Proceedings Series on Social Sciences & Humanities, Volume 23
Proceedings of Seminar Nasional Kebaharuan KUHP Nasional dan Urgensi Pembaharuan KUHAP
ISSN: 2808-103X

Sistem Pembuktian Terbalik Berbasis Inovasi Teknologi dalam KUHAP untuk Penanganan Kejahatan Siber

Petrus Richard Sianturi
Fakultas Hukum, Universitas Katolik Darma Cendika

ARTICLE INFO

Article history:

DOI:
10.30595/pssh.v23i.1551

Submited:
Feb 21, 2025

Accepted:
May 20, 2025

Published:
June 11, 2025

Keywords:

Kejahatan Siber; Sistem Bukti; Inovasi Teknologi

ABSTRACT

Perkembangan teknologi memunculkan fenomena kejahatan siber yang hingga saat ini sangat masif terjadi. Kejahatan siber telah berkembang dalam beragam jenis. Kecanggihan teknologi memungkinkan kejahatan siber dilakukan dengan beragam alat dan cara, sehingga sulit untuk dilakukan penanganannya dalam logika sistem pembuktian konvesional sebagaimana saat ini berlaku. Penelitian ini menjelaskan bagaimana sistem pembuktian negatif tidak dapat digunakan untuk penegakan hukum yang efektif atas kejahatan siber dan sekaligus menjelaskan bagaimana sistem pembuktian terbalik perlu dimaksimalkan dalam pengaturannya pada hukum acara pidana di Indonesia. Penelitian ini menemukan potensi diberlakukannya sistem pembuktian terbalik tanpa mengurangi perlindungan atas hak-hak terduga pelaku atau terdakwa dengan syarat integrasi proses penegakan hukum dengan sistem teknologi itu sendiri. Penelitian ini berkesimpulan bahwa proses penegakan hukum perlu mempertimbangkan penguatan kapasitas tekonologi pada kepolisian and kejaksaan serta penggunaan teknik pembuktian forensik digital dengan beragam jenis dan bentuknya. Penelitian ini juga mengusulkan bahwa pengaturan mengenai sistem pembuktian terbalik perlu diatur dalam KUHAP mendatang.

This work is licensed under a Creative Commons Attribution 4.0 International License.

Corresponding Author:
Petrus Richard Sianturi
Universitas Katolik Darma Cendika
Jl. Dr. Ir. H. Soekarno No.201, Klampis Ngasem, Kec. Sukolilo, Surabaya, Jawa Timur 60117
Email: richardsianturi@ukdc.ac.id

1. PENDAHULUAN

Perkembangan dan masifnya pertumbuhan teknologi dalam ruang siber (*cyberspace*) dua dekade terakhir memunculkan fenomena kejahatan siber (*cybercrime*) yang luas. Ruang siber ini terdiri dari beragam inovasi perangkat keras (*hardware*) hingga perangkat lunak (*software*) yang khususnya terhubung dengan komputer dan jaringan internet.[1] Sistem teknologi yang termanifestasi dalam perangkat seperti komputer dan internet memunculkan fenomena yang disebut sebagai kejahatan siber kontemporer (*contemporary cybercrime*).[2] Europol, lembaga di Uni-Eropa yang bertugas untuk melakukan upaya pencegahan dan penindakan pada kejahatan-kejahatan terorganisasi, kejahatan siber dan terorisme, menyebutkan 10 jenis kejahatan siber, di

[1] Kejahatan siber yang dimaksudkan dalam bagian ini mengarah pada pengertian dua inovasi teknologi tersebut. UNODC, "Comprehensive Study on Cybercrime", *Laporan, Februari 2013*, (United Nations: New York, 2013), hlm. 5-6.
[2] *Ibid*., hlm. 5.

antaranya *adware, backdoor/remote-access trojan (RAT), botnet, file infector, ransomware, scareware, spyware, rootkit, trojan* dan *worm*.[3] Dalam laporannya yang lain, Europol membagi bentuk kejahatan siber menjadi *ransomware* dan *malware, fraud involving non-cash payments* dan *online trade in child sexual exploitation material*.[4]

Di Indonesia, Direktorat Tindak Pidana Siber (Dittipidsiber) Bareskrim Polri mengelompokan dua jenis kejahatan: *computer crime* yang terdiri dari peretasan sistem elektronik (*hacking*), intersepsi atau penyadapan ilegal (*illegal interception*), pengubahan tampilan situs web (*web defacement*), gangguan sistem (*system interference*) dan manipulasi data (*data manipulation*) dan *computer-related crime* yang terdiri dari pornografi dalam jaringan (*online pornography*), perjudian dalam jaringan (*online gamble*), pencemaran nama baik (*online defamation*), pemerasan dalam jaringan (*online extortion*), penipuan dalam jaringan (*online fraud*), ujaran kebencian (online *hate speech*), pengancaman dalam jaringan (*online threat*), akses illegal (*illegal access*), serta pencurian data (*data theft*).[5]

Berdasarkan data kepolisian sepanjang tahun 2023 saja, tercatat sebanyak 3758 kasus kejahatan siber yang ditangani, meliputi kejahatan terkait penipuan, akses ilegal, perjudian hingga pencemaran nama baik. Data lainnya dari Badan Siber dan Sandi Negara (BSSN) memperlihatkan adanya 349 juta lebih anomali trafik akibat *malware, exploit, trojan, ifo leak* dan *info gathering* selama Januari-November 2023 dengan potensi kerugian triliunan rupiah. BSSN juga mencatat adanya sekitar 74 juta anomali trafik selama Januari-Mei 2024 dengan dominasi aktivitas *malware*.[6] Data kepolisian ini dapat menjadi "gambaran kecil" masifnya kejahatan siber yang terjadi di Indonesia sebagaimana data dari *National Cyber Security Index* (NCSI) tahun 2023 yang menempatkan Indonesia pada peringkat 49 dari 176 negara paling tidak aman atas serangan siber khususnya terkait keamanan data.[7]

Munculnya beragam modus kejahatan siber diperkirakan akan terus berkembang karena teknologi itu sendiri masih terus berkembang. Analisis Furnell berdasarkan kerangka historis dan sifat kejahatan memperlihatkan bahwa ada keterkaitan modus kejahatan siber yang berkembang sejak awal hingga saat ini.[8] Dalam hal ini Furnell menegaskan bahwa pemahaman tentang gambaran kejahatan siber saat ini termasuk skala dan sifatnya memerlukan konteks yang lebih luar yaitu trend kejahatan yang dilihat secara historis.[9] Masalahnya, jika modus kejahatan siber terus berkembang sementara regulasi pengaturannya tidak berkembang, kejahatan siber itu tidak akan dapat diatasi secara memadai. Selain perlunya perubahan dari organisasi penegakan hukum seperti polisi, substansi pengaturan juga perlu dilakukan baik dalam konteks rumusan kejahatan sebagai sebuah tindak pidana maupun pengaturan mengenai sistem pembuktiannya.

Sistem pembuktian sangat penting mengingat, sebagaimana dicatat oleh Goodison, Davis, dan Jackson, "beberapa teknologi internet telah dirancang khusus untuk memungkinkan penyembunyian identitas dan lokasi individu yang sedang mengakses atau berbagi informasi."[10] Di samping itu, kejahatan siber dalam segala bentuk barunya telah memunculkan pola perilaku dan karakter pelaku kejahatan[11], objek kejahatan hingga beragam

[3] Penjelasan terhadap bentuk-bentuk kejahatan ini ada pada bagian lain penelitian ini. dikutip dari laman: https://www.europol.europa.eu/crime-areas-and-statistics/crime-areas/cybercrime/high-tech-crime, diakses pada 14 Februari 2025.

[4] EUROPOL, "Crime in the age of technology", *Laporan, 12 Oktober 2023*, The Hague, hlm. 4.

[5] *Computer crime* adalah kelompok kejahatan siber yang menggunakan komputer sebagai alat utama, sedangkan *Computer-related crime* adalah kejahatan siber yang menggunakan komputer sebagai alat bantu. Tentang Kejahatan Siber, dikutip dari laman: www.patrolisiber.id diakses pada 12 Februari 2025.

[6] Agustinus Yoga Primantoro, Potensi Risiko Kejahatan Siber 2024 Makin Kompleks, dikutip dari laman: https://www.kompas.id/baca/ekonomi/2024/01/08/potensi-risiko-kejahatan-siber-masih-berlanjut-pada-2024 diakses pada 12 Februari 2025.

[7] Data Jumlah Serangan Cyber di Indonesia Tahun 2023, dikutip dari laman: https://widyasecurity.com/2024/02/02/data-jumlah-serangan-cyber-di-indonesia-tahun-2023/, diakses pada 12 Februari 2025.

[8] SM Furnell, "Cybercrime: A potrait of the landscape", *Journal of Criminological Research, Policy and Practice, 28 Februari 2019*, University of Plymouth, hlm. 3-5.

[9] *Ibid*.

[10] Sean E. Goodison, dkk, *Digital Evidence and the U.S. Criminal Justice System: Identifying Technology and Other Needs to More Effectively Acquire and Utilize Digital Evidence*, (Priority Criminal Justice Inititive, 2015), hlm. 4.

[11] Mike McGuire & Samantha Dowling, "Cyber Crime: A Review of the Evidence (Chapter 1: Cyber-dependent Crimes)", *Laporan, Oktober 2013*, (United Kingdom: Home Office, 2013), hlm. 23-27.

pola penciptaan korban dengan modus yang sama sekali baru[12], sebagaimana telah disinggung sebelumnya. Kejahatan siber, dalam perkembangannya sampai saat ini, merupakan tantangan tersendiri bagi sistem pembuktian pidana konvensional.[13]

Penelitian ini fokus pada pembahasan mengenai kejahatan siber dan sistem pembuktian terbalik serta inovasi teknologi yang dapat membantu implementasinya. Ini membedakan pada fokus beberapa penelitian yang disertakan dalam penelitian ini Penelitian ini akan melakukan eksplorasi ilmiah dalam kerangka menemukan dan membangun korelasi positif antara beragam bentuk kejahatan siber dengan penguatan sistem pembuktian dalam sistem peradilan pidana Indonesia.

Rumusan Masalah

1. Apa saja kelemahan aturan sistem pembuktian negatif di Indonesia menghadapi beragam bentuk modus baru kejahatan siber?
2. Bagaimana pengaturan sistem pembuktian terbalik dalam kejahatan siber?

2. METODE PENELITIAN

Kejahatan siber sebagai fenomena pelanggaran hukum tidak bisa dilepaskan dari fakta adanya perkembangan dan perubahan dalam masyarakat itu sendiri. Begitu juga sistem pembuktian atas kejahatan siber yang tidak mungkin dilepaskan dari fakta perkembangan kejahatan itu sendiri. Dalam konteks demikian, untuk mendapatkan hasil penelitian yang lebih komprehensif, maka penelitian ini akan menggunakan metode penelitian hukum doktrinal dengan pendekatan deskriptif-analitis. Kajian dilakukan pada bahan-bahan hukum yang digunakan antara lain, namun tidak terbatas pada Kitab Undang-Undang Hukum Pidana; Undang-undang Nomor 8 Tahun 1981 tentang Hukum Acara Pidana; Putusan Mahkamah Konstitusi No. 20/PUU-XIV/2016; Putusan-putusan pengadilan; *Convention on Cybercrime* 2004 dan aturan lainnya yang terkait.

3. HASIL DAN PEMBAHASAN

3.1 Kelemahan Sistem Pembuktian Negatif

Dasar hukum sistem pembuktian tindak pidana di Indonesia diatur dalam KUHAP yang menggunakan parameter hukum berbasis bukti secara negatif (*negatief wettelijk bewijstheorie*).[14] Pasal 183 KUHAP mengatur, "Hakim tidak boleh menghukum seseorang kecuali dia memiliki sekurang-kurangnya dua alat bukti yang sah untuk meyakini bahwa suatu tindak pidana telah terjadi dan bahwa terdakwa bersalah melakukannya."[15] Masalahnya, bukti-bukti dalam kejahatan siber bersifat digital, apakah dalam bentuk algoritma dan rumus ataupun data berbasis *cloud* yang sangat sulit jika dibuktikan melalui sistem pembuktian negatif ini, karena penguasaan bukti itu sendiri praktis ada para pelaku.[16]

Dalam konteks alat bukti, pasal 184 KUHAP mengatur tentang lima alat bukti yang sah, yaitu keterangan saksi, keterangan ahli, surat, petunjuk dan keterangan terdakwa.[17] Dalam teori pembuktian, batasan pengaturan jenis alat bukti adalah dalam parameter alat bukti mana yang dapat digunakan dalam pembuktian suatu perkara hukum (*bewijsmiddelen*). Kemudian, tentang bagaimana proses peradilan memperoleh alat bukti untuk

---

[12] Temuan Fawn T. Ngo dari University of South Florida-Sarasota/Manatee mengemukakan bahwa dalam perkembangan saat ini penanganan korban akibat kejahatan teknologi tidak serta merta terkait faktor individu dan situasional semata. Fawn T. Ngo, "Cybercrime Victimization: An Examination of Individual and Situational Level Factors", *International Journal of Cyber Criminology, Vol 5 Edisi 1 Januari-Juli 2011*, hlm. 776-777.

[13] Paparan oleh Ye Hong dan William Neilson bisa memberikan penjelasan mengenai awal mula kejahatan siber berkembang, pola pelaku kriminal termasuk cara penanganannya. Ye Hong & William Neilson, "Cybercrime and Punishment", *Journal of Legal Studies, Vol. 49, No. 2, Juni 2020*, hlm. 432-434.

[14] Dalam teori hukum pembuktian dikenal empat teori yaitu, pembuktian berdasarkan hukum secara positif (*positief wettelijk bewijstheorie*), pembuktian berdasarkan keyakinan hakim (*conviction intime*), pembuktian berdasarkan keyakinan hakim melalui penalaran yang logis (*la raison rasionnee*) dan pembuktian berdasarkan hukum secara negatif (*negatief wettelijk bewijstheorie*). Bandingkan Eddy OS Hiariej, *Teori dan Hukum Pembuktian*, (Jakarta: Penerbit Erlangga, 2012), hlm. 15-27 dan Andi Hamzah, *Hukum Acara Pidana Indonesia*, (Jakarta: Sinar Grafika, 2017), hlm. 251-257.

[15] Pasal 183 Kitab Undang-Undang Hukum Acara Pidana.

[16] Bukti dalam kejahatan siber umumnya disebut sebagai *electronic evidence* atau *digital evidence*. Yanbo Wu, dkk, "Research on Investigation and Evidence Collection of Cybercrime Cases", *Journal of Physics: Conference Series, 1176, 2019*, hlm. 5.

[17] Dijelaskan bahwa dalam perkembangan terkait kejahatan banyak terjadi perubahan dan memperluas pengertian "sesuatu" sebagai alat bukti. Eddy OS Hiariej menyatakan dua hukum positif terkait masalah ini; UU dan Informasi Anti Terorisme, UU Transaksi Elektronik. Eddy OS Hiariej, *ibid*, hlm. 19-20.

membuktikan suatu perkara hukum. Penekanan yang diperlukan adalah pembuktian diperoleh dengan tidak mengabaikan kepatuhan terhadap hukum, termasuk cara-cara yang dalam proses sistem hukum yang semestinya tidak melanggar peraturan, hukum umum, dan hak asasi manusia. Parameter ketiga ini disebut *bewijsvoering*.

Selanjutnya, mengenai kekuatan pembuktian masing-masing alat bukti (*bewijskracht*), yang dalam hukum acara pidana memiliki derajat yang sama. Namun perlu ditekankan bahwa dalam beberapa aturan, suatu alat bukti hanya boleh menjadi pelengkap alat bukti yang lain. Terkaity dengan itu, diperlukan alat bukti sekurang-kurangnya dua irisan yang cukup disertai dengan keyakinan hakim yang dalam teori pembuktian disebut *bewijsminimum*. Hal ini juga terkait dengan pasal 183 KUHAP, namun *bewijsminimum* yang ditekankan adalah kebebasan hakim terikat pada minimal dua alat bukti. Lalu, tentang beban pembuktian (*bewijslast*, Inggris: *burden of proof*). Dalam pembuktian secara umum, hukum menerapkan asas *actori incumbit probatio* (siapa yang mendalilkan, membuktikan).[18] Dengan begitu, dalam SPP Indonesia, penuntut umum memiliki beban pembuktian ketika suatu perkara pidana diproses.

Oleh karena itu, di Indonesia, alat bukti berupa surat dan dokumen elektronik memang dapat dijadikan sebagai alat bukti dalam penanganan perkara pidana[19], namun belum secara komprehensif digunakan sebagai regulasi yang terintegrasi. Selain itu, belum ada aturan tentang alat bukti elektronik yang merinci dengan jelas bentuk surat elektronik apa saja yang dapat dijadikan alat bukti. Brown menegaskan bahwa pengaturan yang lebih memadai tentang informasi digital sebagai alat bukti digital, forensik digital dalam verifikasi dan pemeriksaan untuk mengakses data digital mengenai pembutkian kasus-kasus kejahatan siber sangat diperlukan.[20]

Keberadaan alat bukti elektronik dalam sistem peradilan pidana dalam konteks kejahatan siber sangat menentukan dapat atau tidaknya suatu kasus kejahatan siber diselesaikan. Untuk itu diperlukan pengaturan mengenai aturan mengenai informasi digital sebagai alat bukti digital, forensik digital dalam verifikasi dan pemeriksaan untuk mengakses data digital mengenai pembuktian kasus-kasus kejahatan teknologi.[21] Untuk yang terakhir yaitu akses terhadap data digital yang dapat diduga terkait dengan terjadinya kejahatan digital, tetap diperlukan kehati-hatian khususnya untuk memastikan bahwa privasi dan hak asasi manusia tidak dilanggar sebagaimana mestinya. Untuk itu, penelitian ini melihat potensi pemberlakuan sistem pembuktian terbalik (*reversal burden of proof*)[22] yang sudah jamak diterapkan dalam beberapa tindak pidana, termasuk tindak pidana korupsi.[23]

3.2 Sistem Pembuktian Terbalik dan Bantuan Inovasi Digital

Pembuktian terbalik adalah kontra dari sistem pembuktian negatif sebagaimana sudah dijelaskan. Beban untuk membuktikan suatu tindak pidana itu terjadi tidak terletak pada terduga pelaku atau terdakwa sendiri dan harus membuktikan bahwa dirinya tidak bersalah sebagaimana dituduhkan atau didakwakan.[24] Penelitian ini melihat kemungkinan bahwa penyidik dan penuntut umum dapat menguasai terlebih dahulu barang atau alat atau hal lain yang diduga kuat menjadi bukti dalam sebuah kejahatan siber, karena dalam kejahatan siber, bukti sangat sulit diidentifikasi dan mudah berubah atau diubah. Setelah penguasaan ini dilakukan, selanjutnya dalam hal pembuktian, terdakwa wajib membuktikan sebaliknya melalui berbagai mekanisme.

---

[18] Atau "siapa yang menuntut, membuktikan". Baca selengkapnya Eddy OS Hiariej, *ibid*, hlm. 23.

[19] Putusan Mahkamah Konstitusi Nomor 20/PUU-XIV/2016.

[20] Mengenai *digital forensic to forensic capacity*, pembahasannya didasarkan pada United Nations Office on Drugs and Crime, *Op.Cit*, 2013, hlm. 159-164. Bandingkan dengan Cameron SD Brown, "Investigating and Prosecuting Cyber Crime: Forensic Dependencies and Barriers to Justice", *International Journal of Cyber Criminology, Vol 9 Edisi 1, Januari-Juni 2015*, hlm. 64-69.

[21] *Ibid*.

[22] Terdapat perbedaan penerjemahan istilah *reversal burden of proof* di beberapa literatur Indonesia. Sebagian menggunakan "pembalikan beban pembuktian" dan sebagian menggunakan "pembuktian terbalik". Awalnya peneliti menggunakan istilah "pembalikan beban pembuktian", namun dalam penelitian ini, peneliti menggunakan istilah "pembuktian terbalik", mengingat teknis dan kemudahan untuk memahaminya.

[23] Petrus Richard Sianturi, "Pembalikan Beban Pembuktian Sebagai Primum Remedium Dalam Upaya Pengembalian Aset Negara Pada Kasus Tindak Pidana Korupsi", *Simbur Cahaya, Vol. 27, No. 1, Juni 2020*, hlm. 33.

[24] Hal ini bertentangan dengan sistem pembuktian negatif sebagaimana KUHAP atur saat ini, termasuk yang pada umumnya diatur oleh banyak sistem hukum termasuk sistem *common law*. Dalam sistem *common law*, dalam hal terdakwa ingin mengajukan bukti, hal itu hanya akan dipertimbangkan sebagai pelengkap dari konsep pembelaan afirmatif (*affirmative defense*). Jefferson, L. Ingram, *Criminal Evidence (11th Ed)*, (Massachusetts: Anderson Publishing, 2012), hlm. 61.

Pengaturan pembuktian terbalik pertama kali diatur dalam pasal 5 ayat (7) Konvensi PBB tentang Pemberantasan Peredaran Gelap Narkotika dan Psikotropika tahun 1988, kemudian diikuti pengaturan dalam pasal 12 ayat (7) Konvensi PBB Menentang Tindak Pidana Transnasional yang Terorganisasi (UNTOC) tahun 2000 dan pasal 31 ayat (8) Konvensi PBB Anti-Korupsi (UNCAC) tahun 2003.[25] Sedangkan di Indonesia, meskipun belum diatur dalam KUHAP, pembuktian terbalik sudah pernah muncul dalam pembahasan tentang perubahan Undang-Undang No. 31 tahun 1971 tentang Pemberantasan Tindak Pidana Korupsi.

Dalam konsep pembuktian terbalik, hal yang paling pokok untuk perlu diperhatikan adalah prinsip hak asasi manusia (*human rights*), penerapan asas praduga tidak bersalah (*presumption of innocent*) dan hak untuk tidak menyalahkan dirinya sendiri (*non-self incrimination*). Tiga hal ini sangat prinsipil dalam penegakan hukum pidana demi menjaga hak-hak terdakwa tidak dilanggar oleh karena sebuah proses penegakan hukum. Dalam konsep pembuktian terbalik, ketiganya tidak ditempatkan dan dijalankan terlebih dahulu karena memang yang ingin dicapai adalah keamanan alat bukti agar proses penegakan hukum dapat berjalan. Romli menyebutkan perlunya pembuktian terbalik dilakukan dengan merujuk pada teori kemungkinan yang seimbang (*balanced probability theory*)[26], dimana jika barang, benda atau hal lainnya yang dijadikan bukti diperoleh secara sah, maka terdakwa berhak untuk menolak melakukan pembuktian terbalik, dan sebaliknya kepada terdakwa tidak dapat dipersalahkan.

Sistem pembuktian terbalik sendiri menenkankan bahwa terduga pelaku, yang menguasai bukti, harus membuktikan dirinya tidak bersalah melakukan kejahatan, Oleh karena itu, sistem pembuktian terbalik mungkin juga akan menimbulkan masalah tentang prinsip praduga tidak bersalah yang menjadi "roh" hukum acara pidana. Namun pembuktian pada alat bukti digital atau elektronik lainnya tidak efektif jika hanya berdasarkan pada sistem pembuktian negatif. Stoykova menyatakan bahwa alat bukti digital (dalam konteks ini kejahatan siber) memang menjadi tantangan nyata dalam pencapaian keadilan dan penegakan prinsip praduga tidak bersalah.[27] Tiga kategori disampaikan Stoykova dalam kaitannya dengan kemungkinan pada terjadinya ketidakadilan dan pelanggaran prinsip praduga tidak bersalah, yaitu penggunaan teknologi yang tidak pantas dan konsisten, jaminan prosedur yang kadaluawarsa dan pelaksanaan pembuktian yang sulit dipertanggungjawabkan.[28]

Maka, selain perlunya sistem pembuktian terbalik diatur secara positif dalam KUHAP, yang lebih penting adalah mengenai mekanisme yang dapat membantu agar pelaksanaannya dapat berjalan dengan tepat dan sekurang-kurangnya minim pelanggaran pada hak-hak terduga pelaku atau terdakwa. Penelitian ini berupaya menawarkan jalan tengah bahwa sistem pembuktian terbalik dapat dilaksanakan dengan seminim mungkin melanggar prinsip keadilan dan prinsip praduga tidak bersalah tersebut. Pengaturan dalam KUHAP mendatang tentang sistem pembuktian terbalik ini pada dasarnya dapat berlaku kepada beragam bentuk kejahatan atau tindak pidana, khususnya yang terkait dengan perkembangan teknologi. Meskipun penelitian ini membahas urgensi pengaturannya dari sudut pandang terjadinya kejahatan teknologi, namun sejatinya, berdasarkan penjelasan yang ada, beban pembuktian yang diserahkan kepada terdakwa akan membantu proses penegakan hukum yag lebih efektif dan efisien.

Beragam kebijakan hukum pidana Indonesia melalui KUHAP mendatang perlu memadai dalam menanggapi perkembangan kejahatan teknologi. Sistem pembuktian terbalik dalam penanganan kejahatan siber dapat berjalan dengan tepat apabila pertama-tama, aparat penegak hukum juga memadai dalam pengetahuan sistem teknologi itu sendiri.[29] Maka, perlu penataan ulang kapasitas lembaga penegak hukum, seperti kepolisian dan kejaksaan serta pengadilan dalam kerangka pelaksanaan pesidangan dalam jaringan atau *e-justice* (sistem manajemen kasus, *video conference*, animasi komputer dan lingkungan virtual).[30] Penguatan kapasitas ini juga perlu diimbangi dengan perlunya secara lebih sering penggunaan sistem dan algoritma teknologi seperti *artificial intelligence* (AI) dalam sebagian atau keseluruhan proses penanganan kasus. Dalam hal ini, AI dapat berguna untuk penilaian risiko (*risk assesment*), pengenalan wajah (*face recognition*), proses kepolisian yang

[25] Romli Atmasasmita, *Globalisasi dan Kejahatan Bisnis*, (Jakarta: Kencana, 2010), hlm. 66-67.
[26] *Ibid*., hlm. 68.
[27] Radina Stoykova, "Digital Evidence: Unaddressed Threats to Fairness and the Presumption of Innocence", *Computer Law & Security Review, Vol. 42, September 2021*, hlm. 2.
[28] *Ibid*.
[29] Tentu yang dimaksudkan dapat berbentuk kerjasama dengan lembaga yang memiliki kapasitas dalam hal sistem teknologi dan/atau menghadirkan ahli yang relevan.
[30] Argumentasi ini mengikuti Ales Zavrsnik dari Institut Kriminologi, Fakultas Hukum Ljubljana. Petrus Richard Sianturi, "Kejahatan Teknologi, Kebijakan Keamanan Siber dan Pengaruhnya pada Sistem Peradilan Pidana", dalam Tanius Sebastian (Ed.), *Pergulatan Negara Hukum, Ketidakadilan, dan Jati Diri Pengemban Hukum Indonesia (Percikan Gagasan tentang Hukum VI)*, (Bandung: Unpar Press, 2024), hlm. 129-130.

prediktif (*predictive policing*)[31], ekstraksi data (*data extraction*) hingga probabilitas genotip (*probabilistic genotyping*).[32] Kelima inovasi teknologi ini memungkinkan untuk menekan kemungkinan pelanggaran hak asasi manusia kepada terduga pelaku atau terdakwa karena alat bukti yang sudah diamankan lebih dahulu sebagai konsekuensi pemberlakuan sistem pembuktian terbalik dapat lebih cepat dan akurat dilakukan penilaian.

Selain itu, untuk membantu pelaksanaan sistem pembuktian terbalik yang efektif dalam penanganan kejahatan siber, diperlukan penguatan sistem teknologi untuk mekanisme pembuktian forensik atas semua alat bukti digital. Tahapan pembuktian forensik ini dibutuhkan untuk memastikan sekaligus mengonfirmasi mengenai kebenaran adanya korelasi antara alat bukti digital yang diamankan oleh aparat penegak hukum dengan kejahatan atau tindak pidana yang diduga telah terjadi.[33] Ada beragam bentuk teknik forensik yang mungkin dapat digunakan misalnya seperti *digital forensic technologies* (DFT), *genetic identification technologies* (GIT), *voice and audio recognition technologies* (VAR) ataupun *artificial intelligence and data analysis* (AIDT).[34] Contoh ini dapat memperlihatkan bahwa sistem peradilan pidana Indonesia sendiri perlu menyesuaikan lagi pada inovasi-inovasi teknologi yang berkembang. Baik penggunaan AI maupun teknik forensik dalam upaya pembuktian pada alat bukti atas terjadinya suatu kejahatan siber, pada dasarnya dapat membantu aparat penegak hukum dalam mengupayakan reformasi pada sebagian atau seluruh sistem peradilan pidana. Upaya pembaharuan KUHAP perlu mempertimbangkan pengaturan akan hal ini.

4. SIMPULAN

Fenomena kejahatan siber adalah ancaman yang nyata dan sudah terjadi di Indonesia. Masyarakat hanya dapat mengharapkan upaya penindakan yang kuat, selain daripada usaha-usaha pencegahan. Oleh karena itu, dalam kerangka penindakan yang komprehensif dan relevan sesuai dengan karakternya sebagai kejahatan berbasis sistem teknologi, maka sistem pembuktian terbalik perlu dipertimbangkan dan diupayakan masuk dalam suatu aturan pada KUHAP yang akan diperbaharui. Kebijakan untuk memperbaharui KUHAP perlu ditempatkan dalam konteks upaya penanggulangan kejahatan dimana upaya itu juga merupakan bagian dari usaha penegakkan hukum, khususnya penegakkan hukum pidana. Dalam konteks penelitian ini, diharapkan bahwa dengan adanya kebijakan hukum pidana untuk merumuskan sistem pembuktian terbalik, maka penegakan hukum (pidana) atas kejahatan siber semakin kuat dan komprehensif.

DAFTAR PUSTAKA

Agustinus Yoga Primantoro, Potensi Risiko Kejahatan Siber 2024 Makin Kompleks, dikutip dari laman: https://www.kompas.id/baca/ekonomi/2024/01/08/potensi-risiko-kejahatan-siber-masih-berlanjut-pada-2024 diakses pada 12 Februari 2025

Atmasasmita, Romli, *Globalisasi dan Kejahatan Bisnis*. Jakarta: Kencana, 2010.

Brown, Cameron S. D, "Investigating and Prosecuting Cyber Crime: Forensic Dependencies and Barriers to Justice", *International Journal of Cyber Criminology, Vol 9, Issue 1. Januari-Juni 2015.*

Chango, Xavier, dkk, "Technology in Forensic Sciences: Innovation and Precesion", *Technologies, 12, 120, 2024*.

Crime Areas and Statictics, dikutip dari laman: https://www.europol.europa.eu/crime-areas-and-statistics/crime-areas/cybercrime/high-tech-crime, diakses pada 14 Februari 2025.

Data Jumlah Serangan Cyber di Indonesia Tahun 2023, dikutip dari laman: https://widyasecurity.com/2024/02/02/data-jumlah-serangan-cyber-di-indonesia-tahun-2023/, diakses pada 12 Februari 2025.

EUROPOL, Crime in the age of technology, *Laporan*, The Hague, 12 Oktober 2023.

Furnell, SM. "Cyber crime: A potrait of the landscape". *Journal of Criminological Research, Policy and Practice, 28 Februari 2019,* . University of Plymouth.

[31] Sistem pembuktian terbalik dalam penanganan kejahatan siber memang seharusnya diberlakukan sejak tahap awal proses kasus dengan perlunya peran kepolisian dalam penyelidikan dan penyidikan (*preliminary investigation*).
[32] *Ibid*., hlm. 130.
[33] Xavier Chango, dkk, "Technology in Forensic Sciences: Innovation and Precesion", *Technologies, 12, 120, 2024*, hlm. 1.
[34] *Ibid*. hlm. 5.

Goodison, Sean E., dkk, "Digital Evidence and the U.S. Criminal Justice System: Identifying Technology and Other Needs to More Effectively Acquire and Utilize Digital Evidence". *Priority Criminal Justice Inititive*, 2015.

Hamzah, Andi, *Hukum Acara Pidana Indonesia*, Jakarta: Sinar Grafika, 2017.

Hiariej, Eddy OS, *Teori dan Hukum Pembuktian*, Jakarta: Penerbit Erlangga, 2012.

Hong, Ye & William Neilson, "Cybercrime and Punishment", *Journal of Legal Studies. Vol. 49, No. 2, Juni 2020*.

Ingram, Jefferson, L, *Criminal Evidence (11th Ed)*, Massachusetts: Anderson Publishing, 2012.

Kitab Undang-Undang Hukum Acara Pidana.

McGuire, Mike & Samantha Dowling, "Cyber Crime: A Review of the Evidence (Chapter 1: Cyber-dependent Crimes)", *Laporan*, United Kingdom: Home Office United, Oktober 2013.

Ngo, Fawn T., "Cybercrime Victimization: An Examination of Individual and Situational Level Factors", *International Journal of Cyber Criminology, Vol 5 Edisi 1 Januari - Juli 2011*.

Putusan Mahkamah Konstitusi Nomor 20/PUU-XIV/2016.

Sianturi, Petrus Richard, "Pembalikan Beban Pembuktian Sebagai Primum Remedium Dalam Upaya Pengembalian Aset Negara Pada Kasus Tindak Pidana Korupsi", *Simbur Cahaya. Vol. 27, No. 1. Juni 2020*.

Sianturi, Petrus Richard, "Kejahatan Teknologi, Kebijakan Keamanan Siber dan Pengaruhnya pada Sistem Peradilan Pidana", dalam Tanius Sebastian (Ed.), *Pergulatan Negara Hukum, Ketidakadilan, dan Jati Diri Pengemban Hukum Indonesia (Percikan Gagasan tentang Hukum VI)*, Bandung: Unpar Press, 2024.

Stoykova, Radina, "Digital Evidence: Unaddressed Threats to Fairness and the Presumption of Innocence", *Computer Law & Security Review, Vol. 42. September 2021*.

Tentang Kejahatan Siber, dikutip dari laman: www.patrolisiber.id diakses pada 12 Februari 2025.

United Nations Office on Drugs and Crime, *Comprehensive Study on Cybercrime*, New York: United Nations, 2013.

Wu, Yanbo, dkk, "Research on Investigation and Evidence Collection of Cybercrime Cases", *Journal of Physics: Conference Series, 1176, 2019*.

Zavrsnik, Ales, "Criminal Justice System's Intervention to Cybersecurity Threats: Panacea or Pandora's Box?, Institut of Criminology", *Dokumen*, ITU Regional Cybersecurity Forum, Bulgaria: Faculty of Law Ljubljana, 7-9 Oktober 2008.