PERLINDUNGAN HUKUM PERUSAHAAN TEKNOLOGI TERHADAP SERANGAN *HACKING* DITINJAU DARI HUKUM POSITIF DAN *MAQASHID SYARIAH*

SKRIPSI

Diajukan Kepada :

Fakultas Syariah

Universitas Islam Negeri Raden Mas Said Surakarta

Untuk Memenuhi Persyaratan Guna Memperoleh

Gelar Sarjana Hukum

Oleh :

ATIKA SUCIATI

NIM. 192131097

PROGRAM STUDI HUKUM PIDANA ISLAM

JURUSAN HUKUM ISLAM

FAKULTAS SYARIAH

UNIVERSITAS ISLAM NEGERI RADEN MAS SAID SURAKARTA

2023

PERLINDUNGAN HUKUM PERUSAHAAN TEKNOLOGI TERHADAP SERANGAN HACKING DITINJAU DARI HUKUM POSITIF DAN *MAQASHID SYARIAH*

HALAMAN JUDUL

SKRIPSI

Diajukan Untuk Memenuhi Syarat

Guna Memperoleh Gelar Sarjana Hukum

Dalam Bidang Hukum Pidana Islam

Disusun Oleh:

ATIKA SUCIATI

NIM. 19.21.3.1.097

Surakarta, 13 Maret 2023

Disetujui dan Disahkan Oleh :

Dosen Pembimbing Skripsi

Suciyani, M. Sos.

NIP. 19900419 201903 1009

SURAT PERNYATAAN BUKAN PLAGIASI

Assalamu'alaikum Wr. Wb.

Yang bertanda tangan di bawah ini :

Nama : Atika Suciati
NIM : 19.21.3.1.097
Jurusan : HUKUM PIDANA ISLAM (*JINAYAH)*

Menyatakan bahwa penelitian skripsi berjudul **"PERLINDUNGAN HUKUM PERUSAHAAN TEKNOLOGI TERHADAP SERANGAN *HACKING* DITINJAU DARI HUKUM POSITIF DAN *MAQASHID SYARIAH*"**.

Benar-benar bukan merupakan plagiasi dan belum pernah diteliti sebelumnya. Apabila dikemudian hari diketahui bahwa skripsi ini merupakan plagiasi, saya bersedia menerima sanksi sesuai peraturan yang berlaku.

Demikian surat ini saya buat dengan sesungguhnya untuk dipergunakan sebagaimana mestinya.

Wassalamu'alaikum Wr. Wb.

Surakarta, 13 Maret 2023

Penyusun

ATIKA SUCIATI

Suciyani, M. Sos.

Dosen Fakultas Syariah

Universitas Islam Negeri Raden Mas Said Surakarta

NOTA DINAS

Hal : Skripsi

Sdri : Atika Suciati

Kepada Yang Terhormat

Dekan Fakultas Syariah

Universitas Islam Negeri

Raden Mas Said

Di Surakarta

Assalamu'alaikum Wr. Wb.

Dengan hormat, bersama ini kami sampaikan bahwa setelah menelaah dan mengadakan perbaikan seperlunya, kami memutuskan bahwa skripsi saudara Jihan Rizqi Nur Hanifah NIM : 19.21.3.1.097 yang berjudul :

"PERLINDUNGAN HUKUM PERUSAHAAN TEKNOLOGI TERHADAP SERANGAN *HACKING* DITINJAU DARI HUKUM POSITIF DAN *MAQASHID SYARIAH*"

Sudah dapat dimunaqosahkan sebagai salah satu syarat memperoleh gelar Sarjana Hukum (S.H) dalam bidang Hukum Pidana Islam (*Jinayah).*

Oleh karena itu kami mohon agar skripsi tersebut segera dimunaqosahkan dalam waktu dekat.

Demikian, atas dikabulkannya permohonan ini disampaikan terimakasih,

Wassalamu'alaikumWr. Wb

Surakarta, 13 Maret 2023

Dosen Pembimbing

Suciyani, M. Sos.

NIP. 19900419 201903 1009

PENGESAHAN

PERLINDUNGAN HUKUM PERUSAHAAN TEKNOLOGI TERHADAP SERANGAN *HACKING* DITINJAU DARI HUKUM POSITIF DAN *MAQASHID SYARIAH*

Disusun Oleh:

ATIKA SUCIATI

NIM. 19.21.3.1.097

Telah dinyatakan lulus dalam ujian munaqosah

Pada hari : Rabu, 10 Mei 2023

Dan dinyatakan telah memenuhi persyaratan guna memperoleh gelar

Sarjana Hukum (Di bidang Hukum Pidana Islam)

Penguji I	Penguji II	Penguji III
Abdullah Tri Wahyudi, S.Ag., S.H., M.H., CM	**Yoga Purnama, S.Pd., M.Pd.**	**Dr. Masrukhin, S.H., M.H.**
NIP. 197504122014111 002	**NIP. 198907222017011 176**	**NIP. 196401191994031 000**

Dekan Fakultas Syariah

Dr. Ismail Yahya, M.A.,

NIP. 19750409 199903 1 001

MOTTO

فَاِنَّ مَعَ الْعُسْرِ يُسْرًا

“Maka sesungguhnya beserta kesulitan ada kemudahan.”

(Al-Insyirah: 5).

PERSEMBAHAN

Alhamdulilah, dengan mengucap syukur kepada Allah SWT yang telah memberikan kekuatan, serta membekali ilmu melalui dosen-dosen UIN Raden Mas Said Surakarta. Atas karunia dan kemudahan yang engkau berikan, akhirnya skripsi ini dapat terselesaikan, shalawat serta salam selalu tercurahkan kepada junjungan kita Nabi Muhammad SAW.

Saya persembahkan terima kasih yang setulus-tulusnya kepada mereka yang telah mendukung secara phisikologi dan materil, memberikan arti hidup, serta orang-orang yang mengisi empat tahun terakhir, dengan segala ketulusan dan kebaikan selama ini. Kupersembahkan bagi mereka yang selalu berusaha untuk ada di kehidupanku khususnya teruntuk :

1. Orang yang paling berjasa dan bersabar dalam hidup saya kedua orang tuaku tercinta Bapak Supriyono dan Ibu Nuryanti yang selalu mendoakan, memberikan ruang untuk bisa tumbuh, dan motivasi untuk segera menyelesaikan perkuliahan. Terimakasih untuk segalanya.
2. Orang-orang yang selalu mendengarkan keluh kesah saya di setiap hari buruk maupun hari baik di hidup saya, kedua kakak saya Arifin Akhbar dan Alim Pramesti.
3. Serta keluarga besar yang tidak bisa saya sebutkan satu-persatu, terima kasih atas doa dan dukungannya selama ini.

PEDOMAN TRANSLITERASI

Pedoman transliterasi yang digunakan dalam penulisan skripsi di Fakultas Syariah Universitas Islam Negeri Raden Mas Said Surakarta didasarkan pada Keputusan Bersama Menteri Agama dan Menteri Pendidikan dan Kebudayaan RI Nomor 158/1987 dan 0543 b/U/1987 tanggal 22 Januari 1988. Pedoman transliterasi tersebut adalah :

1. Konsonan

Fonem konsonan Bahasa Arab yang dalam sistem tulisan Arab dilambangkan dengan huruf, sedangkan dalam transliterasi ini sebagian dilambangkan dengan tanda dan sebagian lagi dilambangkan dengan huruf serta tanda sekaligus. Daftar huruf Arab dan transliterasinya dengan huruf latin adalah sebagai berkut:

Huruf Arab	Nama	Huruf Latin	Nama
ا	Alif	Tidakdilambangkan	Tidak dilambangkan
ب	Ba	B	Be
ت	Ta	T	Te
ث	ṡa	ṡ	Es (dengan titik di atas)
ج	Jim	J	Je
ح	ḥa	ḥ	Ha (dengan titik di bawah)
خ	Kha	Kh	Ka dan ha
د	Dal	D	De
ذ	Żal	Ż	Zet (dengan titik di atas)
ر	Ra	R	Er
ز	Zai	Z	Zet
س	Sin	S	Es
ش	Syin	Sy	Es dan ye
ص	ṣad	ṣ	Es (dengan titik di bawah)
ض	ḍad	ḍ	De (dengan titik di bawah)

ط	ṭa	ṭ	Te (dengan titik di bawah)
ظ	ẓa	ẓ	Zet (dengan titik di bawah)
ع	’ ain	…‘…	Koma terbalik di atas
غ	Gain	G	Ge
ف	Fa	F	Ef
ق	Qaf	Q	Ki
ك	Kaf	Kh	Ka
ل	Lam	L	El
م	Mim	M	Em
ن	Nun	N	En
و	Wau	W	We
ه	Ha	H	Ha (dengan titik di bawah)
ء	hamzah	...’…	Apostrop
ي	Ya	Y	Ye

2. Vokal

Vokal bahasa Arab seperti vocal bahasa Indonesia terdiri dari vocal tunggal atau monoftong dan vocal rangkap atau diftong.

a. Vokal Tunggal

Vokal tunggal bahasa Arab yang lambangnya berupa tanda atau harakat, transliterasinya sebagai berikut:

Tanda	**Nama**	**Huruf Latin**	**Nama**
ـَ	Fatah	A	A
ـِ	Kasrah	I	I
ـُ	Dammah	U	U

Contoh:

No	Kata Bahasa Arab	Transiterasi
1.	كتب	Kataba
2.	ذكر	Żukira
3.	يذهب	Yażhabu

b. Vokal Rangkap

Vokal rangkap bahasa Arab yang lambangnya berupa gabungan antara harakat dan huruf maka transliterasinya gabungan huruf, yaitu :

Tanda dan Huruf	Nama	GabunganHuruf	Nama
أ... ى	Fathah dan ya	Ai	a dan i
أ... و	Fathah dan wau	Au	a dan u

Contoh :

No	Kata Bahasa Arab	Transliterasi
1.	كيف	Kaifa
2.	حول	Ḥaula

3. Vokal Panjang (Maddah)

Maddah atau vokal panjang yang lambangnya berupa harakat dan huruf, transliterasinya berupa huruf dan tandasebagai berikut :

Harakat dan Huruf	Nama	Huruf dan Tanda	Nama
أ... ى	Fathah dan alif atauya	Ā	a dan garis di atas
أ... ى	Kasrah dan ya	Ī	I dan garis di atas
أ... و	Dammah dan wau	Ū	u dan garis di atas

Contoh :

No	Kata Bahasa Arab	Transliterasi
1.	قال	Qāla
2.	قيل	Qīla

3.	يقول	Yaqūlu
4.	رمي	Ramā

4. Ta Marbutah

Transliterasi untuk Ta Marbutah ada dua (2), yaitu :

a. Ta Marbutah hidup atau yang mendapatkan harakat fathah, kasrah atau dammah transliterasinya adalah /t/.
b. Ta Marbutah mati atau mendapat harakat sukun transliterasinya adalah /h/.
c. Apabila pada suatu kata yang di akhir katanya Ta Marbutah diikuti oleh kata yang menggunakan kata sandang /al/ serta bacaan kedua kata itu terpisah maka Ta Marbutah itu ditransliterasikan dengan /h/.

Contoh :

No	Kata Bahasa Arab	Transliterasi
1.	روضةاألطفال	Rauḍah al-aṭfāl / rauḍatul atfāl
2.	طلحة	Ṭalhah

5. Syaddah (Tasydid)

Syaddah atau Tasydid yang dalam sistem tulisan Arab dilambangkan dengan sebuah tanda yaitu tanda Syaddah atau Tasydid. Dalam transliterasi ini tanda Syaddah tersebut dilambangkan dengan huruf, yaitu huruf yang sama dengan huruf yang diberi tanda Syaddah itu.

Contoh :

No	Kata Bahasa Arab	Transliterasi
1.	رّبنا	Rabbana
2.	نّ زل	Nazzala

6. Kata Sandang

Kata sandang dalam bahasa Arab dilambangkan dengan huruf yaitu ال . Namun dalam transliterasinya kata sandang itu dibedakan antara kata sandang yang diikuti oleh huruf Syamsiyyah dengan kata sandang yang diikuti oleh huruf Qamariyyah.

Kata sandang yang diikuti oleh huruf Syamsiyyah ditransliterasikan sesuai dengan bunyinya yaitu huruf /l/ diganti dengan huruf yang sama dengan huruf yang langsung mengikuti kata sandang itu. Sedangkan kata sandang yang diikuti oleh huruf Qamariyyah ditransliterasikan sesuai dengan aturan yang digariskan di depan dan sesuai dengan bunyinya. Baik diikuti dengan huruf Syamsiyyah atau Qamariyyah, kata sandang ditulis dari kata yang mengikuti dan dihubungkan dengan kata sambung.

Contoh :

No	Kata Bahasa Arab	Transliterasi
1.	جلال ر	Ar-rajulu
2.	ا لجلال	Al-Jalālu

7. Hamzah

Sebagaimana yang telah disebutkan di depan bahwa Hamzah ditransliterasikan dengan apostrof, namun itu hanya terletak di tengah dan di akhir kata. Apabila terletak diawal kata maka tidak dilambangkan karena dalam tulisan Arab berupa huruf alif. Perhatikan contoh berikut ini:

No	Kata Bahasa Arab	Transiterasi
1.	أكل	Akala
2.	تأخذون	Ta'khużuna
3.	النؤ	An-Nau'u

8. Huruf Kapital

Walaupun dalam system bahasa Arab tidak mengenal huruf kapital, tetapi dalam transliterasinya huruf capital itu digunakan seperti yang berlaku dalam EYD yaitu digunakan untuk menuliskan huruf awal, nama diri dan permulaan kalimat. Bila nama diri itu didahului oleh kata sandangan maka yang ditulis

dengan huruf capital adalah nama diri tersebut, bukan huruf awal atau kata sandangnya.

Penggunaan huruf awal capital untuk Allah hanya berlaku bila dalam tulisan Arabnya memang lengkap demikian dan kalau penulisan tersebut disatukan dengan kata lain sehingga ada huruf atau harakat yang dihilangkan, maka huruf capital tidak digunakan.

Contoh :

No	Kata Bahasa Arab	Transliterasi
1.	ومامحمّدإلارسول	Wa mā Muhammadun illā rasūl
2.	العالمينالحمدللهرب	Al-ḥamdu lillahi rabbil 'ālamīna

9. Penulisan Kata

Pada dasarnya setiap kata baikfi'il, isim, maupun huruf ditulis terpisah. Bagi kata-kata tertentu yang penulisannya dengan huruf Arab yang sudah lazim dirangkaikan dengan kata lain karena ada huruf atau harakat yang dihilangkan maka penulisan kata tersebut dalam transliterasinya bias dilakukan dengan dua cara yaitu bias dipisahkan pada setiap kata atau bias dirangkai.

Contoh :

No	Kata Bahasa Arab	Transliterasi
1.	لهوخيرالرازقينوإن الله	Wainnallāha lahuwa khairar-rāziqīn / Wainnallāha lahuwa khairur-rāziqīn
2.	فأوفواالكيل والميزان	Fa aufū al-Kaila wa al-mīzāna / Fa aufulkaila wal mīzāna

KATA PENGANTAR

Assalamu'alikum Wr. Wb

Dengan mengucapkan alhamdulillah, puji syukur penulis panjatkan kepada Allah SWT yang telah melimpahkan rahmat, hidayah serta inayah-Nya, sehingga penulis dapat menyelesaikan skripsi yang berjudul **"PERLINDUNGAN HUKUM PERUSAHAAN TEKNOLOGI TERHADAP SERANGAN *HACKING* DITINJAU DARI HUKUM POSITIF DAN *MAQASHID SYARIAH*".**

Skripsi ini disusun untuk menyelesaikan Studi Jenjang Sarjana 1 (S1) Program Studi Hukum Pidana Islam (Jinayah), Fakultas Syariah UIN Surakarta. Dalam penyusunan tugas akhir ini, penyusun telah banyak mendapatkan dukungan dan bantuan dari berbagai pihak yang telah menyumbangkan pikiran, waktu, dan tenaga.Oleh karena itu, penulis sampaikan terimakasih kepada:

1. Bapak Prof. Dr. H. Mudhofir, S.Ag., M.Pd. selaku Rektor UIN Raden Mas Said Surakarta.
2. Bapak Dr. Ismail Yahya, S.Ag., M.A. selaku Dekan Fakultas Syariah UIN Raden Mas Said Surakarta beserta jajaranya.
3. Dr. H. Masrukhin, S.H., M.H., selaku Ketua Jurusan Hukum Islam.
4. Muh. Zumar Aminuddin, S.Ag., M.H., selaku Sekretaris Jurusan Hukum Islam.
5. Bapak Jaka Susila, S.H., M.H. selaku Koordinator Program Studi Hukum Pidana Islam
6. Ibu Lila Pangestu Hadiningrum, M.Pd. selaku Dosen Pembimbing Akademik yang telah memberikan pengarahan kedisiplinan dan nasehatnya kepada penulis selama menempuh studi di UIN Raden Mas Said Surakarta.
7. Bapak Suciyani, M. Sos. selaku Dosen Pembimbing Skripsi yang selalu meluang waktu, pikiran serta memberikan pengarahan hingga terselesainya skripsi ini.

8. Dewan penguji, yang telah meluangkan waktu dan pikirannya untuk menguji skripsi ini guna membawa kualitas penulisan ke arah yang lebih baik.
9. Seluruh staff pengajar (dosen) dan staff pegawai/administrasi Fakultas Syariah, UIN Raden Mas Said Surakarta. yang telah memberikan ilmunya, semoga segala ilmu yang telah diberikan dapat bermanfaat dikehidupan saya.
10. Kepada orang tua dan kakak-kakakku, terima kasih telah memberikan dukungan moril maupun materil serta doa yang tiada henti, curahan kasih sayang, dan dukungan.
11. Teman-teman seperjuangan Prodi Hukum Pidana Islam angkatan 2019 serta sahabat yang telah berjuang bersama dan memberikan motivasi kepada penulis.
12. Semua pihak yang telah membantu terselesaikannya skripsi ini yang tidak dapat disebutkan satu persatu.

Semoga semua bantuan yang telah diberikan kepada penulis dicatat sebagai amal kebaikan di sisi Allah SWT. Penulis menyadari bahwa dalam penyusunan skripsi ini masih terdapat kekurangan dan jauh dari kesempurnaan, oleh karena itu penyusun mengharap kritik dan saran yang membangun untuk tercapainya kesempurnaan skripsi ini. Akhir kata, penyusun berharap semoga skripsi ini dapat bermanfaat bagi semua pihak.

Wassalamu'alaikum Wr. Wb

Surakarta, 13 Maret 2023

Atika Suciati
NIM. 19.21.3.1.097

ABSTRAK

ATIKA SUCIATI, NIM: 192131097 "**PERLINDUNGAN HUKUM PERUSAHAAN TEKNOLOGI TERHADAP SERANGAN *HACKING* DITINJAU DARI HUKUM POSITIF DAN *MAQASHID SYARIAH***". Kasus *hacking* yang marak pada perusahaan teknologi di Indonesia beberapa tahun terakhir, mengakibatkan perusahaan teknologi rugi besar dalam menangani permasalahan *hacking* tersebut. Padahal perusahaan teknologi sendiri menjadi sektor terbesar ekonomi digital. Peneliti menggunakan metode penelitian hukum normatif untuk menemukan aturan hukum, prinsip-prinsip hukum, maupun doktrin-doktrin hukum guna menjawab isu-isu hukum yang dihadapi. Tujuan dari penelitian ini yaitu regulasi dan infrastruktur kelembagaan mengenai perlindungan hukum perusahaan teknologi khususnya dalam menangani *hacking* dapat lebih efektif.

Perusahaan teknologi di Indonesia belum ada perlidungan hukum terhadap serangan *hacking* melalui kelembagaan. Walaupun kewenangan dari perlindungan tersebut telh diberikan kepada Badan Siber dan Sandi Negara (BSSN) maupun DITTIPIDSIBER POLRI, akan tetapi fungsi dari BSSN dan DITTIPIDSIBER POLRI masih belum maksimal jika berurusan dengan perusahaan teknologi. Menurut NCIS, kewenangan kedua lembaga tersebut masih belum cukup untuk dapat melindungi dunia siber nasional khususnya perusahaan teknologi. Walaupun dalam regulasi di Indonesia perlindungan tersebut telah tertuang pada Pasal 40 ayat 1 huruf (s) dan Pasal 52 Undang-Undang No. 28 tahun 2014 tentang Hak Cipta. Sedangkan dalam perspektif *maqashid syariah* dapat mengganggu tercapainya pemeliharaan harta, pemeliharaan agama, pemeliharaan akal, pemeliharaan jiwa, hingga pemeliharaan keturunan.

Kata Kunci: ***Perlindungan Hukum, Perusahaan Teknologi, Hacking, Maqashid Syariah***

ABSTRACT

*ATIKA SUCIATI, NIM: 192131097 "**LEGAL PROTECTION OF TECHNOLOGY COMPANIES AGAINST ATTACKS HACKING VIEWED FROM POSITIVE LEGAL AND MAQASHID SHARIA**". Hacking case which has been rife with technology companies in Indonesia in recent years, causing technology companies to suffer big losses in dealing with problems hacking the. Even though technology companies themselves are the largest sector of the digital economy. Researchers use normative legal research methods to find legal rules, legal principles, and legal doctrines to answer the legal issues they face. The purpose of this research is regulation and institutional infrastructure regarding the legal protection of technology companies, especially in handling hacking can be more effective.*

Technology company in Indonesia have no legal protection against hacking attacks through institutions. Even though the authority for this protection has been given to the National Cyber and Crypto Agency (BSSN) and DITTIPIDSIBER POLRI, the functions of BSSN and DITTIPIDSIBER POLRI are still not maximized when dealing with technology companies. According to NCIS, the authority of the two institutions is still insufficient to protect national cyberspace, especially technology companies. Even though in regulations in Indonesia this protection has been contained in Article 40 paragraph 1 letter (s) and Article 52 of Law no. 28 of 2014 concerning Copyright. Meanwhile in perspective maqashid sharia can interfere with the preservation of property, preservation of religion, preservation of mind, preservation of soul, up to preservation of offspring.

Keywords: ***Legal Protection, Technology Companies, Hacking, Maqashid Sharia***.

DAFTAR ISI

DAFTAR TABEL

DAFTAR GAMBAR

DAFTAR LAMPIRAN

BAB I
PENDAHULUAN

A. Latar Belakang Masalah

Peningkatan mobilisasi di dunia maya semakin tidak terkendali sebagai akibat dari adanya revolusi industri 4.0 yang telah mengaburkan garis antara bidang fisik, digital, dan biologis. Ditambah lagi adanya pandemi *Coronavirus Disease* 2019 dua tahun terakhir, membuat hampir semua orang yang ada di dunia mengharuskan tinggal dan beraktivitas dari rumah. Mobilisasi tersebut juga berdampak pada tingginya ancaman kriminalitas dalam dunia maya (*cybercrime*).[1]

Ancaman *cybercrime* tersebut tidak hanya tertuju pada instansi pemerintah akan tetapi pada individu dan perusahaan teknologi yang memanfaatkan teknologi untuk menjalankan bisnis utamanya. Berdasarkan data BSSN atau Badan Siber dan Sandi Negara terdapat 1.637.973.022 jumlah *anomali* nasional per Desember 2021. Dimana angka tersebut diambil dari berbagai jenis tindak pidana *hacking* yang merugikan sistem jaringan khususnya perusahaan teknologi.[2]

---

[1] Wahyudi Djafar, *Hukum Perlindungan Data Pribadi di Indonesia*, (Yogyakarta: Universitas Gajah Mada, 2020), hlm. 1

[2] Direktorat Operasi Keamanan Siber, *Laporan Tahunan Monitoring Keamanan Siber 2021*, (Jakarta Selatan, 2021), hlm. 16

Tindak pidana *hacking* seringkali menjadi musuh terbesar dari suatu sistem jaringan khususnya perusahaan teknologi. Karena *hacking* dapat mengakibatkan sistem dimata-matai, perubahan pada sistem, mengganggu kinerja sistem, hingga pencurian data penting pada sistem perusahaan teknologi.[3] Dikutip dari KataData.co.id yang merujuk pada Perusahaan Keamanan Siber Global ACRONIS, memperkirakan proyeksi biaya penanganan *cyber* sebesar Rp 78 Miliar per insiden di tahun 2023 ini.[4]

Seperti halnya pencurian 1,3 miliar data registrasi SIM Card yang berhasil dilakukan oleh *attacker* yang beridentitas sebagai @Bjorka pada awal November 2022 lalu. Pencurian data tersebut diketahui diambil dari Kementerian Komunikasi dan Informatika (Kominfo). Data tersebut dijual seharga US$500 ribu atau sekitar Rp 745,6 juta pada salah satu *dark market*.[5]

Kasus kebocoran data oleh salah satu pemegang amanat terbesar pemerintah Indonesia di dunia teknologi tersebut, membuat masyarakat sekaligus perusahaan teknologi mempertanyakan akan keamanan dunia maya. Padahal keamanan di dunia maya tersebut menjadi objek vital

---

[3] Beni Setiawan, *Penegakan Hukum Pidana Terhadap Akses Sistem Komputer Secara Ilegal (Hacking) dan Menimbulkan Kerusakan (Cracking) dalam Kejahatan Dunia Maya (Cybercrime) Menurut Perspektif Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik*, (Jambi: Universitas Batanghari, 2019), hlm. 11

[4] Dikutip dari Katadata.com/ Proyeksi Peretasan & Penipuan 2023, Biayanya Rp78 M per Kebocoran Data (msn.com) pada tanggal 6 Februari pukul 15.24

[5] Dikutip dari CNBCIndonesia.com/ kebocoran data kominfo oleh bjorka - Penelusuran Google pada tanggal 12 Januari 2023 pukul 07.11

perusahaan teknologi dalam menjalankan bisnisnya. Perlu adanya perlindungan khusus untuk meminimalisir kerugian yang diakibatkan oleh tindak pidana *hacking* terutama pada perusahaan teknologi. Perlindungan yang dapat diberikan pemerintah dapat berupa regulasi spesifik dan juga infrastruktur kelembagaan yang memadai, untuk dapat mengimbangi perkembangan kejahatan di dunia maya. Regulasi dan infrastruktur kelembagaan tersebut juga perwujudan dari hak sebagai subjek hukum.[6]

Hak untuk mendapatkan perlindungan sebagai subjek hukum tersebut bukan hanya ada dalam hukum positif saja, akan tetapi juga ada dalam hukum Islam yang berbentuk *maqashid syariah*. Dikutip dari Amir Syarifuddin yang merujuk pada Imam Asy-Syatibi, *maqashid syariah* sendiri merupakan bentuk dari tujuan-tujuan utama perlindungan umat atau mencapai *maslahat* umat manusia. Walaupun dalam *maqashid syariah* tidak ada spesifikasi perlindungan untuk tindak pidana *hacking*. Karena *hacking* sendiri merupakan peristiwa kontemporer yang masih perlu ijtihad dari hakim maupun dari pemimpin.[7]

Maka dari permasalahan-permasalahan tersebut pada penelitian kali ini, penulis mengajukan judul dalam rencana penelitian ini mengenai "**Perlindungan Hukum Perusahaan Teknologi Terhadap Serangan *Hacking* Ditinjau dari Hukum Positif dan *Maqashid Syariah*"** agar dapat mengetahui sejauh mana perlindungan yang telah diberikan

---

[6] Mohammad Iqbal Rasyid, *Perlindungan Hukum Pada Pemanfaatan Teknologi Informasi*, (Depok: Universitas Indonesia, 2018), hlm. 7

[7] Amir Syarifuddin, *Ushul Fiqh Jilid 2*, (Jakarta: Prenada Media, 2008), hlm. 231

pemerintah Indonesia kepada perusahaan teknologi yang terkena *hacking*. Adapun detail metode yang penulis pakai yaitu metode penelitian hukum normatif, yaitu suatu proses untuk menemukan aturan hukum, prinsip-prinsip hukum, maupun doktrin-doktrin hukum guna menjawab isu-isu hukum yang dihadapi.[8] Berikut sistematika penulisan rencana penelitian akan disampaikan dalam beberapa sub-bab ke depan.

B. Rumusan Masalah

Berdasarkan latar belakang masalah di atas, maka yang menjadi pokok permasalahan sebagai berikut:

1. Bagaimana perlindungan hukum perusahaan teknologi terhadap serangan *hacking* di Indonesia?
2. Bagaimana perlindungan hukum perusahaan teknologi terhadap serangan *hacking* dari perspektif *maqashid syariah*?

C. Tujuan Penelitian

Tujuan penulis dalam meneliti dan melakukan pengumpulan data kali ini yaitu:

1. Untuk menganalisis perlindungan hukum yang dapat digunakan perusahaan teknologi di Indonesia.
2. Untuk menganalisis perlindungan hukum perusahaan teknologi yang mengalami serangan *hacking* dari perspektif *maqashid syariah*.

---

[8] Peter Mahmud Marzuki, *Penelitian Hukum*, (Jakarta: Prenada Media, 2005), hlm. 47

D. Manfaat Penelitian

Hasil penelitian ini diharapkan maupun memberikan manfaat dari penelitian sebagai berikut:

1. Manfaat Teoritis

   Hasil penelitian ini diharapkan dapat memberikan manfaat secara teori terhadap referensi literatur dalam memahami perlindungan hukum perusahaan teknologi terhadap serangan *hacking* di Indonesia.

2. Manfaat Praktis

   Hasil penelitian ini diharapkan dapat menjadi pertimbangan hukum dalam memaksimalkan regulasi dan unit kelembagaan sebagai upaya perlindungan hukum bagi perusahaan teknologi yang terkena *hacking* di Indonesia.

E. Kerangka Teori

1. Teori Hukum Progresif

Menurut Satjipto Rahardjo, perlindungan hukum adalah pemberian pengayoman terhadap hak asasi manusia yang dirugikan orang lain dan perlindungan itu diberikan kepada masyarakat agar dapat menikmati semua hak-hak yang diberikan oleh hukum. Hukum melindungi kepentingan seseorang dengan cara mengalokasikan suatu kekuasaan kepadanya untuk bertindak dalam rangka kepentingannya tersebut. Pengalokasian kekuasaan ini dilakukan secara terukur, dalam

arti, ditentukan keluasan dan kedalamannya. Kekuasaan yang demikian itulah yang disebut sebagai hak.[9]

Hak tersebut didapatkan seluruh subjek hukum tanpa terkecuali. Salah satunya yaitu perusahaan teknologi. Sebagai sebuah perusahaan yang menjalankan bisnis menggunakan bantuan teknologi, sebuah perusahaan teknologi dapat melindungi program komputer sebagai sebuah aset perusahaan dengan mendaftarkannya pada Hak Kekayaan Intelektual (HKI). Penegasan bahwa program komputer merupakan ciptaan yang dilindungi tercantum dalam Pasal 40 ayat (1s) Undang-Undang Nomor 19 Tahun 2014 tentang Hak Cipta.[10]

2. Teori Perlindungan Hukum Philipus M. Hadjon

Philipus M. Hadjon menafsirkan konsep perlindungan hukum sebagai suatu kondisi dimana subjektif yang menyatakan hadirnya keharusan pada diri sejumlah subjek hukum untuk segera memperoleh sejumlah hak, guna kelangsungan eksistensi subjek hukum yang dijamin dan dilindungi oleh hukum.[11]

Lebih lanjut menurut Philipus M. Hadjon perlindungan hukum yang diberikan oleh pemerintah dapat dikategorikan menjadi dua bentuk yaitu perlindungan preventif dan perlindungan represif. Kedua perlindungan tersebut diberikan sebagai bentuk pencegahan dan

[9] Satjipto Rahardjo, *Ilmu Hukum*, (Bandung: PT. Citra Aditya Bakti, 2000), hlm. 53-54

[10] Undang-Undang Nomor 28 Tahun 2014 Tentang Hak Cipta (Lembaran Negara Republik Indonesia Tahun 2014 Nomor 266, Tambahan Lembaran Negara Republik Indonesia Nomor 5599)

[11] Philipus M. Hadjon, *Perlindungan Hukum bagi Rakyat Indonesia…*, hlm. 2

penyelesaian akan suatu permasalahan pada subjek hukum. Dalam hal ini perlindungan tersebut diperuntukkan pada perusahaan teknologi yang terkena *hacking*.[12]

3. Teori Mengenai *Hacking*

Hacking atau dalam Bahasa Indonesia disebut dengan peretasan. Menurut Kamus Hukum Online peretasan merupakan segala bentuk perbuatan untuk memasuki suatu sistem elektronik tanpa izin dari pemilik maupun pengguna sistem elektronik yang berhak. Istilah ini merupakan terjemahan dari kata *hacking*.[13]

Menurut Christian Prabowo, dalam konteks keamanan jaringan komputer *hacking* adalah kegiatan menerobos program komputer milik orang atau pihak lain. Sedangkan *hacker* adalah orang yang gemar mencari celah pada komputer, memiliki keahlian membuat, maupun membaca program tertentu, dan terobsesi mengamati keamanan (*security*)-nya. Secara umum *hacker* dibagi menjadi dua jenis yaitu *white hacker* dan *black hacker* atau lebih sering disebut dengan *attacker*.[14]

---

[12] *Ibid.*

[13] Dikutip pada https://kamushukum.web.id/arti-kata/peretasan/ diakses pada 19 Januari 2023 pukul 10.46 WIB

[14] Christian Prabowo, *Keamanan Jaringan*, (Surakarta: Universitas Slamet Riyadi, 2021), hlm. 1

4. Teori *Maqashid Syariah* dalam Hukum Pidana Islam

Dikutip dari Ghofar Shidiq yang merujuk pada Imam Asy-Syatibi, konsep *maqashid syariah* merupakan perwujudan lima hal-hal penting yang perlu dilindungi manusia sebagai umat di dunia. *Maqashid syariah* sendiri bertujuan untuk mewujudkan kebaikan dan menghindarkan manusia dari keburukan atau dalam hal ini disebut juga dengan maslahat. Dapat disimpulkan bahwa *maqashid syariah* merupakan tujuan-tujuan yang hendak diwujudkan dari suatu penetapan hukum. [15]

Dikutip dari Amiruddin Amirullah yang merujuk pada karya Imam Asy Syatibi dalam Kitab al-Muwāfaqāt menjelaskan bahwa maslahat dapat ditinjau dari dua perspektif yang menjadi keistimewaan beliau, yaitu perspektif dari terjadinya *maslahat* dalam kenyataan dan perspektif dari tergantungnya tuntutan *syariat* kepada maslahat. Dalam *maqashid syariah* terdapat lima ruang lingkup yang harus dipelihara oleh umat manusia, yaitu :

a. Memelihara agama atau keberagamaan (حفظ الدين)
b. Memelihara jiwa atau diri atau kehidupan (حفظ النفس)
c. Memelihara akal (حفظ العقل)
d. Memelihara keturunan (حفظ النسل)
e. Memelihara harta (حفظ المال).[16]

---

[15] Ghofar Shidiq, *Teori Maqashid Al Syariah Dalam Hukum Islam*, Vol. XLIV Nomor 118, (Semarang: Universitas Sultan Agung, 2019), hlm. 118

[16] Amir Syarifuddin, *Ushul Fiqh Jilid 2*, (Jakarta: Prenada Media, 2008), hlm. 233-238

Berdasarkan Imam Asy-Syatibi tersebut, pengimplementasian *maqashid syariah* sendiri apabila dilihat dari perlindungan perusahaan teknologi yang terkena *hacking* maka yang menjadi dasar perlindungannya yaitu memelihara harta dan memelihara agama.[17]

F. Tinjauan Pustaka

Tinjauan pustaka yang dipakai oleh penulis dalam penelitian ini diambil dari penelitian orang lain yang telah selesai beberapa tahun terakhir dan berkaitan dengan pembahasan penulis, beberapa diantaranya yaitu sebagai berikut :

Jurnal Beni Setiawan mahasiswa Fakultas Hukum Universitas Batanghari yang berjudul "Penegakan Hukum Pidana Terhadap Akses Sistem Komputer Secara Ilegal (*Hacking*) dan Menimbulkan Kerusakan (*Cracking*) dalam Kejahatan Dunia Maya (*Cybercrime*) Menurut Perspektif Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik". Jurnal ini membahas tentang pemidanaan ditinjau dari Undang-Undang Informasi dan Transaksi Elektronik. Persamaan dengan penelitian ini adalah sama-sama mengkaji tentang *hacking* pada program komputer. Namun perbedaan penelitian ini yaitu pada penerapan dari perlindungannya yang spesifik pada perusahaan teknologi yang terkena *hacking*.

Jurnal yang disusun oleh Dona Budi Kharisma mahasiswa Fakultas Hukum Sebelas Maret yang berjudul "Membangun Kerangka Startup di

---

[17] *Ibid.*

Indonesia". Jurnal ini membahas tentang konsep dasar peraturan startup. Persamaan dengan penelitian ini adalah sama-sama mengkaji tentang konsep dasar peraturan yang berlaku pada startup. Namun perbedaan dengan penelitian ini yaitu konsep dasar peraturan startup tersebut dapat menjadi unsur perlindungan hukum pada perusahaan teknologi terhadap serangan *hacking*.

Jurnal yang disusun oleh Kotim Subandi dan Victor Ilyas Sugara mahasiswa Universitas Muhammadiyah Jakarta yang berjudul "Analisa Serangan Vulnerabilities Terhadap Server Selama Periode WFH di Masa Pandemi Covid-19 Sebagai Prosedur Mitigasi". Jurnal ini meneliti tentang mitigasi yang dapat diterapkan pada sistem keamanan komputer agar tidak terjadi serangan *hacking*. Persamaan dengan penelitian ini adalah sama-sama mengkaji tentang mitigasi keamanan program komputer. Namun perbedaan penelitian ini yaitu penulis mengkajinya secara keseluruhan untuk mengetahui penggunaan keamanan mana yang harus perusahaan teknologi gunakan.

Jurnal yang disusun oleh Stephanie PD, Natasha OA, Enjelina S, Ahmad Redi mahasiswa Universitas Tarumanegara berjudul "Mengelaborasi Hukum Positif Tertulis Indonesia Mengatur Startup, Seminar Nasional Hasil Penelitian dan Pengabdian Kepada Masyarakat 2021". Jurnal ini membahas tentang dampak penerapan peraturan pemerintah pada startup dan masyarakat. Persamaan dengan penelitian ini adalah sama-sama mengkaji tentang dampak regulasi perusahaan sebagai

bentuk perlindungan. Namun perbedaan penelitian ini yaitu pada penerapan perlindungan perusahaan teknologi sebagai bentuk hak yang diberikan kepada perusahaan teknologi sebagai subjek hukum.

G. Metode Penelitian

1. Jenis Penelitian

Metode penelitian yang penulis gunakan yaitu metode penelitian hukum normatif, yang didefinisikan sebagai suatu proses untuk menemukan aturan hukum, prinsip-prinsip hukum, maupun doktrin-doktrin hukum guna menjawab isu-isu hukum yang dihadapi.[18]

Dengan begitu penulis dapat menguraikan terkait perlindungan hukum dalam perspektif hukum positif yang dapat digunakan pada kasus *hacking* dari data sekunder. Dalam penelitian ini juga menggunakan penelitian kepustakaan (*library research*), yaitu penelitian yang dilakukan melalui bahan-bahan pustaka atau literatur kepustakaan atau biasa disebut dengan penelitian deskriptif karena dalam penjelasannya menggunakan yuridis normatif yang bertujuan untuk menjelaskan dan menerangkan suatu produk hukum positif yang berlaku di Indonesia. Dalam penelitian berfokus pada perusahaan teknologi yang terkena *hacking* dari kasus pertama di tahun 2015 hingga kasus terbaru di akhir tahun 2022.[19]

---

[18] Peter Mahmud Marzuki, *Penelitian Hukum*…, hlm. 47

[19] M. Nazir, *Metode Penelitian*, (Jakarta: Ghalia Indonesia, 2003), hlm. 111

2. Sumber Data

Sumber data yang diambil merupakan sumber data sekunder yang berupa penelitian kepustakaan yang dilakukan terhadap berbagai macam bahan hukum yang terbagi menjadi 3 (tiga) yaitu: [20]

a. Bahan Hukum Primer

Bahan hukum primer yang digunakan yaitu Pasal 30 Undang-Undang Nomor 11 Tahun 2008 tentang Penerobosan Sistem Keamanan Komputer, Pasal 40 ayat 2 Undang-Undang Nomor 19 Tahun 2016 atas perubahan Undang-Undang Nomor 11 Tahun 2008 tentang Dasar Perlindungan Pemanfaatan Sistem Informasi Elektronik, Pasal 1 angka 9 dan/atau Pasal 40 ayat 1 huruf (s) dan Pasal 52 Undang-Undang No. 28 tahun 2014 tentang Hak Cipta, maupun peraturan perundang-undangan lain yang relevan.

b. Bahan Hukum Sekunder

Bahan hukum sekunder dalam mendukung penelitian ini yaitu buku, jurnal, dan skripsi yang berkaitan dengan *cyber hacking*, hak cipta, dan *cybersecurity.*

c. Bahan Hukum Tersier

Bahan hukum tersier yang digunakan yaitu kamus dan ensiklopedia yang relevan dengan tema penelitian ini.

---

[20] *Ibid.,* Hlm. 14.

3. Teknik Pengumpulan Data

Pengumpulan data yang penulis gunakan yaitu metode studi dokumentasi. Metode dokumentasi merupakan menganalisis catatan peristiwa yang sudah berlalu. Dokumen dapat berbentuk tulisan, gambar atau karya-karya monumental dari seseorang. Dokumen yang berbentuk tulisan misalnya catatan harian, sejarah kehidupan, cerita, biografi, peraturan, kebijakan. Sejumlah besar fakta dan data tersimpan dalam bahan yang berbentuk dokumentasi. Dokumentasi ini dapat berbentuk surat-surat, catatan harian, laporan, foto, dan sebagainya.[21]

4. Teknik Analisis

Adapun dalam penelitian ini, penulis menggunakan teknik analisis isi (*content analysis*) adalah penelitian yang bersifat pembahasan mendalam terhadap isi suatu informasi tertulis atau tercetak dalam media massa. Analisis ini biasanya digunakan pada penelitian kualitatif. Terdapat beberapa definisi mengenai analisis isi. Analisis isi secara umum diartikan sebagai metode yang meliputi semua analisis mengenai isi teks, tetapi di sisi lain analisis isi juga digunakan untuk mendeskripsikan pendekatan analisis yang khusus. Menurut Holsti, metode analisis isi adalah suatu teknik untuk mengambil

[21] Imam Gunawan, *Metode Penelitian Kualitatif Teori & Praktik*, (Jakarta: Bumi Aksara, 2015), hlm. 143

kesimpulan dengan mengidentifikasi berbagai karakteristik khusus suatu pesan secara objektif, sistematis, dan generalis.[22]

H. Sistematika Penelitian

Dalam penelitian ini, penulis menggunakan sistematika penelitian sebagai berikut:

Bab I, merupakan bagian dari pendahuluan. Dalam bab pendahuluan ini penulis menguraikan latar belakang, rumusan masalah, tujuan penelitian, manfaat penelitian, kerangka teoritis, kemudian tinjauan pustaka yang menjadi sumber pokok dalam penulisan ini dan yang terakhir yaitu sistematika penulisan.

Bab II, merupakan bagian pembahasan mengenai kerangka dasar dari teori-teori perlindungan, teori *hacking,* dan juga *maqashid syariah*.

Bab III, berisi tentang data perlindungan hukum perusahaan teknologi terhadap serangan *hacking* di Indonesia.

Bab IV, berisi tentang analisis perlindungan hukum perusahaan teknologi terhadap serangan *hacking* di indonesia dalam perspektif hukum positif dan *maqashid syariah*.

Bab V, berisi tentang kesimpulan yang didapat oleh penulis dari temuan-temuan melalui metode kepustakaan (*library research*), kritik, serta saran.

---

[22] A.M. Irfan Taufan Asfar, *Analisis Naratif, Analisis Konten, dan Analisis Semiotik*, (Jakarta: UIN Syarif Hidayatullah, 2016), hlm. 2

I. Jadwal Rencana Penelitian

NO	BULAN	SEPTEMBER				OKTOBER				NOPEMBER				DESEMBER				JANUARI				FEBRUARI				MARET		
	KEGIATAN	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3
1.	Penyusunan Proposal	X	X	X	X																							
2.	Konsultasi				X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
3.	Revisi Proposal				X	X	X	X	X																				
4.	Pengumpulan Data							X	X	X	X	X	X	X	X	X													
5.	Analisis											X	X	X	X	X	X												
6.	Penulisan Akhir Naskah Skripsi																X	X	X	X	X	X	X	X	X				
7.	Pendaftaran Munaqasyah																									X		
8.	Munaqasyah																										X	
9.	Revisi Skripsi																											X

BAB II
TINJAUAN UMUM TENTANG PERLINDUNGAN HUKUM PERUSAHAAN TEKNOLOGI

A. Teori Hukum Progresif

Dikutip dari Liky Faizal yang merujuk pada karya Prof. Satjipto Rahardjo, teori hukum progresif merupakan teori yang dicetuskan oleh Prof. Satjipto Rahardjo dengan latar belakang pemikiran adanya penerapan sistem hukum di Indonesia yang selalu statis, koruptif, dan tidak memiliki keberpihakan struktural terhadap hukum yang hidup di tengah masyarakat. Selain itu menurutnya hukum telah kehilangan basis sosial, multikultural, dan ditegakkan secara sentralistik dalam sistem hukum yang berlaku.[1]

Dengan dasar antroposentrisme Prof. Satjipto Rahardjo merumuskan dua tujuan hukum yaitu, hukum dibuat untuk manusia dan bukan sebaliknya dan juga hukum terfokus pada manusia atau subjek hukum secara keseluruhan. Dalam hal ini tujuan dari perlindungan hukum tersebut yaitu sebagai perlindungan perusahaan teknologi yang terkena *hacking*.[2]

---

[1] Liky Faizal, *Problematika Hukum Progresif di Indonesia*, (Lampung: IAIN Raden Intan Lampung, 2017), hlm. 3

[2] Liky Faizal, *Problematika Hukum Progresif* ..., hlm. 4

Definisi perlindungan hukum menurut Prof. Satjipto Rahardjo merupakan sebuah pemberian pengayoman terhadap hak asasi manusia yang dirugikan orang lain dan perlindungan itu diberikan kepada masyarakat agar dapat menikmati semua hak-hak yang diberikan oleh hukum. Dimana hukum sendiri melindungi kepentingan seseorang dengan cara mengalokasikan suatu kekuasaan kepadanya untuk bertindak dalam rangka kepentingannya. Pengalokasian kekuasaan ini dilakukan secara terukur, dalam arti, ditentukan keluasan dan kedalamannya agar tidak terjadi penyalahgunaan kekuasaan atau hal-hal lain yang merugikan subjek hukum. Kekuasaan yang demikian itulah yang disebut sebagai hak.[3]

Hak tersebut didapatkan seluruh subjek hukum tanpa terkecuali. Salah satunya yaitu perusahaan teknologi. Sebagai sebuah perusahaan yang menjalankan bisnis menggunakan bantuan teknologi, sebuah perusahaan teknologi dapat melindungi program komputer sebagai sebuah aset perusahaan dengan mendaftarkannya pada Hak Kekayaan Intelektual (HKI). Penegasan bahwa program komputer merupakan ciptaan yang dilindungi tercantum dalam Pasal 40 ayat (1s) Undang-Undang Nomor 19 Tahun 2014 tentang Hak Cipta.[4]

---

[3] Satjipto Rahardjo, *Ilmu Hukum*, (Bandung: PT. Citra Aditya Bakti, 2000), hlm. 53-54

[4] Beni Setiawan, *Penegakan Hukum Pidana Terhadap Akses Sistem Komputer Secara Ilegal (Hacking) dan Menimbulkan Kerusakan (Cracking) dalam Kejahatan Dunia Maya (Cybercrime) Menurut Perspektif Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik*, (Jambi: Universitas Batanghari, 2019), hlm. 3

B. Teori Hukum Perlindungan Philipus M. Hadjon

Negara hukum yang mengakui adanya konsep-konsep perlindungan hak-hak asasi manusia, negara Indonesia khususnya pemerintah berhak menetapkan batasan-batasan dan kewajiban antara masyarakat dan juga pemerintahan itu sendiri. Salah satu pencetus teori perlindungan hukum yaitu Philipus M. Hadjon yang merumuskan prinsip perlindungan hukum bagi rakyat Indonesia yang berlandaskan Pancasila dan falsafah negara.[5]

Perlindungan hukum menurut Philipus M. Hadjon merupakan tempat utama yang dapat dikaitkan dengan tujuan dari negara hukum. Dimana perlindungan hukum tersebut melindungi harkat dan martabat, serta pengakuan terhadap hak asasi manusia yang dimiliki subjek hukum. Dalam hal ini perlindungan hukum tersebut berkaitan dengan perusahaan teknologi yang terkena *hacking*.[6]

Lebih lanjut menurut Philipus M. Hadjon perlindungan hukum yang diberikan oleh pemerintah dapat dikategorikan menjadi dua bentuk, yaitu :

1. Perlindungan Preventif

   Perlindungan ini memberikan setiap subjek hukum kesempatan untuk mengajukan keberatan atau pendapatnya sebelum suatu keputusan pemerintah berkekuatan hukum tetap.

---

[5] Philipus M. Hadjon, *Perlindungan Hukum bagi Rakyat Indonesia*, (Surabaya: Bina Ilmu, 1987), hlm. 2

[6] Philipus M. Hadjon, *Perlindungan Hukum Bagi Rakyat Indonesia*,.. hlm. 2

Tujuan adanya perlindungan ini yaitu mencegah adanya sengketa atau menghilangkan kesempatan melakukan kejahatan.

Jadi dapat disimpulkan perlindungan ini mengharuskan pemerintah untuk memitigasi risiko adanya kejahatan dan memperbaiki sistem hukum untuk melindungi subjek hukum yang dalam penelitian ini berfokus pada perusahaan teknologi. Selain itu perlindungan ini juga memberikan ruang masyarakat atau semua subjek hukum untuk menyuarakan opini mereka untuk melindungi kepentingan subjek hukum.

2. Perlindungan Represif

Perlindungan ini ada untuk menyelesaikan terjadinya sengketa ataupun kejahatan yang juga termasuk penanganannya di lembaga peradilan. Dengan kata lain upaya represif ini baru dapat dilakukan pada saat telah terjadi tindak pidana atau kejahatan yang tindakannya berupa menjatuhkan hukuman dan/atau sanksi lain.

Dapat disimpulkan perlindungan represif ini lebih menekankan upaya-upaya pemerintah atau dalam hal ini memberikan kewenangannya kepada penegak hukum untuk memberikan sanksi berupa hukuman. Hukuman tersebut hanya dapat dilaksanakan apabila subjek hukum terbukti melakukan tindak pidana.[7]

[7] *Ibid.,* Hlm, 2.

Kedua perlindungan tersebut diberikan sebagai bentuk pencegahan dan penyelesaian akan suatu permasalahan pada subjek hukum yang dalam hal ini perusahaan teknologi.[8] Dengan begitu perusahaan teknologi akan merasakan perlindungan dari pemerintah sebagai lembaga yang berwenang dalam perumusan hukum yang berlaku di masyarakat.

C. Teori *Hacking*

Kata *hacking* diterjemahkan dalam Bahasa Indonesia diartikan sebagai peretasan. Menurut Kamus Hukum Online, peretasan merupakan segala bentuk perbuatan untuk memasuki suatu sistem elektronik tanpa izin dari pemilik maupun pengguna sistem elektronik yang berhak.[9] Dalam arti luas *hacking* merupakan tindakan penyusupan atau perusakan suatu sistem komputer untuk tujuan tertentu.

Sedangkan menurut Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik *hacking* atau tindakan peretasan diartikan sebagai perbuatan setiap orang yang dengan sengaja dan tanpa hak atau melawan hukum mengakses komputer dan/atau sistem elektronik milik orang lain dengan cara apapun.[10]

---

[8] *Ibid.*

[9] Dikutip pada https://kamushukum.web.id/arti-kata/peretasan/ diakses pada 19 Januari 2023 pukul 10.46 WIB

[10] Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik (Lembaran Negara Republik Indonesia Tahun 2008 Nomor 58, Tambahan Lembaran Negara Republik Indonesia Nomor 4843). Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 tentang ITE (Lembaran Negara Republik Indonesia Tahun 2016 Nomor 251)

Seseorang yang memiliki ilmu dan kemampuan *hacking* sendiri disebut sebagai seorang *hacker*. *Hacker* dapat dibedakan menjadi dua yaitu *white hacker* dan *black hacker*. *White hacker* atau lebih sering disebut dengan *ethical hacker* merupakan sebutan seseorang yang memiliki ilmu *hacking* untuk memanfaatkan ilmunya dan kemampuannya, seperti mengelola sebuah jaringan, membantu menunjukkan kelemahan sebuah web, dan membantu merangkai sistem keamanan komputer lain. Sedangkan *black hacker* atau *attacker* merupakan sebutan untuk seseorang yang memanfaatkan ilmu *hacking* yang dimilikinya dengan tujuan yang buruk seperti memata-matai sistem, mencuri data, mengintip password, merusak sistem, dan tindakan perusakan sistem komputer lain.[11]

Pada setiap kasus peretasan umumnya bertujuan untuk mengambil data-data tertentu yang dimiliki target, khususnya perusahaan teknologi. Tetapi ada pula peretasan yang bertujuan menghancurkan data atau sistem tertentu sehingga berdampak seperti kerusakan digital.[12]

Menurut Dr. Allen Harper sendiri, "*... an ethical hacker who uses offensive techniques for defensive purposes. Ethical hacker is an honorable role—one that respects the laws and the rights of others. The ethical hacker subscribes to the notion that the adversary may be beaten to the punch by testing oneself first*".[13]

---

[11] Dedik Kurniawan, "Kitab Hacker", (Jakarta: PT Elex Media Komputindo, 2019), hlm. 1.

[12] Yogi Oktafian Arisandy, *Penegakan Hukum Terhadap Cyber Crime Hacker*, *Journal of Criminal Law and Criminology*, Volume I Nomor 2, (Yogyakarta, 2020), hlm. 163

[13] Allen Harper dkk, *Gray Hat Hacking "The Ethical Hacker Handbook Sixth Edition"*, English Summary Version, (New York: McGraw Hill, 2022), hlm. 31

Maksudnya, seorang *ethical hacker* menggunakan teknik *hacking* untuk pencegahan. *Ethical hacker* merupakan pekerjaan yang mulia karena selalu mengikuti hukum dan regulasi yang ada. *Ethical hacker* juga menganut gagasan bahwa musuh dapat diberantas dengan menguji diri sendiri terlebih dahulu.[14] Lebih lanjut dirujuk dari *National Criminal Intelligence Service* (NCIS) Inggris, *hacking* dapat dibagi kedalam beberapa jenis seperti :

1. *Recreational Hackers*

   Merupakan bentuk peretasan yang biasa dilakukan oleh *hacker* tingkat pemula untuk sekedar mencoba suatu sistem jaringan baik pada instansi pemerintahan maupun pada sistem sebuah perusahaan. Biasanya pada tingkat ini belum terjadi kejahatan yang dapat membahayakan atau merugikan sistem, khususnya perusahaan. Pada tahap ini seorang *hacker* belum bisa dikategorikan sebagai *ethical hacker* atau seorang *attackers*.[15]

2. *Crackers* atau kepanjangan dari *criminal minded hackers*,

   Pada tingkatan ini pelaku *hacking* biasanya memiliki motivasi ekonomis untuk mendapatkan keuntungan finansial, sabotase, hingga pengrusakan data agar diberikan imbalan. Jenis kejahatan ini dapat dilakukan dengan bantuan orang dalam maupun dilakukan sendiri dengan mencari-cari celah kesalahan dari orang

[14] Allen Harper dkk, *Gray Hat Hacking* …, hlm. 31

[15] Beni Setiawan, *Penegakan Hukum Pidana Terhadap Akses Sistem Komputer*…, hlm. 24

dalam. Hal ini juga bisa dilakukan oleh staf yang sakit hati ataupun datang dari kompetitor dalam bisnis sejenis.

3. *Political hackers*

   Hacking jenis ini biasa dilakukan oleh para aktivis politis atau lebih populer dengan sebutan *hacktivist*. Para *hacktivist* dengan sengaja melakukan perusakan terhadap ratusan situs web untuk mengkampanyekan programnya, bahkan tidak jarang dipergunakan untuk menempel pesan untuk menjatuhkan lawan politiknya.[16]

4. *Denial of Service Attack* atau *Distributed Denial of Service*

   Serangan *denial of service attack* atau oleh FBI (*Federal Bureau of Investigation*) dikenal dengan istilah ”*unprecedented*” yang berarti “belum pernah terjadi sebelumnya” dalam kamus Bahasa Indonesia tersebut, memiliki tujuan utama untuk memperlambat kinerja sistem dengan mengganggu akses dari pengguna yang sah (*legitimated*) hingga dapat berakibat pada matinya sistem.

   Serangan *hacking* jenis ini biasanya dimulai dengan mengirimkan data-data yang tidak penting secara terus menerus ke situs web yang diincar. Hingga pemilik situs akan banyak menderita kerugian untuk mengendalikan atau mengontrol kembali situs web agar berjalan normal walaupun akan memakan waktu

[16] Ari Prabawati, *Tutorial Lima Hari Belajar Hacking dari Nol*, (Semarang: Andi Offset, 2010), hlm. 64

lama. *Hacking* jenis ini juga bisa menyabarkan ancaman-ancaman pada situs web untuk membuat pemilik situs melakukan perintah sesuai keinginan *attackers*.[17]

5. *Insider* atau *internal hackers*.

   Kejahatan *hacking* jenis ini biasa dilakukan oleh orang dalam dari perusahaan sendiri. Modusnya dengan menggunakan karyawan yang kecewa atau bermasalah dengan perusahaan. Lalu membuat situs atau sistem program seolah-olah bermasalah karena telah diserang oleh *attackers* luar dan hanya bisa dikendalikan jika memberikan sejumlah uang tertentu.

6. *Viruses*.

   Merupakan jenis program pengganggu (*malicious*) yang sengaja dibuat agar dapat menular melalui aplikasi internet. Sebelumnya pola penularan virus hanya melalui *floppy disc* yaitu virus yang dapat bersembunyi di dalam file dan secara otomatis terunduh oleh user bahkan bisa menyebar melalui kiriman file.

   Virus yang dibuat ini dapat mengakibatkan perubahan pada tampilan laptop, *hang*, mouse bergerak sendiri, keyboard mengetik sendiri, windows explorer error, control panel tidak bisa dibuka, hingga semua file di dalam laptop hilang.[18]

---

[17] Dedik Kurniawan, *Kitab Hacker*…, hlm. 25
[18] *Ibid.,* hlm. 26.

7. *Piracy*

Merupakan jenis *hacking* yang dengan sengaja membajakan *software* untuk mendapatkan keuntungan ekonomis. Akibatnya pihak produsen *software* dapat kehilangan insentif dari karya *software*-nya karena karyanya diretas dari sistem legal dan disalin ke dalam CD-rom yang selanjutnya diperbanyak secara ilegal tanpa seijin pemiliknya (penciptanya).[19]

D. Teori *Maqashid Syariah*

Menurut Muhammad Syukri, salah satu ulama yang dianggap memiliki konsep komprehensif tentang maslahat khususnya *maqashid syariah* yaitu Imam Asy- Syatibi. Beliau mendefinisikan *maqashid syariah* diambil dari dua kata yaitu *al-maqāşid* dan *al-sharīah*. Kata al-maq*āşid* merupakan kata jamak dari *maqsạd* yang berarti maksud dan tujuan. Sedangkan kata *al-sharīah* berarti jalan menuju sumber kehidupan yang berupa hukum Allah SWT.[20] Dikutip dari Amiruddin Amirullah yang merujuk Imam Asy Syatibi dalam karyanya Kitab al-Muwāfaqāt menjelaskan bahwa *maslahat* dapat ditinjau dari dua perspektif yang menjadi keistimewaan beliau, yaitu:

a. Dari terjadinya maslahat dalam kenyataan, yang berarti sesuatu kembali kepada tegaknya kehidupan manusia, kesempurnaan hidupnya, tercapainya keinginan *syahwat* dan akalnya secara mutlak

---

[19] *Ibid.,* Hlm. 24-25.

[20] Muhammad Syukri Albani Nasution dan Rahmat Hidayat Nasution, *Filsafat Hukum Islam dan Maqashid Syariah*, (Jakarta: Kencana, 2020), hlm. 44

b. Dari tergantungnya tuntutan *syariat* kepada *maslahat*, yaitu kemaslahatan yang merupakan tujuan dari penetapan hukum *syariat*. Tujuan tersebut untuk mewujudkan *kemaslahatan* umat, Allah menuntut manusia untuk melakukan sesuatu agar segala aturan-Nya berjalan sebagaimana mestinya.[21]

Lebih lanjut Imam Asy Syatibi mengkategorikan *maqashid syariah* dalam lima ruang lingkup yang harus dipelihara oleh umat manusia, yaitu[22] :

a. Memelihara agama atau keberagamaan (حفظ الدين)

Menurut Imam Asy Syatibi arti dari agama secara umum yaitu kepercayaan kepada Tuhan. Sedangkan dalam arti sempit berarti sekumpulan aqidah, ibadah, hukum, dan Undang-Undang yang disyariatkan oleh Allah SWT. Tujuannya untuk mengatur hubungan manusia dengan Tuhan mereka dan hubungan mereka satu sama lain. Dengan begitu akan terwujud dan tegaknya agama Islam. Islam juga telah mensyariatkan iman dan berbagai hukum pokok yang menjadi dasar agama Islam. Dengan syariat utama yaitu persaksian bahwa tiada Tuhan selain Allah SWT dan Nabi Muhammad adalah utusan Allah, mendirikan shalat, mengeluarkan

[21] Amiruddin Aminullah, *Urgensi Maslahat dalam Perkembangan Hukum Islam, Jurnal Kajian Keislaman*, (Makassar: Universitas Islam Negeri Alauddin Makassar, 2021), hlm. 70-71

[22] Muh Syukri Albani Nasution dan Rahmat Hidayat Nasution, *Filsafat Hukum*.., hlm. 58-59

zakat, berpuasa di bulan Ramadhan, dan menunaikan haji ke Baitullah.[23]

b. Memelihara jiwa atau diri atau kehidupan (حفظ النفس)

Menurut Amir Syarifuddin, memelihara kehidupan atau jiwa merupakan segalanya bagi manusia. Karena dengan terpenuhinya unsur-unsur jaminan keselamatan dalam hidup, kehormatan, dan kebebasan memilih akan menjamin kelangsungan hidup. Dengan begitu eksistensi kehidupan seorang manusia akan tetap terjaga. Hal tersebut juga akan berdampak pada tercapainya tujuan kehidupan manusia di dunia, yaitu *rahmatan lil ālamin* atau bermanfaat bagi alam sekitar. [24]

c. Memelihara akal (حفظ العقل)

Akal manusia merupakan unsur pembeda dari makhluk Allah lain. Pemeliharaan akal dalam Islam berbentuk kewajiban untuk menuntut ilmu dan pengharaman pada hal-hal yang membawa *mudharat* atau keburukan. Seperti pengharaman pada segala yang memabukkan, babi, darah, hewan bertaring, anjing. Pengharaman tersebut dimaksudkan agar manusia dapat hidup sehat di bawah kontrol pikiran yang penuh, dengan begitu manusia dapat membuat keputusan tepat dan melangsungkan hidupnya dengan damai.

---

[23] *Ibid.,* Hlm. 58.

[24] Amir Syarifuddin, *Ushul Fiqh Jilid 2*, (Jakarta: Prenada Media, 2008), hlm. 235

d. Memelihara keturunan (حفظ النسل)

Menurut Imam Asy Syatibi dalam rangka memelihara keturunan, Islam mensyariatkan perkawinan yang sah untuk mendapatkan keturunan serta kelangsungan umat manusia. Karena kelangsungan manusia telah dibentuk yang paling sempurna.

e. Memelihara harta (حفظ المال)

Islam mensyariatkan umatnya untuk memperoleh dan menjaga kekayaan dengan wajib berusaha melalui muamalah, pertukaran, perdagangan, dan kerja sama dalam usaha. Dalam memelihara kekayaan Islam juga mengharamkan pencurian, penipuan, penghianatan, perusakan harta orang lain, mencegah kebodohan dan lalai, serta menghindari dari bahaya.[25]

Kelima pengkategorian *maqashid syariah* tersebut dirumuskan untuk memperjelas tujuan-tujuan *syar'i* yang harus dipelihara oleh manusia. Dengan terpeliharanya kelimanya manusia akan bisa hidup damai dengan makhluk lain. Hal tersebut hanya bisa terwujud dengan adanya pemaksimalan peran-peran pemerintah hingga di tengah masyarakat.[26]

Berikut merupakan maslahat yang dapat diambil dari menerapkan *maqashid syariah* yaitu :

1. Mempermudah pengidentifikasian tujuan, alasan, dan hikmah baik yang umum maupun khusus

[25] *Ibid.,* Hlm. 59.
[26] *Ibid.*

2. Penegasan terhadap karakteristik Islam yang dapat disesuaikan dengan zaman
3. Mempermudah ulama dalam berijtihad dalam bingkai tujuan *syariat* Islam
4. Memperkecil adanya perselisihan dan *taāshub*[27] di antara pengikut mazhab fiqh.[28]

Berdasarkan pendapat Imam Asy-Syatibi tersebut, pengimplementasian *maqashid syariah* sendiri apabila dilihat dari perlindungan perusahaan teknologi yang terkena *hacking* maka yang menjadi dasar perlindungannya yaitu memelihara harta dan memelihara agama.[29]

[27] *Ta'ashub* adalah istilah dalam Islam yang artinya fanatik buta. *Ta'ashub* bukanlah sebuah kenikmatan ataupun sebuah keagungan melainkan sebuah penyakit yang secara sadar atau tidak sadar mampu menginfeksi siapa saja. Penyakit ini termasuk penyakit yang berbahaya dan memiliki kemampuan untuk merusak tatanan syariat Islam.. Dikutip dari Risalah Muslim.com diakses pada 20 Januari 2023 pukul 09.28 WIB

[28] *Ibid.,* hlm. 47.

[29] *Ibid.*

BAB III

GAMBARAN UMUM PERLINDUNGAN HUKUM PERUSAHAAN TEKNOLOGI DARI SERANGAN *HACKING*

A. Data Perlindungan Hukum Perusahaan Teknologi di Indonesia

1. Data Permasalahan dan Terobosan Pemerintah Pada Perusahaan Teknologi Terhadap *Hacking*

Menurut Dona Budi Kharisma, permasalahan dalam melindungi perusahaan teknologi secara umum yaitu *pertama*, belum adanya regulasi khusus untuk mengatur perusahaan teknologi. Walaupun telah disahkan Undang-Undang Nomor 11 Tahun 2020 tentang Cipta Kerja yang dibentuk melalui konsep Omnibus Law, akan tetapi Undang-Undang tersebut belum mencakup mengenai perusahaan teknologi secara khusus.[1]

K*edua* yaitu belum adanya lembaga khusus yang berwenang mengatur kebijakan perusahaan teknologi. Karena setiap industri perusahaan teknologi memiliki karakteristik unik untuk mengatur dan melindunginya. Tidak adanya lembaga khusus tersebut membuat beberapa perusahaan teknologi yang berkembang mengalami tumpang tindih kebijakan. *Over* regulasi tersebut berakibat pada sulitnya perusahaan teknologi untuk berkembang dan berinovasi.[2]

---

[1] Dona Budi Kharisma, *Membangun Kerangka Pengaturan Startup di Indonesia*, *Jurnal Rechtsvinding* Volume 10 Nomor 3, (Surakarta: Universitas Sebelas Maret, 2021), hlm. 434

[2] Dona Budi Kharisma, *Membangun Kerangka Pengaturan Startup…*, hlm. 439

Tantangan dalam meregulasi perusahaan teknologi tersebut juga telah dibahas dalam pertemuan G20 di Hamburg 2017 lalu. salah satu tantangannya yaitu penggunaan dan perlindungan data pribadi. Akan tetapi perlindungan data pribadi ini masih difokuskan pada pengguna, belum mencakup regulasi perlindungan data pribadi pada perusahaan teknologi sebagai pengumpul data pengguna.[3]

Menurut hasil pertemuan G20 ini, pembahasan isu *cross border data flows* mengharuskan Indonesia untuk segera memperbaiki aturan perlindungan data di dalam negeri. Belum lagi, mulai berlaku mengikatnya EU GDPR pada 25 Mei 2018 yang telah berdampak besar bagi perusahaan-perusahaan Indonesia di berbagai sektor, seperti transportasi, e-commerce, perhotelan, maupun sektor lainnya yang melakukan praktik pengumpulan data pribadi.[4] Dari negosiasi dengan negara Asia Tenggara lain, Indonesia mulai merumuskan RUU Perlindungan Data Pribadi dan baru disahkan di tahun 2022 lalu dengan sebutan UU PDP (Undang-Undang Perlindungan Data Pribadi).

Kasus pengungkapan data pribadi pengguna platform *financial technology* (fintech) yang berbasis *peer-to-peer lending* juga menjadi alasan terbesar pentingnya regulasi khusus pada sektor perusahaan

---

[3] Dikutip dari 2017 G20 Digital Economy Ministerial Declaration (utoronto.ca) pada 8 Februari 2023 pada pukul 21.16 WIB

[4] Wahyudi Djafar, *Hukum Perlindungan Data Pribadi di Indonesia*, (Yogyakarta: Universitas Gajah Mada, 2020), hlm. 13

teknologi. Kasus ini bermula pada perusahaan penyedia platform mengakses data-data pribadi yang ada di ponsel pengguna, seperti foto dan nomor kontak yang tersimpan, dengan alasan untuk melakukan *credit scoring* atau penilaian yang penentu kelayakan pinjaman yang dapat diberikan. Namun prakteknya, data yang diakses tersebut justru digunakan untuk proses penagihan, yang dilakukan oleh pihak ketiga, yang tidak terkait dalam perjanjian pengumpulan data.

Selain itu, *debt collector* (pihak ketiga) dalam penagihannya, juga kerap melakukan penyebaran data pribadi pengguna, yang berupa transaksi keuangan dan foto dari pengguna kepada kontak-kontak atau kerabat yang ditemukan dari ponsel kreditur tanpa seizin dari pemilik data. Tidak sedikit pula model penagihan tersebut dilakukan dengan bentuk kekerasan berupa ancaman penyebaran foto pribadi. Sepanjang tahun 2018, Kominfo sendiri setidaknya telah memblokir 738 fintech illegal, umumnya mereka tidak memenuhi persyaratan yang ditentukan oleh Otoritas Jasa Keuangan (OJK), dan kerap melakukan penyalahgunaan data pribadi penggunanya.[5]

Permasalahan-permasalahan yang belum selesai tersebut masih ditambah dengan banyaknya ancaman *hacking* pada perusahaan teknologi. Berdasarkan data BSSN atau Badan Siber dan Sandi Negara terdapat 1.637.973.022 jumlah *anomali* nasional per Desember 2021. Dimana angka tersebut diambil dari berbagai jenis tindak pidana

[5] Wahyudi Djafar, *Hukum Perlindungan Data Pribadi…*, hlm. 14

hacking yang merugikan sistem jaringan instansi pemerintah hingga perusahaan teknologi.[6]

Data anomali tersebut mencerminkan tingginya tingkat ancaman *cybercrime* khususnya *hacking* di Indonesia. Tingginya ancaman *cybercrime* tersebut juga berpengaruh pada rendahnya tingkat pertumbuhan perusahaan teknologi. Seperti data yang diambil oleh MIKTI atau Indonesia Digital Creative Industry Society permasalahan pada regulasi berpengaruh terhadap 14,6% kegagalan perusahaan teknologi.[7] Hal tersebut juga berkaitan dengan rendahnya tingkat keamanan siber nasional.

Menurut data *National Cyber Security Index* (NCSI) 2020, Indonesia menempati ranking 85 dengan nilai 38.96 pada indeks keamanan siber nasional. Sedangkan menurut *Global Cybersecurity Index* Indonesia menempati ranking 24 dari 161 negara.[8] Data lebih lanjut dapat dilihat pada Gambar 1.

---

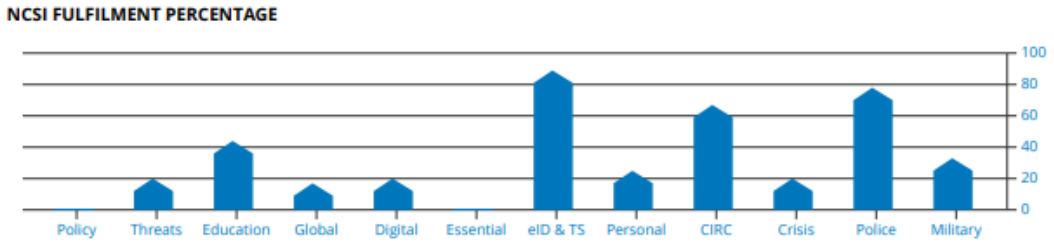
[6] Direktorat Operasi Keamanan Siber, *Laporan Tahunan Monitoring Keamanan Siber 2021*, (Jakarta Selatan, 2021), hlm. 16

[7] MIKTI Indonesia Digital Creative Industry Society, *Mapping dan Database Startup Indonesia 2021*, Edisi 2021, hlm. 20

[8] Dikutip dari National Cyber Security Index ncsi.ega.ee/country/id/ diakses pada 9 Februari 2023 pukul 10.13 WIB.

Gambar 1

Grafik Persentase Pemenuhan NCSI



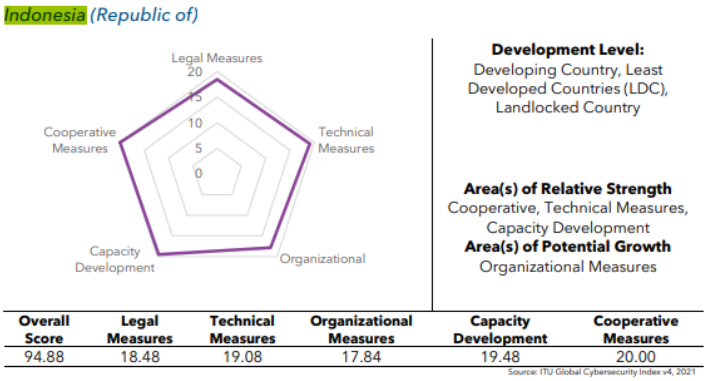
Indikator dari *cyber security* secara keseluruhan pada data yang diambil oleh NCSI ini terdiri dari 3 (tiga) indikator yaitu indikator umum *cyber security,* indikator dasar *cyber security*, dan yang terakhir indikator pengelolaan insiden dan krisis.[9] Sedangkan indikator dalam laporan *Global Cybersecurity Index* 2020 diambil dari tindakan hukum, tindakan teknis, prosedur organisasi terkait, kapasitas pengembangan, dan pengukuran kooperatif. Data selengkapnya dapat dilihat pada Gambar 2.[10]

[9] Dikutip dari National Cyber Security Index ncsi.ega.ee/country/id/ diakses pada 9 Februari 2023 pukul 10.13 WIB.

[10] International Telecommunication Union, *Global Cybersecurity Index* 2020, (ITU Publications), hlm. 87

Gambar 2

Indikator dalam laporan *Global Cybersecurity Index* 2020



Overall Score	Legal Measures	Technical Measures	Organizational Measures	Capacity Development	Cooperative Measures
94.88	18.48	19.08	17.84	19.48	20.00

Source: ITU Global Cybersecurity Index v4, 2021

Hingga penelitian ini dibuat hanya ada 2 (dua) lembaga yang bertugas dan berwenang dalam menangani *cybercrime*. Dua lembaga tersebut yaitu Badan Siber dan Sandi Negara atau dikenal dengan BSSN dan DITTIPIDSIBER POLRI. Kedua lembaga pemerintah tersebut memiliki kewenangan yang berbeda dan terbatas. Kewenangan tersebut sebagai berikut :

a. Badan Siber dan Sandi Negara (BSSN)

Badan Siber dan Sandi Negara (BSSN) telah diatur kewenangannya sesuai Peraturan Presiden Nomor 53 tahun 2017 sebagaimana diubah dalam Peraturan Presiden nomor 133 Tahun 2017. BSSN bertugas melaksanakan keamanan siber secara efektif dan efisien dengan memanfaatkan, mengembangkan, dan

mengkonsolidasikan semua unsur yang terkait dengan keamanan siber.[11]

Berikut merupakan layanan yang diberikan oleh BSSN sebagai lembaga yang berwenang sesuai mandat KOMINFO dalam menangani siber:

1) PPID (Pejabat Pengelola Informasi dan Dokumentasi)

   Layanan ini berupa informasi publik BSSN dan uji konsekuensi yang ditujukan untuk seluruh lapisan masyarakat yang memerlukan informasi dari BSSN.

2) *Honeynet*

   Honeypot merupakan sistem yang dirancang untuk memikat penyerang, sistem ini dibuat mempunyai fungsi dan memberikan interaksi yang sama dengan sistem yang aslinya sehingga penyerang tidak menyadari sudah masuk dalam perangkap. Interaksi penyerang berupa identitas penyerang dan teknik penyerang masuk ke dalam sistem dapat direkam oleh *honeypot* sehingga informasi tersebut dapat menjadi sumber informasi penting dalam mempelajari teknik yang digunakan penyerang. Kumpulan honeypot yang saling terhubung dalam sebuah sistem disebut *Honeynet*.[12]

---

[11] Badan Siber dan Sandi Negara atau BSSN, *Katalog Layanan BSSN Tahun 2021*, hlm. 2

[12] Badan Siber dan Sandi Negara (BSSN), *Katalog Layanan…,* hlm. 12

Tujuan dari pembuatan honeynet ini yaitu mengembangkan sistem deteksi dini (*early warning system*) ancaman siber di masing-masing stakeholder sehingga dapat mendukung terciptanya ranah siber yang aman dan tahan dari serangan siber. Layanan ini diperuntukkan untuk instansi pemerintah, akademisi, infrastruktur kritis nasional dan ekonomi digital. [13]

3) Sertifikasi Elektronik

BSSN melayani penerbitan sertifikasi elektronik, sosialisasi penerapan sertifikat elektronik, konsultasi pemanfaatan sertifikat elektronik, bimbingan teknis, monitoring dan helpdesk. Penerima layanan ini hanya diperuntukkan kepada instansi pemerintah pusat maupun BUMN / BUMD.

4) Asistensi Proteksi Keamanan Informasi Pemerintah (APROKSI)

APROKSI ini mencakup layanan asistensi dalam bidang tata kelola keamanan informasi, layanan keamanan informasi, dan audit keamanan informasi. Layanan ini hanya dikhususkan kepada pemerintah pusat dan daerah.[14]

5) Aduan Siber

Lingkup layanan aduan siber yaitu observasi, investigasi, dan pemberian rekomendasi cara penanggulangan insiden siber

[13] *Ibid.,* Hlm. 12.
[14] *Ibid.,* Hlm. 15.

serta membantu menindaklanjuti aduan insiden siber. Penerima layanan adalah pemerintah, BUMN, BUMD, *e-Commerce*, dan masyarakat yang mendapatkan serangan atau insiden siber.

6) *Government computer security incident response team* (GOV-CSIRT)

Gov-CSIRT Indonesia ini memberikan layanan yang meliputi respon insiden dalam bentuk: triase insiden[15]; koordinasi insiden; dan resolusi insiden. Disertai dengan aktivitas proaktif dalam bentuk: *cyber security drill test*; workshop atau bimbingan teknis; dan asistensi pembentukan CSIRT sektor pemerintah. Layanan ini hanya diperuntukkan untuk instansi pemerintah pusat dan daerah.

7) *Information technology security assessment* (ITSA)

ITSA merupakan layanan penguji kerentanan, pemberian saran dan rekomendasi terkait pengamanan untuk meminimalisir celah kerawanan yang terdapat pada semua sistem informasi. Layanan ini hanya untuk instansi pemerintah pusat dan daerah.

8) *Konsultasi dan assessment indeks* KAMI

Indeks Keamanan Informasi (KAMI) merupakan aplikasi yang digunakan sebagai alat bantu untuk melakukan asesmen

[15] Triase insiden adalah langkah memastikan kebenaran insiden dan pelapor, serta menilai dampak dan prioritas insiden

dan evaluasi tingkat kesiapan yang berupa tata kelola, manajemen risiko, kerangka kerja, pengelolaan aset, aspek teknologi dengan suplemen pengamanan keterlibatan pihak ketiga penyedia layanan, pengamanan layanan infrastruktur penyimpanan (*Cloud*) dan perlindungan data pribadi. Layanan ini diperuntukkan bagi instansi pemerintah baik pusat maupun daerah dan para pelaku ekonomi digital.[16]

9) Layanan konsultasi SDM keamanan siber dan sandi

Bentuk layanan ini berupa pengembangan kompetensi, supervisi, pengelolaan data dan informasi sumber daya manusia yang diperuntukkan kepada instansi pemerintah pusat maupun daerah.

10) Museum Sandi Negara.[17]

b. Direktorat Tindak Pidana Siber (DITTIPIDSIBER POLRI)

Direktorat Tindak Pidana Siber (Dittipidsiber) adalah satuan kerja yang berada di bawah naungan Bareskrim Polri dan bertugas untuk melakukan penegakan hukum terhadap kejahatan siber. Secara umum, Dittipidsiber menangani dua kelompok kejahatan,

[16] *Ibid.,* Hlm. 16-23
[17] *Ibid.,* Hlm. 24-27

yaitu *computer crime*[18] dan *computer-related crime*[19]. Salah satu *computer crime* yang ditangani oleh Dittipidsiber Polri adalah peretasan sistem elektronik (*hacking*).[20]

Dittipidsiber ini memiliki Laboratorium Digital Forensik yang telah meraih ISO 17025:2018 sebagai laboratorium uji dan kalibrasi dalam bidang komputer forensik yang memenuhi standar mutu dalam hal pengelolaan dan teknis pemeriksaan barang bukti digital. Oleh karena itu, Dittipidsiber juga melayani pemeriksaan barang bukti digital dari berbagai satuan kerja, baik dari tingkat Mabes hingga Polsek. Selain itu, Dittipidsiber juga menjalin kerja sama dengan berbagai instansi, baik dalam dan luar negeri, guna memudahkan koordinasi dalam pengungkapan kejahatan siber yang bersifat transnasional dan terorganisir.[21]

Menurut NCIS kedua lembaga siber yang dimiliki Indonesia tersebut belum dapat memenuhi indikator rata-rata keamanan siber secara nasional. Maka diperlukan lembaga khusus lain untuk dapat memenuhi kebutuhan dalam menangani tindak pidana siber.

---

[18] *Computer crime* merupakan bentuk kejahatan siber yang menggunakan komputer sebagai alat utama. Bentuk kejahatannya yaitu peretasan sistem elektronik (*hacking*), intersepsi ilegal (*illegal interception*), pengubahan tampilan situs web (*web defacement*), gangguan sistem (*system interference*), manipulasi data (*data manipulation*).

[19] *Computer-related crime* merupakan kejahatan siber yang menggunakan komputer sebagai alat bantu, seperti pornografi dalam jaringan (*online pornography*), perjudian dalam jaringan (*online gamble*), pencemaran nama baik (*online defamation*), pemerasan dalam jaringan (*online extortion*), penipuan dalam jaringan (*online fraud*), ujaran kebencian (*hate speech*), pengancaman dalam jaringan (*online threat*), akses ilegal (*illegal access*), pencurian data (*data theft*).

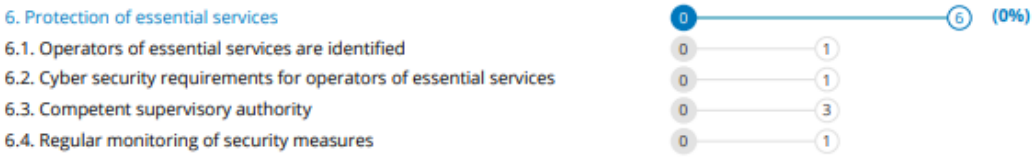
[20] Dikutip dari https://patrolisiber.id/about pada 10 Februari 2023 pukul 07.36 WIB

[21] Dikutip dari https://patrolisiber.id/about pada 10 Februari 2023 pukul 07.36 WIB

Indonesia masih membutuhkan 7 (tujuh) unit pengembangan kebijakan keamanan siber dan 6 (enam) unit pengembang kebijakan mengenai perlindungan layanan publik untuk dapat mengimbangi kebutuhan dari 20% krisis *cyber security* yang ada. Seperti dalam data NCIS 2020 Gambar 3 dan Gambar 4 berikut ini :

Gambar 3
Indikator Pengembang Keamanan Siber

Gambar 4
Indikator Layanan Keamanan Publik



Kebutuhan akan pengkhususan unit penanganan dan mitigasi siber tersebut menjadi isyarat lemahnya perlindungan dunia siber di Indonesia. Hal tersebut juga akan berakibat pada minimnya kemajuan riset kebijakan untuk mendorong sektor sosial dan ekonomi terkait.[22] Untuk dapat memaksimalkan perlindungan perusahaan teknologi dari serangan *hacking*, pemerintah Indonesia masih harus membangun infrastruktur unit kelembagaan dengan teknologi yang canggih. Baik dengan membangun kelembagaan dalam pengkhususan layanan siber

[22] National Cyber Security Index, Riset Keamanan Siber of Indonesia 2020, https://ncsi.ega.ee/country/id/ dikutip pada 9 Februari 2023 pukul 06.59 WIB

dan pembuat kebijakan perusahaan teknologi atau dengan menambah unit-unit layanan pada kedua lembaga tersebut.

2. Regulasi Perlindungan Hukum Pada Perusahaan Teknologi Yang Terkena *Hacking*

Perlindungan perusahaan teknologi jika dilihat dari yuridis maka dapat berupa undang-undang maupun regulasi terkait. Berikut merupakan pasal-pasal yang dapat digunakan sebagai perlindungan :

a. Pasal 30 Undang-Undang No. 11 tahun 2008 sebagaimana diubah Undang-Undang No. 19 tahun 2016 tentang Informasi dan Transaksi Elektronik

Dalam pasal 30 ayat 1 ini berisi larangan terhadap intersepsi terhadap sistem komputer orang lain tanpa seizin pemilik sistem tersebut.

> *(1) Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum mengakses Komputer dan/atau Sistem Elektronik milik Orang lain dengan cara apa pun.*
>
> *(2) Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum mengakses Komputer dan/atau Sistem Elektronik dengan cara apa pun dengan tujuan untuk memperoleh Informasi Elektronik dan/atau Dokumen Elektronik.*
>
> *(3) Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum mengakses Komputer dan/atau Sistem Elektronik dengan cara apa pun dengan melanggar, menerobos, melampaui, atau menjebol sistem pengamanan".*[23]

[23] Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik (Lembaran Negara Republik Indonesia Tahun 2008 Nomor 58, Tambahan Lembaran Negara Republik Indonesia Nomor 4843). Undang-Undang Nomor 19 Tahun

Sedangkan pada ayat 2 dan 3 menerangkan tujuan dan tata cara yang dilakukan untuk mengakses sistem komputer lain baik dengan melanggar, menerobos, melampaui, ataupun menjebol sistem pengamanan dari orang yang dituju. Dengan cara-cara tersebut pengakses ilegal (*attacker*) dapat mengakses informasi rahasia dari sistem yang diretas.

b. Pasal 43 Undang-Undang No. 19 tahun 2016 atas perubahan Undang-Undang No. tahun 2008 tentang Informasi dan Transaksi Elektronik

Pada ayat 1 pasal ini dijelaskan bahwa kewenangan sistem pembuktian dan penyidikan dalam pengadilan bidang teknologi dan informasi transaksi elektronik terdapat pada Penyidik Pegawai Negeri Sipil.

Pada ayat 2 juga dijelaskan bahwa penyidikan yang dilakukan harus memperhatikan perlindungan terhadap privasi, kerahasiaan, kelancaran layanan publik, dan integritas atau keutuhan data sesuai dengan ketentuan peraturan perundang-undangan.[24]

Pasal 43 ayat 1 dan 2 berbunyi, " *(1) Selain Penyidik Pejabat Polisi Negara Republik Indonesia, Pejabat Pegawai Negeri Sipil tertentu di lingkungan Pemerintah yang lingkup tugas dan*

2016 tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 tentang ITE (Lembaran Negara Republik Indonesia Tahun 2016 Nomor 251)

[24] Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik (Lembaran Negara Republik Indonesia Tahun 2008 Nomor 58, Tambahan Lembaran Negara Republik Indonesia Nomor 4843). Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 tentang ITE (Lembaran Negara Republik Indonesia Tahun 2016 Nomor 251)

tanggung jawabnya di bidang Teknologi Informasi dan Transaksi Elektronik diberi wewenang khusus sebagai penyidik sebagaimana dimaksud dalam Undang-Undang tentang Hukum Acara Pidana untuk melakukan penyidikan tindak pidana di bidang Teknologi Informasi dan Transaksi Elektronik.

(2) Penyidikan di bidang Teknologi Informasi dan Transaksi Elektronik sebagaimana dimaksud pada ayat (1) dilakukan dengan memperhatikan perlindungan terhadap privasi, kerahasiaan, kelancaran layanan publik, dan integritas atau keutuhan data sesuai dengan ketentuan peraturan perundang-undangan".[25]

c. Pasal 1 angka 9, Pasal 40 ayat 1 huruf s, dan Pasal 52 Undang-Undang No. 28 tahun 2014 tentang Hak Cipta

Program komputer sebagai sebuah objek hukum telah didefinisikan dalam Pasal 1 angka 9 Undang-Undang No. 28 tahun 2014 tentang Hak Cipta yang berbunyi,

"*Program Komputer adalah seperangkat instruksi yang diekspresikan dalam bentuk bahasa, kode, skema, atau dalam bentuk apapun yang ditujukan agar komputer bekerja melakukan fungsi tertentu atau untuk mencapai hasil tertentu*".[26]

Berkaitan dengan perlindungan dalam undang-undang hak cipta, sebuah program komputer ataupun keamanannya dijamin oleh pemerintah dalam Pasal 40 ayat 1 huruf s dan Pasal 52 Undang-Undang No. 28 tahun 2014 tentang Hak Cipta. Pada Pasal 40 ayat 1 huruf s merupakan ketentuan program komputer sebagai ciptaan yang dilindungi.

---

[25] Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik (Lembaran Negara Republik Indonesia Tahun 2008 Nomor 58, Tambahan Lembaran Negara Republik Indonesia Nomor 4843). Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 tentang ITE (Lembaran Negara Republik Indonesia Tahun 2016 Nomor 251)

[26] Undang-Undang Nomor 28 Tahun 2014 Tentang Hak Cipta (Lembaran Negara Republik Indonesia Tahun 2014 Nomor 266, Tambahan Lembaran Negara Republik Indonesia Nomor 5599)

Sedangkan dalam Pasal 52 tersebut disebutkan bahwa salah satu objek hukum yang dilindungi adalah program komputer. Dengan bunyi pasal sebagai berikut,

> "*Setiap orang dilarang merusak, memusnahkan, menghilangkan, atau membuat tidak berfungsinya sarana kontrol teknologi yang digunakan sebagai pelindung ciptaan/produk hak terkait, kecuali untuk kepentingan pertahanan dan keamanan negara, serta sebab lain sesuai dengan ketentuan peraturan perundang-undangan atau perjanjian lain* ".[27]

d. Pasal 6 Undang-Undang Nomor 8 Tahun 1999 tentang Perlindungan Konsumen

Pasal 6 Undang-undang perlindungan konsumen merumuskan perlindungan terhadap pelaku usaha yang berupa hak-hak diantaranya sebagai berikut :

1) Hak untuk menerima pembayaran yang sesuai dengan kesepakatan mengenai kondisi dan nilai tukar barang dan/atau jasa yang diperdagangkan;
2) Hak untuk mendapat perlindungan hukum dari tindakan konsumen yang beritikad tidak baik;
3) Hak untuk melakukan pembelaan diri sepatutnya di dalam penyelesaian hukum sengketa konsumen;
4) Hak untuk rehabilitasi nama baik apabila terbukti secara hukum bahwa kerugian konsumen tidak diakibatkan oleh barang dan/atau jasa yang diperdagangkan; dan

[27] Undang-Undang Nomor 28 Tahun 2014 Tentang Hak Cipta (Lembaran Negara Republik Indonesia Tahun 2014 Nomor 266, Tambahan Lembaran Negara Republik Indonesia Nomor 5599)

5) Hak-hak yang diatur dalam ketentuan peraturan perundang-undangan lainnya.[28]

e. Tinjauan Pasal 65 dan 66 Undang-Undang Nomor 7 tahun 2014 tentang Perdagangan Melalui Sistem Elektronik dan Peraturan Presiden Nomor 74 tahun 2017 berisi pemetaan sistem dagang nasional berdasarkan sistem online.

Definisi dari perdagangan elektronik terdapat pada ketentuan umum angka 24,

"*Perdagangan melalui sistem elektronik didefinisikan sebagai perdagangan yang transaksinya dilakukan melalui serangkaian perangkat dan prosedur elektronik*".

Pasal 65 Undang-Undang Nomor 7 tahun 2014 berisi regulasi mengenai perdagangan melalui sistem elektronik. Diantaranya keharusan perusahaan atau pelaku usaha untuk menyediakan data atau informasi mengenai identitas, legalitas pelaku usaha atau pelaku distribusi, persyaratan teknis barang, persyaratan atau kualifikasi jasa yang ditawarkan, harga dan cara pembayaran barang dan/ atau jasa, dan prosedur penyerahan barang.[29]

Sedangkan Peraturan Presiden Nomor 74 tahun 2017 mengkhususkan pemetaan sistem dagang nasional berdasarkan

[28] Undang-Undang Nomor 8 Tahun 1999 Tentang Perlindungan Konsumen (Lembaran Negara Republik Indonesia Tahun 1999 Nomor 42, Tambahan Lembaran Negara Republik Indonesia Nomor 3821)

[29] Undang-Undang Nomor 7 Tahun 2014 Tentang Perdagangan (Lembaran Negara Republik Indonesia Tahun 2014 Nomor 45, Tambahan Lembaran Negara Republik Indonesia Nomor 5512)

berbasis online sebagai amanat pasal 66 Undang-Undang Nomor 7 tahun 2014.

f. Pasal 3 Undang-Undang No. 30 tahun 2000 tentang Rahasia Dagang

Perlindungan perusahaan yang terakhir dapat dilihat dalam Pasal 3 mengenai lingkup rahasia dagang. Pada pasal tersebut disebutkan perlindungan rahasia dagang dapat digunakan jika informasi tersebut bersifat rahasia, mempunyai nilai ekonomi, dan diupayakan untuk dijaga kerahasiaannya. Dimana Pasal 3 Undang-Undang No. 30 tahun 2000 tentang rahasia dagang berbunyi,

> "*(1) Rahasia Dagang mendapat perlindungan apabila informasi tersebut bersifat rahasia, mempunyai nilai ekonomi, dan dijaga kerahasiaannya melalui upaya sebagaimana mestinya. (2) Informasi dianggap bersifat rahasia apabila informasi tersebut hanya diketahui oleh pihak tertentu atau tidak diketahui secara umum oleh masyarakat. (3) Informasi dianggap memiliki nilai ekonomi apabila sifat kerahasiaan informasi tersebut dapat digunakan untuk menjalankan kegiatan atau usaha yang bersifat komersial atau dapat meningkatkan keuntungan secara ekonomi. (4) Informasi dianggap dijaga kerahasiaannya apabila pemilik atau para pihak yang menguasainya telah melakukan langkah-langkah yang layak dan patut* ".[30]

Menurut Muhammad Amirullah, regulasi yang telah ada tersebut sudah mengarah pada pengaturan siber Internasional dalam *EU Convention Cybercrime Budapest* 2001 dan EU GDPR. Hal tersebut juga telah termasuk pada penilaian *Global Cybersecurity Index*, Indonesia

[30] Undang-Undang Nomor 30 Tahun 2000 Tentang Rahasia Dagang (Lembaran Negara Republik Indonesia Tahun 2000 Nomor 242, Tambahan Lembaran Negara Republik Indonesia Nomor 3817)

sendiri mendapatkan 95% dari kelima kategori indikator siber dunia. Dimana salah satu indikatornya yaitu indikator hukum[31]

3. Pengaruh Regulasi Hukum Perusahaan Teknologi Yang Terkena *Hacking* di Indonesia

Menurut Dicky Efraim, undang-undang mengenai perusahaan teknologi tersebut berpengaruh besar dalam penyelarasan bisnis perusahaan. Karena adanya kewajiban perusahaan sebagai pelaku usaha dalam menjalankan bisnis berpengaruh besar pada sektor ekonomi nasional. Adanya perlindungan tersebut akan memperkecil celah kejahatan ataupun penyalahgunaan teknologi. Hingga berpengaruh pada perkembangan dan inovasi teknologi industri digital di Indonesia.[32]

Sedangkan menurut Satjipto Rahardjo, perlindungan yang diberikan pada perusahaan teknologi dapat memberikan hak-hak istimewa yang diatur keluasannya. Pemberian hak tersebut juga berkaitan dengan kewajiban dan tanggung jawab yang besar pada perusahaan teknologi.[33]

---

[31] Muhamad Amirullah dkk, *Kajian EU Convention On Cybercrime Dikaitkan Dengan Upaya Regulasi Tindak Pidana Teknologi Informasi*, (Jakarta: Badan Pembinaan Hukum Nasional Departemen Hukum dan Hak Asasi Manusia RI, 2009), hlm. 26

[32] Dicky Efraim Simanungkalit, *Kebijakan Pemerintah Indonesia Dalam Menangani Hacker di Indonesia Tahun 2008-2014*, Journal Ilmu Hubungan Internasional, (Universitas Mulawarman: 2018), hlm. 1301

[33] Ibid hlm. 53

Menurut Sandryones Palinggi, perlindungan hukum terhadap perusahaan teknologi yang terkena *hacking* hingga saat ini berpengaruh pada hal-hal sebagai berikut :

a. Adanya regulasi yang berupa perlindungan terhadap perusahaan teknologi akan memberikan seluruh aspek kenyamanan dan mendorong terciptanya ekosistem industri digital yang baik;
b. Bentuk antisipasi pemerintah terhadap kemunculan industri-industri baru yang juga memanfaatkan kemajuan teknologi. Karena kontribusi pemerintah, para pelaku industri, pakar teknologi, dan asosiasi, dapat ikut bekerja sama dalam menciptakan sebuah aturan main ataupun regulasi untuk menghindari sebuah tindak kecurangan dalam bisnis.[34]
c. Sedangkan menurut Stephanie, perlindungan terhadap perusahaan teknologi akan memberikan hak secara hukum, sekaligus mengawasi atas hak yang diperoleh tersebut. Pembatasan ini bertujuan untuk memberikan perlindungan hukum bagi perusahaan teknologi dan juga masyarakat umum.[35]

---

[34] Sandryones Palinggi dan Erich C. Limbongan, *Pengaruh Internet Terhadap Industri E-Commerce Dan Regulasi Perlindungan Data Pribadi Pelanggan di Indonesia*, (Jakarta: Seminar Nasional Riset dan Teknologi (SEMNAS RISTEK), 2020), hlm. 226

[35] Stephanie PD dkk, *Mengelaborasi Hukum Positif Tertulis Indonesia Mengatur Startup*, Seminar Nasional Hasil Penelitian dan Pengabdian Kepada Masyarakat 2021, (Jakarta: Universitas Tarumanegara, 2021) hlm. 1258

B. Data *Hacking* Yang Pernah Terjadi di Indonesia

1. Latar Belakang Sosial Tindak Pidana *Hacking*

Regulasi-regulasi yang telah dibuat oleh pemerintah Indonesia tersebut merupakan pemecahan sebagian permasalahan *hacking* yang ada. Seperti halnya adanya pembuatan undang-undang khusus mengenai informasi dan transaksi elektronik tahun 2008 yang dilatarbelakangi adanya rasa solidaritas para *hacker* Indonesia kepada negara Palestina yang selalu diinvasi oleh militer Israel. Hal tersebut membuat *hacker* Indonesia melakukan peretasan ke situs-situs pemerintahan Israel sebagai bentuk protes atas perlakuan Israel terhadap Palestina. Walaupun penyerangan dari *hacker* Indonesia ini tidak merusak infrastruktur vital negara Israel.[36] Akan tetapi hal tersebut tidak dapat dibenarkan menurut perundang-undangan.

Dikutip dari Rian Prayudi, adanya tindak pidana *hacking* dipengaruhi oleh dua faktor yaitu faktor internal dan faktor eksternal. Faktor internal yang dimaksud yaitu :

a. Niat pelaku melakukan *hacking* apakah untuk memperoleh keuntungan pribadi atau menguji coba sistem untuk membuat sistem keamanan yang lebih kuat.
b. Moral dan pendidikan, moral yang dimaksud disini yaitu kesadaran akan hukum yang berlaku. Apakah pelaku melakukannya tanpa mengetahui hukum yang berlaku ataukah secara sadar

[36] Dicky Efraim Simanungkalit, *Kebijakan Pemerintah* ..., hlm. 1302

mengabaikan adanya hukum itu sendiri. Sedangkan tingkat pendidikan yang dimaksud disini juga mempengaruhi adanya tindak pidana, banyak dari pelaku memiliki tingkat pendidikan rendah.[37]

Sedangkan yang termasuk dari faktor eksternal pelaku yaitu :

a. Lingkungan tempat tinggal

Lingkungan tempat tinggal pelaku juga berpengaruh besar terhadap perilaku dan pergaulan sosial. Pergaulan sosial yang sering mengabaikan norma-norma menjadi salah satu faktor penyebab adanya kejahatan (*kriminogen*).

b. Tingkat ekonomi

Desakan ekonomi dan minimnya lapangan pekerjaan membuat para pelaku kejahatan di dunia maya nekat memanfaatkan teknologi dan kemampuannya untuk mendapatkan yang bukan miliknya.

c. Perkembangan teknologi global

Adanya perkembangan teknologi global tidak hanya berdampak positif pada kehidupan manusia, tetapi juga berdampak negatif. Salah satu dampak negatif adanya perkembangan teknologi global yaitu keinginan manusia untuk menunjukkan

[37] Rian Prayudi Saputra, *Perkembangan Tindak Pidana Pencurian di Indonesia*, ejournal Pahlawan Vol. 2 No. 2, (Universitas Pahlawan Tuanku Tambusai: 2019), hlm. 50

kemampuannya dan terlihat unggul dari orang lain. Begitu juga dengan para *black hacker* atau *attacker* yang menunjukkan kemampuannya dengan akun anonim untuk mendapatkan validasi dari orang lain.[38]

2. Penanggulangan *Hacking* di Indonesia

Dikutip dari *KataData.co.id*, proyeksi peretasan dan penipuan pada tahun 2023 mencapai Rp 78 Miliar pada setiap kebocoran data. Proyeksi ini merupakan biaya penanganan tindak pidana peretasan (*hacking*) dan penipuan online.[39] Dimana menurut *Acronis*[40] perusahaan siber asal Singapura memperkirakan tren serangan siber pada tahun 2023 ini yaitu:

a. *Phising*

Menurut BSSN *phising* merupakan suatu teknik siber untuk mengelabui korban yang bertujuan mendapatkan informasi sensitif korban seperti nama, tanggal lahir, usia, alamat rumah, username, password, atau keterangan sensitif lain. Berdasarkan Laporan BSSN 2021, aktivitas *phising* di Indonesia menyebar melalui dua

---

[38] Rian Prayudi Saputra, *Perkembangan Tindak Pidana ...,* hlm. 50-51

[39] Dikutip dari Katadata.com/ Proyeksi Peretasan & Penipuan 2023, Biayanya Rp78 M per Kebocoran Data (msn.com) pada tanggal 6 Februari pukul 15.24

[40] Acronis adalah perusahaan teknologi global yang berkantor pusat di Swiss dan Singapura. Dengan layanan melindungi data, aplikasi, sistem, dan produktivitas setiap organisasi dari serangan siber ataupun kegagalan perangkat keras, bencana alam, dan kelalaian manusia. Dikutip dari *Acronis.com* pada 7 Februari pukul 09.13 WIB

sektor yaitu 91% *Web Phising* dan 9% lain merupakan *Email Phising*.

Web Phising sendiri merupakan web ilegal yang dibuat untuk mendapatkan informasi sensitif korban dengan modus *verifikasi account* karena sistem yang aman tidak akan pernah meminta pengguna untuk mengirim password ataupun tampilan pada web yang bernada ancaman seperti "Jika anda tidak merespon dalam waktu 48 jam, account anda akan ditutup".[41]

Sedangkan *email phising* merupakan modus peretasan (*hacking*) dengan mengirimkan email dengan judul (Subject) yang menarik sehingga membuat korban menjadi penasaran dan tertarik untuk membuka email tersebut. Email tersebut berisi file sisipan (*attachment*) atau *link* yang tampak sah. Jika salah satu karyawan perusahaan teknologi mengklik *link* tersebut maka korban akan secara otomatis mengunduh program berbahaya. Apabila program berbahaya ini terinstall, maka secara otomatis bekerja pada komputer korban dan mencuri kredensial, password, akun, dan informasi rahasia lainnya yang dimiliki perusahaan.[42]

Menurut laporan BSSN 2021 tipe file yang dikirim melalui *email phising* 36,24% diantaranya merupakan file *xlsx*. Dengan judul email sebagian besar berhubungan dengan finansial seperti

[41] Adi Nugroho (ed.), *Laporan Tahunan Monitoring Keamanan Siber Tahun 2021*, (Jakarta Selatan: Badan Siber dan Sandi Negara atau BSSN), hlm. 44-45

[42] Adi Nugroho (ed.), *Laporan Tahunan Monitoring*…, hlm. 53

tagihan, pembayaran, bukti pembayaran, permintaan kwitansi, hadiah, dan sebagainya.[43]

Prosedur yang dapat digunakan untuk menangani *phising* pada perusahaan teknologi yaitu :

1) Melakukan *update security* pada *website*
2) Jika perusahaan masih menggunakan sistem *wordpress* maka dianjurkan untuk menggunakan *wordpress* versi terbaru
3) Hubungi perusahaan hosting untuk melakukan *takedown*/penutupan alamat *website* palsu.
4) Jika masih belum berhasil men-*takedown* alamat website palsu maka dapat menghubungi pusat aduan siber dari Badan Siber dan Sandi Negara untuk membantu proses *takedown*.[44]

b. Pemanfaatan celah *Multi-Factor Authentication* (MFA) pada *platform* perusahaan

Menurut Muhammad Adi Nugraha, *Authentication* merupakan proses pengidentifikasian elektronik dari seseorang atau badan hukum. Sedangkan *Multi-Factor Authentication* (MFA) merupakan cara memverifikasi identitas pengguna dengan menggunakan lebih dari dua faktor. Faktor-faktor yang digunakan biasanya merupakan sesuatu yang diketahui pengguna seperti *password* atau *passphrase* atau PIN, dan sesuatu yang dimiliki pengguna seperti token atau

[43] *Ibid.,* Hlm. 55.

[44] *Ibid.,* Hlm. 51.

sertifikat software, serta sesuatu yang berada di pengguna seperti *personal security question* atau sidik jari atau retina.[45]

Seperti sistem keamanan pada umumnya, MFA ini juga terdapat celah kerentanan yang dapat dimanfaatkan peretas untuk mengeksploitasi informasi rahasia yang dimiliki perusahaan. *Federal Bureau of Investigation* (FBI) dan *Cybersecurity and Infrastructure Security Agency* (CISA) juga telah merilis peringatan keamanan mengenai adanya aktivitas peretasan yang memanfaatkan kerentanan konfigurasi MFA (*Multi Factor Authentication*) ini pada aplikasi MFA Duo dan kerentanan CVE-2021-34527[46] terhadap Organisasi Non Pemerintahan/*Non Governmental Organization* (NGO), yang memungkinkan peretas untuk mendaftarkan perangkat baru dan mengakses jaringan korban.[47]

---

[45] Muhammad Adi Nugraha dkk, *Pengamanan Website E-Commerce Menggunakan Multi-Factor Authentication*, jurnal Ilmu Komputer dan Sistem Informasi Vol.9 No. 1, (Jakarta:Universitas Tarumanegara, 2021), hlm. 158

[46] CVE-2021-34527 merupakan kerentanan *Windows Print Spooler Remote Code Execution* yang dikenal dengan istilah *Print NightMare* oleh para peneliti keamanan siber. Peretas menggunakan celah ini untuk mendapatkan hak akses Administrator melalui *Local Privilege Escalation*. Lalu menggunakan *Multi Factor Authentication* aplikasi Duo untuk mencegah perangkat terkoneksi dengan Server Authentication, dan kemudian memanfaatkan mendaftarkan perangkat baru dengan menggunakan akun sah yang tidak lagi digunakan/tidak aktif. Serangan tersebut digunakan untuk melakukan pencurian data yang tersimpan di *Cloud Storage*, *email* ataupun konten lainnya.

[47] Badan Siber dan Sandi Negara atau BSSN, *Peringatan Keamanan Aktivitas Peretasan Jaringan Dengan Memanfaatkan Kerentanan Aplikasi Multi Faktor Otentikasi dan Kerentanan Printer Spooler*, (Jakarta Selatan: Badan Siber dan Sandi Negara atau BSSN, 2022), hlm. 1

Menurut BSSN celah MFA ini dapat diminimalisir dengan prosedur sebagai berikut[48] :

1) Menerapkan *Multi Factor Authentication* pada seluruh pengguna tanpa terkecuali. Sebelum mengimplementasi ini organisasi juga sebaiknya melakukan reviu konfigurasi untuk memproteksi terhadap skenario "*fail open*" dan *re-enrollment*;
2) Mengimplementasikan fitur *time-out* dan *lock-out features* untuk mencegah proses *Brute Force Attack*;
3) Memastikan akun yang tidak digunakan/tidak aktif untuk dinonaktifkan seluruhnya pada layanan *Active Directory*, MFA *systems* dan lainnya;
4) Memperbaharui perangkat lunak, termasuk sistem operasi, aplikasi dan *firmware* yang digunakan untuk mencegah eksploitasi dengan menggunakan kerentanan yang telah ada *exploit*-nya;
5) Menerapkan *password* yang kuat dan unik untuk seluruh akun;
6) Secara berkelanjutan memonitor log pada perangkat jaringan untuk mengidentifikasi aktivitas mencurigakan dan upaya percobaan login yang dilakukan;
7) Menerapkan kebijakan notifikasi apabila terdapat kejadian keamanan atau aktifitas anomali untuk seluruh perubahan terhadap akun/grup akun, dan apabila terhadap aktivitas proses

[48] Badan Siber dan Sandi Negara atau BSSN, *Peringatan …*, hlm. 5

yang mencurigakan seperti (ntdsutil, rar, regedit, dan lainnya.).[49]

c. *Ransomware*

Menurut laporan BSSN tahun 2021, serangan *ransomware* menjadi jenis serangan kedua terbanyak dengan 15 laporan.[50] *Ransomware* sendiri merupakan sebuah jenis *malware* yang menyerang korban dengan cara mengunci seluruh file yang dimiliki, meminta tebusan terhadap korban, dan peretas akan memberikan kunci untuk digunakan korban dalam membuka dokumen yang dimiliki setelah korban membayar sesuai dengan tarif yang diberikan oleh peretas.[51]

Secara global menurut data *Emsisoft*[52], Indonesia termasuk dalam 10 besar negara yang melaporkan insiden serangan *ransomware* sebanyak 13,80% *submission* berasal dari Indonesia. Terdapat 3 sektor sasaran terbanyak selama tahun 2021 yaitu sektor penerbangan, sektor perbankan, dan BUMN.[53]

---

[49] *Ibid.,* Hlm. 6.

[50] Adi Nugroho (ed.), *Laporan Tahunan Monitoring*…, hlm. 71

[51] *Ibid.,* Hlm. 73.

[52] *Emsisoft* kepanjangan dari Emisi Software Gmbh yang merupakan perusahaan pengembang keamanan perangkat lunak (*software*) yang berasal New Zealand yang didirikan oleh CEO Christian Mairoll pada tahun 2003. Dikutip dari Emisoft.com pada 7 Februari 2023 pukul 10.14 WIB

[53] *Ibid.,* Hlm. 150-151.

Menurut BSSN cara agar terhindar dari serangan *ransomware* yaitu sebagai berikut[54] :

1) Membangun stabilitas/keamanan dan perlindungan perangkat hingga ke level *endpoints;*
2) Membangun tim tanggap insiden / poin kontak penanganan insiden;
3) Selalu memonitor sistem keamanan secara aktif melalui tim khusus;
4) Melakukan prosedur *backup* (terpisah dari sistem utama) dan *restore* secara berkala;
5) Memastikan seluruh *backup* data *terenkripsi*/terkunci
6) Evaluasi sistem yang digunakan yang telah dinyatakan *End of Support* (EOS);
7) Lakukan segmentasi jaringan organisasi atau tentukan zona demiliterisasi yang menghilangkan komunikasi yang tidak diatur antara jaringan TI dan OT;
8) Terapkan kebijakan *strong and unique password*
9) Aktifkan fitur *log* pada sistem infrastruktur perusahaan secara terpusat
10) Bangun budaya keamanan siber di lingkungan perusahaan
11) Kontrol pengembangan dan penggunaan aplikasi pada perusahaan pusat maupun cabang

[54] *Ibid.,* Hlm. 159.

12) Terapkan kebijakan *Autentikasi Multi-Faktor* (MFA) untuk semua pengguna tanpa terkecuali terhadap semua layanan yang disediakan organisasi khususnya untuk email web, virtual private network, remote access, dan akun yang dapat mengakses sistem kritis
13) Buat kebijakan mengenai pemisahan pemakaian perangkat pribadi dan perangkat perkantoran
14) Buat, latih, dan perbarui program tanggap insiden siber pada pegawai secara berkala.[55]

d. *Malware*

Menurut Sastya Hendri Wibowo, *malware* merupakan sebuah program yang dibuat khusus untuk bekerja memasuki perangkat komputer secara ilegal. *Malware* ini dapat mengakibatkan kerusakan pada system, server, dan jaringan komputer.[56]

Malware sendiri memiliki beberapa jenis, salah satunya Botnet yang menempati peringkat pertama top anomali pada tahun 2021. Menurut laporan BSSN tahun 2021, Botnet menyumbang 44,62% dari serangan anomali pada tahun tersebut. Botnet sendiri merupakan jaringan komputer yang terinfeksi oleh malware yang berada di bawah kendali satu pihak peretas. Botnet dapat dirancang

[55] *Ibid.,* Hlm. 159-163.

[56] Diana Purnama Sari (ed.), *Cybercrime di Era Digital*, (Sumatera Barat: PT Global Eksekutif Teknologi, 2022), hlm. 25

untuk pengiriman spam, pencurian data, *ransomware*, *click fraud*, *Denial-of-Service* (DoS), dan lain-lain.[57]

BSSN merekomendasikan perusahaan untuk memitigasi *malware* Mylo Bot dengan prosedur sebagai berikut :

1) Lakukan *update* dan *patch* perangkat komputer dan antivirus yang digunakan;
2) Melakukan pencadangan data yang ada di komputer secara berkala;
3) Gunakan *password* yang kuat;
4) Hindari akses terhadap situs web atau domain yang tidak terpercaya; dan
5) Hindari untuk mengunduh dan membuka e-mail dari alamat pengirim yang tidak dikenal.[58]

3. Regulasi *Hacking* Yang Dapat di Pidanakan

Menurut *Convention on Cybercrime* di Budapest tanggal 23 November 2001, bentuk-bentuk kejahatan komputer dibagi menjadi 4 (empat) kategori yaitu:

a. *Offences against the confidentiality, integrity and availability of computer data and systems*, (kejahatan terhadap kerahasiaan,

[57] *Ibid.,* Hlm. 17.

[58] *Ibid.,* Hlm. 18.

integritas, dan ketersediaan data dan sistem komputer) yang meliputi:

1) *Illegal access* (mengakses tanpa hak)

Secara umum seseorang yang mengakses sistem elektronik orang lain sudah merupakan bentuk pidana *hacking*. Bentuk perbuatan pada pasal 30 ayat 3 Undang-Undang No. 11 tahun 2008 tentang Informasi dan Transaksi Elektronik yang dimaksud dengan mengakses ilegal yaitu dengan cara apapun melanggar, menerobos, melampaui, atau menjebol sistem keamanan orang lain.[59]

2) *Illegal interception* (menyadap tanpa hak)

Penyadapan ilegal merupakan bentuk kejahatan dengan perbuatan melawan hukum baik intersepsi atau penyadapan. Kecuali oleh pihak berwenang untuk mengungkapkan suatu kejahatan lain. Intersepsi atau penyadapan ilegal diatur dalam pasal 31 ayat 1 Undang-Undang Nomor 19 tahun 2016 atas perubahan Undang-Undang No. 11 tahun 2008 tentang Informasi dan Transaksi Elektronik. Objek pidana pada pasal tersebut yaitu informasi elektronik dan/atau dokumen

[59] Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik (Lembaran Negara Republik Indonesia Tahun 2008 Nomor 58, Tambahan Lembaran Negara Republik Indonesia Nomor 4843). Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 tentang ITE (Lembaran Negara Republik Indonesia Tahun 2016 Nomor 251)

elektronik dalam komputer dan/atau sistem elektronik tertentu milik elektronik.[60]

3) *Data interference* (merusak data)

Perusakan data yang dimaksud disini adalah mengubah, menambah, mengurangi, melakukan transmisi, merusak menghilangkan, memindahkan, menyembunyikan dengan cara apapun. Peraturan mengenai perusakan data ini tertuang pada pasal 32 ayat 1 *jo* 48 Undang-Undang Nomor 19 tahun 2016 atas perubahan Undang-Undang No. 11 tahun 2008 tentang Informasi dan Transaksi Elektronik. Objek pidana pada pasal tersebut yaitu informasi elektronik dan/atau dokumen elektronik dalam komputer dan/atau sistem elektronik tertentu milik elektronik.[61]

4) *Systems interference* (mengganggu sistem)

Tindak pidana yang mengakibatkan terganggunya sistem elektronik dan tidak dapat bekerja sebagaimana mestinya ini diatur pada pasal 33 *jo* 49 Undang-Undang Nomor 19 tahun

---

[60] Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik (Lembaran Negara Republik Indonesia Tahun 2008 Nomor 58, Tambahan Lembaran Negara Republik Indonesia Nomor 4843). Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 tentang ITE (Lembaran Negara Republik Indonesia Tahun 2016 Nomor 251)

[61] Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik (Lembaran Negara Republik Indonesia Tahun 2008 Nomor 58, Tambahan Lembaran Negara Republik Indonesia Nomor 4843). Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 tentang ITE (Lembaran Negara Republik Indonesia Tahun 2016 Nomor 251)

2016 atas perubahan Undang-Undang No. 11 tahun 2008 tentang Informasi dan Transaksi Elektronik. Objek pidana pada pasal tersebut yaitu informasi elektronik dan/atau dokumen elektronik dalam komputer dan/atau sistem elektronik tertentu milik elektronik. Perbuatan pada pasal ini yaitu tindakan apapun yang ditujukan pada sistem elektronik orang lain

5) *Misuse of devices* (menyalahgunakan perlengkapan)

Perbuatan penyalahgunaan yang diatur pada pasal 34 jo 50 Undang-Undang Nomor 19 tahun 2016 atas perubahan Undang-Undang No. 11 tahun 2008 tentang Informasi dan Transaksi Elektronik yaitu memproduksi, menjual, mengadakan untuk digunakan, mengimpor, mendistribusikan, menyediakan, atau memiliki perangkat keras atau perangkat lunak komputer yang dirancang atau secara khusus dikembangkan untuk memfasilitasi perbuatan pada pasal 27 sampai dengan pasal 33 Undang-Undang Nomor 19 tahun 2016 atas perubahan Undang-Undang No. 11 tahun 2008 tentang Informasi dan Transaksi Elektronik.[62]

[62] Nudirman Munir, *Pengantar Hukum Siber Indonesia. Edisi Ketiga*, (Depok: Raja Grafindo Persada, 2017), hlm. 63

b. *Computer related offences* (kejahatan yang berhubungan dengan komputer), yang meliputi:

1) *Computer related forgery* (kejahatan yang berhubungan dengan pemalsuan)

Pemalsuan yang dimaksudkan disini adalah perbuatan manipulasi yang hanya dapat dilakukan terhadap informasi dan/atau data elektronik yang telah ada. Pemidanaan pemalsuan ini tertuang dalam pasal 35 *jo* 51 ayat 1 Undang-Undang Nomor 19 tahun 2016 atas perubahan Undang-Undang No. 11 tahun 2008 tentang Informasi dan Transaksi Elektronik. Bentuk perbuatan yang dilarang pada pasal ini yaitu manipulasi, penciptaan, perubahan, penghilangan, pengrusakan pada informasi dan/atau data elektronik yang bertujuan agar informasi dan/atau data elektronik tersebut dianggap seolah-olah otentik.[63]

2) *Computer related fraud* (kejahatan yang berhubungan dengan penipuan)

Penipuan online ini diatur pada pasal 28 ayat 1 *jo* 45 ayat 2 Undang-Undang Nomor 19 tahun 2016 atas perubahan Undang-Undang No. 11 tahun 2008 tentang Informasi dan Transaksi Elektronik. Dengan bentuk perbuatan menyebarkan berita bohong dan menyesatkan yang mengakibatkan kerugian

[63] *Ibid.,* Hlm. 64.

konsumen dalam transaksi elektronik. Konteks yang digunakan pasal ini merupakan penipuan melalui sistem elektronik baik dikirim melalui layanan aplikasi pesan, penyiaran daring, situs/media sosial, lokal pasar (*marketplace*), iklan, dan/atau layanan transaksi lainnya melalui sistem elektronik.[64]

c. *Content related offences yang meliputi offences related to child pornography* (kejahatan yang bermuatan pornografi anak)

Kejahatan yang bermuatan pornografi anak tertuang pada pasal 52 ayat 1 *jo* 27 ayat 1 Undang-Undang Nomor 19 tahun 2016 atas perubahan Undang-Undang No. 11 tahun 2008 tentang Informasi dan Transaksi Elektronik. Anak yang dimaksudkan merupakan anak sebagai pihak yang harus mendapatkan perlindungan hukum.

Pasal 27 ayat 1 sendiri berisi tindak pidana ITE yang melarang mendistribusikan dan/atau mentransmisikan dan/atau membuat dapat diaksesnya Informasi elektronik dan/atau dokumen elektronik yang memiliki muatan yang melanggar kesusilaan.

Jika perbuatan pada pasal 27 ayat 1 dilakukan terhadap informasi elektronik dan/atau dokumen elektronik yang menyangkut eksploitasi seksual terhadap anak, maka penjatuhan

[64] Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik (Lembaran Negara Republik Indonesia Tahun 2008 Nomor 58, Tambahan Lembaran Negara Republik Indonesia Nomor 4843). Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 tentang ITE (Lembaran Negara Republik Indonesia Tahun 2016 Nomor 251)

pidana maksimumnya dapat ditambah dengan sepertiganya (baik penjara maupun denda).

d. *Offences related to infringements of copyrights and related rights* (kejahatan yang berhubungan dengan Hak Kekayaan Intelektual).[65]

Kejahatan ini memiliki unsur perbuatan yang tertuang pada pasal 112 *jo* pasal 52 Undang-Undang Nomor 28 Tahun 2014 tentang Hak Cipta yaitu merusak, memusnahkan, menghilangkan, atau membuat tidak berfungsinya sarana kontrol teknologi yang digunakan sebagai pelindung ciptaan atau produk hak terkait. Perbuatan-perbuatan tersebut ditujukan agar dapat digunakan secara komersial oleh orang lain.[66]

Regulasi yang telah ada tersebut merupakan regulasi yang dibuat berdasarkan hasil konvensi siber di Budapest 2001. Walaupun regulasi di Indonesia telah mengarah dan memenuhi indikator yang dikategorikan dalam hasil konvensi tersebut, akan tetapi tidak menutup kemungkinan regulasi tersebut telah usang dan perlu adanya pembaharuan internasional untuk dapat melindungi dunia siber dalam skala nasional di setiap negara. Maka dari itu perlu adanya kajian lebih lanjut mengenai dampak dan keefektifan dari penerapan hasil konvensi siber tersebut.[67]

---

[65] Nudirman Munir, *Pengantar* ..., hlm. 64.

[66] Undang-Undang Nomor 28 Tahun 2014 Tentang Hak Cipta (Lembaran Negara Republik Indonesia Tahun 2014 Nomor 266, Tambahan Lembaran Negara Republik Indonesia Nomor 5599).

[67] *Ibid.*

BAB IV
ANALISIS PERLINDUNGAN HUKUM PERUSAHAAN TEKNOLOGI TERHADAP SERANGAN *HACKING* DITINJAU DARI HUKUM POSITIF DAN *MAQASHID SYARIAH*

A. Analisis Perlindungan Hukum Perusahaan Teknologi Terhadap Serangan *Hacking* Ditinjau Dari Hukum Positif

1. Analisis Perlindungan Hukum Perusahaan Teknologi

Menurut Herry Irawan dan Puspita Kencana Sari, perusahaan teknologi adalah sebuah usaha yang baru berjalan dan menerapkan inovasi teknologi untuk menjalankan *core business*-nya yang juga dapat memecahkan sebuah masalah di masyarakat.[1] Inovasi teknologi dalam pemecahan permasalahan-permasalahan di masyarakat juga dibagi menjadi beberapa sektor bisnis.

Prinsip perlindungan sesuai kesepakatan dalam Konvensi Cybercrime di Budapest pada 2001 menyatakan,

> "*... convinced of the need to pursue, as a matter of priority, a common criminal policy aimed at the protection of society against cybercrime, inter alia by adopting appropriate legislation and fostering international cooperation*".[2]

[1] Herry Irawan dan Puspita Kencana Sari, *Buku Bisnis Informasi*, (Ponorogo: Uwais Inspirasi Indonesia, 2018), hlm. 37

[2] Council Of Europe, *Convention on Cybercrime*, Konferensi XI Budapest 2001, hlm. 1

Maksudnya, perlindungan bagi masyarakat yang dalam hal ini termasuk perusahaan teknologi terhadap *cybercrime* harus menjadi prioritas. Hal tersebut dapat melalui pembentukan kebijakan kriminal bersama dengan negara-negara lain. Salah satunya dengan memberlakukan perundang-undangan yang sesuai kebutuhan dan mendorong kerjasama internasional.

Lembaga siber di Indonesia yang berwenang melakukan kerjasama internasional yaitu Badan Siber dan Sandi Negara (BSSN). Akan tetapi kewenangan tersebut masih kurang menurut badan NCIS[3]. Karena untuk melindungi dunia siber nasional dibutuhkan infrastruktur dan kebijakan yang tepat. Dimana Indonesia sendiri masih kekurangan lembaga edukasi siber, unit pengembangan kebijakan keamanan siber, dan unit pengembang perlindungan layanan publik.

Kurangnya infrastruktur kelembagaan tersebut berpengaruh besar terhadap perkembangan inovasi teknologi yang digunakan oleh perusahaan untuk pengembangan bisnis. Seperti halnya menurut Dona Budi Kharisma, bahwa dibutuhkan regulasi untuk mendorong dan melindungi startup atau perusahaan teknologi sebagai pelaku utama ekosistem ekonomi digital.[4]

---

[3] NCIS atau *National Criminal Intelligence Service* merupakan lembaga investigasi bentukan Uni Eropa yang bertugas dalam riset investigasi *cyber crime* dari 161 negara

[4] Dona Budi Kharisma, *Membangun Kerangka Pengaturan Startup di Indonesia*, *Jurnal Rechtsvinding* Volume 10 Nomor 3, (Surakarta: Universitas Sebelas Maret, 2021), hlm. 438

Menurut Floriant A.Schmidt dalam karyanya *Digital Labour Markets in the Platform Economy*, perusahaan teknologi dibagi menjadi beberapa jenis sesuai sektor bisnis. Seperti pada Gambar 5 dan Gambar 6 yang merupakan contoh pembagian sektor bisnis perusahaan teknologi yang ada di Amerika Serikat. Jika dibandingkan dengan sektor perusahaan teknologi yang didirikan dan dikembangkan oleh orang Indonesia maka akan seperti pada Gambar 7.[5]

[5] Floriant A. Schmidt, *Digital Labour Markets in the Platform Economy Mapping the Political Challenges of Crowd Work and Gig Work*, English Version, (German: Friedrich-Ebert-Stiftung, 2017), hlm. 6-7

Gambar 5
Pembagian Sektor Perusahaan Teknologi Secara Umum di Amerika Serikat

Gambar 6

Pembagian Penyedia Jasa Komersial di Amerika Serikat

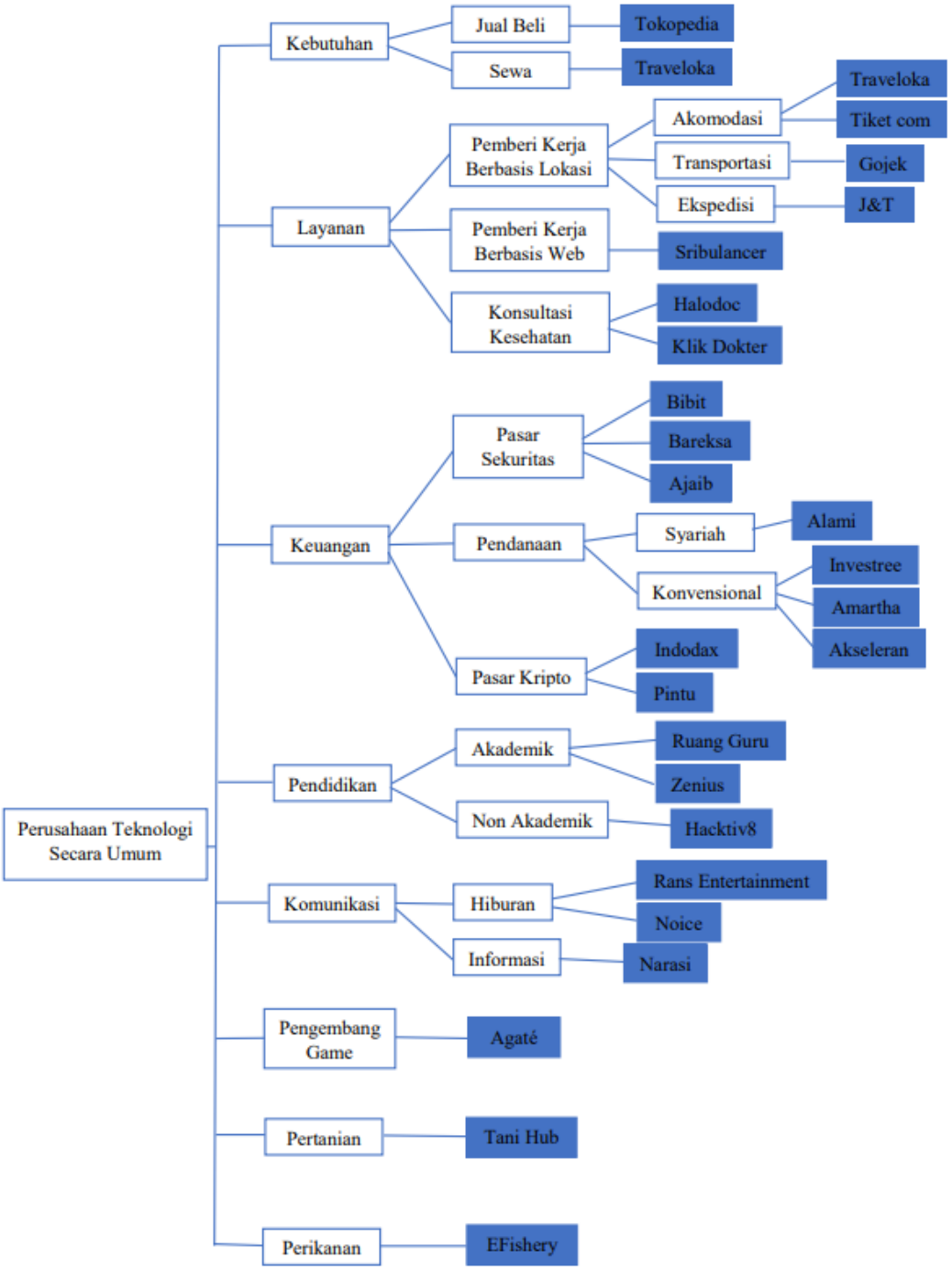
Sedangkan menurut Stephanie, perusahaan teknologi di Indonesia sendiri masih terbatas pada beberapa sektor. Seperti sektor jual-beli online (*ecommerce*), transportasi, keuangan, pendidikan, pertanian, perikanan, dan pengembang game.[6]

Berikut merupakan contoh startup atau perusahaan teknologi yang dikembangkan dan didirikan oleh orang Indonesia, *Ecommerce* (Bukalapak, Tokopedia, Zalora), *Logistic* (J&T Express, Gojek, Maxim), *Travel Agency* (Tiket.com, Traveloka, Pegipegi), *Fintech* (Ajaib, Indodax, Alami, Kredit Gogo, UangTeman, Modalku). Jika dipetakan menjadi map maka akan menjadi seperti pada Gambar 7.

[6] Stephanie PD dkk, *Mengelaborasi Hukum Positif Tertulis Indonesia Mengatur Startup*, Seminar Nasional Hasil Penelitian dan Pengabdian Kepada Masyarakat 2021, (Jakarta: Universitas Tarumanegara, 2021) hlm. 1254

Gambar 7

Pembagian Sektor Perusahaan Teknologi di Indonesia



Pemetaan sektor bisnis pada perusahaan teknologi yang dikembangkan dan didirikan oleh orang Indonesia tersebut tidak lepas dari regulasi. Regulasi yang hingga saat ini belum ada pengkhususan dari lembaga berwenang membuat inovasi teknologi dan pengembangan bisnisnya terbatas. Pengembangan inovasi teknologi tersebut jika tidak diawasi oleh lembaga khusus akan memperbesar masalah persaingan bisnis dan teknologi. Dimana hal tersebut juga akan berpengaruh pada masyarakat Indonesia sebagai pengguna aktif dari adanya teknologi tersebut.

Berikut merupakan pemetaan regulasi pemanfaatan teknologi sebagai bentuk perlindungan terhadap perusahaan teknologi[7] :

a. *E-commerce*

Menurut Laudon and Laudon, *e-commerce* atau *electronics commerce* merupakan kegiatan perdagangan atau transaksi jual beli melalui sistem elektronik atau internet. Perdagangan dalam sistem elektronik ini dapat berupa transaksi retail ataupun grosir.[8] Sedangkan definisi dari transaksi elektronik diatur dalam Pasal 1 Ayat 2 Undang-Undang Informasi dan Transaksi Elektronik yaitu, setiap transaksi secara elektronik baik melalui *marketplace* maupun pada *platform e-commerce*. Transaksi elektronik tersebut termasuk sebagai perbuatan hukum yang menggunakan komputer,

[7] Dona Budi Kharisma, *Membangun Kerangka …*, hlm. 439

[8] Kenneth C. Laudon dan Jane P. Laudon, *Management Information Systems Managing The Digital Firm*, English Version, *Global Editional*, (Edinburgh: Pearson Education Limited, 2014), hlm. 402

jaringan komputer, dan/atau media elektronik lain.[9] Indonesia sendiri telah berhasil mengembangkan perusahaan teknologi di bidang *e-commerce* seperti Tokopedia, Bukalapak, dan Zalora.

Perkembangan perusahaan *e-commerce* tersebut tidak lepas dari regulasi yang terdapat pada Undang-Undang Nomor 7 Tahun 2014 tentang Perdagangan, Peraturan Pemerintah Nomor 80 Tahun 2019 tentang Perdagangan Melalui Sistem Elektronik (PMSE), dan Peraturan Presiden Nomor 74 Tahun 2017 tentang Peta Jalan Sistem Perdagangan Nasional Berbasis Elektronik.[10]

Perlindungan yang dibutuhkan perusahaan teknologi pada sektor *ecommerce* dari serangan *hacking* adalah data informasi pengguna layanan, keamanan sistem komputer dari gangguan, perlindungan dan pengawasan transaksi. Karena hingga penelitian ini dibuat industri *e-commerce* masih menjadi sasaran utama yang bernilai ekonomi tinggi bagi para *attacker*.

Kasus kebocoran data Bukalapak, Tokopedia, dan Lazada menjadi daftar panjang perusahaan teknologi korban *hacking* yang terus berulang pada sektor *ecommerce*. Hal tersebut membuat kerugian materil dan non materil berupa besarnya biaya penanganan hingga turunnya kepercayaan masyarakat pada perusahaan teknologi. Maka dari itu dibutuhkan perlindungan sekaligus pengawasan dari pemerintah pada perusahaan teknologi.

---

[9] Rio Christiawan, Aspek Hukum Startup, (Jakarta Timur: Sinar Grafika, 2022), hlm. 43
[10] *Ibid,* Hlm. 439

b. *Financial Services* (Fintech)

Sesuai pasal 3 ayat 1 perusahaan teknologi *financial service* memanfaatkan adanya sistem teknologi dengan memberikan lima layanan kemudahan yaitu sistem pembayaran digital (*digital payment*), pendukung pasar, manajemen investasi dan manajemen risiko, pinjaman pembiayaan dan penyedia modal. Layanan finansial tersebut secara umum dibagi menjadi dua kategori yaitu[11] :

1) Pasar sekuritas (*Securities Market*),

Kemudahan dalam membeli kepemilikan sebuah perusahaan ataupun aset digital yang memiliki nilai ekonomis di masyarakat. Perusahaan Indonesia yang memanfaatkan teknologi dalam memberikan layanan ini adalah Bibit, Bareksa, Ajaib, Ipot, Indodax, Pintu, Toko Crypto, dll).

2) Pinjaman dan Pembiayaan berbasis teknologi (*Peer-to-peer lending* dan *Crowdfunding*)

Kemudahan pemberian pinjaman pada pemilik bisnis maupun perseorangan untuk meminjam maupun menggalang dana pada proyek tertentu. Layanan ini biasa menggunakan *prinsip peer to peer lending* ataupun *crowdfunding*. Perusahaan teknologi yang didirikan dan

[11] Peraturan Bank Indonesia Nomor 19/12/PBI/ 2017 tentang Penyelenggaraan Teknologi Finansial

berasal dari Indonesia yang berhasil memberikan layanan ini adalah Alami, Akseleran, Investree, Amartha.[12]

Kemudahan-kemudahan dalam bertransaksi tersebut membuat para *attacker* mencari celah keamanan dari sistem perbankan maupun sistem perusahaan teknologi yang terafiliasi dengan bank. *Attacker* akan mencoba berbagai cara untuk bisa mencuri ataupun memanfaatkan kelengahan pengguna untuk membuat jaminan peminjaman dengan bantuan teknologi seperti AI (*Artificial Intelegent*). Dengan resiko tersebut dibutuhkan perlindungan yang lebih melalui infrastruktur pendukung. Mulai dari kelembagaan yang profesional hingga alat-alat yang memadai untuk meminimalisir celah dari *attacker*.[13]

Regulasi yang berkaitan dengan layanan finansial hanya ada pada Peraturan Bank Indonesia (PBI) Nomor 22 /20/PBI/ 2020 Tentang Perlindungan Konsumen Bank Indonesia, PBI Nomor 23 /6/PBI/ 2021 Tentang Penyedia Jasa Pembayaran, PBI Nomor 23 /7/PBI/ 2021 Tentang Penyelenggaraan Infrastruktur Sistem Pembayaran, Peraturan Otoritas Jasa Keuangan (POJK) Nomor 77 /POJK.01/ 2016 Tentang Layanan Pinjam Meminjam Uang Berbasis Teknologi Informasi, POJK Nomor 13 /POJK.02/ 2018 Tentang Inovasi Keuangan Digital di Sektor Jasa Keuangan,

[12] *Ibid.,* Hlm. 439
[13] *Ibid.*

POJK Nomor 57 /POJK.04/ 2020 Tentang Penawaran Efek Melalui Layanan Urun Dana Berbasis Teknologi Informasi.[14]

Kasus *hacking* pada BRI Life (Juli 2021), Bank Jatim (Oktober 2021), hingga BSI Mobile Banking (8-9 Mei 2023) menjadi kasus *hacking* yang tidak dapat diremehkan.[15] Karena data pegawai bank, data pengguna bank hingga transaksi terakhir dapat dicuri oleh para *attacker* dan di jual di *dark web*. Kasus *hacking* tersebut mengakibatkan mobile banking tidak dapat diakses oleh pengguna selama beberapa hari, terhapusnya sistem data pengguna, hingga bank harus mempertanggungjawabkan kelalaiannya.

c. Perusahaan Transportasi dan Makanan

Perusahaan teknologi dibidang transportasi dan makanan merupakan salah satu perusahaan penyedia layanan antar orang, barang, dan makanan. Pengaturan mengenai layanan ini terdapat pada Undang-Undang Nomor 22 Tahun 2009 tentang Lalu Lintas dan Angkutan Jalan, Undang-Undang Nomor 18 Tahun 2012 Tentang Tentang Pangan, Peraturan Menteri Perhubungan Nomor 118 Tahun 2018 Tentang Penyelenggaraan Angkutan Sewa Khusus, Peraturan Badan Pengawas Obat dan Makanan Tahun

[14] *Ibid.,* Hlm. 439

[15] Dikutip dari CNBC Indonesia https://www.cnbcindonesia.com/tech/20230513070118-37-436999/terungkap-gang-hacker-ransomeware-akui-retas-layanan-bsi pada 18 Mei 2023 pukul 19.38 WIB

2020 Tentang Pengawasan Obat dan Makanan yang Diedarkan Secara Daring.[16]

Regulasi-regulasi yang telah ada ini belum sepenuhnya melindungi perusahaan teknologi di sektor layanan transportasi dan makanan. Belum terpenuhinya sistem pelacak pesanan palsu (pesanan fiktif), kerentanan peretasan (*hacking*) pada akun driver maupun pengguna membuat pengawasan sistem harus lebih dioptimalkan. Perusahaan teknologi transportasi dan makanan yang didirikan, dikembangkan, dan berasal dari Indonesia sendiri yaitu Gojek dan Maxim.

d. Perusahaan Pendidikan (*Teched*)

Perusahaan teknologi di sektor pendidikan atau lebih sering disebut dengan *teched* memberikan layanan kemudahan pembelajaran akademik maupun pelatihan *soft skill*. Perusahaan teknologi sektor pendidikan di Indonesia yang berhasil berkembang seperti Ruang guru, Zenius, dan Hacktiv8.

Pengaturan bagi perusahaan teknologi pada sektor pendidikan ini meliputi Undang-Undang Nomor 20 Tahun 2003 Tentang Sistem Pendidikan Nasional, Peraturan Menteri Pendidikan Dan Kebudayaan Nomor 109 Tahun 2013 Tentang Penyelenggaraan Pendidikan Jarak Jauh Pada Pendidikan Tinggi, Peraturan Menteri Pendidikan Dan Kebudayaan Nomor 119

[16] *Ibid.,* Hlm. 439

Tahun 2014 Tentang Penyelenggaraan Pendidikan Jarak Jauh Jenjang Pendidikan Dasar dan Menengah.[17]

Belum adanya infrastruktur yang memadai dalam dunia pendidikan memperbesar peluang peretasan pada soal-soal ujian. Mulai dari pencurian soal-soal ujian, manipulasi jawaban dengan sistem pemrograman tertentu (AI), hingga pemalsuan sertifikat pelatihan menjadi pekerjaan rumah regulator dan lembaga perlindungan sekaligus pengawas terkait.

e. Perusahaan Online Media dan Travel

Perusahaan teknologi online media membutuhkan perlindungan dalam pengawasan sistem dan publikasi. Agar informasi yang dipublikasi dapat memberikan informasi akurat tanpa menggunakan ‘headline kontroversial’ ataupun penyebaran informasi hoax kepada masyarakat. Pengawasan pada sistem online media juga perlu diperketat menjelang ‘pesta demokrasi’ yang berlangsung pada 2024 mendatang. Untuk meminimalisir adanya *hacktivist* yang menyerang dan mengganggu sistem.[18]

Sedangkan pada perusahaan teknologi di sektor travel perlindungan dibutuhkan pada sistem untuk meminimalisir adanya peretasan disaat *booking*, gangguan sistem pembayaran, peretasan dengan memanfaatkan akun yang tidak aktif.

---

[17] *Ibid.*
[18] *Ibid.,* Hlm. 43

Regulasi yang mencakup perusahaan online media dan travel ada pada Undang-Undang Nomor 40 Tahun 1999 Tentang Pers, Undang-Undang Nomor 10 Tahun 2009 Tentang Kepariwisataan, Peraturan Menteri Pariwisata Nomor 10 Tahun 2018 Tentang Pelayanan Perizinan Berusaha Terintegrasi Secara Elektronik Sektor Pariwisata.[19]

Perusahaan teknologi penyedia layanan online media yang berasal, dikembangkan, dan didirikan oleh orang Indonesia sendiri ada Narasi, Detik com, Jawa Pos, dll. Sedangkan perusahaan teknologi di sektor travel ada Traveloka, PegiPegi. Di sektor lain ada jasa ekspedisi seperti J&T dan sektor jasa pemberi kerja seperti Sribulancer.

Perlindungan pada perusahaan teknologi online media dan travel sangat diperlukan untuk menjamin sistem komputer berjalan tanpa gangguan dari pihak lain yang ingin meneror hingga merusak sistem. Hal tersebut diperlukan agar kasus *hacking* seperti pada Narasi tidak terjadi lagi. Apalagi Indonesia akan merayakan ‘pesta demokrasi’ di 2024 nanti.

f. Developer Game (Pengembang Permainan)

Menurut Jusuf Ariz, industri pengembangan game di Indonesia belum memiliki regulasi perlindungan khusus. Hal tersebut membuat perusahaan teknologi pada industri ini

[19] *Ibid.,* Hlm. 439

mengalami banyak permasalahan seperti tidak adanya keberagaman (*diversity*), baik isi (*content*) dan keberagaman kepemilikan (*ownership*), dominasi pasar yang memunculkan persaingan tidak sehat antar perusahaan pengembang game, hingga pembatasan pada regulasi media yang berdampak pada kesulitan pengembang game untuk berkembang. Karena pada dasarnya regulasi mempunyai sisi menjaga aturan pasar agar tidak terciptanya monopoli atau bahkan komersialisasi media.[20]

g. Perusahaan Teknologi Pertanian

Menurut Rika Reviza, aspek yang harus diawasi meliputi infrastruktur inovasi teknologi, peningkatan akses pasar, dan anggaran pembangunan untuk mendukung ekspor pertanian. Agar perusahaan teknologi di industri pertanian tidak hanya memasarkan hasil pertaniannya di dalam negeri. Akan tetapi hingga ke luar negeri (ekspor) dengan bantuan pemanfaatan teknologi digital. Ekspor produk pertanian menjadi tantangan tersendiri mengingat sifat produk pertanian yang mudah rusak dan harus memenuhi standar keamanan pangan internasional.[21] Untuk mengekspor produk pertanian petani juga sering menemui hambatan seperti regulasi, kekurangan sarana dan prasarana untuk

---

[20] Jusuf Ariz Wahyuono, *Ekonomi Politik Pengembang Game Lokal Spesialisasi dan Ekspansi Bisnis PT Git Solution dan Noobzilla di Yogyakarta*, Journal Communication Spectrum, (Yogyakarta: Universitas Gajah Mada, 2021), hlm. 139-140

[21] Rika Reviza Rachmawati dan Endro Gunawan, *Peranan Petani Milenial Mendukung Ekspor Hasil Pertanian di Indonesia*, Forum Penelitian Agro Ekonomi, Vol. 38 No. 1, (Jawa Barat: Pusat Sosial Ekonomi dan Kebijakan Pertanian, 2020), hlm. 78

proses produksi, serta standar *Good Manufacturing Practices* (GMP)[22].

Pengawasan terhadap perusahaan teknologi di sektor pertanian juga perlu ditingkatkan agar kasus seperti Tanihub yang merubah bisnisnya menjadi perusahaan *fintech* tidak terjadi lagi. Perlindungan terhadap sistem informasi perusahaan teknologi perlu diperketat agar tidak terjadi peretasan yang mengganggu proses pengiriman dan dominasi pasar. Selain itu pengawasan yang ketat juga harus selalu diterapkan agar proses ekspor ini tidak menjadi lahan penyelundupan barang ilegal.[23]

h. Perusahaan Teknologi Perikanan

Secara umum usaha perikanan dibedakan menurut jenisnya ada 2 (dua), yaitu perikanan tangkap dan perikanan budidaya. Perikanan tangkap dilakukan dengan cara memburu dan menangkap ikan dengan menggunakan sarana penangkapan yang dilakukan oleh nelayan ataupun perusahaan penangkapan ikan di laut maupun di perairan umum, seperti sungai, waduk, danau, dan rawa. Perikanan budidaya dilakukan melalui pemanfaatan wilayah pesisir pantai yang tenang dan terlindung

[22] GMP merupakan suatu pedoman produksi agar produsen memenuhi persyaratan yang telah ditentukan untuk menghasilkan produk bermutu sesuai standar negara yang dituju.

[23] Rika Reviza Rachmawati dan Endro Gunawan, *Peranan…,* hlm. 78

untuk memelihara komoditas yang bernilai ekonomis dengan menggunakan teknologi budidaya tertentu.[24]

Menurut pasal 25 c ayat 2 Undang-undang Nomor 31 Tahun 2004 *jo* Undang-undang Nomor 45 Tahun 2009 tentang Perikanan terdapat berbagai model pengelolaan sumber daya perikanan, salah satunya *Co-management* didefinisikan sebagai pembagian tanggung jawab dan wewenang antara pemerintah dengan perusahaan yang bergerak di bidang perikanan serta pengguna sumberdaya lokal (masyarakat).[25]

Penerapan prinsip partisipasi pada industri perikanan diatur pada Undang-Undang No. 31 Tahun 2004, sebagaimana diubah dengan Undang-Undang Nomor 45 Tahun 2009 tentang Perubahan atas Undang-Undang Nomor 31 Tahun 2004 tentang perikanan (Undang-Undang No. 45 Tahun 2009) dapat dilihat dari ketentuan Pasal 60 ayat (2) yang menyatakan bahwa pemberdayaan nelayan kecil dan pembudidaya ikan kecil juga dapat dilakukan oleh masyarakat.

Adanya peraturan-peraturan tersebut ternyata mengakibatkan adanya tumpang tindih antar peraturan. Menurut Dyah Ayu, salah satu contoh inefisiensi peraturan yang ada di

---

[24] Dyah Ayu Widowati dkk, *Penerapan Prinsip Good Goverment Dalam Peraturan Pengelolaan Perikanan Yang Berkelanjutan di Indonesia*, Jurnal Hukum Volume 35 Nomor 1, (Yogyakarta:Universitas Gajah Mada, 2019), hlm. 20

[25] Undang-Undang Nomor 31 Tahun 2004 Tentang Perikanan (Lembaran Negara Republik Indonesia Tahun 2004 Nomor 118, Tambahan Lembaran Negara Republik Indonesia Nomor 4433).

bidang perikanan adalah terjadinya tumpang tindih aturan antara Undang-Undang Nomor 1 Tahun 2014 tentang Perubahan Atas Undang-Undang Nomor 27 Tahun 2007 tentang Pengelolaan Wilayah Pesisir dan Pulau-Pulau Kecil (Undang-Undang No. 1 Tahun 2014) dan Undang-Undang Nomor 4 Tahun 2009 tentang Pertambangan Mineral dan Batubara (Undang-Undang No. 4 Tahun 2009), yang mengakibatkan terjadinya kriminalisasi terhadap nelayan.[26]

Maka dari itu adanya pemanfaatan teknologi di industri perikanan seharusnya dapat mempermudah pemerintah dalam pengolahan data, penentuan regulasi, dan pembagian kewenangan yang proporsional. Agar tercipta pemberdayaan nelayan dan pembangunan perikanan yang berkelanjutan. Untuk bisa merealisasikan tujuan tersebut perlu adanya pengawasan yang ketat dan perlindungan pada perusahaan teknologi pengelola agar tidak dikriminalisasi dengan meretas sistem informasi yang dimiliki.[27]

Dapat disimpulkan kekurangan dari regulasi yang ada pada beberapa industri tersebut, tumpang tindihnya peraturan yang ada, hingga kurangnya kewenangan lembaga khusus untuk melindungi perusahaan teknologi dari serangan *hacking* membuat perusahaan teknologi sulit berkembang. Perlindungan dan pengawasan pada

[26] Dyah Ayu Widowati dkk, *Penerapan Prinsip Good Goverment* ...., hlm. 29
[27] *Ibid*.

setiap sektor industri juga harus diperketat agar tidak terjadi monopoli dan persaingan tidak sehat antar bisnis.

Akan tetapi dalam penelitian ini lebih berfokus pada perusahan-perusahaan yang menjadi korban serangan *hacking*. Dimana hingga penelitian ini dibuat ada beberapa sektor industri yang menjadi korban yaitu industri perbankan, *ecommerce*, akomodasi, hingga sektor informasi digital (jurnalistik).

2. Analisis *Hacking* di Indonesia

Keempat kategori *hacking* yang dirumuskan melalui konvensi internasional siber pada bab sebelumnya, beberapa tindak kejahatan *hacking* pernah terjadi pada perusahaan teknologi yang didirikan dan dikembangkan di Indonesia. Tabel 1 berikut merupakan contoh kasus-kasus tindak pidana *hacking* perusahaan teknologi yang pernah terjadi di Indonesia :

No.	**KORBAN *HACKING***	**BENTUK *HACKING***	**PELANGGARAN/ PIDANA**
1.	Lazada (2015)	Mengubah halaman web melalui *backdoor malware* berteknologi PHP (*Defacing*).	Pasal 48 ayat 1 jo pasal 32 ayat 1 Undang-Undang No. 19 tahun 2016 tentang Informasi dan Transaksi Elektronik (*Data Interface*)
2.	Tiket.com dan Citilink (Oktober 2016)	Pencurian kode booking tiket penerbangan lalu menjualnya melalui Facebook	Pasal 30 Undang-Undang No. 11 tahun 2008 sebagaimana diubah Undang-Undang No. 19 tahun 2016

3.	Bukalapak (Maret 2019), Uniqlo (April-Mei 2019) Tokopedia (Mei 2020) BPJS Kesehatan (2021) BRI Life (Juli 2021) Bank Jatim (Oktober 2021) Peduli Lindungi (2022) BSI Syariah (Mei 2023)	Pencurian Data Pengguna hingga pegawai	Pasal 67 ayat 1 dan 3 Undang-Undang Perlindungan Data Pribadi
4.	DigiPos milik Best Software (2020)	Dengan sengaja dan tanpa hak turut serta mengakses sistem elektronik milik orang lain dengan cara apapun (Akses Ilegal)	Pasal 30 ayat 1 dan Pasal 46 ayat 1 Undang-Undang No. 11 tahun 2008 sebagaimana diubah Undang-Undang No. 19 tahun 2016 tentang Informasi dan Transaksi Elektronik. [28]
5.	Narasi (Oktober 2022)	Serangan Penolakan Layanan Secara Terdistribusi (DDoS)	Pasal 30, Pasal 32 Undang-Undang No. 19 tahun 2016 atas perubahan Undang-Undang No. 11 tahun 2008 tentang Informasi dan Transaksi Elektronik (Pasal 18 Ayat 1 Undang-Undang Pers karena telah menghalang-halangi kegiatan jurnalistik)

[28] Putusan Pengadilan Negeri Pelaihari Nomor 10/Pid.Sus/2021/PN Pli

Kasus peretasan raksasa *e-commerce* bentukan Alibaba Group ini menjadi titik awal adanya peretasan yang terjadi pada *e-commerce* di Indonesia. Walaupun peretasan ini tidak menimbulkan kerugian secara materiil, tetapi peretasan yang terjadi pada Januari 2015 ini telah mengganggu tampilan platform. Dikutip dari *Katadata.co.id*, *attacker* telah memanipulasi tampilan yang berkaitan dengan promosi penjualan beberapa produk di Lazada. Tampilan promosi tersebut diubah menjadi gambar monster kartun yang sedang tersenyum, dengan keterangan "Tidak ada unsur menjatukan, politik, dll cuman ngetest doang kok, no backdoor just nitip file peace.. Lazada Got pwnz???lolz." dan meninggalkan identitas "SultanHaikal, d3b~X, Index Php, Coup De Grace, Brian Kamikaze, dan Mdn_Newbie".[29]

Peretasan kedua pada platform Lazada berhasil mencuri 1,1 Juta akun pengguna pada November 2020 lalu. Belum ada penjelasan lebih lanjut mengenai peretasan kedua ini, tetapi data-data yang telah diretas tersebut telah ditemukan pada salah satu *dark web Reid Forum*.[30] Walaupun *dark web Reid Forum* telah berhasil dibekukan melalui kerjasama internasional pihak

[29] Dikutip dari Selain Tokopedia, Tiga E-Commerce Ini Pernah Diretas - E-commerce Katadata.co.id pada 8 Maret 2023 pukul 19.30 WIB

[30] Dikutip dari Instagram Ngomongin Uang pada 10 Maret 2023 pukul 07.25 WIB https://www.instagram.com/p/CiXAx21Jotd/?igshid=YmMyMTA2M2Y=

Indonesia, Amerika Serikat, dan beberapa negara lain. Akan tetapi kemunculan situs *dark web* lain tidak bisa dibendung.

Sedangkan kasus *hacking* perusahaan teknologi asal Indonesia yang menggemparkan yaitu terjadinya pencurian kode booking pesawat Citilink melalui situs Tiket.com pada 2016 lalu. Dikutip dari CNN Indonesia, pencurian kode booking ini dilakukan dengan cara meretas sistem jual beli Tiket.com oleh 2 orang siswa sma (MKU dan AL 19 tahun) dan 1 orang mantan mahasiswa (NTU 27 tahun). Pencurian kode booking ini mengakibatkan Tiket.com mengalami kerugian hingga Rp 1,9 Miliar. Kasus ini telah ditangani oleh Siber POLRI sejak 30 Maret 2017, tetapi hingga penelitian ini dibuat belum ada putusan atau kejelasan lebih lanjut.[31]

Kasus pencurian data pengguna dari Bukalapak, Uniqlo, dan Tokopedia ini menjadi titik disahkannya Undang-Undang Perlindungan Data Pribadi pada Oktober 2022 lalu. Dikutip dari *Katadata.co.id*, kebocoran data pengguna dari ecommerce Bukalapak mencapai 31 Juta akun. Data pengguna yang berhasil diretas *attacker* tersebut dijual melalui *dark web* bernama *Dream Markets* dengan harga US$5000 Sedangkan pada kasus kebocoran data 91 Juta pengguna dan *merchant* Tokopedia,

[31] Dikutip dari Pembobol Situs Tiket.com Lulusan SMA, Pernah Retas 400 Situs (cnnindonesia.com) pada 8 Maret 2023 pukul 19.30 WIB

terdiri dari nama, email, kata sandi, dan nomor handphone. Data-data ini juga dijual di *dark web* senilai US$5000.[32]

Peretasan perusahaan teknologi BUMN pertama yang masuk dan dapat diadili di pengadilan yaitu peretasan pada DigiPos milik Best Software pada 2020 lalu. DigiPos merupakan salah satu anak perusahaan dari Telkom Indonesia. Berdasarkan putusan yang dipublikasi, terdakwa *attacker* dan temannya berhasil meretas saldo pulsa dari aplikasi DigiPos senilai Rp 200 Juta. Dari hasil persidangan terdakwa *attacker* dihukum dengan pidana kurungan 2 tahun 6 bulan dan denda Rp 300 Juta.[33]

Kasus peretasan terbaru perusahaan teknologi di Indonesia pada 2022 lalu juga dialami oleh Narasi. Perusahaan yang bergerak pada sektor informasi dan berita ini diserang oleh *attacker* yang hingga penelitian ini masih belum ditemukan. Menurut Sekjen Aji dari Narasi, penyerangan melalui pesan spam hingga Serangan Penolakan Layanan Secara Terdistribusi (DDoS) pada platform Narasi ini juga terpengaruh pada lemahnya regulasi dan Infrastruktur kelembagaan siber di Indonesia.[34]

---

[32] Dikutip dari Selain Tokopedia, Tiga E-Commerce Ini Pernah Diretas - E-commerce Katadata.co.id pada 8 Maret 2023 pukul 19.30 WIB

[33] Putusan Pengadilan Negeri Pelaihari Nomor 10/Pid.Sus/2021/PN Pli

[34]Dikutip dari Narasi Newsroom pada 10 Maret 2023 pukul 07.17 WIB https://www.instagram.com/reel/Ci9IPdtB_EE/?igshid=YmMyMTA2M2Y=

Kelima kasus tersebut merupakan contoh bentuk kasus *hacking* perusahaan teknologi yang beroperasi di Indonesia dengan pendiri orang Indonesia, kecuali kasus *hacking* pertama pada perusahaan teknologi Lazada yang beroperasi di Indonesia. Dari kelima bentuk *hacking* yang terjadi dari tahun 2015 hingga 2022 tersebut, beberapa bentuk *hacking* masih terjadi lagi pada perusahaan teknologi lain. Hal tersebut menjadi salah satu bukti lemahnya perlindungan, pengawasan, hingga penanganan insiden *hacking* pada perusahaan teknologi di Indonesia.

Bukan hanya itu, pengkhususan lembaga pengawasan dan pengembang kebijakan siber dalam perusahaan teknologi seperti yang menjadi indikator keamanan siber nasional dianggap penting. Hal tersebut dikarenakan adanya perbedaan sektor industri maupun keunikan dimasing-masing sektor industri dalam menjamin perlindungan keamanan dan kerahasiaan perusahaan.

3. Analisis Perlindungan Hukum Perusahaan Teknologi dan *Hacking* di Indonesia

Pengayoman sebagai bentuk perlindungan hukum yang dicetuskan oleh Satjipto Rahardjo dapat diimplementasikan dalam perumusan kebijakan.[35] Kebijakan yang akan dirumuskan tersebut juga harus disesuaikan dengan kebutuhan dan kerahasiaan di berbagai

[35] Satjipto Rahardjo, *Ilmu Hukum*, (Bandung: PT. Citra Aditya Bakti, 2000), hlm. 53-54

sektor industri perusahaan teknologi. Dasar hukum perlindungan hukum juga telah dirumuskan pada Pasal 40 ayat 2 Undang-Undang Nomor 19 Tahun 2016 atas perubahan Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik yang berbunyi,

> *(2) Pemerintah melindungi kepentingan umum dari segala jenis gangguan sebagai akibat penyalahgunaan Informasi Elektronik dan Transaksi Elektronik yang mengganggu ketertiban umum, sesuai dengan ketentuan peraturan perundang-undangan*.

Lebih lanjut menurut BPHN yang dirujuk pada Muhamad Amirulloh, kepentingan-kepentingan hukum di bidang Teknologi Informasi dan Komunikasi (TIK) yang perlu mendapat perlindungan meliputi kepentingan individu atau korporasi, kepentingan masyarakat dan kepentingan pemerintah atau negara baik di bidang ekonomi, sosial budaya maupun pertahanan-keamanan. Perlindungan terhadap kepentingan-kepentingan hukum tersebut dilakukan berdasarkan asas keseimbangan, dalam arti masing-masing kepentingan hukum mendapat perlindungan hukum yang sama.[36]

Hal tersebut juga ada dalam ketentuan Pasal 1 ayat (2) Undang-Undang Perlindungan Saksi dan Korban yang menyebutkan,

> "*Korban adalah seseorang yang mengalami penderitaan fisik, mental dan/atau kerugian ekonomi yang diakibatkan oleh suatu tindak pidana*"

---

[36] Muhamad Amirulloh dkk, *Kajian EU Convention On Cybercrime Dikaitkan Dengan Upaya Regulasi Tindak Pidana Teknologi Informasi*, (Jakarta: Badan Pembinaan Hukum Nasional Departemen Hukum dan Hak Asasi Manusia Republik Indonesia, 2009), hlm. 18

Dalam penerapannya pemerintah bukan hanya merumuskan regulasi pada Undang-Undang, akan tetapi bertanggung jawab akan perlindungan keberlanjutan yang kewenangannya dapat diberikan pada lembaga khusus. Baik pembentukan lembaga baru yang khusus mengembangkan kebijakan siber, menerima dan menangani layanan siber pada perusahaan teknologi, sekaligus lembaga yang berwenang dalam pengawasan hak yang diberikan pada perusahaan teknologi yang dikembangkan di Indonesia.

Sedangkan sesuai teori Philipus M. Hadjon perlindungan hukum dari pemerintah sendiri dikategorikan menjadi dua bentuk yaitu :

a. Perlindungan Preventif

Perlindungan hukum preventif diartikan sebagai kesempatan kepada masyarakat yang dalam hal ini perusahaan teknologi untuk mengajukan keberatan atau pendapatnya sebelum ada putusan atau regulasi yang definitif. Hal ini bertujuan untuk mencegah terjadinya sengketa.[37] Perlindungan ini mengharuskan pemerintah untuk memitigasi risiko adanya kejahatan dan memperbaiki sistem hukum untuk melindungi khususnya perusahaan teknologi.

Perlindungan preventif ini jika dikaitkan dengan perlindungan hukum perusahaan teknologi terhadap serangan *hacking* maka pemerintah sebagai pelaksana mandat utama

[37] *Ibid.,* Hlm. 2.

perumusan kebijakan hukum, berkontribusi besar terhadap pemberlakuan kebijakan hukum. Pemerintah juga dapat membuat lembaga khusus untuk mempermudah pengkhususan pengambilan kebijakan di setiap sektor industri yang memiliki karakteristik bermacam-macam. Dengan begitu perkembangan inovasi teknologi di Indonesia dapat berjalan beriringan dengan regulasi yang adaptif.

Selain itu perusahaan teknologi yang memiliki akses informasi mengenai pengguna juga diharuskan memitigasi jaringan perusahannya secara berkala. Menurut Kotim Subandi, tindakan *hacking* sendiri dapat dimitigasi dengan mendeteksi *vulnerability*. *Vulnerability* adalah suatu kelemahan yang menjadi ancaman nilai *integrity*, *confidentiality*, dan *availability* dari suatu aset digital. Salah satu cara mendeteksi *vulnerability* pada sistem yaitu dengan *penetration test* (pentest). Pentest adalah salah satu metode yang dapat digunakan untuk melakukan analisa dan evaluasi terhadap suatu jaringan komputer (*server*) secara keseluruhan.[38] Karena jaringan komputer tersebut selalu diakses seluruh karyawan dan merupakan tempat pertukaran data serta penyimpanan seluruh informasi terkait dengan kepentingan bisnis.

[38] Kotim Subandi dan Victor Ilyas Sugara, *Analisa Serangan Vulnerabilities Terhadap Server Selama Periode WFH di Masa Pandemi Covid-19 Sebagai Prosedur Mitigasi*, Seminar Nasional Sains dan Teknologi 2021, (Jakarta: Universitas Muhammadiyah Jakarta, 2021), hlm. 3

b. Perlindungan Represif

Perlindungan represif bertujuan untuk menyelesaikan sengketa permasalahan.[39] Sengketa permasalahan dalam konteks *hacking* pada perusahaan teknologi sendiri hingga saat ini belum banyak yang masuk ranah pengadilan. Lemahnya infrastruktur pendeteksi *attacker* menjadi salah satu permasalahan terbesar polisi siber di Indonesia. Hal tersebut juga berakibat pada kenaikan angka *anonymous* penyerang sistem informasi perusahaan teknologi. Apabila permasalahan tersebut tidak ditangani secara serius maka perkembangan inovasi teknologi di Indonesia akan terhambat.

Menurut Alcianno G. Gani, hambatan tersebut dapat diatasi dengan berbagai cara. *Pertama*, memodernisasi infrastruktur penyidikan dunia siber dengan begitu pelaksanaan investigasi dapat mendeteksi kejahatan teknologi rendah maupun teknologi tinggi. Infrastruktur yang canggih juga termasuk bentuk perlindungan kepada perusahaan teknologi. Karena infrastruktur tersebut dapat memberikan peringatan awal akan adanya ancaman dari para *attacker*.[40]

---

[39] *Ibid.,* Hlm. 3.

[40] Alcianno G. Gani, *Cybercrime (Kejahatan Berbasis Komputer)*, Jurnal Tidak dipublikasikan 2018, hlm. 26

Kedua, membuat lembaga khusus yang bertugas merumuskan kebijakan-kebijakan perlindungan perusahaan teknologi dan mempekerjakan penyidik siber yang handal. Penyidik siber tersebut juga dapat direkrut dari *stakeholder* professional, agar memudahkan penyelidikan hingga penyidikan kasus *hacking*. Dengan profesionalitas para ahli siber tersebut, akan lebih banyak *attacker* yang ditangkap dan diberikan hukuman yang berefek jera.[41]

Ketiga, memperketat regulasi dengan regulasi yang kuat tersebut, seorang *attacker* tidak akan mudah mengeksploitasi celah perundang-undangan. Eksploitasi pada celah perundang-undangan tersebut juga terjadi akibat lemahnya regulasi dan hukuman yang tidak berefek jera. Efek jera ini bukan hanya tentang pidana penjara atau denda. tetapi lebih dari itu. Salah satu negara bagian di Amerika berhasil menggunakan hukuman percobaan atau pembebasan bersyarat.

Hukuman ini merupakan pembatasan individu terhadap perangkat tertentu yang dapat dilakukan dengan cara pemantauan komputer atau penelusuran komputer oleh petugas. Ataupun para *attacker* tersebut dapat dipekerjakan sebagai pakar keamanan informasi oleh perusahaan swasta

[41] Alcianno G. Gani, *Cybercrime (Kejahatan Berbasis Komputer)* …, hlm. 26

> karena keahlian dan pengetahuan mereka tentang kejahatan komputer. Hukuman-hukuman tersebut ternyata lebih efektif daripada pidana kurungan.[42]

Perlindungan-perlindungan tersebut sangat diperlukan perusahaan teknologi agar dapat meminimalisir adanya *hacking* pada sistem jaringan yang berisi informasi penting bisnis. Hal tersebut hanya dapat direalisasikan jika pemerintah dapat memaksimalkan potensi dan perumusan kebijakan secara tepat sasaran. Dengan dukungan kolaborasi yang kuat antara pemerintah pusat, Kementerian Komunikasi dan Informatika, lembaga khusus siber, dan *stakeholder* professional siber.

Berdasarkan perlindungan melalui tindakan preventif dan represif yang dicetuskan oleh Philipus M. Hadjon tersebut, Indonesia masih membutuhkan pengkhususan kelembagaan dalam menangani layanan siber, khususnya *cyber hacking*. Karena hingga penelitian ini dibuat perusahaan-perusahaan teknologi yang menjadi korban *hacking* tersebut belum mendapat perlindungan dari pemerintah yang bersifat represif. Dimana perusahaan-perusahaan tersebut hanya dapat melakukan aduan pada petugas BSSN (Badan Siber dan Sandi Negara) yang selanjutnya tidak ada satupun dari perusahaan teknologi (swasta) yang mendapatkan penanganan represif.

---

[42] *Ibid.,* Hlm. 27.

Hal tersebut juga akan berdampak menurunnya kinerja bisnis dan pengembangan inovasi teknologi perusahaan teknologi di Indonesia. Bukan hanya itu, jika kasus *hacking* tidak ditangani dengan serius dan diberikan perlindungan maka juga akan berdampak pada pemecatan karyawan perusahaan teknologi yang berarti akan ada lebih banyak pengangguran dan pencari kerja di Indonesia. Karena menurut Sekjen Aji (Sekretaris Jenderal Narasi Tv) perlindungan dan penanganan kasus *hacking* pada perusahaan teknologi di Indonesia masih sangat lemah dan belum ditangani dengan serius.

B. Analisis Perlindungan Hukum Perusahaan Teknologi Terhadap Serangan *Hacking* di Indonesia Perspektif *Maqashid Syariah*

1. Analisis *Maqashid Syariah*

Akibat dari belum adanya perlindungan pada perusahaan teknologi yang terkena *hacking*, dapat mengganggu tercapainya *maqashid syariah*. Karena tujuan dari *maqashid syariah* sendiri yaitu untuk melindungi dan mencapai tujuan *syari'i* pada seluruh umat manusia. Jika dampak-dampak tersebut dianalisis berdasarkan pengkategorian *maqashid syariah* maka akan menjadi seperti berikut[43] :

a. Memelihara agama atau keberagamaan (حفظ الدين)

Menurut Imam Asy Syatibi arti dari agama secara umum yaitu kepercayaan kepada Tuhan. Sedangkan dalam

[43] *Ibid.*, Hlm. 58-59.

perlindungan hukum perusahaan teknologi yang terkena *hacking*, tujuannya untuk mengatur hubungan manusia dengan Allah SWT dan hubungan mereka satu sama lain. Dengan begitu adanya perlindungan hukum perusahaan teknologi yang terkena *hacking* menjadi salah satu indikator tegaknya agama Islam. Pemerintah sebagai *amirul mu'minin* (pemimpin) bertanggung jawab atas pemberian perlindungan subjek hukum, khususnya perusahaan teknologi.[44]

b. Memelihara jiwa atau diri atau kehidupan (حفظ النفس)

Menurut Amir Syarifuddin, memelihara kehidupan atau jiwa merupakan terpenuhinya unsur-unsur jaminan keselamatan dalam hidup, kehormatan, dan kebebasan memilih akan menjamin kelangsungan hidup. Hal tersebut juga akan berdampak pada tercapainya tujuan kehidupan manusia di dunia, yaitu *rahmatan lil ālamin* atau bermanfaat bagi alam sekitar.[45] Pengimplementasikan pada perlindungan hukum perusahaan teknologi yang terkena *hacking*, maka dampak dari tidak adanya perlindungan tersebut akan mengganggu umat manusia dalam memelihara jiwa. Karena tidak adanya perlindungan perusahaan teknologi juga akan berimbas pada karyawan yang bekerja pada perusahaan tersebut. Jika perusahaan teknologi tersebut hingga bangkrut

[44] *Ibid.,* Hlm. 58.
[45] *Ibid*., Hlm. 235

karena serangan *hacking*. Tidak menutup kemungkinan karyawan hingga pemilik perusahaan yang terkait akan terganggu dalam memenuhi kebutuhan sehari-harinya.

c. Memelihara akal (حفظ العقل)

Akal manusia merupakan unsur pembeda dari makhluk Allah lain. Pemeliharaan akal dalam Islam yang terkait dengan perlindungan hukum dari serangan *hacking*, dapat berbentuk regulasi dan perlindungan berkelanjutan dari sebuah lembaga yang berwenang. Hal tersebut diperlukan dalam upaya meminimalisir adanya dampak yang ditimbulkan dari kasus-kasus *hacking* yang menimpa perusahaan teknologi yang juga akan berimbas pada seluruh karyawan maupun pengguna.

Al-Qur'an Surat Al-A'raf Ayat 169 juga menyebutkan larangan menggunakan akal untuk melanggar peraturan yang ada, sebagaimana bunyi ayat berikut :

فَخَلَفَ مِنْۢ بَعْدِهِمْ خَلْفٌ وَّرِثُوا الْكِتٰبَ يَأْخُذُوْنَ عَرَضَ هٰذَا الْاَدْنٰى
وَيَقُوْلُوْنَ سَيُغْفَرُ لَنَاۚ وَاِنْ يَّأْتِهِمْ عَرَضٌ مِّثْلُهٗ يَأْخُذُوْهُۗ اَلَمْ يُؤْخَذْ عَلَيْهِمْ
مِّيْثَاقُ الْكِتٰبِ اَنْ لَّا يَقُوْلُوْا عَلَى اللّٰهِ اِلَّا الْحَقَّ وَدَرَسُوْا مَا فِيْهِۗ وَالدَّارُ
الْاٰخِرَةُ خَيْرٌ لِّلَّذِيْنَ يَتَّقُوْنَۗ اَفَلَا تَعْقِلُوْنَ

Artinya :

Kemudian, setelah mereka, datanglah generasi (yang lebih buruk) yang mewarisi kitab suci (Taurat). Mereka mengambil harta benda (duniawi) yang rendah ini (sebagai ganti dari kebenaran). Lalu, mereka berkata, "Kami akan diampuni."

Jika nanti harta benda (duniawi) datang kepada mereka sebanyak itu, niscaya mereka akan mengambilnya (juga). Bukankah mereka sudah terikat perjanjian dalam kitab suci (Taurat) bahwa mereka tidak akan mengatakan kepada Allah, kecuali yang benar, dan mereka pun telah mempelajari apa yang tersebut di dalamnya? Negeri akhirat itu lebih baik bagi mereka yang bertakwa. Maka, tidakkah kamu mengerti?.[46]

Pada konteks perlindungan hukum perusahaan teknologi terhadap serangan *hacking*, ayat tersebut sebagai dasar adanya larangan penggunaan akal untuk kepentingan pribadi yang merugikan orang lain. Karena pada dasarnya kesenangan di dunia hanyalah sementara dan akhirat merupakan tujuan yang kekal di dalamnya.

d. Memelihara keturunan (حفظ النسل)

Menurut Imam Asy-Syatibi dalam rangka memelihara keturunan, Islam mensyariatkan perkawinan yang sah untuk mendapatkan keturunan serta kelangsungan umat manusia. Memelihara keturunan juga termasuk pada implementasi dari perlindungan hukum perusahaan teknologi yang terkena *hacking*, karena dampak dari pemecatan karyawan dapat mengganggu keberlangsungan anak-anak dari karyawan perusahaan. Tidak menutup kemungkinan data perusahaan teknologi yang dicuri juga dapat dipergunakan untuk eksploitasi anak-anak.

[46] Departemen Agama RI, *Al-Qur'an dan Terjemahannya*, (Jakarta: Yayasan Penyelenggara Penerjemah, 1998), hlm. 172

e. Memelihara harta (حفظ المال)

Islam mensyariatkan umatnya untuk memperoleh dan menjaga kekayaan dengan wajib berusaha melalui muamalah, pertukaran, perdagangan, dan kerja sama dalam usaha.[47] Salah satu keutamaan menjaga harta dalam konteks perlindungan hukum perusahaan teknologi yang terkena *hacking*, yaitu ada pada kekayaan intelektual seperti program komputer hingga aset penting lain yang bernilai ekonomis. Hal tersebut diperlukan untuk dapat menjamin perusahaan bisa berjalan secara optimal dari segi finansial.

Kelima pengkategorian *maqashid syariah* tersebut dirumuskan untuk memperjelas tujuan-tujuan *syar'i* yang harus dipelihara oleh manusia. Dengan terpeliharanya kelimanya manusia akan bisa hidup damai dengan makhluk lain. Hal tersebut hanya bisa terwujud dengan adanya pemaksimalan peran-peran pemerintah dalam merumuskan kebijakan hingga perlindungan sekaligus pengawasan pada lembaga khusus.[48]

2. Perlindungan Hukum Perusahaan Teknologi Terhadap Serangan *Hacking* Perspektif *Maqashid Syariah*

Berdasarkan Imam Asy Syatibi tersebut, pengimplementasian *maqashid syariah* sendiri apabila dilihat dari perlindungan perusahaan

[47] *Ibid.,* Hlm. 59.
[48] *Ibid.*

teknologi yang terkena *hacking* maka yang menjadi dasar perlindungannya sesuai urutan kepentingan seperti berikut[49] :

a. Memelihara Harta

Memelihara harta menjadi poin utama yang terganggu jika perlindungan perusahaan teknologi yang terkena *hacking* tidak ada. Karena sebagai perusahaan teknologi yang memiliki nilai ekonomis dan berhasil dalam menjalankan bisnisnya, perlu adanya perlindungan atas kerahasiaan dan kekayaan yang dimiliki perusahaan yang juga berkaitan dengan harta dalam Islam. Harta yang dimaksud pada hal ini yaitu program komputer, aset perusahaan, hingga meminimalisir adanya pengeluaran yang besar untuk penanganan *hacking*.

b. Memelihara Agama

Sedangkan dalam pemeliharaan agama, *attacker* yang menjadi salah satu musuh terbesar sistem jaringan perusahaan karena perbuatannya yang mencuri data penting perusahaan, memata-matai sistem, hingga mengganggu kerja sistem merupakan hal yang dilarang oleh agama. Hal tersebut hanya bisa diminimalisir melalui sistem hukum yang kuat dan berefek jera. Dengan didukung oleh infrastruktur canggih dan peran lembaga profesional siber, baik dari penyidik siber maupun dari *stakeholder* profesional yang dipekerjakan

[49] *Ibid.*

pemerintah. Hukum Islam dapat mengkategorikan peretas sebagai pencuri yang dapat dikenai hukuman *tāzir*.

Hukuman *tāzir* tersebut bukan dimaksudkan untuk memperberat hukuman pada *attacker*. Akan tetapi membuat hukuman yang diberikan efektif untuk mencegah adanya tindakan yang sama. Menurut Syahrul Anwar yang merujuk pada Jumhur Ulama, jika dikaitkan dengan teori *Zawajir* dan *Jawabir*. Perlindungan hukum dapat dikategorikan pada teori *Zawajir*, yang berarti pencegahan. Tujuan utama *zawajir* pada penentuan hukuman yaitu sebagai tindakan preventif bagi orang lain supaya tidak melakukan tindak pidana yang sama setelah melihat pelaksanaan hukuman *attacker* (hukuman berefek jera).[50]

Kewajiban pemeliharaan harta perusahaan teknologi dan pemeliharaan agama bukan hanya kewajiban dari perusahaan saja, akan tetapi terdapat peran penting pemerintah untuk merumuskan kebijakan. Agar perusahaan teknologi dapat berkontribusi dalam perekonomian nasional dan tetap pada *syariat* agama.

c. Memelihara Jiwa

[50] Syahrul Anwar, *Hakikat Manusia dan Eksistensi Hukum Pidana Islam dalam Sistem Hukum Pidana Nasional*, (Bandung: Widina Media Utama, 2022), hlm. 31

Pemeliharaan jiwa menjadi kategori ketiga dalam konteks perlindungan hukum perusahaan teknologi dari serangan *hacking*. Karena dalam urgensinya jiwa hanya dapat terganggu apabila kasus hacking tersebut berdampak besar pada perusahaan teknologi. Seperti adanya pemecatan karyawan ataupun kebangkrutan dari perusahaan yang terkena *hacking* tersebut.

d. Memelihara Akal

Kategori keempat dalam konteks perlindungan hukum perusahaan teknologi dari serangan *hacking* yaitu memelihara akal, karena kasus hacking ini bisa berdampak buruk apalagi terhadap pendiri maupun pemilik dari perusahaan teknologi. Selain itu kerugian non materiil dari data yang dicuri pada pengguna juga akan mempengaruhi kredibilitas perusahaan.[51]

e. Memelihara Keturunan

Kategori *maqashid syariah* yang terakhir dalam konteks perlindungan hukum perusahaan teknologi dari serangan *hacking* yaitu memelihara keturunan. Karena dampak yang ditimbulkan pada keturunan hanya dapat terjadi apabila ada pemecatan karyawan ataupun ada

[51] *Ibid.,* Hlm. 31

eksploitasi data pengguna yang berkenaan dengan anak-anak.[52]

Kelima kategori pemeliharaan *maqashid syariah* tersebut menjadi penting dan perlu upaya maksimal untuk dapat melindungi perusahaan teknologi terhadap serangan *hacking*. Karena adanya maqashid syariah sendiri diperuntukkan untuk seluruh umat dalam melindungi dan memelihara diri dan lingkungan di kehidupan dunia.

[52] *Ibid.*

BAB V

PENUTUP

A. Kesimpulan

Dapat disimpulkan perlindungan hukum perusahaan teknologi terhadap serangan *hacking* pada perspektif hukum positif di Indonesia yaitu melalui Badan Siber dan Sandi Negara (BSSN) maupun DITTIPIDSIBER POLRI belum ada. Karena hingga penelitian ini dibuat masih saja ada perusahaan teknologi yang mengalami *hacking*. Hal tersebut merupakan indikasi kurangnya kewenangan pada unit pengembang kebijakan siber hingga unit layanan publik yang menurut NCIS sangat diperlukan bagi sebuah negara melindungi dunia siber nasional. Waluapun regulasi tindak pidana *hacking* tersebut telah ada pada Pasal 30 Undang-Undang Nomor 11 Tahun 2008 sebagaimana diubah Undang-Undang Nomor 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik.

Sedangkan perlindungan hukum perusahaan teknologi terhadap serangan *hacking* dalam perspektif *maqashid syariah* dapat mengganggu tercapainya *maqashid syariah* pada kategori pemeliharaan harta, pemeliharaan agama, pemeliharaan jiwa, pemeliharaan akal, hingga pemeliharaan keturunan.

B. Saran

Berdasarkan penelitian yang peneliti lakukan, berikut beberapa saran yang dapat peneliti sarankan :

1. Bagi pemerintah pusat, perlindungan hukum pada perusahaan teknologi yang berkelanjutan hanya dapat diimplementasikan dengan dukungan regulasi hukum yang tepat dan infrastruktur teknologi maupun kelembagaan yang maksimal. Pembangunan lembaga khusus perlindungan hukum siber yang khusus menangani dan mengawasi perusahaan teknologi sejajar dengan Badan Siber dan Sandi Negara (BSSN) dirasa sangat penting. Ataupun penambahan pada lembaga edukasi siber, unit pengembangan kebijakan keamanan siber, dan unit pengembang perlindungan layanan

publik. Dengan begitu perusahaan teknologi dapat mengembangkan inovasinya secara maksimal dan juga berkontribusi besar pada perekonomian nasional.

2. Selanjutnya saran untuk masyarakat umum agar lebih berhati-hati dalam memposting maupun menyimpan data diri dan selalu gunakan aplikasi yang aman dan terpercaya agar terhindar dari penyalahgunaa data pribadi maupun tindak pidana *hacking*.
3. Saran untuk peneliti selanjutnya, penelitian ini masih terbatas dalam spesifikasi penelitian. Maka dari itu peneliti harap pada penelitian selanjutnya dapat meneliti lebih spesifik perkembangan regulasi maupun perlindungan setiap sektor industri perusahaan teknologi. Mulai dari *ecommerce*, *fintech*, *edutech*, dll

DAFTAR PUSTAKA

Amirulloh, M. Ida Padmanegara. Tyas Dian Anggraeni. 2009. *Kajian EU Convention On Cybercrime Dikaitkan Dengan Upaya Regulasi Tindak Pidana Teknologi Informasi*. Jakarta: Badan Pembinaan Hukum Nasional Departemen Hukum dan Hak Asasi Manusia Republik Indonesia

Anwar, Syahrul. 2022. *Hakikat Manusia dan Eksistensi Hukum Pidana Islam dalam Sistem Hukum Pidana Nasional*. Bandung: Widina Media Utama.

Arisandy, Yogi Oktafian. 2020. *Penegakan Hukum Terhadap Cyber Crime Hacker*. *Journal of Criminal Law and Criminology*. Volume I Nomor 2. Yogyakarta

A. Schmidt, Floriant. 2017. *Digital Labour Markets in the Platform Economy Mapping the Political Challenges of Crowd Work and Gig Work*. English Version. German: Friedrich-Ebert-Stiftung

Badan Siber dan Sandi Negara atau BSSN. 2022. *Peringatan Keamanan Aktivitas Peretasan Jaringan Dengan Memanfaatkan Kerentanan Aplikasi Multi Faktor Otentikasi dan Kerentanan Printer Spooler*. Jakarta Selatan: Badan Siber dan Sandi Negara atau BSSN

Budi, Eko. Dwi Wira. Ardian Infantono. 2021. *Strategi Penguatan Cyber Security Guna Mewujudkan Keamanan Nasional di Era Society 5.0* Vol. 3. Yogyakarta: Akademi Angkatan Udara.

C. Laudon, Kenneth dan Jane P. Laudon. 2014. *Management Information Systems Managing The Digital Firm*. English Version, *Global Editional*. Edinburgh: Pearson Education Limited.

Christiawan, Rio. 2022. Aspek Hukum Startup. Jakarta Timur: Sinar Grafika.

Direktorat Operasi Keamanan Siber. 2021. *Laporan Tahunan Monitoring Keamanan Siber 2021*. Jakarta Selatan.

Djafar, Wahyudi. 2020. *Hukum Perlindungan Data Pribadi di Indonesia*. Yogyakarta: Universitas Gajah Mada

Faizal, Liky. 2017. *Problematika Hukum Progresif di Indonesia*. Lampung: IAIN Raden Intan Lampung.

Gunawan, Imam. 2015. *Metode Penelitian Kualitatif Teori & Praktik*. Jakarta: Bumi Aksara.

G. Gani, Alcianno. 2018. *Cybercrime (Kejahatan Berbasis Komputer)*

Hadjon, Philipus M. 1987. *Perlindungan Hukum bagi Rakyat Indonesia*. Surabaya: Bina Ilmu.

Harper, Allen. Ryan Linn. Stephen Sims. Michael Baucom. Daniel Fernandez. Huáscar Tejeda. Moses Frost. 2022. *Gray Hat Hacking "The Ethical Hacker Handbook Sixth Edition"*. English Summary Version. New York: McGraw Hill.

International Telecommunication Union (ITU). 2020. *Global Cybersecurity Index* 2020. ITU Publications

Irawan, Herry. Puspita Kencana Sari.2018. *Buku Bisnis Informasi*. Ponorogo: Uwais Inspirasi Indonesia.

Khambali, Muhammad. 2017. *Perlindungan Hukum Masyarakat Terhadap Cybercrimes Berbasis Keadilan Bermartabat*. Yogyakarta: Universitas Proklamasi

Kharisma, Dona Budi. 2021. *Membangun Kerangka Pengaturan Startup di Indonesia*. *Jurnal Rechtsvinding* Volume 10 Nomor 3. Surakarta: Universitas Sebelas Maret.

Kurniawan, Dedik. 2019. *Kitab Hacker*. Jakarta: PT Elex Media Komputindo

Marzuki, Peter Mahmud. 2009. *Penelitian Hukum*. Jakarta: Kencana Prenada Media Group.

MIKTI Indonesia Digital Creative Industry Society. 2021. *Mapping dan Database Startup Indonesia 2021*, Edisi 2021

Munir, Nudirman. 2017. *Pengantar Hukum Siber Indonesia. Edisi Ketiga*. Depok: Raja Grafindo Persada.

Nasution, M. S. A. Rahmat Hidayat Nasution 2020. *Filsafat Hukum Islam dan Maqashid Syariah*. Jakarta: Kencana

Nazir, Muhammad. 2003. *Metode Penelitian*. Jakarta: Ghalia Indonesia.

Nugraha, M. A. Desi Arisandi. Novario Jaya Perdana. 2021. *Pengamanan Website E-Commerce Menggunakan Multi-Factor Authentication*, jurnal Ilmu Komputer dan Sistem Informasi Volume 9 Nomor 1. Jakarta:Universitas Tarumanegara.

Nugroho, Adi (ed.). 2021. *Laporan Tahunan Monitoring Keamanan Siber Tahun 2021*. Jakarta Selatan: Badan Siber dan Sandi Negara atau BSSN

Prabawati, Ari. 2010. *Tutorial Lima Hari Belajar Hacking dari Nol*. Semarang: Andi Offset.

Prabowo, Cristian. 2021. *Keamanan Jaringan.* Universitas Slamet Riyadi.

Rahardjo, Satjipto. 2000. *Ilmu Hukum. Bandung*: PT. Citra Aditya Bakti.

Rachmawati, Rika Reviza. Endro Gunawan. 2020. *Peranan Petani Milenial Mendukung Ekspor Hasil Pertanian di Indonesia*. Forum Penelitian Agro Ekonomi. Vol. 38 No. 1. Jawa Barat: Pusat Sosial Ekonomi dan Kebijakan Pertanian.

Sari, Diana Purnam. (ed.). 2022. *Cybercrime di Era Digital.* Sumatera Barat: PT Global Eksekutif Teknologi. Prabowo, Cristian. 2021.

Setiawan, Beni. 2019. *Penegakan Hukum Pidana Terhadap Akses Sistem Komputer Secara Ilegal (Hacking) dan Menimbulkan Kerusakan (Cracking) dalam Kejahatan Dunia Maya (Cybercrime) Menurut Perspektif Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik*. Jambi: Universitas Batanghari

Simanungkalit, D. E. 2018. *Kebijakan Pemerintah Indonesia Dalam Menangani Hacker di Indonesia Tahun 2008-2014*, Jurnal Ilmu Hubungan Internasional. Universitas Mulawarman.

Stephanie PD. Natasha OA. Enjelina S. Ahmad Redi. 2021.

Mengelaborasi Hukum Positif Tertulis Indonesia Mengatur Startup. Seminar Nasional Hasil Penelitian dan Pengabdian Kepada Masyarakat 2021. Jakarta: Universitas Tarumanegara.

Subandi, Kotim. Victor Ilyas Sugara. 2021. *Analisa Serangan Vulnerabilities Terhadap Server Selama Periode WFH di Masa Pandemi Covid-19 Sebagai Prosedur Mitigasi*. Seminar Nasional Sains dan Teknologi 2021. Jakarta: Universitas Muhammadiyah Jakarta

Syarifuddin, Amir. 2008. *Ushul Fiqh Jilid 2*. Jakarta: Prenada Media.

Shidiq, Ghofar 2019. *Teori Maqashid Al Syari'ah Dalam Hukum Islam*, Vol. XLIV NO. 118. Semarang: Universitas Sultan Agung.

Taufan Asfar, A.M. Irfan. 2016. *Analisis Naratif, Analisis Konten, dan Analisis Semiotik*. Jakarta: UIN Syarif Hidayatullah.

Wahyuono, J. A. 2021. *Ekonomi Politik Pengembang Game Lokal Spesialisasi dan Ekspansi Bisnis PT Git Solution dan Noobzilla di Yogyakarta*. Journal Communication Spectrum. Yogyakarta: Universitas Gajah Mada

Widowati, D. A. Rizky Septiana Widyaningtyas. Agi Tiara. and Christopher Bagas Wirawan. 2019. *Penerapan Prinsip Good Governance Dalam Peraturan Pengelolaan Perikanan Yang Berkelanjutan di Indonesia*, Volume 35, Nomor 1. Yogyakarta: Fakultas Hukum Universitas Gadjah Mada.

LAMPIRAN 1 Data Indikator Pemenuhan Siber Nasional

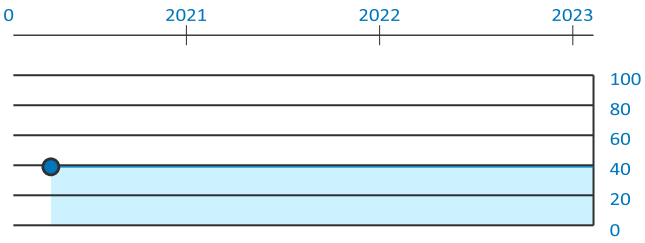
NCSI national cyber security index

85. Indonesia 38.96

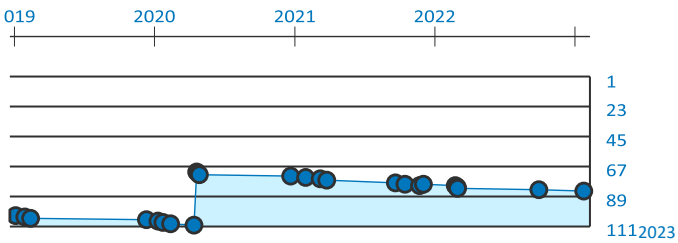
Population	258.7 million
Area (km^2)	1.9 million
GDP per capita ($)	13.1 thousand

85th	National Cyber Security Index	39 %
24th	Global Cybersecurity Index	95 %
111th	ICT Development Index	43 %
59th	Networked Readiness Index	52 %

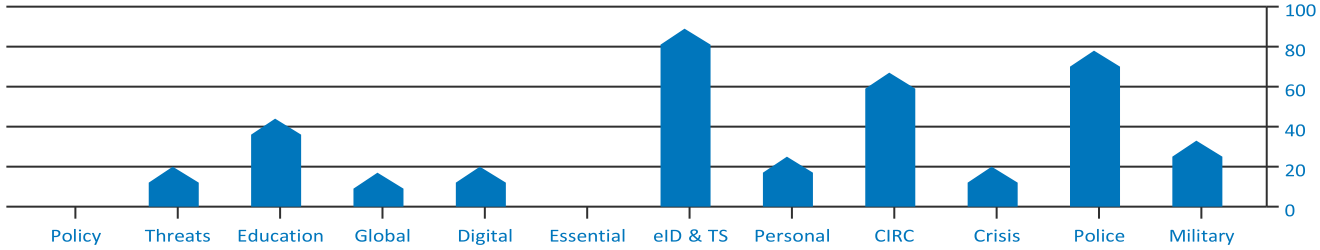
NCSI DEVELOPMENT TIMELINE



RANKING TIMELINE



NCSI FULFILMENT PERCENTAGE



GENERAL CYBER SECURITY INDICATORS

1. Cyber security policy development	0	7	(0%)
1.1 Cyber security policy unit	0	3	
1.2 Cyber security policy coordination format	0	2	
1.3 Cyber security strategy	0	1	
1.4 Cyber security strategy implementation plan	0	1	
2. Cyber threat analysis and information	1	5	(20%)
2.1 Cyber threats analysis unit	0	3	
2.2 Public cyber threat reports are published annually		1	
2.3 Cyber safety and security website	0	1	
3. Education and professional development	4	9	(44%)
3.1 Cyber safety competencies in primary or secondary education	0	1	
3.2 Bachelor's level cyber security programme		2	
3.3 Master's level cyber security programme	0	2	
3.4 PhD level cyber security programme	0	2	
3.5 Cyber security professional association		2	
4. Contribution to global cyber security	1	6	(17%)
4.1 Convention on Cybercrime	0	1	
4.2 Representation in international cooperation formats		1	
4.3 International cyber security organisation hosted by the country	0	3	
4.4 Cyber security capacity building for other countries	0	1	

BASELINE CYBER SECURITY INDICATORS

5. Protection of digital services	1 / 5	(20%)
5.1. Cyber security responsibility for digital service providers	1	
5.2. Cyber security standard for the public sector	0 / 1	
5.3. Competent supervisory authority	0 / 3	
6. Protection of essential services	0 / 6	(0%)
6.1. Operators of essential services are identified	0 / 1	
6.2. Cyber security requirements for operators of essential services	0 / 1	
6.3. Competent supervisory authority	0 / 3	
6.4. Regular monitoring of security measures	0 / 1	
7. E-identification and trust services	8 / 9	(89%)
7.1. Unique persistent identifier	1	
7.2. Requirements for cryptosystems	0 / 1	
7.3. Electronic identification	1	
7.4. Electronic signature	1	
7.5. Timestamping	1	
7.6. Electronic registered delivery service	1	
7.7. Competent supervisory authority	3	
8. Protection of personal data	1 / 4	(25%)
8.1. Personal data protection legislation	1	
8.2. Personal data protection authority	0 / 3	

INCIDENT AND CRISIS MANAGEMENT INDICATORS

9. Cyber incidents response	4 / 6	(67%)
9.1. Cyber incidents response unit	3	
9.2. Reporting responsibility	1	
9.3. Single point of contact for international coordination	0 / 2	
10. Cyber crisis management	1 / 5	(20%)
10.1. Cyber crisis management plan	0 / 1	
10.2. National-level cyber crisis management exercise	0 / 2	
10.3. Participation in international cyber crisis exercises	1	
10.4. Operational support of volunteers in cyber crises	0 / 1	
11. Fight against cybercrime	7 / 9	(78%)
11.1. Cybercrimes are criminalised	1	
11.2. Cybercrime unit	3	
11.3. Digital forensics unit	3	
11.4. 24/7 contact point for international cybercrime	0 / 2	
12. Military cyber operations	2 / 6	(33%)
12.1. Cyber operations unit	0 / 3	
12.2. Cyber operations exercise	2	
12.3. Participation in international cyber exercises	0 / 1	

NCSI is held and developed by e-Governance Academy Foundation
Company code: 90007000 Rotermanni 8 P: +372 663 1500
10111 Tallinn E: ncsi@ega.ee
Estonia W: www.ega.ee

DAFTAR RIWAYAT HIDUP

1. Nama : Atika Suciati
2. NIM : 19.21.31.097
3. Tempat, Tanggal lahir : Karanganyar, 14 Desember 2000
4. Jenis kelamin : Perempuan
5. Alamat : Perum. Ringin Asri, Rt. 04/12 Bejen, Karanganyar, Karanganyar
6. Nama ayah : Supriyono
7. Nama ibu : Supri Nuryanti
8. Riwayat Pendidikan
   a. SD Negeri 04 Bejen Lulus tahun 2013
   b. SMP Muhammadiyah Darul Arqom Karanganyar lulus tahun 2016
   c. SMA Negeri 2 Karanganyar lulus tahun 2019
   d. Universitas Islam Negeri (UIN) Surakarta Masuk Tahun 2019

Demikian daftar riwayat hidup ini saya buat dengan sebenarnya.

Surakarta, 13 Maret 2023

Penulis