UU ITE), serta ketiadaan pengaturan pengujian keamanan platform. Tidak komprehensifnya UU ITE menimbulkan cabang-cabang persamalahan seperti ketiadaan pengaturan lebih lanjut di aturan pelaksana mana pun, ketidaksamaan definisi, tumpang tindih wewenang penerima laporan sertifikasi Sistem Manajemen Pengamanan Informasi (selanjutnya disebut dengan SMPI), dan polemik pihak penyelenggara PST.

Kebobrokan regulasi PST yang sangat penting untuk menjamin PDP konsumen terlihat dari laporan Patroli Siber yang menunjukkan peningkatan kasus kebocoran data pribadi sebesar 810% sejak tahun 2016 hingga 2020.[10] Bila diakumulasikan total kasus serta kerugian sejak tahun 2015-2020, angka yang didapatkan sebesar 25.759 kasus dengan kerugian Rp. 5.050.000.000.000 triliun.[11] Terlebih, laporan terakhir yaitu pada tahun 2021 menunjukkan 12.152 kasus dengan total kerugian Rp. 3.880.000.000.000 triliun.[12] Perlu diketahui juga bahwa kasus kebocoran data pribadi konsumen dalam bisnis digital merupakan fenomena gunung es sehingga masih banyak hal yang mengancam para konsumen kedepannya.

Dampak dari buruknya PDP akibat PST yang tidak diatur dengan baik oleh hukum berimplikasi pada kerugian secara materi dan psikis terhadap konsumen bisnis digital. Selain itu, banyak PSE privat yang dibobol sistemnya oleh peretas sehingga

[10] Dwi Hadya Jayani, "Pencurian Data Pribadi Makin Marak Kala Pandemi", *https://databoks.katadata.co.id/datapublish/2021/09/07/pencurian-data-pribadi-makin-marak-kala-pandemi*, diakses tanggal 23 Januari 2022.
[11] Deky Paryadi, "Pengawasan E Commerce Dalam Undang-Undang Perdagangan Dan Undang-Undang Perlindungan Konsumen", *Jurnal Hukum Dan Pembangunan*, Vol. 48, No. 3, hlm. 657.
[12] Vika Azkiya Dihni, "Kerugian Akibat Kejahatan Siber Capai Rp 3,88 Triliun, Apa Saja Bentuknya?", *https://databoks.katadata.co.id/datapublish/2021/10/07/kerugian-akibat-kejahatan-siber-capai-rp-388-triliun-apa-saja-bentuknya*, diakses tanggal 23 Januari 2022.

aktivitas bisnis digital terganggu. Bila dilihat dari *magnus effectus* (efek besar), maka problematika ini berujung pada tercederainya perekonomian negara secara serius.

Berdasarkan problematika yang telah dipaparkan, polemik formulasi regulasi PST secara *mutatis mutandis* telah mengkhianati amanat konstitusi dan menderogasi hak privasi individu. Permasalahan tersebut menjadi sangat urgen untuk diteliti, sehingga menjadi perlu untuk dikaji lebih lanjut mengenai problematika perlindungan hukum data pribadi konsumen di era bisnis digital dan reformulasi *penetration stress test* sebagai ius constituendum dalam perlindungan data pribadi konsumen.

Adapun tujuan dalam penelitian ini ialah untuk memahami dan menganalisa problematika yuridis dari perlindungan hukum data pribadi konsumen di era bisnis digital dan untuk membuat rancangan yang tepat terkait rumusan regulasi *penetration stress test* yang berfungsi sebagai perlindungan preventif pada data pribadi konsumen karena memastikan kewajiban platform bisnis digital memang mampu mengelola data dengan aman yang ideal di Indonesia guna menghadapi permasalahan bisnis digital. Peneliti melakukan beberapa tinjauan terhadap penelitian-penelitian terdahulu yang relevan dengan problematika yang dibawa guna menciptakan *novelty* sehingga memberikan kontribusi pengembangan pengkajian perlindungan hukum terhadap data pribadi konsumen di era bisnis digital dimana beberapa penelitian tersebut di antaranya penelitian dengan berjudul "Perlindungan Hukum Atas Kebocoran Data Pribadi Konsumen Pada Perdagangan Elektronik Lokapasar (*Marketplace*)" oleh Kadek Dio Ramadi Natha dan rekan-rekannya,[13] penelitian berjudul "Perlindungan Hukum Data Pribadi Konsumen Dalam Platform E Commerce" oleh Ida Ayu Gede Artinia Cintia Purnami Singarsa,[14] dan penelitian berjudul "Perlindungan Hukum Terhadap Data

[13] Kadek Dio Ramadi Natha, I Nyoman Putu Budiartha, Ni Gusti Sri Astiti, 2022, "Perlindungan Hukum Atas Kebocoran Data Pribadi Konsumen Pada Perdangan Elektronik Lokapasar (*Marketplace*)", *Jurnal Preferensi Hukum*, Vol. 3, No.1, hlm. 143.
[14] Ida Ayu Gede Artinia Cintia Purnami Singarsa, 2021, "Perlindungan Hukum Data Pribadi Konsumen Dalam Platform E Commerce", *Jurnal Kertha Desa*, Vol. 9, No. 11, hlm. 81.

Pribadi Konsumen Dalam Transaksi e-Commerce" oleh Herdi Setiawan dan rekan-rekannya.[15] Semua penelitian tersebut berfokuskan pada permasalahan perlindungan hukum data pribadi konsumen di bisnis digital *e-commerce* yang masih belum komprehensif karena hanya diatur dalam Pasal 26 UU ITE serta ketiadaan pengaturan spesifik untuk perlindungan data pribadi.

Penelitian-penelitian terdahulu yang telah disinggung memiliki kesamaan dengan tulisan ini yaitu sama-sama membahas perlindungan hukum data pribadi konsumen di era bisnis digital dengan mempermasalahkan ketidakkomprehensifan hukum dalam UU ITE. Sedangkan perbedaannya ialah penelitian ini berfokuskan pada pengaturan *Penetration Stress Test* sebagai upaya perlindungan hukum preventif. Selain itu, terdapat penelitian terdahulu yang berjudul "Perlindungan Hukum terhadap Data Pribadi dalam Transaksi *E-Commerce*: Perspektif Hukum Islam dan Hukum Positif" oleh Parida Angriani.[16] Pada penelitian ini mengkaji perlindungan data pribadi dari perspektif antara hukum islam dan hukum positif dengan kajian utamanya ada pada UU ITE. Persamaan penelitian tersebut dengan tulisan ini ialah sama-sama mengkaji perlindungan hukum data pribadi dari UU ITE, sedangkan perbedaannya ialah tulisan ini tidak mengkaji dan menganalisa dari perspektif hukum islam, melainkan fokus pada perlindungan hukum secara preventif dengan pembaruan pengaturan *Penetration Stress Test*.

Terakhir, terdapat penelitian terdahulu yang berjudul "Perlindungan Hak Privasi atas Data Diri di Era Ekonomi Digital" oleh Ananthia Ayu di mana penelitiannya berfokuskan pada perbandingan hukum perlindungan privasi di era ekonomi digital

[15] Herdi Setiawan, Mohammad Ghufron AZ, Dewi Astutty, 2020, "Perlindungan Hukum Terhadap Data Pribadi Konsumen Dalam Transaksi e-Commerce", *MJL Merdeka Law Journal,* Vol. 1, No. 2, hlm. 102.
[16] Parida Angriani, 2021, "Perlindungan Hukum terhadap Data Pribadi dalam Transaksi E-Commerce: Perspektif Hukum Islam dan Hukum Positif", *DIKTUM: Jurnal Syariah dan Hukum*, Vol. 19, No. 2, hlm. 149.

antara Indonesia dengan Jerman.[17] Perbedaan penelitian tersebut dengan tulisan ini ialah tulisan ini tidak melakukan perbandingan hukum hak privasi dengan Jerman dan tidak luas dalam ranah privasi. Sedangkan persamaannya ialah sama-sama meneliti perlindungan hukum data pribadi di era digital.

B. Metode Penelitian

Jenis penelitian adalah penelitian hukum normatif. Penelitian ini adalah penelitian hukum dengan menempatkan hukum sebagai konstruksi sistem normatif dalam peraturan perundang-undangan.[18] Penelitian hukum normatif didasarkan pada topik hukum primer maupun hukum sekunder, yaitu penelitian yang berpatokan kepada kaidah atau yang terkandung dalam peraturan perundang-undangan.[19] Penelitian ini mengacu kepada pemecahan masalah (*problem solution*)[20] menggunakan pendekatan peraturan perundang-undangan (*statute approach*) dan pendekatan konseptual (*conceptual approach*)[21] mengacu kepada solusi permasalahan. *Statute approach*[22] dilakukan untuk mengkaji ketentuan hukum positif terkait Perlindungan Data Pribadi yang masih bersifat parsial dan sektoral di Indonesia. Sementara, *conceptual approach* dilakukan guna menemukan suatu pembenahan dan pembaharuan dalam menanggulangi permasalahan yang ada dan sedang dikaji, yaitu terkait konsep PST.

[17] Anathia Ayu D., Titis Anindyajati, Abdul Ghoffar, 2019, *Perlindungan Hak Privasi atas Data Diri di Era Ekonomi Digital*, Hasil Penelitian Pusat Penelitian Dan Pengkajian Perkara, Dan Pengelolaan Perpustakaan Kepaniteraan Dan Sekretariat Jenderal Mahakamah Konstitusi, hlm. 4-12.
[18] Amiruddin and Zainal Asikin, 2012, *Pengantar Metode Penelitian Hukum*, Ctk. Keenam, Rajawali Pers, Jakarta, hlm. 118.
[19] Soerjono Soekanto, 1984, *Pengantar Penelitian Hukum*, UI Press, Jakarta, hlm. 20.
[20] *Ibid*, hlm. 10.
[21] Johny Ibrahim, 2007, *Teori Dan Metodologi Penelitian Hukum Normatif*, Bayumedia, Malang, hlm. 391.
[22] Peter Mahmud Marzuki, 2008, *Penelitian Hukum*, Ctk. Kedua, Kencana, Jakarta, hlm. 96.

C. Hasil Penelitian dan Pembahasan

1. Problematika Perlindungan Hukum Data Pribadi Konsumen di era Bisnis Digital

Konstitusi secara filosofis telah memberikan garansi terhadap hak privasi sebagai bagian dari hak konstitusional warga negara. Aksioma tersebut telah terkristalisasikan dalam rumusan Pasal 28G Ayat (1) UUD NRI Tahun 1945 yang berbunyi:

> Setiap orang berhak atas perlindungan diri pribadi, keluarga, kehormatan, martabat dan harta benda yang di bawah kekuasaannya, serta berhak atas rasa aman dan perlidungan dari ancaman ketakutan untuk berbuat atau tidak berbuat sesuatu yang merupakan hak asasi.

Jaminan konstitusional ini merupakan bentuk pengadopsian nilai HAM universal ke dalam jantung normatif di Indonesia sehingga hukum positif di negara ini memiliki paradigma hak privasi yang sama dengan dunia.

Norma konstitusional di Indonesia bertalian erat dengan instrumen hukum internasional yang juga mengatur mengenai hak privasi (*privacy rights*), yakni pengaturan hak privasi dalam *Article* 12 *Universal Declaration of Human Rights* (selanjtnya disebut dengan UDHR).[23] Adapun *Article 12* UDHR berbunyi:

> *No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks.*

Narasi dalam Article 12 UDHR tersebut, kemudian diadopsi secara afirmatif oleh *Article 17 verse 1 International Convenant Civil and Political Rights* (selanjutnya disebut dengan ICCPR) yang substansinya secara garis besar sama.[24] Makna yang terkandung di dalamnya adalah jaminan atas perlindungan privasi terhadap individu dari segala penyerangan sewenang-wenang.

[23] Resolusi PBB No.G.A.Res. 217A (III)" (1948), *Article* 12 *Universal Declaration of Human Rights*, hlm. 4.
[24] Resolusi PBB No.G.A.Res. 2200A (XXI)" (2002)., *Article 17 verse 1 International Convenant Civil and Political Rights*, hlm. 10.

Tafsir terhadap *Article 12* UDHR dan *Article 17* ICCPR oleh Mahkamah Konstitusi melalui Putusan Nomor 50/PUU-VI/2008 tentang Perkara Pengujian Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik menjadi titik terang. Penafsiran terhadap kata "privasi" dalam putusan tersebut yang dimaknai sebagai urusan pribadi/masalah pribadi sebagaimana diatur dalam Pasal 28G Ayat 1 UUD NRI Tahun 1945.[25] Sehingga dalam hal ini, Negara berdasarkan amanat konstitusional wajib untuk menjaga dan melindungi hak atas privasi setiap warga negara.

Hak atas privasi selanjutnya berevolusi secara panjang sejak diakui sebagai bagian dari hak asasi manusia yang diatur dalam UDHR. Perkembangan selanjutnya, hak atas privasi kemudian beririsan dan saling terkait dengan hak atas informasi sehingga melahirkan konsepsi baru yakni hak PDP.[26] Pedoman pengaturan PDP yang lahir ini dari akar hak privasi juga dikonsepkan secara jelas.[27]

Pedoman pengaturan PDP secara dasar di dunia telah diatur dalam *Article 11 Organisation for Economic Co-operation and Development* (selanjutnya disebut dengan OECD) *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*.[28] Data pribadi sebagai materi muatan utama dari kedua konvenan tersebut sifatnya sangat esensial, karena penggunaannya berkaitan erat dengan transaksi bisnis digital seperti pada *e-commerce, e-payment*, pariwisata, industri, transportasi, dan lain-lain.[29]

[25] Putusan Mahkamah Konstitusi Nomor 50/PUU-VI/2008, hlm. 99.
[26] Erna Priliasari, "Pentingnya Perlindungan Data Pribadi Dalam Transaksi Pinjaman Online (The Urgency Of Personal Protection In Peer To Peer Lending)", *Majalah Hukum Nasional*, Vol. 49, No. 2, 2019, hlm. 21.
[27] Anggi Anggraeni Kusumoningtyas and Puspitasari, "Dilema Hak Perlindungan Data Pribadi Dan Pengawasan Siber: Tantangan Di Masa Depan," *Jurnal Legislasi Indonesia*, Vol. 17, No. 2, 2020, hlm. 242.
[28] Guidelines Convention on the Organisation for Economic Co-Operation and Development (OECD) No. C(80)58/FINAL", *Article* 11 OECD *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*, hlm. 15.
[29] Sinta Dewi, "Privasi Atas Data Pribadi: Perlindungan Hukum Dan Bentuk Pengaturan Di Indonesia", *Jurnal De Jure*, Vol. 15, No. 2, 2015, hlm. 165.

Ironisnya, eksistensi PDP masih menjadi diskursus yang harus diperbaiki. Hal ini dikarenakan PDP sangat rentan terhadap intervensi untuk dieksploitasi secara tidak berhak.[30] Selain itu, regulasi PDP masih belum mengakomodir terkait persoalan pada ranah privat. Berdasarkan penelitian Lembaga Studi dan Advokasi Masyarakat (selanjutnya disebut dengan ELSAM) menunjukkan bahwa masih adanya permasalahan regulasi yang mengatur perihal data pribadi konsumen. Hasil studi tersebut menunjukkan masih adanya regulasi perlindungan data pribadi yang bersifat parsial dan sektoral dalam 30 peraturan perundang-undangan.[31] Implikasi dari realita normatif tersebut ialah munculnya celah hukum yang seakan menggelar karpet merah bagi para peretas platform PSE privat dengan memanfaatkan buruknya sistem keamanan di mana hal ini sesungguhnya dapat dicegah dengan adanya pemanfaatan dari *Penetration Stress Test* (PST).

Penetration Stress Test (PST) merupakan serangkaian metode yang terdiri dari dua pengujian pada suatu sistem, yaitu *penetration test* dan *stress test.* Metode *pertama*, yaitu *penetration test* menurut *UK National Cyber Security Center,* secara garis besar mengartikan *penetration test* sebagai metode menguji keamanan sistem teknologi informasi dengan cara meretas menggunakan alat dan teknik yang sama oleh Peretas.[32] *Penetration test* harus dilaksanakan dengan izin dari PSE.[33] Tujuan utama *penetration test* ialah untuk mengidentifikasi kerentanan (celah) dalam sistem keamanan, sehingga celah dapat dihilangkan sebelum adanya pihak yang tidak berhak mengeksploitasi sistem, alhasil PSE dapat mengidentifikasi secara akurat, cepat dan

[30] Raphael Gellert and Serge Gutwirth, "The Legal Construction Of Privacy And Data Protection," *Computer Law & Security Review*, Vol. 29, No. 5, 2013, hlm. 526.
[31] Denico Doly, "Politik Hukum Pengaturan Perlindungan Data Pribadi", *Bidang Hukum Info Singkat Kajian Terhadap Isu Aktual Dan Strategis*, Vol. X, No. 08/II/Puslit, 2018, hlm. 3.
[32] National Cyber Security Centre, "Penetration Testing Advice on How to Get the Most from Penetration Testing," *https://www.ncsc.gov.uk/guidance/penetration-testing,* diakses tanggal 25 Januari 2022.
[33] Ahmad Ridha Kelrey dan Aan Muzaki, 2019, "Pengaruh Ethical Hacking Bagi Kerentanan Data Perusahaan," *Jurnal Cybersecurity Dan Forensik Digital*, Vol. 2, No. 2, hlm. 78.

mampu menerapkan strategi perbaikan terhadap celah yang telah dilaporkan dan diketahui melalui pengujian ini.

Metode *kedua*, yaitu *stress test* merupakan pengujian yang dilakukan untuk menguji reabilitas, stabilitas, dan keandalan dari suatu sistem teknologi. Pengujian ini akan dilakukan untuk melihat respon dari sistem bilamana dilakukan pengaksesan dalam jumlah yang banyak (*overload*) pada waktu tertentu.[34] Hal ini dipertegas oleh pernyataan H. Anthony Chan seorang peneliti senior di Huawei Technologies dan Profesor di Hong Kong University beliau mengatakan, *stress test* dilakukan dengan membebani sistem melebihi batas yang dapat ditampung. Hal ini untuk menemukan titik kegagalan dalam suatu sistem dan menguji pemulihan dari kegagalan sistem yang terjadi.[35]

Melihat kedua pengertian tersebut, maka definisi dari PST adalah suatu uji penilaian terhadap pertahanan keamanan untuk mencari celah serta menguji keandalan suatu sistem jika diakses pada saat bersamaan, apabila terdapat malfungsi pada sistem, maka PSE dapat memulihkan dan menutup celah sebagai langkah preventif. Oleh karena itu, di era bisnis digital penerapan PST merupakan suatu keharusan yang dilakukan setiap PSE untuk menghindari adanya Peretasan sistem keamanan yang berdampak pada kebocoran data pribadi pengguna (konsumen) di mana hal ini perlu diatur dalam peraturan perundang-undangan guna menjadikan setiap platform wajib menerapkannya disertai dengan pengawasan dan penegakannya.

UU ITE sebagai tulang punggung hukum siber (*cyberlaw*) di Indonesia sayangnya masih belum komprehensif dalam mendukung upaya PDP konsumen. Hal ini disebabkan oleh dua akar permasalahan di dalamnya yaitu perihal Lembaga Sertifikasi Keandalan dan pengujian keamanan platform yang disinggung secara tidak

[34] Molavi Arman, 2016, "Analisa Kinerja Web Server E-Learning Menggunakan Apache Benchmark Dan Httperf", *Jurnal Integrasi*, Vol. 8, No. 2, hlm. 93.
[35] H. Anthony Chan, "Annual Symposium Reliability and Maintainability: Accelerated Stress Testing for Both Hardware and Software", Los Angeles, 2004, hlm. 346.

menyeluruh. Selain itu, undang-undang yang hanya merekognisi sekilas, turut diperburuk dengan ketiadaan pengaturan lebih lanjut dalam peraturan pelaksana yang sering menjadi rujukan utama juga yaitu Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem Dan Transaksi Elektronik (selanjutnya disebut PP PSTE).

Akar permasalahan pertama yaitu perihal Lembaga Sertifikasi Keandalan yang pengaturannya dalam Pasal 10 Ayat (1) UU ITE hanya menyebutkan kewajiban penyelenggaraan transakasi elektronik dapat disertifikasi oleh Lembaga Sertifikasi Keandalan. Tidak ada pengaturan lain seperti fungsi, tujuan, cakupan kewenangan, dan hal-hal umum terkait Lembaga Sertifikasi Keandalan yang seharusnya diatur secara umum dalam payung hukum ini. Lubang kekurangan ini justru langsung ditutup dengan ketentuan pelimpahan pada peraturan pemerintah yang dicantumkan dalam Pasal 10 UU ITE ayat (2).[36]

Aturan pelaksana yang diharapkan menjadi pelengkap sayangnya tidak mengatur secara komprehensif juga mengenai Lembaga Sertifikasi Keandalan. Pada PP PSTE di mana fungsi, tujuan, cakupan kewenangan, dan pola hubungan Lembaga Sertifikasi Keandalan dengan Lembaga-lembaga lain belum ditemukan di dalamnya. Alih-alih melengkapi regulasi ini dengan hal-hal esensial tersebut, pelimpahan justru kembali dilakukan melalui ketentuan Pasal 37 ayat (6) PP PSTE yang mengatakan pengaturan lebih lanjut diatur dalam peraturan menteri di mana hingga sekarang masih belum dibentuk. Ketidaklengkapan PP PSTE menunjukkan pertentangannya dengan risalah politik hukumnya sendiri yaitu urgensi pengaturan yang komprehensif guna mengatur transaksi di era transformasi digital. Namun, secara bersamaan aturan pelaksana terkait Lembaga Sertifikasi Keandalan sebenarnya lebih cocok bila dibentuk

[36] Enni Soerjati, 2008, *Lembaga Sertifikasi Keandalan Sebagai Salah Satu Upaya Perlindungan Hukum Terhadap Konsumen Dalam Transaksi Elektronik Di Indonesia*, Tesis, Pasca Sarjana UI, Depok, hlm. 11.

dalam peraturan pemerintah tersendiri mengingat kompleksitasnya mendorong keperluan akan wadahnya sendiri.

Akar permasalahan kedua yaitu ketiadaan pengaturan pengujian. Sejauh ini, regulasi keamanan preventif platform digital swasta tidak memiliki pengaturan, terdapat Peraturan BSSN Nomor 4 Tahun 2021 Tentang Pedoman Manajemen Keamanan Informasi Sistem Pemerintahan Berbasis Elektronik Dan Standar Teknis Dan Prosedur Keamanan Sistem Pemerintahan, Berbasis Elektronik, tetapi hal tersebut hanya khusus platform pemerintah dan tidak ada ketentuan pengaturan khusus perihal *Penetration Stress Test*.[37] Kata pengujian hanya disebutkan, dalam Pasal 34 ayat (2) UU ITE, tetapi tidak ada penjelasan secara rinci mengenai pengertian dan pengaturan teknisnya. Di dalam bagian penjelasan juga hanya diberi keterangan "cukup jelas" sehingga tidak ada perincian lebih lanjut. Definisi dari pengujian keamanan saja bahkan juga tidak dijelaskan sehingga berimplikasi pada aturan pelaksananya. Hal ini terlihat bila menilik Pasal 12, Pasal 94 ayat (1) butir g beserta bagian penjelasan perihal manajemen risiko dan Pasal 24 ayat (2) beserta bagian penjelasan PP PSTE terkait sistem pencegahan dan penanggulangan di mana tidak mengatur penentuan metode pengujian yang konkret seperti PST.[38]

Implikasi problematika mulai dari tataran hierarki undang-undang serta PP ini mengarah permasalahan pada tataran di bawahnya lagi sehingga menciptakan kekacauan regulasi yang semakin tidak terkendali. Bentuk dari implikasi tersebut diantaranya ialah ketidaksamaan definisi, polemik pihak penyelenggara PST, serta tumpang tindih wewenang penerima laporan sertifikasi SMPI.

[37] Lihat dalam Pasal 2 Peraturan BSSN No. 4 Tahun 2021 Tentang Pedoman Manajemen Keamanan Informasi Sistem Pemerintahan Berbasis Elektronik Dan Standar Teknis Dan Prosedur Keamanan Sistem Pemerintahan, Berbasis Elektronik (Berita Negara Tahun 2021 Nomor 541).
[38] Lihat dalam Pasal 24 ayat (2) Peraturan Pemerintah Nomor 71 Tahun 2019 Tentang Penyelenggaraan Sistem Dan Transaksi Elektronik (Lembaran Negara Republik Indonesia Tahun 2019 Nomor 185).

Pertama, ketidaksamaan definisi PST dalam berbagai peraturan. PST pengertiannya masih bersifat terpisah, yakni *Penetration test* dan *Stress test*. *Penetration test* baru disinggung dalam Peraturan Otoritas Jasa Keuangan (selanjutnya disebut dengan POJK) No. 57/POJK.04/2020[39], tetapi definisinya hanya ditemukan dalam bagian format daftar kesiapan infrastruktur sistem elektronik. Ketentuan ini juga hanya untuk kegiatan penawaran efek melalui sistem elektronik. Sementara, pengertian *Stress test* baru terdapat dalam Surat Edaran Otoritas Jasa Keuangan (selanjutnya disebut dengan SEOJK) No. 21/SEOJK.03/2017 yang garis besarnya terkait uji ketahanan sistem perihal manajemen proses transaksi dalam skala besar.[40] Sayangnya, pengertian ini hanya untuk kegiatan bank umum saja.

Ketentuan tentang PST baru disinggung dalam Pasal 8 butir f dan Pasal 9 butir d Peraturan Menteri Komunikasi dan Informasi Nomor 11 Tahun 2018 (selanjutnya disebut dengan Permekominfo 11/2018)[41], di mana Penyelenggara Sertifikasi Elektronik harus memiliki laporan mengenai pengujian sistem elektronik (*stress test*) dan analisis keamanan informasi (*penetration test*). Namun, ketentuan tersebut masih belum mendefinisikan PST dan hanya ditujukan kepada Penyelenggara Sertifikasi Elektronik. Akibat dari ketiadaan dan ketidakjelasan definisi konkrit terkait PST menimbulkan ketidakpastian hukum. Ketidakpastian hukum lahir karena terdapat ketidakjelasan sehingga menimbulkan penafsiran yang berbeda-beda pada suatu substansi norma.[42]

[39] Lihat dalam Peraturan Otoritas Jasa Keuangan Nomor 57/POJK.04/2020 Tentang Penawaran Efek Melalui Layanan Urun Dana Berbasis Teknologi Informasi (Lembaran Negara Republik Indonesia Tahun 2020 Nomor 281).
[40] Lihat dalam Surat Edaran Otoritas Jasa Keuangan Nomor 21/SEOJK.03/2017 Tentang Penerapan Manajemen Risiko Dalam Penggunaan Teknologi Informasi Oleh Bank Umum.
[41] Lihat dalam Pasal 8 hutuf f dan Pasal 9 huruf d Peraturan Menteri Komunikasi Dan Informatika Nomor 11 Tahun 2018 Tentang Penyelenggaraan Sertifikasi Elektronik (Berita Negara Republik Indonesia Tahun 2018 Nomor 1238).
[42] Syafruddin Kalo, 2007, *Penegakan Hukum Yang Menjamin Kepastian Hukum Dan Rasa Keadilan Masyarakat*, Pengukuhan Pengurus Tapak Indonesia Koordinator Daerah Sumatera Utara, Medan, hlm. 4.

Kedua, polemik penunjukkan pihak penyelenggara PST. Ketidakjelasan pengaturan mengenai lembaga sertifikasi keandalan di tataran undang-undang dan peraturan pemerintah menyebabkan ambiguitas dalam menentukan penyelenggara PST. Pasalnya, pengaturan mengenai Lembaga sertifikasi keandalan yang seharusnya menjadi pihak penyelenggara PST dalam rangka menerbitkan sertifikat keandalan, justru diejawantahkan dalam bentuk yang berbeda di tataran peraturan menteri dan di bawahnya sebagai Lembaga Sertifikasi SMPI. Konsekuensi dari kebijakan hukum ini ialah kebuntuan dari Lembaga Sertifikasi Keandalan dan rujukan pengaturan pihak yang berwenang menjadi penyelenggara PST berkiblat pada Peraturan Menteri Komunikasi dan Informasi Nomor 4 Tahun 2016 tentang Sistem Pengamanan Manajemen Informasi (selanjutnya disebut dengan PermenKominfo 4/2016) dan Peraturan Badan Siber dan Sandi Negara Nomor 8 Tahun 2020 tentang Sistem Manajemen Pengamanan Informasi (selanjutnya disebut dengan Peraturan BSSN 8/2020).

Berdasarkan Pasal 5 Ayat (2) PermenKominfo 4/2016 menyatakan bahwa penerapan pengujian dilakukan secara mandiri oleh PSE.[43] Adapun dalam Pasal 13 Peraturan BSSN 8/2020 juga memberikan keleluasan yang sama dengan penambahan diperbolehkan untuk menunjuk pihak lain seperti tenaga ahli berkewarganegaraan Indonesia atau lembaga konsultan yang diakui BSSN.[44] Kebebasan berlebih yang diberikan kepada PSE dalam menguji platformnya memunculkan permasalahan. Banyak sekali pihak yang cenderung memilih penyelenggaraan PST sebatas formalitas guna menghindari pengeluaran besar. Hal ini sangat berbahaya mengingat kegagalan dalam melakukannya dapat berimplikasi pada sistem yang diuji rusak sehingga tujuan

[43] Lihat dalam Pasal 5 Ayat (2) Peraturan Menteri Komunikasi Dan Informatika Nomor 4 Tahun 2016 Tentang Sistem Manajemen Pengamanan Informasi (Berita Negara Republik Indonesia Tahun 2016 Nomor 551).
[44] Lihat dalam Pasal 13 Peraturan Badan Siber Dan Sandi Negara Nomor 8 Tahun 2020 Tentang Sistem Pengamanan Dalam Penyelenggaraan Sistem Elektronik (Berita Negara Republik Indonesia Tahun 2020 Nomor 1375).

awalnya tidak terwujud.[45] Selain itu, kebebasan penunjukan yang berlebihan dapat menjerumuskan pada pengujian yang menjadi penipuan (*fraud*) atas dasar kesepakatan di bawah meja antara penguji dan yang diuji.

Ketiga, pertentangan Pasal 31 Peraturan BSSN 8/2020 dengan Pasal 18 Permenkominfo 4/2016 terkait pihak yang berwenang menerima laporan dari lembaga sertifikasi SMPI. Polemik penyelenggara PST tidak hanya berhenti pada persoalan siapa yang berhak menyelenggarakannya, tetapi juga perihal penyerahan laporan oleh Lembaga Sertifikasi SMPI. Tumpang tindih hubungan dan kewenangan antara Kominfo dan BSSN terlihat pada Pasal 18 Ayat (1) PermenKominfo 4/2016, di mana kewajiban lembaga sertifikasi menyampaikan laporan hasil sertifikasi SMPI kepada Direktur Jenderal Aplikasi Informatika.[46] Sedangkan, dalam Pasal 31 Peraturan BSSN 8/2020 secara garis besar menyebutkan kewajiban lembaga sertifikasi dalam menyerahkan hasil laporan sertifikasi SMPI minimal 2 kali dalam setahun kepada Kepala BSSN.[47] Hal ini, menimbulkan suatu ambiguitas dalam kewenangan kedua lembaga negara tersebut sehingga memunculkan perbedaan interpretasi.

Regulasi PST yang buruk ini pada akhirnya menunjukkan banyaknya ketidakpastian hukum yang sangat esensial. Menurut Lord Lloyd ketidakpastian hukum sangat diperlukan karena

> *…law seems to require a certain minimum degree of regularity and certainty, without that it would be impossible to assert that what was operating in a given territory amounted to a legal system*".[48]

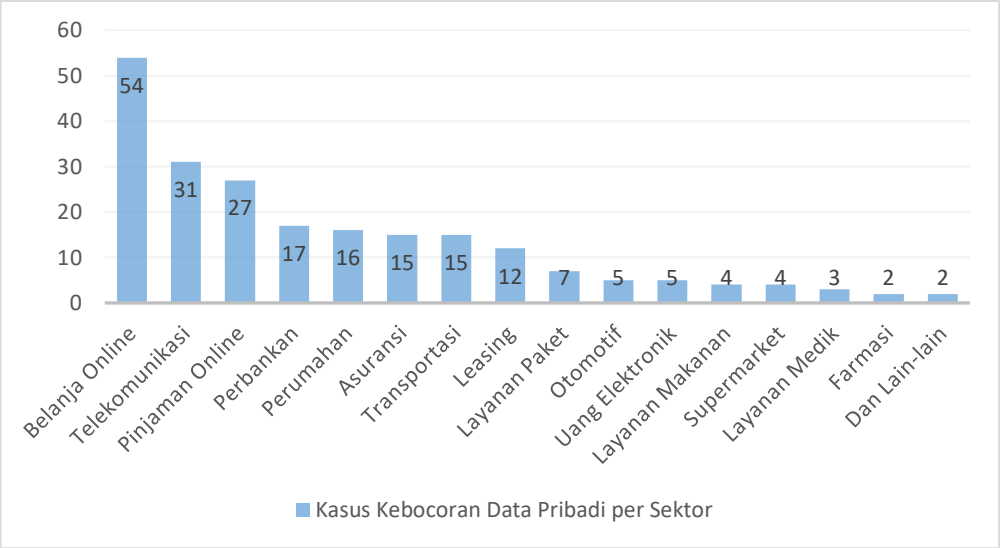
[45] S M Salim Reza, Wahidul Hasan, and Sajib Chakraborty, "A Comparative Overview on Penetration Testing," in Conference: 4th International Conference On Advance In Computing", Kuala Lumpur: Electronics & Electrical Technology (CEET-2015), 2015), hlm 25.
[46] Lihat dalam Pasal 18 Ayat (1) Lihat dalam Pasal 5 Ayat (2) Peraturan Menteri Komunikasi dan Informatika Nomor 4 Tahun 2016 tentang Sistem Manajemen Pengamanan Informasi (Berita Negara Republik Indonesia Tahun 2016 Nomor 551).
[47] Lihat dalam Pasal 31 Peraturan Badan Siber Dan Sandi Negara Nomor 8 Tahun 2020 Tentang Sistem Pengamanan Dalam Penyelenggaraan Sistem Elektronik (Berita Negara Republik Indonesia Tahun 2020 Nomor 1375).
[48] Mirza Satria Buana, 2010, *Hubungan Tarik-Menarik Antara Asas Kepastian Hukum (Legal Certainpi) Dengan Asas Keadilan (Substantial Justice) Dalam Putusan-Putusan Mahkamah Konstltusi*, Tesis, Magister Ilmu Hukum Universitas Islam Indonesia, Yogyakarta, hlm. 34.

Pandangan ini dikembangkan oleh Tony Prayogo di mana hasil dari ketidakpastian hukum akan menimbulkan ketidakpastian (*rechtsonzekerheid*) yang berbuah kekacauan (*rechtsverwarring*) dikarenakan ketidaktegasan sistem hukum yang dapat dipengaruhi keadaan subjektif.[49] Kekacauan ini tentu saja menjadi nestapa bagi semua pihak.

Kekacauan yang berimplikasi pada kebocoran data pribadi secara masif, menimbulkan nestapa terhadap konsumen, platform, bahkan negara yang dapat dibuktikan berdasarkan diagram batang yang divisualisasikan di bawah ini:

Grafik 1.

Kasus Kebocoran Data Pribadi per Sektor



Sumber: Lokadata.id[50]

Selama bulan Juni tahun 2020 saja, terdapat kebocoran data pribadi konsumen di berbagai sektor privat yang totalnya mencapai 165 kasus sebagaimana yang diitunjukan pada grafik di atas. Kenyataan ini menunjukkan kebocoran data pribadi

[49] R. Tony Prayogo, "Penerapan Asas Kepastian Hukum Dalam Peraturan Mahkamah Agung Nomor 1 Tahun 2011 Tentang Hak Uji Materiil Dan Dalam Peraturan Mahkamah Konstitusi Nomor 06/Pmk/2005 Tentang Pedoman Beracara Dalam Pengujian Undang-Undang", *Jurnal Legislasi Indonesia*, Vol. 13, No. 2, 2016 , hlm. 194.

[50] Ayyi and Shila, "Kasus Kebocoran Data Semakin Banyak, Belanja Daring Paling Rentan,", *https://lokadata.id/artikel/kasus-kebocoran-data-semakin-banyak-belanja-daring-paling-rentan*, diakses tanggal 30 Desember 2021.

dapat menghantui konsumen di *cyberspace* kapan pun dan di manapun seolah tidak ada tempat yang aman bagi mereka. Tahun 2020 memang menjadi puncak dari maraknya kasus kebocoran data pribadi dimana pada Kuartal II Tahun 2020 terdapat 39,6 juta akun diretas sehingga terjadi banyak kebocoran data pribadi. Terlepas dari adanya penurunan jumlah kebocoran data pribadi pada Kuartal I Tahun 2023 yaitu menjadi 142,081,103 akun yang telah diretas, angka tersebut masih menunjukan tingginya kebocoran data pribadi terjadi.[51]

Kasus kebocoran data pribadi bahkan terjadi pada platform besar di mana angka korban per kasusnya sangat besar. Tahun 2020 menjadi masa kelam yang tercatat dalam sejarah upaya PDP di mana banyak terjadi kasus-kasus yang menghasilkan korban dalam jumlah besar. Pada bulan Mei kebocoran data pribadi konsumen di platform Tokopedia sebanyak 91.000.000 kasus, bulan Juli di platform Kredit Plus sebagnyak sebanyak 890.000 kasus, dan bulan November di platform Red Doorz sebanyak 5.800.000 kasus serta di platform Cermati sebanyak 2.900.000 kasus.[52] Permasalahan utama data pribadi yang bocor dalam berbagai kasus sebenarnya bukan hanya terletak pada kuantitas, melainkan eksploitasi ilegal pasca dicuri.

Terdapat satu kasus besar pada tahun 2020 yang memberikan gambaran terkait ancaman eksploitasi data pribadi konsumen bisa ditemukan dalam tragedi platform Bhineka.com. Kasus ini terjadi pada Mei 2020 di mana 1.200.000 data pribadi konsumen bocor. Pembobol platform ini bernama *ShinyHunters* telah memperjualbelikan data pribadi konsumen yang dicurinya di *deep web* seharga Rp 17.900.000 per data.[53] Eksploitasi berupa perdagangan data pribadi konsumen yang

[51] Surfshark, 2023, "*Global Data Breach Stats*", *https://surfshark.com/research/data-breach-monitoring*, diakses tanggal 26 Mei 2023.
[52] Pusat Operasi Keamanan Siber Nasional BSSN, 2021, *Laporan Tahunan Monitoring Keamanan Siber 2020*, Jakarta, hlm. 45.
[53] Deanne Destriani Firmansyah Putri and Muhammad Helmi Fahrozi, "Upaya Pencegahan Data Konsumen Melalui Pengesahan RUU Perlindungan Data Pribadi (Studi Kasus E-Commerce Bhinneka.Com Case Study)", *Procceding: Call for Paper, 2nd National Conference on Law Studies: Legal Development Towards a Digital Society Era*, Vol. 2, No. 1, 2020, hlm. 262.

dilakukan ini sama saja dengan mengobjektifikasi manusia sehingga sangat merendahkan harkat dan martabat korban. Selain itu, konsumen sebagai korban tentu saja mengancam mereka secara materi dan psikis.

Kerugian secara materi dan psikis yang diterima konsumen akibat kebocoran data pribadinya dapat dibuktikan secara empiris berdasarkan hasil wawancara yang dilakukan penulis terhadap 10 responden yang menggunakan berbagai platform seperti Instagram, Wattpad, Shopee, Tokopedia, Whatsapp, Bukalapak, dan BRIMO. Hasil wawancara yang dilakukan menunjukkan 8:10 (delapan dari sepuluh) responden merasakan dampak psikis seperti khawatir, malu, dan takut. Selain itu, 7:10 (tujuh dari sepuluh) responden juga mengalami kehilangan kendali atas akunnya sendiri sehingga menghalangi aktivitas mereka dalam ruang siber (*cyberspace*) termasuk perihal transaksi digital.

Dampak masif problematika perlindungan data pribadi terhadap konsumen yang mewabah ini pada akhirnya berimplikasi pada negara. Menurut penelitian Frost dan Sullivan, menunjukkan kerugian ekonomi di Indonesia akibat insiden keamanan siber senilai 3,7% dari total PDB Indonesia atau sebesar 932 milliar USD.[54] Riset ini juga menunjukkan 61% perusahaan menunda upaya transformasi digital karena khawatir dengan risiko di ruang siber. Setengah dari perusahaan yang menjadi objek studi ini juga mengalami insiden keamanan siber (22%) atau ragu pernah mengalaminya karena tidak menguji pemeriksaan pembobolan data (27%) sehingga totalnya sebesar 49%. Selain itu, perusahaan besar memiliki potensi kehilangan dan mengalami kerugian ekonomi sebesar 16,3 juta USD atau 200 kali lebih tinggi dari kerugian ekonomi kelas menengah.[55] Kalkulasi secara rili pada perekonomian negara

[54] World Banks, "Asia Pacific GDP Information,", *https://data.worldbank.org/indicator/NY.GDP.MKTP.CD,* diakses tanggal 23 Januari 2022.
[55] Vishnum, "Ancaman Keamanan Siber Menyebabkan Kerugian Ekonomi Bagi Organisasi Di Indonesia Sebesar US$34.2 Miliar,", *https://news.microsoft.com/id-id/2018/05/24/ancaman-keamanan-siber-menyebabkan-kerugian-ekonomi-bagi-organisasi-di-indonesia-sebesar-us34-2-miliar/#_ftn1,* diakses tanggal 23 Januari 2022.

ini menjadi bukti PDP yang lemah dapat menghambat atau bahkan mencederai perekonomian negara secara serius.

Berdasarkan pemaparan data dan dampak dalam tataran *grassroot* tersebut, membuktikan buruknya regulasi PST sebagai malapetaka upaya PDP konsumen. Realita ini seharusnya membangkitkan gairah pemerintah selaku mandataris rakyat untuk berusaha menemukan gagasan atas problematika era digital yang sukar ditangani ini. Oleh karena itu, perlindungan hukum secara preventif dalam hal ini menjadi fokus utama yang harus diperbaiki.

Perlindungan preventif, pada hakikatnya menjadi kebutuhan hukum yang lebih dibutuhkan oleh konsumen di dunia bisnis digital. Hal ini selaras dengan pernyataan Philipus. M. Hadjon bahwa perlindungan hukum secara preventif, selalu ditujukan untuk menyelesaikan sengketa.[56] Alasan logis aksioma ini yaitu untuk mencegah tercederainya hak-hak konsumen yang sepantasnya mereka dapatkan secara utuh. Oleh karena itu, perlu direformulasikannya PST sebagai perlindungan hukum preventif yang baik untuk melindungi hak konsumen di dunia bisnis digital.

2. *Penetration Stress Test* Sebagai Kewajiban Platform Disertai Mekansime Pengawasan dan Penegakan Hukum

Berdasarkan postulat problematika di mana urgensi akan perlindungan hukum terhadap hak privasi sangat membutuhkan formulasi preventif yang tepat. Hal ini tidak terlepas dari *Right to Privacy* yang dikonsepkan sebagai *secrecy* oleh Richard Posner di mana "*being left alone and concealment of information as limited access to the self*".[57] Selaras dengan itu Francis Chlapowski menyatakan bahwa privasi

[56] Philipus M. Hadjon, 1988, *Perlindungan Hukum Bagi Rakyat Indonesia*, Bina Ilmu, Surabaya, hlm. 5.
[57] Wahyudi Djafar dan M Jodi Santoso, 2019, *Perlindungan Data Pribadi Konsep, Instrumen Dan Prinsipnya*, Lembaga Studi dan Advokasi Masyarakat (ELSAM), Jakarta, hlm. 4.

merupakan harta milik (*property*).[58] Paradigma kedua pakar ini, menjadi landasan filosofis perumusan PDP berorientasikan *user centric*.

Kebijakan perdagangan elektronik diarahkan kepada tanggung jawab pemberian perlindungan hukum kepada pengguna (*user's centric*). Hal tersebut dijabarkan sebagai hal krusial untuk diperhatikan oleh penyelenggara perdagangan melalui sistem elektronik, seperti berdasarkan asas itikad baik, efisien, dan efektif, serta melindungi kepentingan hak konsumen.[59] Pernyataan tersebut menjadi tonggak kewajiban PSE untuk memberikan keamanan transaksi terhadap hak konsumen di era bisnis digital.

Langkah awal mereformulasi pengaturan PST di Indonesia, dapat dilakukan melalui perbaikan pada UU ITE mengingat fungsinya sebagai payung hukum siber Indonesia di era bisnis digital. Gagasan ini dapat menjadi masukan tambahan yang relevan dengan Surat Presiden Nomor R-58/Pres/12/2021 RUU tentang Perubahan Kedua Atas UU Nomor 11/2008 tentang ITE yang diserahkan kepada DPR pada 16 Desember 2021.[60]

Penambahan substansi dilakukan dengan memberikan definisi normatif yang konkret mengenai pengujian keamanan dalam Pasal 1 UU ITE berbunyi

> Pengujian keamanan adalah serangkaian metode wajib yang telah diatur dalam peraturan perundang-undangan yang dilakukan untuk menguji keamanan PSE yang dilakukan secara berhak dan di bawah pengawasan badan berwenang".

Selain memperjelas definisi dari pengujian itu sendiri, perlu bentuk kepastian dari Lembaga penyelenggara sertifikasi keandalan yang mumpuni secara normatif dan implementasinya mengingat perannya nanti sebagai eksekutor PST.

[58] Francis S. Chlapowski, "The Constitutional Protection of Information Privacy", *Boston University Law Review*, Vol. 71, 1991, hlm. 133.
[59] Imam Lukito, "Tantangan Hukum Dan Peran Pemerintah Dalam Pembangunan E-Commerce," *Jurnal Ilmiah Kebijakan Hukum*, Vol. 11, No. 3, 2017, hlm. 359.
[60] Lihat dalam Surat Presiden Nomor R-58/Pres/12/2021 RUU Tentang Perubahan Kedua Atas UU Nomor 11/2008 Tentang ITE.

Revisi UU ITE guna menciptakan kepastian hukum (*rechtszekerheid*) perihal penyelenggara PST yang tepat, maka akan lebih baik bila dirumuskan badan independen di bawah negara yang akan berperan selaku penguji berbasis PST, pengawas rutin dan penerbit sertifikat keandalan. Badan ini dinamai Badan Pengujian dan Sertifikasi Sistem Keandalan Informasi dan Elektronik (selanjutnya disebut dengan BP2SKIE). Definisi normatif badan ini berbunyi:

Badan Pengujian dan Sertifikasi Sistem Keandalan Informasi dan Elektronik atau disebut BP2SKIE adalah badan yang berwenang melaksanakan kewajiban pengujian sistem dan melaksanakan sertifikasi keandalan keamanan PSE secara berkala berdasarkan peraturan perundang-undangan.

Selain itu, perlu dibuat Bab baru dalam UU ITE yang khusus mengatur Manajemen Keamanan PSE mencakup asas-asas manajemen keamanan PSE, tujuan pengujian keamanan, fungsi pengujian keamanan, dan pelimpahan pada PP baru yang akan mengatur lebih rinci mengenai pengujian keamanan berorientasi pada teori *user centric* dan pendelegasian kepada perpres mengenai BP2SKIE.

Mengingat ketiadaan aturan pelaksana terkait Lembaga Sertifikasi Keandalan, maka akan dibentuk Peraturan Pemerintah Sistem Manajamen Penyelenggara Informasi Elektronik (selanjutnya disebut dengan PP SMPIE). Pengaturan yang lebih jelas dan terang tercantum dalam PP SMPIE secara garis besar terdapat dua, yaitu mengenai PST dan lembaga sertifikasi keandalan. Definisi normatif terkait PST akan dijabarkan secara konkret dalam Pasal 1 PP SMPIE yang berbunyi:

> *Penetration Stress Test* atau PST adalah metode pengujian gabungan antara *penetration test* dan *stress test* yang wajib dilakukan dalam pelaksanaan pengujian per tahun.

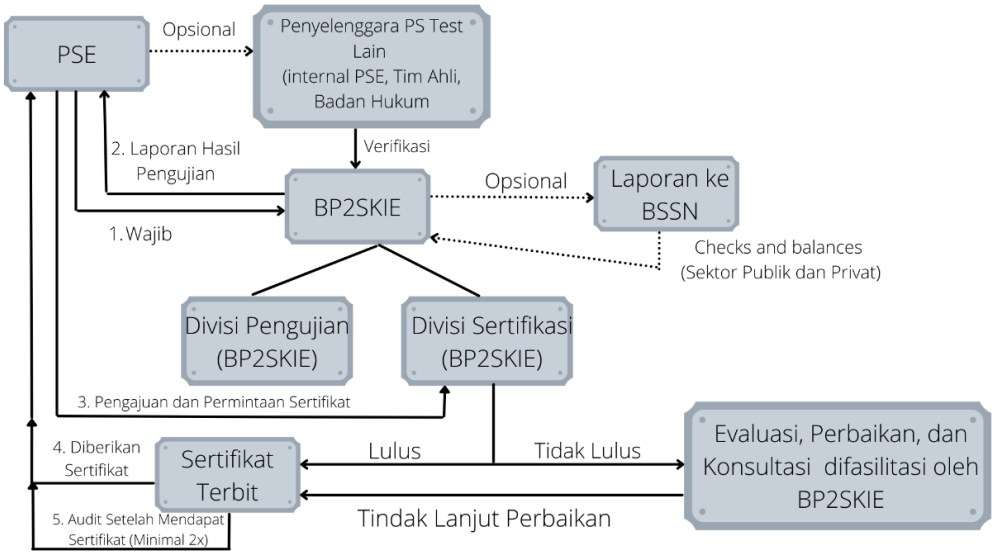
Cakupan pengaturan PP SMPIE melingkupi: 1) Bab I Hak dan Kewajiban Penguji; 2) Bab II Hak dan Kewajiban PSE; 3) Bab III Hak dan Kewajiban Lembaga Sertifikasi; 4)

Bab IV Mekanisme Koordinasi Antar Para Pihak; 5) Bab V pengujian; 6) Bab VI Sanksi Administratif; 7) Bab VII Ketentuan Peralihan; 8) Bab VIII Penutup.

Skema hubungan antara para pihak yang dibangun berdasarkan substansi PP SMPI tertera di bawah ini:

Gambar 1.

Skema Hukuman antara BP2SKIE dengan Para Pihak



Sumber: Hasil Olah Penulis

Hubungan antara BP2SKIE dengan PSE ialah penguji dan penyelenggara sertifikasi dengan yang diuji dan menerima sertifikat keandalan serta keamanan berbasiskan metode PST di mana dapat diurutkan, diantaranya: 1) Kewajiban PSE untuk menguji sistem keamanan dan keandalan platformnya dengan basis utamanya menggunakan metode PST ke divisi pengujian BP2SKIE (bila sudah melakukan PST dengan pihak lain, maka tetap wajib verifikasi pengujian ulang dengan BP2SKIE); 2) Laporan hasil pengujian diserahkan kepada PSE tersebut guna menentukan langkah yang harus ditempuh dalam memperbaiki sistemnya; 3) Tindak lanjut dari menyikapi hasil

pengujian tersebut adalah mengajukan permintaan sertifikat keandalan dan keamanan kepada divisi sertifikasi BP2SKIE di mana pada tahap ini akan ditentukan lulus atau tidak; 4) Pemberian sertifikat keandalan dan keamanan kepada PSE dapat terjadi berdasarkan 2 cara yaitu bila tidak lulus maka harus melalui evaluasi, perbaikan, dan konsultasi yang difasilitasi oleh BP2SKIE. Sedangkan bila lulus, maka dapat langsung menerima sertifikatnya; 5) Setelah PSE mendapatkan sertifikat keandalan dan keamanan tersebut, maka BP2SKIE wajib melakukan audit dan pengujian kembali secara berkala sebanyak 2 kali dalam setahun.

Hubungan BP2SKIE dengan pihak lain perihal tindak lanjut yang akan dikenai pada PSE yang tidak memperbaiki *platform*-nya pasca pengujian PST sehingga membahayakan konsumen dalam beraktifitas (terutama transaksi digital) dapat dikenai sanksi administratif. PSE akan dikenai sanksi administratif mengacu pada PP SMPIE di mana bentuknya berupa peringatan tertulis dan penutupan platform disertai pencabutan izin usaha bila peringatan tertulis tidak diindahkan. Penutupan dan pencabutan izin usaha dilakukan dengan cara memberikan surat rekomendasi kepada instansi terkait yang membawahi sektor PSE tersebut misalnya seperti platform *fintech* yang dinaungi oleh Otoritas Jasa Keuangan, *e-commerce* oleh Kementerian Perdagangan, *e-health* oleh Kementerian Kesehatan, dan lain-lain. Pihak instansi terkait yang menerima surat rekomendasi tersebut yang berwenang untuk mencabut izin PSE yang bersangkutan. Eksekusi dari semua kinerja ini tetap dilaksanakan dengan menjaga rahasia dagang yang mengacu pada Undang-Undang Nomor 30 Tahun 2000 tentang Rahasia Dagang.

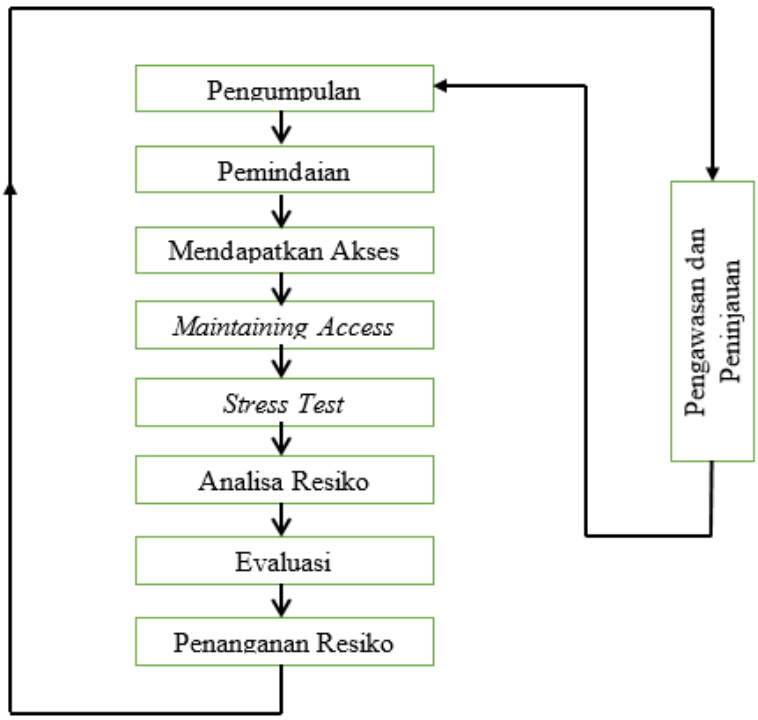
PP SMPIE juga akan mengatur hubungan *check and balances* antara BP2SKIE dan BSSN dengan saling memberikan laporan kinerja masing-masing di mana sifatnya opsional. Hubungan antara badan ini tidak dapat saling mengintervensi mengingat hierarkinya yang sejajar, merupakan badan independen, serta memiliki sektor yang

berbeda di mana BP2SKIE fokus privat dan BSSN kepada publik. Hal ini dilakukan agar ada keselarasan sinergi dalam menejamin perlindungan hukum secara preventif melalui penguatan regulasi pengujian PST guna melindungi data pribadi konsumen baik di sektor privat (bisnis digital) maupun publik (*e-government*).

Skema selanjutnya terkait pengujian yang dilakukan penguji (baik oleh eksternal maupun oleh BP2SKIE) terhadap PSE agar membentuk sistem keamanannya terjaga secara berkala dan berkelanjutan. Berikut pemaparannya:

Gambar 2.

Skema Pelaksanaan PSE oleh BP2SKIE



Sumber: Hasil Olah Penulis

Pemaparan skema di atas dapat dijelaskan dimulai dari proses pengumpulan informasi tingkatan awal seperti alamat IP, informasi terkait server, dan lain-lain yang berkaitan dengan *website*. Setelah itu, dilakukan pemindaian dengan mencari celah keamanan yang dapat disusupi serta BPSK berusaha mendapatkan akses guna

melancarkan serangan yang bertujuan agar memperoleh informasi yang lebih akurat ke dalam sistem keamanan dari platform.

Proses vital selanjutnya ialah *Maintaining Access* yaitu berusaha selama mungkin menyusup ke dalam untuk mencuri informasi berharga seperti data pribadi dan kemudian mengekstraknya. Setelah itu, masuk ke bagian esensial yaitu *Stress test* di mana penguji memasukan beragam aktivitas untuk menguji ketangguhan dan keandalan sistem untuk mengetahui seberapa banyak dan lama sistem ini akan *down* jika diakses dalam waktu bersamaan. Pasca pengujian selesai, maka dilakukan tahap menyikapi hasil dari PST tersebut.

Analisa risiko menjadi pembuka evaluasi dengan memberikan penilaian dampak dan kemungkinan ancaman yang akan terjadi terhadap sistem yang sedang diuji. Selanjutnya dilakukan evaluasi untuk membantu platform dalam menutup celah yang ada dan memulihkan sistem keamanannya dengan baik. Cakupan dilaksanakannya PST juga perlu untuk mengembangkan keamanan sehingga proses penanganan risiko dengan mengadopsi tambahan kontrol keamanan atau meningkatkan sistem kontrol keamanan yang ada, menghindari risiko dengan tidak membiarkan suatu tindakan yang memicu risiko muncul menjadi hal yang perlu.

Hal terakhir yang akan dilaksanakan ialah evaluasi dan penanganan risiko yang akan menyediakan, memperoleh, serta berdiskusi terkait manajemen risiko sehingga kesadaran dan ilmu sistem keamanan meningkat serta perbaikan sistemnya sebagai bentuk tindak lanjut yang nyata. Pasca semua rangkaian implementasi pengujian sistem keamanan berbasiskan metode PST dilaksanakan, pengawasan dan peninjauan sebagai bentuk evaluasi keefektifan secara berkala tetap dilaksanakan. Semua ini untuk menciptakan pengawasan kualitas keamanan PDP dengan menciptakan keajegan kegiatan PST secara berkelanjutan dan berkala.

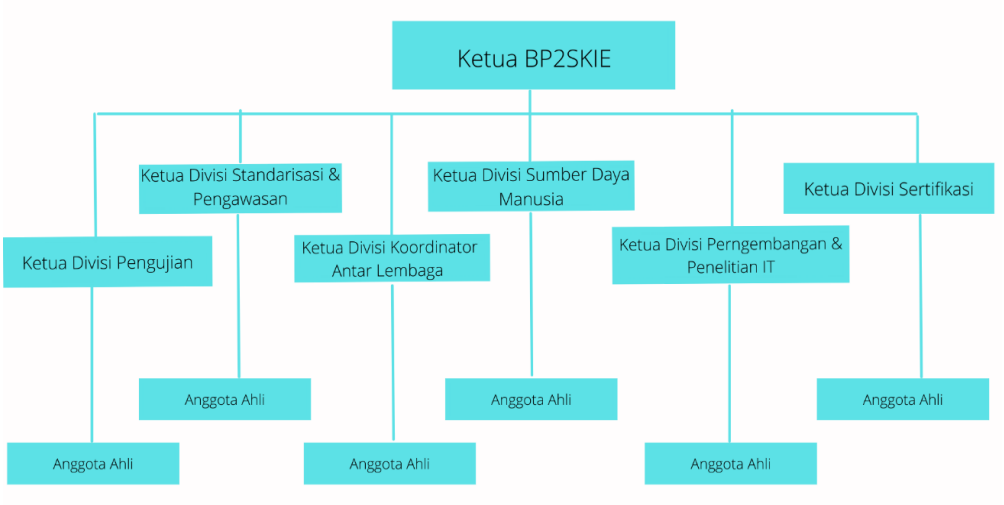
Hal esensial lain yang perlu diatur dalam reformulasi PST ialah kejelasan eksistensi BP2SKIE. Wadah normatif yang tepat untuk mengatur BP2SKIE secara rinci adalah Peraturan Presiden dengan nama "Peraturan Presiden tentang Badan Pengujian dan Sertifikasi Sistem Keandalan Informasi Elektronik" (selanjutnya disebut dengan Perpres BP2SKIE) yang merupakan pendelegasian dari UU ITE. *Ratio legis* pemilihan wadah normatif berupa perpres karena perlunya atensi bersama pada BP2SKIE guna menjaga sistem keamanan setiap PSE privat melalui pengujian. Substansi Perpres BP2SKIE mencakup: 1) Bab I Kedudukan, Tugas, Dan Fungsi; 2) Bab II Susunan Organisasi; 3) Bab III Jabatan, Pengangkatan, Dan Pemberhentian; 4) Bab IV Pendanaan; 5) Bab V Ketentuan Peralihan; 6) Bab VI Penutup.

Tupoksi dari BP2SKIE secara garis besar di antaranya; *Pertama*, menyelenggarakan pengujian sistem keamanan 2 kali dalam setahun terhadap platform dengan salah satu metode wajibnya adalah PST; *Kedua*, bekerja sama dengan badan lain yang diantaranya BSSN dan Instansi-instansi terkait lain untuk menciptakan iklim ruang siber yang aman dalam melakukan transaksi digital serta memiliki ketangguhan PDP yang baik; *Ketiga*, mengembangkan metode dan teknologi sistem keamanan informasi guna melindungi data pribadi konsumen dalam suatu platform. BP2SKIE berwenang untuk menguji, mengsertifikasi, mengevaluasi, memberikan rekomendasi atau layanan konsultasi, dan memberikan bantuan pengembangan sistem keamanan informasi terhadap PSE. Perlu digaris bawahi juga bahwa tupoksi dan wewenang BP2SKIE hanya mencakup platform milik privat.

Struktur organisasi yang dimiliki BP2SKIE memiliki gambaran seperti berikut:

Gambar 3.

Struktur Organisasi BP2SKIE



Sumber: Hasil Olah Penulis

Berdasarkan gambar yang tertera, BP2SKIE akan mempunyai 6 divisi di mana ketua dan anggotanya akan diisi oleh anggota ahli yang memiliki pengetahuan sistem keamanan informasi yang andal serta pengetahuan yang banyak mengenai serangan siber (*cyberattack*) guna menciptakan PST yang berkualitas.

Anggota ahli akan direkrut melalui pengadaan BP2SKIE *penetration hacking competition* (selanjutnya disebut dengan BP2SKIE PH *Competition*) dibuka kepada publik. Peserta yang dapat ikut serta hanya warga negara Indonesia serta identitasnya tidak boleh anonim. Lomba ini akan diadakan atas dasar surat edaran BP2SKIE. Perekrutan melalui kompetisi ini dilakukan dengan cara membuka pendaftaran untuk *platform-platform* privat dengan sistem pertahanan yang kuat menjadi objek PST. Peretas yang akan berpartisipasi harus mendaftarkan diri terlebih dahulu agar terdata dan setelah itu melaksanakan PST pada platform yang menjadi objek. Peretas yang berhasil meretas, menemukan kerentanan, dan memberikan evaluasi yang paling terbaik terhadap platform berdasarkan penilaian panitia penyelenggara BP2SKIE PH *Competition* akan direkrut untuk menjadi anggota ahli. Semua ini akan dilaksanakan mengacu pada panduan kompetisi yang ditetapkan oleh BP2SKIE PH *Competition*.

BP2SKIE PH *Competition* yang digagas ini, terinspirasi dari perekrutan Peretas secara legal yang dilakukan oleh Department of Defense (selanjutnya disebut dengan DoD) Amerika Serikat bekerja sama dengan perusahaan HackerOne menciptakan wadah *penetatrion test* bernama *Hack the Pentagon* pada 17 Juni 2016. Pelaksanaan dilakukan dengan menyediakan target *penetration test* berupa lima *website* publik di mana hasil dari *penetaration test* tersebut langsung digunakan untuk evaluasi. Kebijakan ini berhasil merekrut 1,410 orang untuk berpartisipasi dan mengumpulkan laporan kerentanan sebanyak 1.189 hanya dalam waktu 13 menit dengan 138 laporan dianggap paling valid. Bahkan sebagai tindak lanjut keberhasilan ini, DoD membuat panduan bernama *DoD Vulnerability Disclosure Policy* dan *website* khusus untuk melakukan *penetration test.*[61] Contoh sukses ini tentu saja menjadi bukti harapan nyata dalam gagasan ini.

Berdasarkan gagasan tersebut, reformulasi PST sebagai upaya perlindungan hukum secara preventif terhadap data pribadi konsumen di era bisnis digital sudah tepat. Seperti yang termaktub dalam *Article* 33 dan 34 United Nations Guidelines Consumer Protection yang secara garis besarnya mewajibkan setiap negara memformulasikan regulasi perlindungan kepentingan konsumen dengan standar yang jelas dan memfasilitasi upaya perlindungannya.[62] Ketentuan normatif internasional ini selaras dengan postulat hukum CST Kansil bahwa "perlindungan hukum harus ditujukan untuk menciptakan rasa aman secara psikis dan fisik dari gangguan maupun ancaman siapapun".[63]

Oleh karena itu, penyempurnaan perlindungan konsumen dengan pemanfaatan teknologi untuk mencegah ancaman pihak anonim di ruang siber menjadi *ius*

[61] HackerOne, "Hack The Pentagon," *https://www.Hackerone.com/hack-the-pentagon*, diakses tanggal 29 Januari 2022.
[62]Guidelines PBB UNCTAD/DITC/CPLP/MISC/2016/1, *Article* 33 dan *Article* 34 United Nations Guidelines for Consumer Protection, hlm. 6.
[63] C.S.T Kansil, 1989, *Pengantar Ilmu Hukum Dan Tata Hukum Indonesia*, Penerbit Balai Pustaka, Jakarta, hlm. 40.

constituendum dikarenakan hakikat utama dari perlindungan data pribadi ialah mencegah informasi rahasia tersebut terdiseminasi. Bila mengandalkan perlindungan hukum secara represif, maka esensi menjaga kerahasiaan data pribadi tidak bisa dipulihkan sepenuhnya karena telah terjadi diseminasi.

D. Kesimpulan

Hukum Siber di Indonesia yang masih parsial dan sektoral mengakibatkan ketidakefektifan dalam menghadapi era bisnis digital. Bahkan UU ITE sebagai tulang punggung *cyberlaw* belum mengakomodir perlindungan hukum terhadap data pribadi konsumen secara komprehensif seperti perihal Lembaga Sertifikasi Keandalan dan Pengujian Keamanan platform yang hanya disinggung secara sekilas. Aturan pelaksana dari UU ITE yaitu PP PSTE juga tidak mengakomodir dengan baik hal-hal esensial ini dan belum dibentuknya peraturan pemerintah yang mengatur secara khusus Lembaga sertifikasi keandalan dan pengujian yang diselenggarakannya. Implikasi dari akar permasalahan ini adalah ketidaksamaan definisi, polemik pihak penyelenggara PST yang seharusnya dilakukan oleh Lembaga Sertifikasi Keandalan, tumpang tindih wewenang penerima laporan sertifikasi SMPI. Semua ketidaksistematisan atau kekacauan ini berimplikasi pada ketidakpastian hukum sehingga perlindungan kepada konsumen di bisnis digital gagal dan mengakibatkan korban berjatuhan dalam jumlah banyak baik secara materi maupun psikis. Atas kegagalan formulasi regulasi PST sebagai basis utama PDP konsumen di bisnis digital, maka dibutuhkan pembentukan lembaga independen yang menjadi tonggak utama penyelenggara PST sebagai basis utama pengujian sistem keamanan platform PSE dalam rangka melaksanakan perlindungan hukum secara preventif Maka dari itu, revisi berupa penambahan substansi pada UU ITE, pembentukan PP SMPIE, dan Perpres BP2SKIE yang inti keseluruhan kebijakan hukum ini ditujukan untuk mereformulasikan regulasi PST

lebih komprehensif melalui pembentukan Badan Pengujian dan Sertifikasi Sistem Keandalan Informasi Elektronik (BP2SKIE) dan pengaturan lebih rinci mengenai kewajiban PST dalam pengujian keamanan platform.

Daftar Pustaka

Buku

Amiruddin, and Zainal Asikin, 2012, *Pengantar Metode Penelitian Hukum*, Ctk. Keenam, Rajawali Pers, Jakarta.

Aprita, Serlika, 2020, *Hukum Dan Hak Asasi Manusia*, Mitra Wacana Media, Bogor.

Djafar, Wahyudi, dan M. Jodi Santoso, 2019, *Perlindungan Data Pribadi Konsep, Instrumen, Dan Prinsipnya*, Lembaga Studi dan Advokasi Masyarakat (ELSAM), Jakarta.

Doly, Denico, 2018, *Politik Hukum Pengaturan Perlindungan Data Pribadi*, Pusat Penelitian Badan Keahlian DPR RI, Jakarta.

Hadjon, Philipus M, 1988, *Perlindungan Hukum Bagi Rakyat Indonesia*, Bina Ilmu, Surabaya.

Ibrahim, Johny, 2007, *Teori Dan Metodologi Penelitian Hukum Normatif*, Bayumedia, Malang.

Kalo, Syafruddin, 2007, *Pengukuhan Pengurus Tapak Indonesia Koordinator Daerah Sumatera Utara*, Pengurus Tapak Indonesia Koordinator Daerah Sumatera, Medan.

Kansil, C.S.T, 1989, *Pengantar Ilmu Hukum Dan Tata Hukum Indonesia*, Penerbit Balai Pustaka, Jakarta.

Marzuki, Peter Mahmud, 2008, *Penelitian Hukum*, Ctk. Kedua, Kencana, Jakarta.

Muchsin, 2003, *Perlindungan dan Kepastian Hukum Bagi Investor*, Magister Ilmu Hukum Program Pascasarjana Universitas Sebelas Maret, Surakarta.

Pusat Operasi Keamanan Siber Nasional BSSN, 2021, *Laporan Tahunan Monitoring Keamanan Siber 2020*, Pusat Operasi Keamanan Siber Nasional BSSN, Jakarta.

Soekanto, Soerjono, 1984, *Pengantar Penelitian Hukum*, UI Press, Jakarta.

Syafrizal, Ismail Marzuki, Muhammad Iqbal, Syamsul Bahri, dkk, 2021, *Pengantar Ilmu Sosial*, Yayasan Kita Menulis, Medan.

Jurnal

Brown, Russel. "Rethinking Privacy", *Alberta Law Review*, Vol. 43, No. 589, 2006.

Chanine Ghanem, Mohammed, dan Thomas M Chen, "Reinforcement Learning for Efficient Network Penetration Testing", *Journal Information*, Vol. 11, No. 6, 2020.

Chlapowski, Francis S, "The Constitutional Protection of Information Privacy", *Boston University Law Review*, Vol. 7, 1991.

Dewi, Sinta, "Privasi Atas Data Pribadi: Perlindungan Hukum Dan Bentuk Pengaturan Di Indonesia", *Jurnal De Jure*, Vol. 15, No. 2, 2015.

Kusumoningtyas, Anggi Anggraeni, and Puspitasari, "Dilema Hak Perlindungan Data Pribadi Dan Pengawasan Siber: Tantangan Di Masa Depan", *Jurnal Legislasi Indonesia*, Vol. 17, No. 2, 2020.

Lukito, Imam, "Tantangan Hukum Dan Peran Pemerintah Dalam Pembangunan E-Commerce", *Jurnal Ilmiah Kebijakan Hukum*, Vol. 11, No. 3, 2017.

Matompo, Osgar S, "Pembatasan Terhadap Hak Asasi Manusia Dalam Prespektif Keadaan Darurat", *Jurnal Media Hukum*, Vol. 21, No. 1, 2014.

Negley, Glenn, "Philosophical Views on the Value of Privacy", *Law & Contemporary Problems Review*, Vol. 31, No. 319, 1966.

Paryadi, Deky, "Pengawasan E Commerce Dalam Undang-Undang Perdagangan Dan Undang-Undang Perlindungan Konsumen", *Jurnal Hukum Dan Pembangunan*, Vol. 48, No. 3, 2018.

Priliasari, Erna, "Pentingnya Perlindungan Data Pribadi Dalam Transaksi Pinjaman Online (The Urgency Of Personal Protection In Peer To Peer Lending)," *Majalah Hukum Nasional*, Vol. 49, No. 2, 2019.

Putri, Firmansyah, Deanne Destriani, dan Muhammad Helmi Fahrozi, "Upaya Pencegahan Data Konsumen Melalui Pengesahan RUU Perlindungan Data Pribadi (Studi Kasus E-Commerce Bhinneka.Com Case Study)", *Procceding: Call for Paper, 2nd National Conference on Law Studies: Legal Development Towards a Digital Society Era*, Vol. 2, No. 1, 2020.

Sefriani, and Sri Wartini, "Corporate Social Responsibility Dan Tanggung Jawab Negara Terhadap Hak Ekonimi, Sosial, Dan Budaya Di Indonesia", *Jurnal Yustisia*, Vol. 4, No. 2, 2015.

Sonia Ginasari, Ni Luh Ayu, kadek Suar Wibawa, and Ni Kadek Ayu Wirdiani, "Pengujian Stress Testing API Sistem Pelayanan Dengan Apache JMeter", *Jurnal Ilmiah Teknologi dan Komputer*, Vol. 2, No. 2, 2021.

Tesis

Buana, Mirza Satria, 2010, *Hubungan Tarik-Menarik Antara Asas Kepastian Hukum (Legal Certainpi) Dengan Asas Keadilan (Substantial Justice) Dalam Putusan-Putusan Mahkamah Konstltusi*, Tesis, Magister Ilmu Hukum Universitas Islam Indonesia, Yogyakarta.

Soerjati, Enni, 2008, *Lembaga Sertifikasi Keandalan Sebagai Salah Satu Upaya Perlindungan Hukum Terhadap Konsumen Dalam Transaksi Elektronik di Indonesia*, Tesis Magister Hukum, Fakultas Hukum Universitas Indonesia

Paper

Reza, S M Salim, Wahidul Hasan, and Sajib Chakraborty, "A Comparative Overview on Penetration Testing", Conference: 4th International Conference On Advance In Computing, Electronics & Electrical Technology (CEET-2015), Kuala Lumpur, 26-27 September 2015.

Internet

Ayyi, and Shila, "Kasus Kebocoran Data Semakin Banyak, Belanja Daring Paling Rentan", *https://lokadata.id/artikel/kasus-kebocoran-data-semakin-banyak-belanja-daring-paling-rentan*, diakses tanggal 30 Desember 2021.

Dihni, Vika Azkiya, "Kerugian Akibat Kejahatan Siber Capai Rp 3,88 Triliun, Apa Saja Bentuknya?", *https://databoks.katadata.co.id/datapublish/2021/10/07/kerugian-akibat-kejahatan-siber-capai-rp-388-triliun-apa-saja-bentuknya*, diakses tanggal 23 Januari 2022.

HackerOne, "Hack The Pentagon", *https://www.Hackerone.com/hack-the-pentagon*, diakses tanggal 29 Januari 2022.

Jayani, Dwi Hadya, "Pencurian Data Pribadi Makin Marak Kala Pandemi", *https://databoks.katadata.co.id/datapublish/2021/10/07/kerugian-akibat-kejahatan-siber-capai-rp-388-triliun-apa-saja-bentuknya*, diakses tanggal 23 Januari 2022.

Vishnum, "Ancaman Keamanan Siber Menyebabkan Kerugian Ekonomi Bagi Organisasi Di Indonesia Sebesar US$34.2 Miliar", *https://news.microsoft.com/id-id/2018/05/24/ancaman-keamanan-siber-menyebabkan-kerugian-ekonomi-bagi-organisasi-di-indonesia-sebesar-us34-2-miliar/#_ftn1*, diakses tanggal 23 Januari 2022.

World Banks, "Asia Pacific GDP Information," *https://data.worldbank.org/indicator/NY.GDP.MKTP.CD*, diakses tanggal 23 Januari 2022.

Peraturan Perundang-Undangan

Peraturan Badan Siber dan Sandi Negara Nomor 8 Tahun 2020 tentang Sistem Pengamanan dalam Penyelenggaraan Sistem Elektronik (Berita Negara Republik Indonesia Tahun 2020 Nomor 1375).

Peraturan Menteri Komunikasi dan Informatika Nomor 11 Tahun 2018 tentang Penyelenggaraan Sertifikasi Elektronik (Berita Negara Republik Indonesia Tahun 2018 Nomor 1238).

Peraturan Menteri Komunikasi dan Informatika Nomor 4 Tahun 2016 tentang Sistem Manajemen Pengamanan Informasi (Berita Negara Republik Indonesia Tahun 2016 Nomor 551).

Peraturan Otoritas Jasa Keuangan Nomor 57/POJK.04/2020 tentang Penawaran Efek Melalui Layanan Urun Dana Berbasis Teknologi Informasi (Lembaran Negara Republik Indonesia Tahun 2020 Nomor 281).

Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik (Lembaran Negara Republik Indonesia Tahun 2019 Nomor 185).

Surat Edaran Otoritas Jasa Keuangan Nomor 21/SEOJK.03/2017 Tentang Penerapan Manajemen Risiko Dalam Penggunaan Teknologi Informasi Oleh Bank Umum.

Surat Presiden Nomor R-58/Pres/12/2021 RUU tentang Perubahan Kedua Atas UU Nomor 11/2008 tentang ITE,

Undang-Undang Dasar Negara Republik Indonesia Tahun 1945 (Lembaran Negara Republik Indonesia Tahun 1959 Nomor 75).

Putusan Pengadilan

Putusan Mahkamah Konstitusi Nomor 50/PUU-VI/2008.

Peraturan Internasional

Guidelines Convention on the Organisation for Economic Co-operation and Development (OECD) No. C(80)58/FINAL.

Resolusi PBB No.G.A.Res. 217A (III) (1948).

Resolusi PBB No.G.A.Res. 2200A (XXI).

Guidelines PBB UNCTAD/DITC/CPLP/MISC/2016/1.