BAB I

PENDAHULUAN

A. Latar Belakang

Pada era digital seperti sekarang teknologi informasi berkembang sangat cepat. Teknologi memberikan perubahan cara manusia dalam berbagai hal termasuk juga dalam berinteraksi dan berkomunikasi. Di masa lalu manusia dalam berinteraksi terbatas akan jarak dan waktu, namun pada masa sekarang jarak dan waktu bukan lagi menjadi permasalahan dalam interaksi antar individu atau bahkan kelompok.

Penggunaan teknologi menjadi keharusan guna meningkatkan efektifitas, efisiensi dan produktifitas dalam hal interaksi sesama manusia. Penerapan hal yang demikian menciptakan hal yang kita kenal dengan *cyberspace* atau dunia maya. Istilah *Cyberspace* pertama kali digunakan oleh John Parry Harlow pada tahun 1990 yang merujuk pada interaksi daring berupa aktivitas antar manusia yang saling berbicara menggunakan telepon. atau dapat diartikan sebagai ruang yang tercipta dikarenakan aktivitas interaksi manusia dengan menggunakan teknologi komunikasi sehingga memunculkan kesadaran bahwa tempat ini ada dan aktif digunakan manusia.[1]

Maraknya aktivitas pada *cyberspace* tentunya memberikan dampak-dampak positif dengan berbagai kemudahan yang ditawarkannya namun perlu disadari bahwasanya aktivitas pada *cyberspace* tidak sesederhana yang terlihat. Aktivitas pada *cyberspace* memiliki sisi-sisi lain yang orang awam kadang sulit memahaminya dan hanya terfokus pada kemudahan-kemudahan yang ia dapatkan dan enggan untuk melihat sisi negatif dari *cyberspace*. Kemudahan akses dan kecepatan transaksi yang luar biasa di *cyberspace* memberikan celah bagi pihak-pihak yang tak bertanggungjawab untuk melakukan kejahatan.

Cybercrime dilihat dari jenis aktivitasnya dapat berupa *hacking, cracking, phishing, identity theft*, dan lain-lain. Dampak kerugian atas praktik

[1] Sigid Suseno, 2012, *Yurisdiksi Tindak Pidanaa Siber*, Refika Aditama, Bandung, h.83.

cybercrime yang timbul antara lain kebocoran data pribadi, manipulasi data, pelanggaran privasi, kerusakan sistem, dan lain sebagainya. [2]

Dari macam-macam bentuk *cybercrime* yang telah dikenal oleh masyarakat, baru-baru ini menjadi sorotan adalah hacking atau peretasan. Pada awalnya memang peretasan atau hacking memiliki tujuan yang baik sebagai upaya untuk meningkatkan keamanan suatu perangkat digital serta sistem jaringan komputer. Namun, dia era sekarang hacking dimaknai sebagai upaya atau aktivitas tanpa izin untuk menyusup ke perangkat digital, komputer, dan sistem jaringan berupa website atau situs tertentu. petasan merupakan dampak dari perkembangan teknologi komputer dan internet.[3] Kemudian, pada praktik peretasan pelaku yang melakukan aktivitas ini disebut peretas (*hacker*).

Peretasan di Indonesia sendiri bukan merupakan bentuk kejahatan baru, pada tahun 2021 saja beberapa kasus peretasan sudah terjadi dan menjadi sorotan masyarakat. Pertama, kasus peretasan situs milik Badan Penyelenggara Jaminan Sosial atau BPJS, yaitu pjs-kesehatan.go.id yang berakibat 279 juta data penduduk Indonesia bocor dan dijual dalam forum online. Kedua, Pada 27 Juli 2021, perusahaan asuransi BRI Life yang jadi korban peretasan. Insiden ini membuat sekitar 2 juta data nasabah BRI Life diduga bocor dan dijual dengan harga 7.000 dollar AS (sekitar Rp 101,6 juta, kurs 27 Juli 2021) di dunia maya.Ketiga , peretasan pada aplikasi Electronic Health Alert (e-HAC) buatan Kementerian Kesehatan (Kemenkes) dampaknya data milik 1,3 juta masyarakat Indonesia yang tersimpan di aplikasi e-HAC disebut bocor.[4] Selain tiga peretasan itu, masih terdapat peretasan situs Sekretariat Kabinet Republik Indonesia, kepolisian indonesia,

---

[2] https://www.humonline.com/klinik/a/jerat-hukum-pelaku-icracking-i-menurut-ruu-pdp-dan-uu-ite-lt4f235fec78736, diakses pada 10 Desember 2022 pukul 19.09.

[3] Andi, 2002, *Kamus Lengkap Dunia Komputer*, Wagana Komputer, Yogyakarta , hlm. 201.

[4] https://tekno.kompas.com/read/2021/12/21/06540017/8-kasus-peretasan-yang-terjadi-di-indonesia-sepanjang-2021?page=all., pada 25 Oktober 2022 pukul 19.23.

Badan Intelijen Negara, dan banyak tindak peretasan lain yang dialami warga negara mulai dari media sosial hingga data pribadinya

Peretasan yang baru-baru ini terjadi dilakukan oleh pihak yang menyatakan identitasnya sebagai Bjorka, Bjorka melakukan peretasan pada situs Kementerian Komunikasi dan Informasi (Kominfo). Praktek peretasan tersebut berhasil meretas 1,3 miliar data pribadi warga negara Indonesia berupa data registrasi kartu SIM berupa NIK, nomor telepon, penyedia kartu SIM yang digunakan, hingga tanggal registrasi.

Data-data yang kerap kali menjadi sasaran para peretas adalah data pribadi milik warga negara Indonesia sehingga dirasa cukup penting keamanan data pribadi menjadi sorotan. Konsep tentang perlindungan data pribadi pada awalnya bermula dari konsep hak atas privasi. Konsep hak privasi pertama kali dikembangkan oleh Warren dan Brandheis yang menurut mereka bahwa setiap orang memiliki hak untuk dirinya pribadi menikmatia hidupnya. Hak menikmati hidup merupakan hak untuk tidak diganggu oleh orang lain, korporat atau negara.[5]

Kasus-kasus peretasan yang silih berganti dengan berbagai modus operandi pelaku menjadi hal yang tentunya akan sangat merugikan baik bagi perusahaan swasta, pemerintah, masyarakat dan pihak-pihak lain yang akan mengalami kendala dalam aktivitas digitalnya jika terjadi suatu peretasan. Pelaku kejahatan cyber juga terus meningkat dikarenakan kemudahan akan akses internet dan perasaan aman dikarenakan pada saat melakukan kejahatan melalui media elektornik. Peningkatan kejehatan dibidang cyber crime terutama peretasan menjadikan pemahan seperti apa penerapan hukum pidana di Indonesia dalam menindak para pelaku tersebut dan tentangan dalam penerapan saksi pidana bagi para pelaku kejahatan ini.

Praktik peretasan jika dipahami secara cermat tidak semata hanya merugikan website yang mengalami peretasan semata. Jika peretasan dilakukan pada website-website yang bersifat sangat rahasia dan dipergunakan untuk kebutuhan pihak kepolisian, militer atau kementerian pertahan dan keamanan tentunya dampak yang

[5] Samuel D. Warren dan Louis D. Brandheis, *The Rights to Privacy*, Harvard Law Review Vol. 4 No. 5, The Right to Privacy (Warren & Brandeis) (harvard.edu).

ditimbulkan akan sangat besar bahkan dapat mengancam kestabilan serta keamanan negara. Peretasan pada website milik Tentara Nasional Indonesia juga dapat berdampak bocornya strategi militer yang nantinya dapat digunakan pihak lain untuk mengancam kedaulatan Indonesia, kemudian menyebabkan gagalnya suatu operasi militer sehingga berdampak lebih luas.

Dengan dampak yang sangat bervariatif dari ringan hingga dampak berupa ancaman kedaulatan negara, peretasan website ini sudah seharusnya pengaturan secara lebih terperinci terkait pertanggungjawaban pidana bagi para pelaku kejahatan tersebut. Pengaturan yang kini belaku di Indonesia masih mengkategorikan peretasan website sebagi satu bentuk kejahatan tanpa mempertimbangkan website serta dampak yang ditimbulkan dari kejahatan cyber ini. Oleh karena itu, penting dilakukan kajian terhadap kejahatan cyber peretasan website yang terjadi di Indonesia untuk melihat sejauh apa penerapan hukum pidana dalam menindak para pelakunya.

Pada tahun 2021 praktik peretasan pada server DigiPos Telkomsel yang dilakukan oleh pelaku atas nama Tahyan Bin Dul Wahid. Pelaku meretas server tersebut sehingga dengan sedemikian rupa dapat mengakses pemilik akun di sana dan mendapatkan pulsa telkomsel untuk dipergunakan olehnya. Kasus peretasan ini juga terjadi pada tahun 2020 namun berbeda dengan kasus sebelumnya si pelaku peretasan atas nama Agus Dwi Cahyo Alias Adchacker Alias 13chmod37 Alias Xgxs melakukan peretasan pada website yang dikelola oleh pemerintah dan tercatat ada tujuh website yang berhasil diretas. Maksud peretasan yang dilakukan Agus adalah untuk mendapatkan sejumlah biaya perbaikan atas peretasan yang dia lakukan.

Dua perkara diatas menjadi menarik untuk diteliti dikarenakan perbedaan website yang diretas oleh pelaku peretasan antara website milik pemerintah yang berfungsi untuk pelayanan publik dan website milik swasta yang digunakan untuk kebutuhan pihak swasta dalam melakukan transaksi tertentu. Didasari faktor ini pertanggungjawaban pidana dari pelaku peretasan tentunya akan berbeda dengan demikian menjadi penting untuk membahas seperti apa pertanggungjawaban pidana para pelaku peretasa dari dua website dengan kegunaan yang berbeda dalam sebuah penelitian secara lebih lanjut.

Berdasarkan penjelasan atas fenomena yang terjadi dan praktek peretasan yang semakin marak terjadi di masa sekarang, menjadi penting untuk mengetahui seperti apa pertanggungjawaban pidana pelaku peretasan website. Berangkat dari berbagai aspek terkait praktek peretasan dan keresahan penulis, maka menjadi keharusan bagi penulis untuk membahas hal ini dalam skripsi dengan judul "**PERTANGGUNGJAWABAN PIDANA PELAKU PERETASAN WEBSITE BERDASARKAN HUKUM POSITIF INDONESIA.**"

B. Rumusan Masalah

1. Bagaimana penerapan pertanggungjawaban pidana terhadap pelaku peretasan website di Indonesia?
2. Bagaimana pertanggungjawaban pidana pelaku peretasan website berdasarkan hukum positif indonesia (studi perbandingan Putusan Nomor: 9/Pid.Sus/2021/PN Pli dan Nomor: 527/Pid.Sus/2020/PN Smn)?

C. Ruang Lingkup Penelitian

Sejalan dengan permasalahan yang terjadi, maka ruang lingkup penelitian hanya sebatas pada permasalahan pertanggungjawaban pidana pelaku peretasan. Pembahasan yang akan penulis sampaikan pada penelitian kali ini hanya sebatas penerapan hukum dan pertanggungjawaban pidana dari pelaku peretasan website.

D. Tujuan dan Manfaat

1.4.1. Tujuan Penelitian

Adapun tujuan dari penelitian ini adalah

a. Untuk mengetahui penerapan pidana terhadap pelaku peretasan website di Indonesia.
b. Untuk mengetahui pertanggungjawaban pelaku peretasan website yang dimiliki oleh swasta dan pemerintah.

1.4.2. Manfaat Penelitian

a. Manfaat Teoritis

Hasil penelitian ini penulis harapkan dapat menjadi referensi bagi penulis, teman-teman yang memiliki ketertarikan pada bidang hukum dan para penegak hukum tentang pertanggungjawaban pidana pelaku peretasan.

b. Manfaat Praktis

Penelitian terhadap permasalahan ini dapat memberi pengetahuan dan pemahaman mengenai penagturan hukum dan pertanggungjawaban pidana *cybercrime* khususnya peretasan.

E. Metode Penelitian

1.5.1. Jenis Penelitian

Kegiatan penelitian merupakan proses pengumpulan data dan analisis terhadap data-data yang telah didapat, penelitian harus dilakukan secara logis serta sistematis agar mendapat jawaban atas pertanyaan atau solusi dari suatu permasalahan.

Penelitian kali ini merupakan penelitian hukum normatif yang berfokus pada bahan-bahan seperti peraturan perundang-undangan serta bahan-bahan kepustaakn lainnya. Penelitian Hukum Normatif juga merupakan penelitian hukum yang dilakukan dengan cara meneliti bahan pustaka atau data sekunder.[6] Merujuk pendapat Peter Mahmud Mrzuki bahwa penelitian hukum normative merupakan proses yang digunakan agar dapat menemukan siatu aturan hukum, prinsip hukum, dan doktrin hukum sehingga dapat menjawab fenomena hukum yang terjadi di tengah-tengah masyarakat.[7]

1.5.2. Pendekatan Masalah

Di dalam penelitian hukum terdapat beberapa pendeketan. Dengan pendekatan tersebut, peneliti akan mendapatkan informasi dari berbagai

[6] Soerjono Soekanto dan Sri Mamudji, 1995, *Penelitian Hukum Normatif (suatu tinjauan singkat) Cet. IV*,Raja Grafindo Persada,Jakarta,hlm. 23.

[7] Peter Mahmud Marzuki,2010, *Penelitian Hukum,Kencana Prenada*, Jakarta, hlm. 35.

aspek mengenai isu yang sedang dicoba untuk mencari jawabannya. Pada penelitian ini pendekatan yang digunakan adalah pendekatan perundang-undang (*statute approach*), pendekatan kasus (*case approach)*, dan pendekatan konseptual (*conceptual approach).*

Pendekatan perundang-undangan (statute approach) dilakukan dengan menelaah semua peraturan perundang-undangan dan regulasi yang bersangkutan dengan isu hukum yang sedang ditangani.[8] Pendekan perundang-undangan digunakan untuk dapat menjawab isu hukum tentang pertanggungjawaban pidana pelaku peretasan website di Indonesia. Penelitian ini penulis menggunakan Undang-undang Nomor 19 Tahun 2016 tentang Perubahan atas Undang Undang No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik dalam pertanggungjawaban pidana pelaku peretasan website.

Pendekatan Kasus merupakan pendekatan dengan melakukan telaah pada kasus-kasus yang berkaitan dengan isu hukum yang dihadapi. Pada penelitian kali ini pendeketan kasus diimplementasikan dengan menelaah Putusan Pengadilan Negeri Nomor: 9/Pid.Sus/2021/PN. Pli dan Putusan Nomor : 527/Pid.Sus/2020/PN. Smn, kedua putusan ini merupakan dua kasus peretasan website yang berbeda. Putusan Pengadilan Negeri Nomor: 9/Pid.Sus/2021/PN. Pli merupakan putusan tentang putusan peretasan website milik swasta sedangkan Putusan Pengadilan Negeri Nomor : 527/Pid.Sus/2020/PN merupakan putusan terhadap kasus peretasan website milih pemerintah.

Pendektan Konseptual pada penelitian kali ini dengen merujuk pada asas, prinsip dan konsep hukum serta pendapat para ahli guna menemukan konsep yang sekiranya ideal dalam isu hukum yang diteliti. Pendektan konseptual akan memberikan saran atau masukan sehingga diharapakan meciptkan kondisi yang lebih baik.

---

[8] Zulfi Diane Zaini,2011, *Implementasi Pendekatan Yuridis Normatif dan Pendekatan normatif Sosiologis dalam penelitian ilmu hukum*,Jurnal Pranata Hukum,Volume 6,No 2, diakses dari Implementasi Pendekatan Yuridis Normatif dan Pendekatan Normatif Sosiologis dalam Penelitian Ilmu Hukum | Zaini | PRANATA HUKUM (ubl.ac.id)

1.5.3. Sumber Data

Penelitain hukum normatif menurut Soerjono Soekanto dan Sri Mamudji menerangkan bahwa penelitian hukum normatif adalah penelitian hukum dengan cara meneliti bahan pustaka atau data sekunder.[9] Sehingga sumber data yang digunakan dalam penelitian hukum normatif terdiri dari 3 sumber bahan hukum:

a. Bahan Hukum Primer

Hukum Primer yaitu bahan yang mempunyai kekuatan mengikat secara yuridis dan bersifat otoritatif.[10] Sumber Bahan Hukum Primer yaitu bahan hukum yang terdiri atas peraturan perundang-undangan secara hierarki dan putusan-putusan pengadilan

1) Undang-undang Dasar Republik Indonesia Tahun 1945
2) Undang-undang Nomor 8 Tahun 1981 tentang Hukum Acara Pidana
3) Undang Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik
4) Undang-undang Nomor 19 Tahun 2016 tentang Perubahan atas Undang Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.
5) Undang-undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi
6) Putusan Pengadilan Negeri Pelaihari Nomor : 9/Pid. Sus/2021/PN Pli
7) Putusan Pengadilan Negeri Sleman Nomor : 527/Pid. Sus/2020/PN Smn

b. Bahan Hukum Sekunder

Bahan hukum sekunder yaitu bahan yang tidak memiliki dasar untuk mengikat yuridis dan berperan untuk meperjelas bahan hukum primer.[11]Bahan hukum sekunder pada penelitian kali ini berupa buku, jurnal ilmiah, artikel, karya tulis hukum atau pandangan ahli hukum.

---

[9] Ishaq, 2017, *Metode Penelitian Hukum Dan Penulisan Skripsi, Tesis, Serta Disertas*i, Penerbit Alfabeta,Bandung, hlm 6

[10] Peter Mahmud Marzuki, 2008, *Penelitian Hukum*, Kencana, Jakarta, hlm 142

[11] Ibid.

c. Bahan Hukum Tersier

Bahan yang menunjukkan petunjuk hingga penjelasan dari bahan hukum primer dan bahan hukum sekunder seperti kamus (hukum), kamus bahasa Indonesia dan ensiklopedia.[12] Selain itu juga internet menjadi salah satu bahan hukum yang digunakan dalam penelitian ini.

1.5.4. Teknik Pengumpulan Data

Dalam mengumpulkan data yang menunjang penelitian ini, penulis menggunakan teknik pengumpulan melalui studi pustaka (library research). Studi kepustakaan merupakan metode pengumpulan data dengan mepelajari teori dari berbagai ahli hukum kemudian dipahami yang berkaitan dengan penelitian.

Studi pustaka diimplementasikan dengan mepelajari, membaca dan mengkasi segala sumber yang berhubungan dengan penelitian. Usaha-usaha pemahan dan pembelajaran dilakukan terhadap sumber-sumber hukum yang digunakan dalam penelitian ini.

1.5.5. Teknik Analisa Data

Teknik Analisis Data, merupakan langkah-langkah dalam penglohan bahan hukum yang telah terlebih dahuku dikumpulkan sehingga dengan upaya teknika analisis data ini dapat menjawab rumusan masalah. Upaya menjawab rumusan masalah pada penelitian ini adalah dengan cara analisis kualitatif.

Data-data yang telah diperoleh akan diproses melalui teknik analisi konten, teknik ini adalah teknik analisi terhadapp isi dokumen yang terdiri dari buku, jurnal, artikel dan lain sebagainya yang berkiatan dengan undang-undang peretasan website dan pertanggungjawaban pidana bagi pelaku peretasan website.

[12] Amiruddin dan Zainal Asikin, 2003, *Pengantar Metode Penelitian Hukum*, PT. Rajate Grafindo Persada, Jakarta, hlm.118.