BAB I

PENDAHULUAN

1.1 Latar Belakang Masalah

Dunia yang memasuki era globalisasi telah membuka batas-batas antara manusia dibelahan bumi utara dan belahan bumi selatan. Globalisasi adalah suatu fenomena khusus dalam peradaban manusia yang bergerak terus dalam masyarakat global dan merupakan bagian dari proses manusia global itu (Nurhaida, 2015). Manusia yang terpisah dengan jarak yang jauh dan putaran waktu yang berbeda dapat saling bertukar informasi bahkan mampu saling berinteraksi. Komunikasi yang tadinya terbatas hanya karena tingkat keberlangsungannya yang hanya dapat dilakukan dengan bertatap muka secara langsung kini dapat dilakukan hanya dengan berdiam diri di rumah dan menatap layar ponsel. Dampak dari globalisasi ini tidak hanya bisa dirasakan oleh orang dewasa, intensitas penggunaan ponsel atau telepon pintar juga didominasi oleh anak-anak di bawah umur. Penggunaan ini bisa menjadi alternatif media pendidikan maupun sebagai sarana hiburan seperti bermain game, menonton kartun, atau yang lainnya. Berdasarkan tingginya penggunaan ponsel mendorong peningkatan dalam menggunakan layanan internet, media online, platform digital, serta jejaring sosial yang lainnya. Ponsel yang saat ini digunakan harus selalu terhubung dengan provider penyedia jasa layanan paket internet atau biasa disebut sebagai kuota internet.

Akses digital yang sangat mudah menjadi tantangan bagi pemerintah sebagai eksekutor yang berperan penting dalam menjaga data pribadi warganya. Perlindungan data pribadi merupakan salah satu hak asasi yang tidak boleh diganggu ataupun digunakan secara ilegal oleh orang lain apalagi bila disebarkan ke muka publik. Perlindungan data pribadi dalam Pasal 28 G Undang-undang Dasar Tahun 1945 tergolong pada perlindungan diri pribadi. Peraturan ini bersifat mendunia dan diakui oleh banyak negara dengan versi masing-masing sesuai dengan keadaan negara tersebut.

Penggunaan gawai yang memerlukan data pribadi sebagai prasyarat menimbulkan masalah baru yakni permasalahan pencurian data, penyebaran informasi pribadi, dan pengalihan kepemilikan sebuah akun secara ilegal. Kegiatan-kegiatan tersebut umum dikenal sebagai *hacking* dan pelakunya disebut *hacker*. Data dan informasi yang didapatkan oleh *hacker* berasal dari sumber data yang tingkat pengamanannya rendah, sehingga akses untuk membuka dan mengetahui isi datanya menjadi mudah. Baru-baru ini yang terjadi di Indonesia dengan pencurian dan penyebaran data pribadi yang dilakukan oleh seorang *hacker* yang kita kenal dengan sebutan Bjorka. Kemunculan Bjorka menjadi tugas dan tantangan baru bagi pemerintah untuk segera membenahi sistem keamanan data yang pada hal ini ditujukan kepada Kementerian Komunikasi dan Informatika.

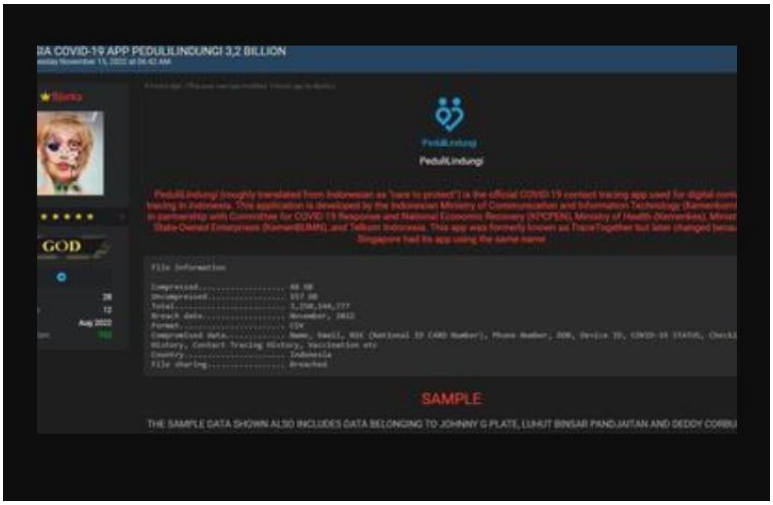
Bjorka hanya satu dari sekian banyak permasalahan sistem keamanan *cyber*, namun begitu menyita perhatian masyarakat sehingga memberikan dampak bagi aktivitas yang sehari-hari tidak dapat dilepaskan dari penggunaan gawai. Masalah ini juga menjadi ancaman bagi reputasi Kementerian Komunikasi dan Informatika yang bisa saja menurun atau malah menjadi naik. Semua tergantung bagaimana Kementerian Komunikasi dan Informatika menangani kasus ini, berhasil atau tidaknya penanganan kasus sehingga masyarakat merasa aman dari kasus sejenis yang bisa saja terjadi lagi dikemudian hari. Reputasi merupakan hal yang sangat penting bagi sebuah institusi negara agar mendapat kepercayaan dari warganya sehingga kebijakan-kebijakan yang diterapkan mampu diterima semua pihak dan segala aktivitas yang dilakukan mampu menggalang dukungan masyarakat. Untuk itu diharapkan kedepannya Kementerian Komunikasi dan Informatika mampu meningkatkan sensitivitas dalam lingkup digital agar kejadian seperti ini dapat dicegah, sehingga tidak menimbulkan keresahan di tengah-tengah masyarakat Indonesia dan tidak mengancam reputasi Kementerian Komunikasi dan Informatika itu sendiri.

Peretas atau *hacker* pada awalnya merupakan kata yang merujuk pada hal positif dikarenakan memiliki arti bagi seseorang yang memiliki kemampuan untuk merombak segala sesuatu yang berkaitan dengan komputer serta didalamnya termasuk mengotak-atik sistem untuk menjadikan hal yang lebih baik (Ginanjar, 2018). Namun, kata *hacker* berubah menjadi negatif dikarenakan sebuah peristiwa yang terjadi di Jerman yang menyebabkan kerugian bagi sebuah bank. Namun definisi dari *hacker* itu sendiri sebetulnya tidak memiliki kesepakatan secara khusus. *Hacker* yang didefinisikan justru akan memunculkan pertanyaan dan pernyataan yang baru (Balock, 2015). Ada hal yang menarik ketika mendefinisikan *hacker* yang ternyata rujukan positif atau negatifnya definisi tersebut merupakan rekonstruksi dari media.

Pada kasus *hacker* Bjorka identitas berdasarkan bentukan media dan persepsi publik bermuara pada definisi *hacker* sebagai perbuatan yang negatif dan ilegal. Kasus ini berawal dari unggahan Bjorka tentang contoh data dari 26 juta data riwayat pencarian milik pengguna operator internet IndiHome di Breached Forums pada 20 Agustus 2022 dan bersedia memberikan data itu dengan memberinya label harga. Informasi yang dirincikan dengan dugaan milik para pengguna IndiHome yang bocor meliputi data domain, platform, peramban (*browser*), URL, *Google Keyword*, *IP Address*, resolusi layar, lokasi pengguna, *e-mail*, gender, nama, dan nomor induk kependudukan (NIK). Pada 31 Agustus 2022 Bjorka kembali melancarkan aksinya dengan menjual data registrasi kartu SIM prabayar dengan klaim data curian sebanyak 1,3 miliar data. Data ini dijual seharga 50.000 Dollar Amerika Serikat atau setara Rp. 743.000.000.

Perbuatan Bjorka tidak berhenti sampai disitu pada 6 September 2022 ia mengklaim bahwa memiliki 105 juta data penduduk Indonesia yang ia sebut diperoleh dari peladen (*server*) Komisi Pemilihan Umum (KPU). Data ini dijual Bjorka senilai 5.000 Dollar AS atau sekitar Rp. 74.400.000. Karena ulahnya membuat publik resah namun pihak berwajib tidak kunjung dapat menangkapnya, ia kembali berulah dengan klaim atas kepemilikan dokumen

surat menyurat Presiden Joko Widodo (Jokowi) dan ia membocorkan data itu pada 10 September 2022. Namun, unggahan klaim dokumen yang dilakukan Bjorka ini dipastikan tidak ada surat menyurat Presiden Jokowi yang diretas, pernyataan ini bersumber dari Sekretariat Presiden Heru Budi Hartono. Kasus peretasan ini terus berlanjut hingga pada 10 sampai 11 September 2022 Bjorka membocorkan data pribadi milik sejumlah pejabat negara. Ulah Bjorka terus berlanjut ketika kebocoran data milik instansi pemerintah yakni aplikasi MyPertamina yang saat itu para konsumen Pertamina diwajibkan untuk mendaftarkan diri dan kendaraannya untuk dapat membeli bahan bakar bersubsidi. Data MyPertamina yang berhasil dibocorkan oleh Bjorka mencapai 44.000.000.



Gambar 1.1 Unggahan *Hacker* Bjorka

Sumber: https://www.liputan6.com/tekno/read/5126589/pakar-data-pedulilindungi-yang-bocor-dan-dijual-bjorka-valid-pemerintah-harus-lakukan-digital-forensic

Pada Maret 2023 ini Bjorka telah beberapa kali membocorkan data masyarakat Indonesia pada Breached Forum sebagai mana rinciannya telah dimuat pada media online TiNews.com. Data-data tersebut meliputi data *SIM card* sebanyak 1,3 Miliar, *database* Universitas Muhammadiyah Palangka Raya, *database* pelanggan IndiHome, data PT Sigma bagian dari PT Pertamina, dan *database* 44 juta pelanggan MyPertamina. Berdasarkan keterangan, data-data tersebut terdiri dari nama, NIK, nomor ponsel, dan berbagai data penting

lainnya. Pada 13 Maret lalu, Bjorka menjual 19 juta data BPJS Ketenagakerjaan dan 3,2 miliar data peduli lindungi dalam platform yang sama dengan harga yang beragam.

Data-data yang diretas oleh Bjorka memang tidak secara signifikan dapat dikategorikan sebagai data rahasia. Namun sudah sepatutnya bagi pemerintah dan instansi negara lainnya untuk berbenah diri dan meningkatkan sistem pengamanan digitalnya agar data-data yang seharusnya tidak dapat diakses sembarangan tidak mudah untuk diretas.

1.2 Identifikasi Masalah

Berdasarkan latar belakang yang di uraikan di atas, identifikasi masalah yang akan diteliti ialah sebagai berikut.

a) Bagaimana reputasi Kementerian Komunikasi dan Informatika saat terkena krisis *hacker* Bjorka?
b) Apakah dampak dari krisis *hacker* Bjorka terhadap reputasi Kementerian Komunikasi dan Informatika?
c) Apakah Kementerian Komunikasi dan Informatika bertanggung jawab atas terjadinya kasus *hacker* Bjorka ini?
d) Apa upaya pertanggungjawaban yang dilakukan Kementerian Komunikasi dan Informatika untuk menanggulangi krisis yang ditimbulkan oleh *hacker* Bjorka?
e) Siapa saja yang diajak Kementerian Komunikasi dan Informatika untuk berpartisipasi secara aktif dalam mengentaskan masalah *hacker* Bjorka ini?
f) Mengapa krisis peretasan yang disebabkan oleh *hacker* Bjorka dapat terjadi?
g) Apakah upaya-upaya yang dilakukan oleh Kementerian Komunikasi dan Informatika untuk menanggulangi kasus ini berhasil?
h) Bagaimana sikap Kementerian Komunikasi dan Informatika dalam menyampaikan informasi seputar *hacker* Bjorka?

1.3 Pembatasan Masalah

Berdasarkan pemaparan latar belakang pada halaman sebelumnya, agar penelitian ini dapat di fokuskan kepada topik pembahasan utama yang menjadi permasalahan pokok pada penelitian ini. Oleh karena itu, penelitian ini dibatasi hanya pada kasus *hacker* Bjorka yang menyerang Kementerian Komunikasi dan Informatika.

1.4 Rumusan Masalah

Rumusan masalah yang terdapat pada penelitian ini ialah sebagai berikut.

"Seberapa besar pengaruh manajemen krisis kasus hacker Bjorka terhadap reputasi Kementerian Komunikasi dan Informatika".

1.5 Tujuan Penelitian

Tujuan diadakannya penelitian, yaitu untuk mengukur:

a) Manajemen krisis kasus *hacker* Bjorka.
b) Reputasi Kementerian Komunikasi dan Informatika.
c) Pengaruh manajemen krisis kasus *hacker* Bjorka dengan reputasi Kementerian Komunikasi dan Informatika.

1.6 Signifikansi Penelitian

a) Signifikansi Akademis

Pada penelitian ini, teori yang digunakan ialah teori-teori *public relations* yang berkaitan dengan management krisis serta pengelolaan reputasi untuk mengetahui dan mengukur sejauh mana teori-teori tersebut saling berkaitan satu sama lain berdasarkan kasus yang terdapat pada penelitian ini. Penelitian ini akan memberikan sumbangsi dalam pengembangan teori dari management krisis dan reputasi berdasarkan kasus *hacker* Bjorka yang melanda Indonesia dan Kementerian Komunikasi dan Informatika.

b) Signifikansi Praktis

Penelitian ini akan memberikan pengetahuan tentang pengelolaan reputasi yang baik berdasarkan management krisis dan memberikan masukan kepada Kementerian Komunikasi dan Informatika sebagai institusi pemerintahan agar mampu mengelola reputasinya secara lebih baik sehingga mampu menanggulangi berbagai permasalahan di masa mendatang.

Penelitian ini juga akan memberikan dampak terhadap kementerian lain untuk lebih memperhatikan setiap isu yang berkembang di masyarakat agar lebih cepat untuk ditanggapi dan mampu ditangani secara cepat sehingga tidak berlarut-larut dan menimbulkan keresahan di tengah masyarakat.