Studi Kasus Hukum Siber – 5PSIA
Pertemuan III – Pelanggaran UU ITE

Kelompok :

1. Benedict - 2331098
2. Leonardo Dicaprio - 2331101
3. William Tarmon - 2331102
4. Nicholas Winata - 2331108
5. Hendra - 2331207
6. Ripto - 2331020
7. Heriyanto - 2331016
8. Kevin huang – 2331241

Source:

1. https://jurnal.peneliti.net/index.php/JIWP/article/view/9474
2. https://news.detik.com/berita/d-6657819/bareskrim-tangkap-55-wna-6-wni-sindikat-fraud-internasional-di-jakarta

kasus yang termasuk ke dalam kategori kejahatan hukum siber yang melanggar UU ITE dan melibatkan yurisdiksi negara lain.

- Pada April 2023, Direktorat Tindak Pidana Umum Bareskrim Polri menangkap **55 warga negara asing (WNA) dan 6 WNI** dalam sebuah sindikat penipuan online internasional di Jakarta. Para tersangka menggunakan *media elektronik* (telepon, komputer, tablet) untuk menipu korbannya. Modusnya misalnya mengaku sebagai polisi dan memeras korban, atau menjual barang elektronik tanpa mengirimnya setelah dibayar. Kasus ini jelas termasuk **kejahatan siber** karena pelaku menggunakan teknologi informasi dan jaringan elektronik lintas negara sebagai alat penipuan

Soal

1. Apa unsur dalam kasus tersebut yang membuat ini termasuk kejahatan dalam hukum siber ?

    a. **Media elektronik**: Penipuan dilakukan via telepon, internet, dan perangkat digital (71 iPad, 68 HP, laptop, modem, dll. disita dari lokasi). Ini memenuhi unsur “transaksi elektronik” yang diatur UU ITE.
    b. **Penyebaran informasi palsu**: Tersangka sengaja menyampaikan berita bohong/misleading (mis. mengaku polisi, janji barang elektronik) untuk merugikan korban. Pasal 28(1) UU ITE melarang menyebarkan berita bohong yang merugikan pihak lain lewat media elektronik.
    c. **Kerugian pihak lain**: Aksi ini mengakibatkan kerugian korban (secara finansial) yang berada di luar Indonesia. Menurut pasal 28(1) UU ITE, unsur kerugian (material) merupakan konstitutif delik penipuan elektronik.

d. **Sengaja dan tanpa hak**: Pelaku melakukan tindakan ini dengan kesengajaan dan tanpa hak (tidak ada kewenangan hukum). Karakteristik kejahatan siber seperti dilakukan secara ilegal di ruang maya juga tercermin di sini.

2. Apa dasar hukum dalam penegakan hukum siber dalam kasus tersebut ?

   Penindakan kasus ini berdasar **UU No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik** (UU ITE) beserta perubahan terakhir (UU 19/2016 atau UU 27/2022). Undang-undang ini mencakup kejahatan penipuan elektronik. Secara spesifik: Pasal 28 ayat (1) UU ITE mengancam pidana bagi yang dengan sengaja menyebarkan berita bohong dan menyesatkan sehingga menyebabkan kerugian. Sanksinya diatur Pasal 45A ayat (1) UU ITE (pidana penjara maksimal 6 tahun dan/atau denda Rp 1 miliar). Selain itu, tindakan "akses ilegal" ke sistem elektronik dapat dipidana menurut Pasal 30 UU ITE, dan pasal lain terkait kejahatan siber. Karena pelaku adalah WNA, penegakan hukum juga mengacu UU No. 6/2011 tentang Keimigrasian (Pasal 19 ayat (1) dan Pasal 122 huruf a) yang mengatur keimigrasian dan tindakan administrasi terhadap WNA.

3. Bagaimana penegakan hukum terhadap kejahatan siber tersebut di Indonesia?

   Penegakan dilakukan oleh Bareskrim Polri bersama instansi Imigrasi. Polisi (Ditipidum Bareskrim) melakukan penyelidikan forensik digital dan razia, menahan para tersangka beserta alat bukti (telepon, komputer, dokumen). Setelah penangkapan, 55 WNA tersebut diserahkan ke pihak Imigrasi untuk diproses lebih lanjut. Sesuai prosedur, pihak kepolisian mengawal proses **pendeportasian** tersangka ke negara asal mereka. Misalnya, pada Mei 2023 Bareskrim mengawal pemulangan 52 WNA asal Tiongkok yang diduga terlibat jaringan penipuan internasional via media elektronik. Seluruh proses ini merujuk pada UU ITE (penipuan elektronik) dan UU Keimigrasian – sebagaimana disampaikan bahwa penegakan terhadap WNA di Indo masuk ranah Ditjen Imigrasi.

4. Apakah kasus tersebut melibatkan pihak negara asing dan terdapat permasalahan dalam penentuan yurisdiksi dalam kasus tersebut?

   Kasus ini **melibatkan pihak asing secara langsung**. Semua pelaku utama adalah WNA (diduga Cina), dan para korban berada di luar negeri (Negara tujuan penipuan misalnya Singapura, Thailand, China). Karena kejahatan terjadi di wilayah Indonesia, hukum nasional berhak menuntut pelakunya (yurisdiksi teritorial). Namun, korban yang merupakan warga negara lain menyebabkan masalah yurisdiksi substantif – sulit menghadirkan saksi korban asing dalam persidangan Indonesia. Untuk mengatasi ini, pemerintah memutuskan melakukan deportasi pelaku ke negara asalnya, agar penuntutan dapat dilanjutkan di sana. Dengan kata lain, tidak diperlukan kerja sama melalui saluran hukum internasional (misalnya ekstradisi), karena pelaku sudah ditangkap dalam wilayah hukum RI dan akhirnya diserahkan oleh pemerintahan. Meski demikian, kasus menunjukkan perlunya kerja sama antarnegara dalam pemulangan bukti dan pendampingan penuntutan pidana lintas batas.

5. Bagaimana menurut tanggapan saudara/i penegakan Hukum Siber terkati dengan kasus tersebut di Indonesia dan bagaimana kritik dan saran terkait dengan implementasi, efektivitas dan pengembangan hukum siber di Indonesia?

   Kasus ini memperlihatkan bahwa aparat penegak di Indonesia dapat menindak tegas sindikat penipuan online lintas negara. Kerja sama Polri-Imigrasi dan pemanfaatan UU ITE serta UU Keimigrasian membuahkan penangkapan puluhan tersangka dan pendeportasian mereka. Namun, fenomena semacam ini juga menegaskan tantangan penegakan hukum siber di era global: sifat lintas batas kejahatan siber mengaburkan yurisdiksi nasional dan sering kali membuat penyelesaian hukum menjadi kompleks.
   Dari perspektif reformasi hukum, beberapa hal perlu diperhatikan. UU ITE terbaru (UU 27/2022) sudah berupaya menambah pendekatan restorative justice dan perlindungan data pribadi, tetapi masih perlu mempertegas pasal terkait penipuan dan informasi palsu agar tidak multitafsir (hindari “pasal karet”). Selain itu, kasus ini menunjukkan pentingnya memperkuat **kerja sama internasional** – misalnya mempercepat perjanjian Mutual Legal Assistance (MLAT) dan pertukaran informasi forensik digital antar kepolisian – sehingga korban di luar negeri bisa diajak kooperatif dalam penyidikan.
   Penegak hukum juga disarankan meningkatkan kapasitas khusus (PPNS, satgas siber) dan teknologi forensik agar penyelidikan lebih cepat dan menyeluruh. Dari sisi kebijakan, edukasi masyarakat tentang bahaya penipuan online lintas negara perlu digencarkan. Secara keseluruhan, efektivitas UU ITE tergantung keseriusan aparat dan koordinasi antar-lembaga serta antar-negara; kritik utama sering muncul terkait pemahaman pasal dan lambatnya kerja sama internasional, sehingga pengembangannya harus menyorot aspek hukum ekstrateritorial dan penanganan korban asing.