



Jurnal Ilmiah Penegakan Hukum

Available online <http://ojs.uma.ac.id/index.php/gakkum>

Implementasi Penyidikan Terhadap Tindak Pidana Siber Dalam Perspektif Perbandingan Hukum: Indonesia dan Inggris Raya

Implementation of Investigations into Cyber Crimes in a Comparative Legal Perspective: Indonesia and the United Kingdom

Manayra Aisha Putri Indradjaja*, Sigid Suseno & Budi Arta Atmaja

Fakultas Hukum, Universitas Padjadjaran, Indonesia

*Corresponding Email: manayra18001@mail.unpad.ac.id

Abstrak

Tulisan ini bertujuan untuk membahas pelaksanaan penyidikan terhadap tindak pidana siber di Indonesia dan Inggris Raya. Pelaksanaan penyidikan merupakan proses penting untuk memastikan bahwa suatu tindak pidana termasuk di dalamnya tindak pidana siber dapat ditangani secara efektif, pelaku kejahatan dapat diadili berdasarkan ketentuan hukum yang berlaku, dan hak-hak korban dapat dilindungi. Masalah dalam tulisan ini difokuskan untuk mengeksplorasi pelaksanaan penyidikan terhadap tindak pidana siber di kedua negara tersebut mengingat seiring dengan majunya era digital tindak pidana siber menjadi suatu tantangan yang berkelanjutan bagi pelaksanaan penegakan hukum. Guna mendekati masalah ini dipergunakan acuan teori perbandingan hukum pidana untuk membandingkan ketentuan hukum dan memahami hukum asing agar dapat dijadikan pertimbangan untuk pembaharuan hukum nasional. Data-data dikumpulkan melalui pendekatan perundang-undangan dan pendekatan komparatif serta dianalisis secara kualitatif. Kajian ini menyimpulkan bahwa terdapat faktor pembeda dari pelaksanaan penyidikan terhadap tindak pidana siber di Indonesia dan Inggris Raya. Pelaksanaan penyidikan tindak pidana siber di Indonesia berada di bawah koordinasi penyidik kepolisian sedangkan di Inggris Raya yang melakukan penyidikan terhadap tindak pidana siber dibagi menjadi dua, yakni pihak kepolisian yang menangani kasus tindak pidana siber pada tingkat regional dan National Crime Agency yang menangani kasus tindak pidana siber yang bersifat lintas batas serta berisiko tinggi.

Kata Kunci: Penyidikan; Tindak Pidana Siber; Perbandingan Hukum.

Abstract

This paper aims to discuss the implementation of investigations into cybercrime in Indonesia and the United Kingdom. The implementation of investigations is an important process to ensure that a crime including cybercrime can be handled effectively, the perpetrators can be prosecuted based on applicable legal provisions, and the rights of victims can be protected. The problem in this paper is focused on exploring the implementation of investigations into cybercrime in both countries considering that along with the advancement of the digital era, cybercrime has become an ongoing challenge for law enforcement. In order to approach this problem, a reference is used for comparative criminal law theory to compare legal provisions and understand foreign laws so that they can be used as considerations for national legal reform. Data were collected through a statutory approach and a comparative approach and analyzed qualitatively. This study concludes that there are differentiating factors in the implementation of investigations into cybercrime in Indonesia and the United Kingdom. The implementation of investigations into cybercrime in Indonesia is under the coordination of police investigators, while in the United Kingdom, investigations into cybercrime are divided into two, namely the police who handle cybercrime cases at the regional level and the National Crime Agency which handles cross-border and high-risk cybercrime cases.

Keywords: Investigation; Cyber Crime; Comparative Legal.

How to Cite: Indrajaja, M.A.P., Suseno, S., & Atmaja, B.A. (2024). Implementasi Penyidikan Terhadap Tindak Pidana Siber Dalam Perspektif Perbandingan Hukum: Indonesia dan Inggris Raya, *Jurnal Ilmiah Penegakan Hukum*, 11 (2): 162-172

PENDAHULUAN

Tindak pidana siber merupakan suatu dampak negatif yang ditimbulkan dari perkembangan dunia digital. Pelaku dari tindak pidana siber merupakan seseorang yang memiliki keahlian dalam mengoperasikan ilmu komputer, dapat menguasai algoritma serta program komputer, memiliki kemampuan dalam menganalisis cara kerja sistem komputer, dan mampu menemukan celah untuk melemahkan sistem komputer sehingga dapat masuk kedalamnya untuk melakukan tindakan jahat seperti pencurian data (Sahat, 2020). Selain itu, pelaku tersebut memiliki kemampuan untuk terus mengembangkan teknik dan strategi baru (Rian Dwi Hapsari & Kuncoro Galih, 2023).

Terdapat berbagai macam metode dengan memanfaatkan teknologi komputer ataupun internet agar suatu tindak pidana siber dapat terjadi melalui berbagai macam bentuk serangan siber, seperti *Malware*, *Ransomware*, *Phising*, *Denial of Service*, *Distributed Denial of Service*, *Exploits*, dan lain sebagainya. Kemudian terdapat jenis kelompok tindak pidana siber yang sering terjadi, yaitu perbuatan tidak sah dalam mengakses suatu sistem dan layanan komputer (Maskun, 2013). Pelaku kejahatan dalam kelompok tindak pidana tersebut dengan cara yang tidak sah, tanpa izin, dan/atau tanpa sepengetahuan dari pemiliknya memasuki sistem jaringan komputer yang telah dijadikan sebagai target untuk dilakukannya suatu perbuatan pidana (Dikdik & Elisatris Gultom, 2009).

Indonesia sebagai negara yang memanfaatkan perkembangan teknologi, disaat yang bersamaan rentan mendapatkan ancaman terhadap ruang siber yang menjadi suatu konsekuensi dari perkembangan teknologi yang terjadi. Pemanfaatan terhadap ruang siber di Indonesia terindikasi mendapatkan serangan siber dari negara lain. Berdasarkan catatan yang dibuat oleh BSSN,

pada tahun 2023 terdapat sebanyak 403,9 juta anomali yang terjadi di Indonesia. Dampak dari aktivitas anomali tersebut mempengaruhi penurunan kapabilitas dari perangkat dan jaringan, pencurian terhadap data sensitif milik korban, hingga penurunan reputasi bagi organisasi yang terserang (BSSN, 2023).

Kemudian data yang diperoleh dari pihak kepolisian menyatakan pada tahun 2023 terdapat sebanyak 3.758 kasus tindak pidana siber dengan rincian sebagai berikut (Tribrata News, 2023):

Jenis Tindak Pidana	Jumlah
Penipuan	1.414
Pencemaran nama baik	838
Pornografi	457
Akses ilegal	353
Judi Online	250

Berdasarkan data tersebut memperlihatkan perbedaan jumlah signifikan antara serangan siber yang ditemukan oleh BSSN dengan penindakan yang dilakukan oleh kepolisian. Salah satu faktor yang menyebabkan hal tersebut terjadi karena alat bukti elektronik yang digunakan untuk membuktikan suatu tindak pidana siber tidak mudah dikumpulkan karena karakteristiknya yang dapat berubah secara cepat.

Pada tahun 2022-2023 terdapat beberapa serangan siber di Indonesia yang mengakibatkan kerugian secara materil dan immateril, seperti kebocoran data penduduk dan pejabat Indonesia yang dilakukan oleh *Hacker Brojka* (CCN Indonesia, 2023). Adapula serangan berupa dugaan pengenaan virus *ransomware* yang dilakukan oleh kelompok *Hacker LockBit 3.0* yang mengakibatkan gangguan pada sistem Bank Syariah Indonesia (BSI) (tvonenews, 2023). Selain itu, pada tahun 2024 terdapat serangan siber terbaru pada Pusat Data Nasional Sementara (PDNS) 2 yang mengakibatkan terhambatnya layanan publik milik pemerintah Indonesia. Berdasarkan pemaparan tersebut memperlihatkan bahwa Indonesia masih sering menjadi target

serangan siber yang dilakukan oleh para *hacker*.

Penindakan terhadap pelaku kejahatan berdasarkan sistem peradilan pidana dilakukan melalui proses penyelidikan dan penyidikan terlebih dahulu. Kepolisian merupakan instansi penegak hukum dan memiliki fungsi untuk melakukan pelaksanaan penyelidikan dan penyidikan terhadap suatu peristiwa pidana yang terjadi di Indonesia. Penyidik Polri saat melakukan penegakan hukum terhadap tindak pidana siber memerlukan bantuan atau dukungan dari *stakeholder* siber lainnya, seperti PPNS pada Kementerian Komunikasi dan Informatika Republik Indonesia (Kominfo), Badan Siber dan Sandi Negara (BSSN), dan Badan Intelijen Negara (BIN).

Pada penelitian ini akan dilakukan perbandingan implementasi penyidikan terhadap tindak pidana siber dengan Inggris Raya. Adapun alasannya karena Inggris Raya merupakan salah satu negara yang seringkali dijadikan target serangan siber terutama berkenaan dengan penyebaran *ransomware* yang mengancam infrastruktur nasional sehingga menimbulkan risiko terhadap keamanan nasional. Kemudian Inggris Raya memiliki badan penegak hukum nasionalnya tersendiri diluar pihak kepolisian yang memiliki wewenang untuk menyelidiki serta memberantas kejahatan serius dan terorganisir termasuk di dalamnya tindak pidana siber.

Proses penyidikan terhadap tindak pidana siber di Indonesia dan Inggris Raya memiliki perbedaan signifikan yang digunakan oleh aparat penegak hukum di kedua negara tersebut. Penegak hukum di Indonesia sering kali menghadapi kendala seperti terbatasnya sumber daya manusia dan kurang memadainya sarana teknologi (Alief Tanding Pamungkas dkk, 2024). Sementara itu, pihak pemerintah di Inggris Raya telah menyadari bahwa diperlukannya respon terpadu

terhadap ancaman siber, sehingga dalam prosesnya melibatkan orang-orang terlatih, teknologi terbaru, dan penerapan strategi yang sesuai (Jakub Wolyniec, 2018).

Maka dari itu, dengan dilakukannya identifikasi dan perbandingan mengenai implementasi penyidikan terhadap tindak pidana siber di kedua negara tersebut diharapkan akan memperoleh wawasan yang lebih mendalam mengenai hambatan dan solusi dalam pelaksanaan penyidikan terhadap tindak pidana siber mengingat tindak pidana siber seiring dengan majunya era digital menjadi suatu tantangan yang berkelanjutan bagi pelaksanaan penegakan hukum di berbagai negara.

METODE PENELITIAN

Penelitian ini menggunakan metode pendekatan yuridis normatif yang berfokus pada pendekatan perundang-undangan dan pendekatan komparatif. Data yang digunakan sebagai sumber utama adalah data sekunder, seperti teori, konsep, asas hukum, peraturan perundang-undangan dan literatur yang berkaitan dengan masalah yang akan diteliti (Soerjono Soekanto & Sri Mamudji, 2015). Kemudian berkenaan dengan komparatif, yaitu penelitian yang membandingkan ketentuan hukum yang berlaku di beberapa negara. Perbandingan yang dilakukan adalah pelaksanaan penyidikan terhadap tindak pidana siber antara negara Indonesia dan negara Inggris Raya. Adapun data-data yang telah didapatkan akan dianalisis dan disusun secara kualitatif.

HASIL DAN PEMBAHASAN

Pelaksanaan Penyidikan Terhadap Tindak Pidana Siber di Indonesia

Tindak pidana siber memiliki perbedaan karakteristik dari tindak pidana konvensional baik pada aspek pelaku, modus operandi, korban ataupun tempat terjadinya tindak pidana. Adapun aspek yang paling membedakan, yaitu pada tindak

pidana siber aktivitas kejahatan dilakukan melalui sarana komputer ataupun jaringan komputer. Dampak dari tindak pidana siber dapat berupa tercurinya data pribadi seseorang hingga hilangnya pekerjaan seseorang. Selain itu, tindak pidana siber dapat mengganggu keadaan stabilitas ekonomi, politik, dan sosial suatu negara bahkan sampai pada tahap yang membahayakan infrastruktur kritis negara (Dwi Shinta, dkk, 2024).

Penyelidikan merupakan proses yang penting dalam mengidentifikasi dan memastikan bahwa terhadap suatu peristiwa memang benar telah terjadinya suatu tindak pidana. Sedangkan penyidikan merupakan tindakan mengumpulkan bukti untuk membuat terang suatu tindak pidana agar dapat menemukan siapa tersangkanya. Penyelidikan dan penyidikan merupakan dua fase tindakan yang saling memiliki keterkaitan agar dapat menyelesaikan pemeriksaan terhadap suatu peristiwa pidana yang terjadi (Yahya Harahap, 2014). Selain itu, proses penyelidikan dan penyidikan perlu dilakukan untuk menjamin kepastian hukum sehingga tidak menimbulkan kesalahan dalam menentukan seorang tersangka.

Pasal 1 butir 1 KUHAP menyatakan bahwa penyidik adalah pejabat polisi negara Republik Indonesia atau pejabat pegawai negeri sipil tertentu yang diberi wewenang khusus oleh undang-undang untuk melakukan penyidikan. Berkenaan dengan proses dimulainya penyelidikan dan penyidikan dilakukan setelah pihak kepolisian mendapatkan laporan, pengaduan, ataupun informasi dari masyarakat terkait adanya dugaan atau terjadinya suatu tindak pidana. Selanjutnya informasi tersebut perlu diadakan penelitian dan penyaringan terlebih dahulu. Apabila dilihat secara umum, pada saat melakukan penyidikan terhadap tindak pidana siber tidak jarang pihak kepolisian melibatkan koordinasi dengan pihak-pihak tertentu untuk dapat memastikan telah terjadinya suatu tindak pidana (Aco Agus & Riskawati, 2016).

Kepolisian dalam melaksanakan penegakan hukum terhadap suatu tindak pidana merupakan bagian dari subsistem peradilan pidana. Sistem peradilan pidana sendiri di dalamnya mengenal

istilah *open system*, yakni suatu sistem yang pergerakannya sangat dipengaruhi oleh berbagai macam bidang yang ada dalam kehidupan manusia. Sistem peradilan pidana akan selalu mengalami *interface* (interaksi, interkoneksi, dan interdependensi) dengan lingkungannya yang terdiri dari masyarakat, ekonomi, teknologi, edukasi, politik ataupun subsistem peradilan pidana itu sendiri (Muladi, 2018). Maka dari itu, dapat dikatakan bahwa *open system* dalam sistem peradilan pidana memungkinkan adanya keterlibatan dari instansi di luar penegak hukum.

Selain Penyidik Polri terdapat penyidik lainnya, yaitu Pejabat Penyidik Pegawai Negeri Sipil (PPNS) tertentu di lingkungan pemerintah. PPNS yang lingkup tugas dan tanggungjawabnya di bidang teknologi informasi dan transaksi elektronik diatur dalam Pasal 43 UU ITE. Adapun kedudukan dari Pejabat PPNS berada di bawah koordinasi dan pengawasan dari penyidik Polri (Yahya Harahap, 2014). Berkenaan dengan tindak pidana siber, Penyidik Polri pada saat melakukan tugasnya memerlukan koordinasi dengan instansi lainnya, seperti Badan Siber dan Sandi Negara (BSSN) dan Badan Intelijen Negara (BIN).

BSSN pada Direktorat Operasi Keamanan Siber secara aktif melakukan deteksi dan penanggulangan serangan siber serta menginformasikan notifikasi ancaman serangan siber ataupun anomali trafik kepada *stakeholder* terdampak untuk segera ditindaklanjuti. Sedangkan BIN memiliki peran dalam merespon terjadinya suatu kebocoran data khususnya dalam melakukan pencarian kebutuhan informasi yang berhubungan dengan keamanan negara (Apryan Anggara & Ruhly Kesuma, 2023). BIN dapat dikatakan pula sebagai alat negara yang memiliki tugas dan kewenangan dalam menjalani fungsi intelijen baik dalam negeri dan luar negeri serta koordinasi terkait dengan pelaksanaan intelijen negara.

Berkenaan dengan BSSN berdasarkan Pasal 54 Peraturan Badan Siber dan Sandi Negara Nomor 6 Tahun 2021 Tentang Organisasi dan Tata Kerja Badan Siber dan Sandi Negara mengatur bahwa Direktorat Operasi Keamanan Siber

menyelenggarakan fungsi dalam pelaksanaan dukungan penyidikan, forensik digital, dan perbantuan keterangan ahli. Adapun bentuk dukungan penyidikan tersebut berupa koordinasi yang dilakukan antara pihak kepolisian dan BSSN terkait informasi yang berhubungan dengan adanya dugaan tindak pidana berupa pemeriksaan terhadap suatu peristiwa untuk menentukan bahwa tindak pidana memang telah terjadi (antaranews, 2023).

Kemudian koordinasi lainnya berupa pelaksanaan kerjasama guna mengumpulkan bukti permulaan yang cukup. BSSN dalam hal ini bertugas untuk melaksanakan keamanan siber secara efektif dan efisien, baik dalam identifikasi, deteksi, proteksi, penanggulangan, pemulihan, dan pemantauan insiden keamanan siber dan sandi nasional, serta pengelolaan krisis siber nasional. Sedangkan berkenaan dengan forensik digital yang dilakukan oleh BSSN dilengkapi dengan sertifikasi CHFI (*Computer Hacking Forensics Investigator*) yang bertujuan untuk membantu proses penyelidikan dan pengungkapan berbagai kasus kejahatan (antaranews, 2023). Hasil pemeriksaan forensik digital yang memuat mengenai akar permasalahan dari suatu kejadian insiden siber kemudian akan diserahkan kepada penyelenggara sistem elektronik terdampak untuk selanjutnya ditindak secara hukum oleh Dittipidsiber Bareskrim Polri.

Meskipun demikian, tidak semua kasus melibatkan BSSN dalam investigasinya karena BSSN memiliki keterbatasan wewenang sehingga tidak dapat melakukan penyidikan terhadap ancaman siber yang berpotensi menjadi suatu tindak pidana siber yang sedang terjadi apabila tidak dimintakan bantuan oleh sistem penyelenggara elektronik terdampak ataupun permintaan dukungan penyidikan dari Penyidik Polri. Sedangkan mengenai perbantuan keterangan ahli, BSSN dapat merumuskan keterangan sebagai ahli forensik digital dan memberikan rekomendasi terkait forensik digital.

Pada tahun 2023 terdapat sebanyak 3.758 kasus tindak pidana siber yang mana diantaranya

terdapat sebanyak 353 kasus akses ilegal. Adapun beberapa contoh kasus yang melibatkan kerjasama antara pihak kepolisian dengan BSSN, seperti kebocoran data penduduk dan data sejumlah pejabat Indonesia yang dilakukan oleh Hacker Bjorka. Indonesia sepanjang tahun 2022 mengalami beberapa dugaan kasus kebocoran data yang dialami oleh perusahaan, lembaga, ataupun instansi pemerintah. Hal tersebut dapat terungkap karena perolehan data-data yang dijual bebas pada forum *online*. Hacker Bjorka melakukan serangan siber sehingga mengakibatkan kebocoran data yang dialami oleh beberapa perusahaan, seperti kebocoran data terhadap sekitar 17 juta pelanggan Perusahaan Listrik Negara (PLN) yang terjadi pada tanggal 18 Agustus 2022 dan kebocoran data terhadap 26 juta riwayat pencarian yang dimiliki oleh pelanggan layanan internet IndiHome yang terjadi pada tanggal 20 Agustus 2022 (Kompas, 2022).

Selain Hacker Bjorka, dikenal pula Hacker LockBit 3.0 yang memiliki kemampuan dalam melakukan serangan siber berupa *ransomware*. Kelompok *ransomware* LockBit 3.0 mengklaim telah mencuri sebanyak 1,5 TB data milik Bank Syariah Indonesia (BSI) yang diantaranya terdapat 15 juta data nasabah berserta dengan *password* yang digunakan untuk melakukan akses internal dan layanan yang disediakan (liputan6, 2024). Selanjutnya pada tahun 2024 terjadi pula pengembangan virus terbaru dari *Ransomware* LockBit 3.0 bernama *Brain Cipher Ransomware* yang menyerang PDNS 2 di Surabaya (nasional tempo, 2024). Banyaknya serangan siber yang terjadi tersebut mengakibatkan terganggunya layanan publik di berbagai instansi pemerintahan.

Indonesia pada praktiknya mengalami banyak serangan siber, tetapi banyak pula serangan siber yang tidak dilaporkan karena terdapat kesulitan dalam mengumpulkan bukti pendukung. Persoalan mengenai alat bukti tersebut berkaitan dengan terdapatnya karakteristik dari tindak pidana siber, yaitu target atau media yang menjadi tempat dilakukannya tindak pidana memiliki sifat yang mudah diubah,

dihapus, atau disembunyikan oleh pelaku tindak pidana siber (Nyoman Amie Sandrawati, 2022).

Selain itu, korban dari insiden siber khususnya penyelenggara sistem elektronik terdampak pada saat mendapatkan notifikasi ancaman serangan ataupun anomali trafik yang diinformasikan oleh BSSN tidak jarang memberikan respon yang terlambat sehingga sistem yang digunakan dalam serangan siber telah berubah dan tidak dapat dicegah atau dipulihkan.

Berdasarkan pemaparan sebelumnya memperlihatkan bahwa diperlukannya suatu instansi pemerintahan yang memiliki keahlian dalam mendeteksi serangan siber untuk diberikan kewenangan sebagai Pejabat PPNS agar dapat menindak secara langsung suatu dugaan terjadinya tindak pidana siber yang menyerang data komputer, sistem komputer, atau sistem internet. Sehingga pembentukan Pejabat PPNS tersebut diharapkan dapat memaksimalkan pelaksanaan penegakan hukum terhadap tindak pidana siber yang semakin marak terjadi.

Pelaksanaan Penyidikan Terhadap Tindak Pidana Siber di Inggris Raya

Tindak pidana siber sebagai realitas kehidupan yang terjadi pada masyarakat dan dapat menimbulkan banyak korban tidak terkecuali terjadi pada masyarakat Inggris Raya termasuk di dalamnya negara Inggris, Skotlandia, Wales, dan Irlandia Utara. Pihak kepolisian di Inggris Raya, agar dapat menyelidiki suatu insiden perlu memiliki pemahaman bahwa suatu perbuatan tindak pidana telah terjadi. Selain itu, pihak kepolisian di Inggris Raya pada umumnya menangani kasus tindak pidana siber yang lebih kecil atau tindak pidana yang melibatkan kejahatan konvensional dengan menggunakan elemen digital.

Akan tetapi, penelitian menunjukkan pelaporan yang dilakukan oleh korban dari tindak pidana siber lebih kecil dibandingkan dengan korban tindak pidana konvensional. Pihak kepolisian mengalami kesulitan dalam mengidentifikasi kejahatan yang sedang terjadi di dunia maya (Joanna Curtis and Gavin Oxburgh, 2023). Pihak kepolisian menyatakan adanya

ketidakpastian mengenai peran siapa yang harus melakukan investigasi dan timbul kebingungan bagi korban mengenai kepada siapa mereka melakukan pelaporan. Tanggung jawab mungkin dianggap berada di tangan polisi, *National Fraud Investigation Bureau* (NFIB), NCA, lembaga keuangan atau perusahaan asuransi (Joanna Curtis and Gavin Oxburgh, 2023). Maka dari itu, diperlukan pemahaman yang sama antara masyarakat yang menjadi korban dan instansi yang memiliki kepentingan mengenai respon yang seharusnya diberikan pada saat terjadi suatu tindak pidana siber.

Adapun *National Police Chiefs' Council* (NPCC) sebagai badan koordinasi yang terdiri dari Kepala Kepolisian dari seluruh kepolisian yang berada di Inggris dan Wales dalam menghadapi tindak pidana siber, seperti mengidentifikasi risiko bahaya dan melindungi kelompok rentan di dunia nyata dan digital, meningkatkan sumber daya manusia sehingga memiliki kemampuan yang tepat (pengetahuan, keterampilan, dan alat) untuk menangani kejahatan yang semakin kompleks, meningkatkan kolaborasi serta memperkuat hubungan agar terciptanya keselamatan publik dengan tepat. Kehadiran NPCC seharusnya dapat memberikan evaluasi dan pemahaman bagi pihak kepolisian untuk membantu korban dan memberikan pemahaman bagi instansi terkait dalam menghadapi tindak pidana siber.

Selain pihak kepolisian, pada Inggris Raya memiliki badan penegak hukum lainnya dalam mengatasi tindak pidana siber, yaitu *National Crime Agency* (NCA). NCA merupakan departemen pemerintah nonkementerian yang beroperasi secara independen dan bekerja sebagai garis terdepan penegakan hukum, membangun gambaran intelijen mengenai ancaman kejahatan serius terorganisir, melakukan pengejaran terhadap pelanggar paling serius dan berbahaya serta mengembangkan dan memberikan kemampuan khusus atas nama penegak hukum dan mitra lainnya. NCA dalam hal ini mengatur mengenai "*Government Cyber Security Strategy: 2022 to 2030*" sebagai suatu strategi dan kebijakan

pemerintahan untuk membangun sektor publik yang tangguh terhadap ancaman siber.

NCA dalam hal ini memiliki unit khusus yang memiliki fokus pada kejahatan siber, yaitu *National Cyber Crime Unit* (NCCU) yang secara khusus bertugas menyelidiki dan menangani kejahatan siber yang serius di seluruh Inggris dan Wales. NCCU memiliki tugas dalam merespon insiden siber yang bersifat kritis, berskala besar atau kompleks. Selain itu, NCCU dapat melakukan aktivitas jangka panjang untuk melawan penjahat pada dunia maya dan memiliki kewenangan dalam memberikan bantuan untuk menutup layanan yang menjadi sarana bagi pelaku insiden siber tersebut.

Adapun klasifikasi kejahatan dalam dunia maya, yakni serangan terhadap individu, institusi swasta, dan institusi publik. Pada praktiknya, suatu perusahaan yang terdampak serangan siber menjadi pihak yang menanggung kerugian finansial terbesar dibandingkan dengan individu. Namun dampak yang terjadi terhadap individu tidak dapat diremehkan, karena individu cenderung dianggap sebagai sasaran yang mudah dijadikan target kejahatan bagi penjahat dunia maya. Individu paling memungkinkan dijadikan target pada kasus penipuan kartu bank. Jumlah total insiden penipuan dalam dunia siber pada tahun 2016 melebihi 2,5 juta (66 persen dari keseluruhan insiden) sedangkan untuk penipuan belanja online berjumlah lebih dari 1 juta insiden, yaitu 28 persen dari seluruh insiden (Juraj Sikra, Karen V. Renaud, dan Daniel R. Thomas, 2023).

Kemudian berkenaan dengan kejahatan siber terhadap institusi swasta pada Survei Pelanggaran Keamanan Siber tahun 2022 (*The 2022 Cyber Security Breaches Survey*) melaporkan bahwa terdapat 39 persen bisnis di Inggris Raya diserang pada tahun 2022, sebagian besar melalui upaya phishing sebanyak 83 persen. Penjahat dunia maya dapat menyamar sebagai email CEO, untuk melakukan transfer dana yang cepat ke penyuplai (dikenal sebagai 'penipuan CEO' atau 'kompromi email bisnis'). Usaha Kecil dan Menengah (UKM) sangat rentan terhadap berbagai

serangan semacam ini (Juraj Sikra, Karen V. Renaud, dan Daniel R. Thomas, 2023).

Pada tahun 1999, NCA telah memperkirakan sebanyak 1 juta kejahatan dalam dunia maya yang terjadi di Inggris Raya. Berbagai ancaman dunia maya terjadi dengan menargetkan perusahaan sebagai sasarannya yang mana pada tahun 2017 terdapat insiden besar yang berdampak pada pengusaha mencakup serangan berupa *ransomware* dan *distributed denial of service attacks* (DDoS), pelanggaran data besar-besaran, gangguan rantai pasokan, berita palsu dan operasi informasi. Hal tersebut merupakan sumber hilangnya keuntungan baik bagi perusahaan besar ataupun perusahaan kecil. Adapun bukti yang memperlihatkan bahwa serangan *ransomware* semakin meluas, yakni terjadinya serangan *ransomware WannaCry* pada bulan Mei tahun 2017. Menurut laporan *The Cyber Threats to UK Business* pada tahun 2018, serangan *ransomware WannaCry* terjadi dengan sangat cepat dan virusnya mereplikasi secara acak sehingga menginfeksi 300.000 perangkat di 150 negara bagian dan mempengaruhi berbagai layanan di seluruh dunia, termasuk layanan kesehatan *the British National Health Service* (NHS) (Jakub Wołyniec, 2018).

Kemudian pada bulan Desember 2019, Maksim Yakubets, warga negara Rusia, didakwa di Amerika Serikat (AS) terkait dengan dua skema peretasan komputer internasional dan penipuan bank yang terpisah. Yakubets menjalankan *Evil Corp*, kelompok kejahatan dunia maya paling berbahaya di dunia yang menciptakan dan menyebarkan *malware* sehingga menyebabkan kerugian finansial sebesar ratusan juta pound di Inggris. Sedangkan pada bulan Desember 2021 dilaporkan bahwa 48% warga Inggris Raya mengalami kejahatan dalam dunia maya (Juraj Sikra, Karen V. Renaud, dan Daniel R. Thomas, 2023). Pada umumnya, suatu negara yang masyarakatnya menghabiskan lebih banyak waktu dalam melakukan kegiatan dengan menggunakan internet memiliki potensi dan risiko yang lebih

besar untuk menjadi korban dari suatu tindak pidana siber, termasuk Inggris Raya.

Ancaman terhadap dunia maya di Inggris Raya dilakukan oleh berbagai macam aktor, termasuk kelompok yang disponsori oleh negara, organisasi kriminal yang berfokus pada finansial, dan peretas yang memiliki tujuan politik. Kelompok-kelompok tersebut tidak diatur secara jelas terkait batasan mengenai kelompok kriminal siber yang dapat beroperasi dengan dukungan implisit dari negara untuk selanjutnya memilih target karena alasan politik, atau menjual layanan serangan siber kepada pihak lain. Meskipun sebagian besar aktivitas peretas bersifat mengganggu, namun pelaku yang lebih berkompeten dapat menimbulkan kerusakan yang lebih besar (Adam Clark, 2024).

Terdapat banyak tantangan saat melakukan investigasi terhadap tindak pidana siber yang akhirnya menimbulkan ketidakberdayaan ketika menghadapi kejahatan-kejahatan yang terjadi dalam dunia maya serta adanya ketimpangan antara pesatnya perkembangan kejahatan dunia maya dan lambatnya proses investigasi yang berjalan. Selain itu, kurangnya pengetahuan yang relevan dengan tindak pidana siber juga menimbulkan perasaan resah karena ketidaktauan terkait cara terbaik untuk menangani tindak pidana siber yang terjadi pada masyarakat. Adapun kesulitan lainnya, yaitu saat melacak perkembangan kejahatan dunia maya dan kecepatan perkembangan dunia maya itu sendiri, mulai dari teknik yang berbeda pada saat melakukan kejahatan hingga *platform* media sosial baru yang digunakan sebagai sarana kejahatan (Lee Hadlington, 2018).

Kejahatan siber merupakan persoalan yang cukup mengkhawatirkan dikarenakan pelaku kejahatan umumnya beroperasi dengan mengganggu sistem teknologi dan informasi serta meminta pembayaran kepada korban agar serangan siber dihentikan. Kelompok peretas dapat menargetkan organisasi besar termasuk pemerintah dan penyedia layanan umum yang bersifat penting (Adam Clark, 2024). Maka dari itu, selain pihak kepolisian dan NCA terdapat pula

beberapa instansi yang berfokus dalam menghadapi dan mencegah tindak pidana siber, seperti *National Cyber Security Centre* (NCSC).

NCSC merupakan organisasi yang memiliki peran dalam memberikan respon terhadap insiden yang terjadi di Inggris Raya. Selain itu, NCSC memiliki tugas untuk memahami keamanan siber dan memahami pengetahuan mengenai keamanan siber yang dijadikan panduan bagi masyarakat, menanggapi insiden keamanan siber untuk mengurangi kerugian yang ditimbulkan oleh pelaku serangan siber terhadap organisasi ataupun negara secara lebih luas, mengembangkan keamanan siber di Inggris Raya dengan menggunakan keahlian industri dan akademis, serta mengurangi risiko dengan mengamankan jaringan sektor publik dan swasta. Kemudian, pemerintah di Inggris Raya berupaya untuk meningkatkan penerapan panduan keamanan siber milik NCSC, melakukan investasi dalam keamanan siber, meningkatkan jumlah profesional siber yang terampil, dan memperkuat tanggung jawab keamanan siber menurut undang-undang (Adam Clark, 2024). NCSC pada praktiknya melakukan kerjasama dengan otoritas keuangan dan NCA untuk meningkatkan ketahanan dunia maya khususnya di sektor keuangan Inggris Raya.

Berdasarkan pemaparan diatas berkenaan dengan lembaga penegakan hukum terhadap tindak pidana siber di Inggris Raya, terhadap NCA memiliki fokus tanggungjawab atas penegakan hukum dalam menangani kejahatan yang melibatkan serangan besar terhadap infrastruktur negara, seperti serangan *ransomware* yang meluas sehingga memerlukan keahlian teknis siber yang baik dalam penanganannya. Sedangkan pihak kepolisian di Inggris Raya memiliki tanggungjawab atas penegakan hukum di wilayah masing-masing dan berperan dalam menangani kasus kejahatan di tingkat regional, baik kejahatan yang menyerang individu, bisnis kecil, atau organisasi lokal. Meskipun begitu, tidak menutup kemungkinan bagi keduanya dalam melakukan koordinasi dalam menghadapi tindak pidana siber yang terjadi di Inggris Raya.

Perbandingan Pelaksanaan Penyidikan Terhadap Tindak Pidana Siber di Indonesia dan Inggris Raya

Peter de Cruz menyatakan bahwa pada saat melakukan kajian perbandingan terdapat delapan tahapan yang perlu diperhatikan (Peter de Cruz, 1999). Pertama, melakukan identifikasi terhadap masalah yang akan diteliti. Kedua, mengidentifikasi hukum asing beserta dengan keluarga hukumnya. Ketiga, menentukan sumber hukum yang relevan. Keempat, mengumpulkan data hukum yang berhubungan. Kelima, mengorganisasikan seluruh data yang telah dikumpulkan berdasarkan dengan kelompoknya dalam perbandingan tersebut. Keenam, melakukan penyusunan jawaban terhadap masalah yang diteliti. Ketujuh, menganalisis secara kritis prinsip hukum berdasarkan dengan maknanya (Ratno Lukito, 2022).

Indonesia dan Inggris Raya merupakan dua negara yang rentan mengalami serangan siber sehingga dapat mengganggu individu yang ada di dalamnya dan mengancam keamanan negara itu sendiri. Pelaksanaan penyidikan terhadap tindak pidana siber di Indonesia dan Inggris Raya memiliki beberapa persamaan meskipun terdapat perbedaan dalam pelaksanaannya. Kedua negara ini memiliki aturan hukum yang mengatur berbagai jenis kejahatan siber, seperti UU ITE milik Indonesia dan *Computer Misuse Act* 1990 milik Inggris Raya. Selain itu, terdapat regulasi lainnya mengenai perlindungan data, yaitu UU Perlindungan Data Pribadi milik Indonesia dan *General Data Protection Regulation* milik Inggris Raya.

Penyidikan tindak pidana siber di Indonesia dan Inggris Raya memanfaatkan forensik digital untuk mengumpulkan, menganalisis, dan mengamankan alat bukti elektronik dengan menggunakan perangkat lunak dan perangkat keras yang digunakan untuk memeriksa sistem komputer atau sistem jaringan terdampak. Penyidik dalam menangani tindak pidana siber memiliki tantangan dalam menghadapi jenis kejahatan siber yang terus berkembang. Maka dari

itu, penyidik perlu memiliki keterampilan dalam menangani kasus-kasus tindak pidana siber dengan didukung oleh pelatihan khusus berkenaan dengan forensik digital seperti pelatihan *Computer Hacking Forensics Investigator* (CHFI).

Kemudian terdapat perbedaan mengenai lembaga penegak hukum yang melakukan penyelidikan dan penyidikan terhadap tindak pidana siber di Indonesia dan Inggris Raya. Pelaksanaan penyidikan di Indonesia dilakukan dengan melibatkan beberapa instansi yang memiliki perannya masing-masing di bawah koordinasi lembaga penegak hukum, yakni pihak kepolisian khususnya pada Direktorat Tindak Pidana Siber dalam menanggulangi dan mengatasi banyaknya tindak pidana siber di Indonesia.

Sedangkan di Inggris Raya, tindak pidana siber ditangani oleh beberapa lembaga penegak hukum, seperti NCA yang memiliki unit khusus untuk menangani kejahatan siber bernama *National Cyber Crime Unit* (NCCU) dan kepolisian daerah (*police forces*) yang memiliki unit kejahatan sibernya tersendiri dalam menangani tindak pidana siber di tingkat lokal. NCCU yang merupakan bagian dari NCA memimpin Inggris Raya dalam melakukan perlawanan terhadap kejahatan yang terjadi di dunia siber.

NCCU memiliki kemampuan untuk memimpin respon terhadap ancaman siber prioritas, termasuk penjahat elit dan "ikonis tak tersentuh", serta bekerjasama dengan mitra di Inggris Raya dan luar negeri untuk merespons dengan kecepatan dan skala terhadap insiden siber kritis. Kemudian NCCU dapat memberikan dukungan serta mengkoordinasikan respon dalam pelaksanaan penegakan hukum terhadap tindak pidana siber secara berkelanjutan.

Berdasarkan pemaparan sebelumnya, pencegahan risiko tindak pidana siber yang meluas dapat dilakukan melalui perbaikan dan penyempurnaan respon dalam penanganannya. Pemberian kewenangan penyidikan kepada suatu instansi di Indonesia yang memiliki keahlian khusus untuk menghadapi tindak pidana siber yang mengancam keamanan negara, memiliki

dampak yang meluas dan bersifat sangat merugikan merupakan hal yang dapat dipertimbangkan dengan melihat pelaksanaan penyidikan terhadap tindak pidana siber di Inggris Raya. Akan tetapi, dalam pertimbangan tersebut perlu memperhatikan pula mengenai pengaturan hukum positif, koordinasi, serta kerjasama antara penegak hukum atau instansi terkait yang ada di Indonesia agar tidak menimbulkan kebingungan.

Penyesuaian aturan dan koordinasi antara penegak hukum serta instansi di luar penegak hukum dalam gerakannya perlu dilakukan agar tercapainya tujuan resosialisasi dengan harapan agar para pelaku menyadari bahwa perbuatannya tidak dibenarkan oleh hukum sehingga pelaku tersebut diharapkan tidak melakukan kejahatannya kembali agar terciptanya rasa aman di dalam kehidupan Masyarakat sehingga penegakan hukum terhadap tindak pidana siber dapat berjalan secara responsif dan efektif.

SIMPULAN

Terdapat faktor pembeda dari proses penyidikan terhadap tindak pidana siber di Indonesia dan Inggris Raya. Proses penyidikan tindak pidana siber di Indonesia dilakukan oleh penyidik kepolisian sebagai penegak hukum. Namun, karena sifat dari tindak pidana siber yang dinamis dan memiliki sarana yang mudah diubah menjadi suatu kendala sehingga diperlukan Pejabat PPNS yang memiliki keahlian untuk mendeteksi serangan siber yang dapat membahayakan keamanan negara. Sedangkan di Inggris Raya pihak kepolisian berfokus pada tindak pidana siber dalam lingkup regional yang berdampak pada masyarakat setempat dan memiliki penegak hukum lainnya yang berperan dalam mengatasi tindak pidana siber dalam lingkup yang lebih luas serta dapat membahayakan keamanan negara, seperti NCA. Meskipun begitu, antara kepolisian dan NCA tetap dapat melakukan koordinasi khususnya pada saat menangani kasus tindak pidana siber yang kompleks.

DAFTAR PUSTAKA

- A. Aco Agus dan Riskawati, (2016), "Penanganan Kasus CyberCrime di Kota Makassar (Studi Pada Kantor Kepolisian Resort Kota Besar Makassar)", Jurnal Supremasi, XI(1).
- Adam Clark, "Cybersecurity in the UK", House of Commons Library, 2024.
- Ade Kurniawan, "Polisi dan BSSN Mulai Penyelidikan Kasus Serangan Kelompok Hacker ke Sistem Bank Syariah Indonesia", diakses pada tanggal 25 September 2023 pukul 13.11, <https://www.tvonenews.com/berita/nasional/123699-polisi-dan-bssn-mulai-penyelidikan-kasus-serangan-kelompok-hacker-ke-sistem-bank-syariah-indonesia?page=1>
- Alief Tanding Pamungkas, dkk, (2024), "Krisis Penegakan Hukum Cybercrime di Indonesia: Hambatan dan Jalan Keluar", Delictum: Jurnal Hukum Pidana dan Hukum Pidana Islam, 2(2).
- Apryan Anggara dan Ruhly Kesuma, (2023), "Hacker Bjorka: Pihak yang Berperan dalam Mencegah Kebocoran Data", Jurnal Hukum Magnum Opus, 6(1).
- Bill Clinton dan Yudha Pratomo, "Kasus Data Bocor di Indonesia Sepanjang 2022, dari PLN, Pertamina, hingga Aksi Bjorka", (Kompas.com, 29 Desember 2022), diakses pada 20 April 2024 pukul 15.56, <https://tekno.kompas.com/read/2022/12/29/09020067/kasus-data-bocor-di-indonesia-sepanjang-2022-dari-pln-pertamina-hingga-aksi?page=all>
- CNN Indonesia, "BSSN Buka Suara soal Bjorka yang Belum Juga Tertangkap", (ccnindonesia.com, 19 Januari 2023), diakses pada tanggal 25 September 2023 pukul 12.33, <https://www.cnnindonesia.com/teknologi/20230119153931-192-902611/bssn-buka-suara-soal-bjorka-yang-belum-juga-tertangkap>
- Dikdik dan Elisatris Gultom, *Cyber Law Aspek Hukum Teknologi Informasi*, Bandung: Refika Aditama, 2009.
- Direktorat Operasi Keamanan Siber, "Lanskap Keamanan Siber Indonesia 2023", diakses pada 4 April 2024 pukul 22.12, hlm. 14, <https://www.bssn.go.id/wp-content/uploads/2024/03/Lanskap-Keamanaan-Siber-Indonesia-2023.pdf>
- Dwi Shinta, dkk, (2024), "Dampak Cyber Crime Terhadap Keamanan Nasional dan Strategi Penanggulangannya: Ditinjau Dari Penegakan Hukum", Jurnal Bevinding, 2(1).
- Hreeloita Dharma Shanti, "BSSN siap lakukan koordinasi kasus kebocoran data pinjol bersama Polri", (antaranews.com, 24 Oktober 2023), diakses pada tanggal 25 Oktober 2023 pukul

- 14.19,
<https://www.antaranews.com/berita/3789801/bssn-siap-lakukan-koordinasi-kasus-kebocoran-data-pinjol-bersama-polri>
- Iskandar, "Mengenal Ransomware LockBit, Kelompok Hacker Paling Ganas yang Curi 1,5 TB Data BSI", (liputan6.com, 14 Januari 2024), diakses pada tanggal 21 April 2024 pukul 19.11, <https://www.liputan6.com/tekno/read/5285489/mengenal-ransomware-lockbit-kelompok-hacker-paling-ganas-yang-curi-15-tb-data-bsi?page=4>
- Jakub Wołyńiec, (2018), "The UK Government's response To Cyber Threats", *Teka of Political Science and International Relations*, 13(2).
- Joanna Curtis and Gavin Oxburgh, (2023), "Understanding cybercrime in 'real world' policing and law enforcement", *The Police Journal: Theory, Practice and Principles* 2023, 96(4).
- Juraj Sikra, Karen V. Renaud, and Daniel R. Thomas, (2023), "UK Cybercrime, Victims and Reporting: A Systematic Review", *Commonwealth Cybercrime Journal*, 1(1).
- Lee Hadlington, et al., (2018), "A Qualitative Exploration of Police Officers' Experiences, Challenges, and Perceptions of Cybercrime", *Policing*, 15(1).
- Maria Rosari, "BSSN lakukan forensik digital dalam dugaan kebocoran data KPU", (antaranews.com, 1 Desember 2023), diakses pada tanggal 11 Januari 2023 pukul 15.59, <https://www.antaranews.com/berita/3849831/bssn-lakukan-forensik-digital-dalam-dugaan-kebocoran-data-kpu>
- Maskun, *Kejahatan Siber (Cyber Crime) Suatu Pengantar*, Jakarta: Prenada Media Group, 2013.
- Muladi, *Kapita Selekta Sistem Peradilan Pidana*, Semarang: Badan Penerbit Universitas Diponegoro, 2018.
- Nyoman Amie Sandrawati, (2022), "Antisipasi Cybercrime dan Kesenjangan Digital dalam Penerapan TIK di KPU", *Jurnal Tata Kelola Pemilu Indonesia*, 3(2).
- Peter de Cruz, *Comparative Law in a Changing World*. London dan Sydney: Cavendish Publishing Limited edisi dua, 1999.
- Peraturan Presiden Nomor 28 Tahun 2021 tentang Badan Siber dan Sandi Negara.
- Ratno Lukito, "Compare But Not to Compare": Kajian Perbandingan Hukum di Indonesia", *Jurnal Undang: Jurnal Hukum*, 5(2).
- Rian Dwi Hapsari dan Kuncoro Galih, (2023), "Ancaman Cybercrime di Indonesia sebuah tinjauan Pustaka Sistematis", *Jurnal Konstituen*, 5(1).
- Sahat Maruli, *CYBER LAW*, Bandung: Cakra, 2020.
- Soerjono Soekanto dan Sri Mamudji, *Penelitian Hukum Normatif: Suatu Tinjauan Singkat*, Jakarta: Rajawali Pers, 2015.
- Tribrata News, "Polri: Kasus Kejahatan Siber di 2023 Turun hingga 1.075 Perkara dari 2022", (Tribratane.ws.polri.go.id, 27 Desember 2023), diakses pada 8 September 2024 pukul 18.24, <https://tribratane.ws.sulut.polri.go.id/polri-kasus-kejahatan-siber-di-2023-turun-hingga-1-075-perkara-dari-2022/>
- Yahya Harahap, *Pembahasan Permasalahan dan Penerapan KUHAP Penyidikan dan Penuntutan (Edisi Kedua)*, Jakarta: Sinar Grafika, 2014.