MAKALAH

Kasus Bocornya Data BPJS Kesehatan (Indonesia, 2021)

Disusun Untuk Memenuhi Tugas Mata Kuliah Etika Profesi

Dosen Pengampu

Hairil Kurniadi Siradjuddin S.kom., M.kom.

Oleh :

Ajuan Sahmir (07352311078)

PROGRAM STUDI INFORMATIKA

FAKULTAS TEKNIK

UNIVERSITAS KHAIRUN

2025

Kata pengantar

Dafar Isi

BAB I

PENDAHULUAN

1.1 Latar Belakang

Perkembangan teknologi informasi memberikan berbagai kemudahan dalam pengelolaan data dan penyampaian informasi, terutama dalam sektor pelayanan publik seperti kesehatan. Layanan berbasis digital memungkinkan efisiensi tinggi dalam pencatatan, penyimpanan, dan distribusi data. Salah satu contoh implementasi sistem digital adalah BPJS Kesehatan, yang memanfaatkan teknologi informasi untuk mendukung layanan kepada masyarakat secara luas.

Namun, di balik kemudahan tersebut terdapat ancaman serius yang tidak dapat diabaikan, yaitu risiko kebocoran data pribadi. Data pribadi merupakan aset berharga yang harus dijaga keamanannya karena bisa disalahgunakan oleh pihak yang tidak bertanggung jawab. Kebocoran data dapat menimbulkan kerugian besar, baik dari segi sosial, ekonomi, maupun hukum. Salah satu kasus besar yang sempat menggemparkan publik Indonesia adalah kebocoran data BPJS Kesehatan pada tahun 2021.

Kasus ini mengungkap bahwa lebih dari 270 juta data penduduk Indonesia yang terdaftar dalam BPJS Kesehatan bocor dan diperjualbelikan di forum dark web. Data yang bocor meliputi nama lengkap, Nomor Induk Kependudukan (NIK), tanggal lahir, alamat, nomor telepon, hingga informasi gaji. Kebocoran ini tidak hanya menimbulkan keresahan di masyarakat, tetapi juga merusak kepercayaan publik terhadap sistem pelayanan digital pemerintah.

Fenomena ini menunjukkan bahwa Indonesia masih memiliki banyak pekerjaan rumah dalam hal perlindungan data pribadi dan keamanan siber. Sistem informasi yang tidak dilengkapi dengan perlindungan yang memadai menjadi celah besar yang bisa dimanfaatkan oleh pihak yang berniat jahat. Oleh karena itu, kasus ini penting untuk dikaji lebih dalam guna memahami penyebab, dampak, dan langkah-langkah yang harus diambil untuk mencegah kejadian serupa di masa depan.

1.2 Rumusan Masalah

1. Apa yang menyebabkan kebocoran data BPJS Kesehatan pada tahun 2021?
2. Bagaimana aspek hukum terkait kebocoran data ini menurut perspektif cyberlaw di Indonesia?
3. Apa saja dampak dan langkah penanggulangan dari kasus tersebut?

1.3 Tujuan Penulisan

1. Menjelaskan kronologi dan penyebab kebocoran data BPJS Kesehatan.
2. Mengkaji peraturan hukum yang mengatur tentang keamanan dan perlindungan data.

3. Menganalisis dampak dan upaya yang dilakukan untuk menanggulangi kasus tersebut.

BAB II

LANDASAN TEORI

2.1 Cybercrime

Cybercrime adalah kejahatan yang dilakukan dengan menggunakan teknologi komputer dan jaringan internet sebagai sarana utama. Bentuk-bentuk cybercrime meliputi pencurian data, hacking, penyebaran malware, dan kejahatan berbasis sistem informasi lainnya. Dalam konteks kasus BPJS, kebocoran data termasuk dalam kategori pencurian data dan penyalahgunaan informasi pribadi.

2.2 Cyberlaw

Cyberlaw adalah hukum yang mengatur aktivitas di dunia maya, khususnya yang berkaitan dengan kejahatan digital. Di Indonesia, beberapa regulasi yang relevan antara lain:

1. UU No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE), yang telah diubah dengan UU No. 19 Tahun 2016.
2. Peraturan Pemerintah No. 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik (PSTE).

3. UU No. 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP).

BAB III

PEMBAHASAN

3.1 Kronologi dan Isi Kebocoran

Pada Mei 2021, data pribadi milik peserta BPJS Kesehatan ditemukan dijual di forum dark web oleh akun bernama 'Kotz'. Data tersebut mencakup nama lengkap, NIK, tanggal lahir, alamat, nomor HP, hingga gaji. Pemeriksaan awal menunjukkan bahwa data tersebut valid dan berasal dari database yang tidak dienkripsi dengan baik.

3.2 Motif dan Penyebab

Motif utama pelaku adalah ekonomi—menjual data pribadi dalam jumlah besar yang memiliki nilai tinggi di pasar gelap. Penyebab utama kebocoran diduga karena:

1. Kurangnya sistem keamanan jaringan (enkripsi, firewall, dsb).
2. Celah dalam sistem atau aplikasi yang belum diperbarui.
3. Lemahnya manajemen akses data di internal BPJS.

3.3 Dampak

1. Pencurian identitas dan potensi penipuan.
2. Menurunnya kepercayaan publik terhadap sistem pelayanan digital pemerintah.
3. Potensi kerugian finansial dan sosial bagi individu yang datanya bocor.

3.4 Penanggulangan

1. Pemerintah melakukan investigasi melalui Kementerian Kominfo dan BSSN.
2. Pemblokiran situs tempat data bocor dipublikasikan.
3. Dorongan terhadap revisi dan penguatan regulasi perlindungan data pribadi.

BAB IV

PENUTUP

4.1 Kesimpulan

Kasus bocornya data BPJS Kesehatan merupakan contoh nyata dari cybercrime yang berdampak luas terhadap masyarakat. Lemahnya sistem keamanan informasi dan belum optimalnya penerapan cyberlaw di Indonesia menjadi celah yang perlu segera dibenahi. Perlindungan data pribadi harus menjadi prioritas dalam era digital.

4.2 Saran

1. Pemerintah dan lembaga penyedia layanan publik harus memperkuat sistem keamanan informasi.
2. Penerapan UU PDP harus disosialisasikan dan ditegakkan secara ketat.
3. Masyarakat perlu diedukasi mengenai pentingnya menjaga data pribadi.

DAFTAR PUSTAKA

- Undang-Undang No. 11 Tahun 2008 tentang ITE.
- Undang-Undang No. 27 Tahun 2022 tentang Perlindungan Data Pribadi.
- Kominfo.go.id. "Kronologi Dugaan Kebocoran Data BPJS".
- Tirto.id. "Kebocoran Data BPJS: Apa yang Sebenarnya Terjadi?"
- Detik.com. "Data BPJS Kesehatan Bocor, Ini Kata Kominfo".