INNOVATIVE: Journal Of Social Science Research
Volume 4 Nomor 6 Tahun 2024 Page 7048-7056
E-ISSN 2807-4238 and P-ISSN 2807-4246
Website: https://j-innovative.org/index.php/Innovative

Penanganan Dan Tantangan *Cybercrime* Di Era Digital Perspektif Kriminologi

Deri Malian[1]✉
Program Pascasarjana Kriminologi, Universitas Indonesia
Email: deri.malian25@gmail.com[1]✉

Abstrak

Penelitian ini bertujuan untuk mengetahui dan menguji penanganan dan tantangan Cybercrime di era digital persfektif kriminologi. Tantangan yang dihadapi dalam menangani cybercrime atau kejahatan siber telah berkembang menjadi salah satu isu kriminologi yang paling kompleks dan mendesak. Cybercrime mencakup spektrum yang sangat luas dari aktivitas ilegal yang dilakukan melalui atau memanfaatkan teknologi informasi dan komunikasi, seperti peretasan (hacking), phishing, penipuan online, penyebaran malware, ransomware, serta pelanggaran privasi dan pencurian identitas. Penelitian ini menggunakan pendekatan kuantitatif, peneliti dapat mengkaji kasus-kasus nyata dari cybercrime secara rinci,memeriksa berbagai aspek dari bagaimana kejahatan siber terjadi, bagaimana pihak berwenang menangani kasus tersebut, dan tantangan spesifik yang muncul dalam proses penanganan. Dalam perspektif kriminologi, cybercrime di era digital dianalisis sebagai fenomena kompleks yang melibatkan interaksi antara faktor sosial, ekonomi, dan teknologi. Teori Strain dan Kontrol Sosial menjelaskan bahwa tekanan sosial, seperti kesulitan finansial atau ketidakpuasan hidup, dapat memotivasi individu untuk terlibat dalam kejahatan siber sebagai cara untuk mencapai tujuan yang sulit dicapai dengan cara konvensional, sementara kekurangan ikatan sosial dapat meningkatkan risiko terlibat dalam kejahatan.

Kata Kunci: *Cybercrime,Persfektif Kriminologi,Sosial,Ekonomi dan Teknologi*

Abstract

This research aims to understand and examine the handling and challenges of cybercrime in the digital era from a criminological perspective. The challenges faced in addressing cybercrime have evolved into one of the most complex and urgent issues in criminology. Cybercrime encompasses a broad spectrum of illegal activities conducted through or exploiting information and communication technology, such as hacking, phishing, online fraud, malware dissemination, ransomware, as well as privacy violations and identity theft. This study employs a quantitative approach, allowing the researcher to analyze real-life cybercrime cases in detail, examine various aspects of how cybercrime occurs, how authorities handle these cases, and the specific challenges that arise during the handling process. From a criminological perspective, cybercrime in the digital era is analyzed as a complex phenomenon involving interactions between social, economic, and technological factors. Strain Theory and Social Control Theory explain that social pressures, such as financial difficulties or life dissatisfaction, can motivate individuals to engage in cybercrime as a means to achieve goals that are hard to attain through conventional means, while a lack of social bonds can increase the risk of involvement in crime.

Keyword: *Cybercrime, Criminological, Social, Economic and Technological Perspective*

PENDAHULUAN

Perkembangan Internet telah membawa masyarakat ke tingkat evolusi berikutnya. Perkembangan yang sangat pesat ini menjadi boomerang dan tempat kejahatan yang dilakukan oleh orang yang tidak bertanggungjawab sehingga mendorong para kriminolog untuk membahas perlunya suatu disiplin ilmu untuk mempelajari dan menganalisis perilaku kriminal di dunia maya. Kejahatan, perilaku pelaku, dan viktimisasi yang terjadi di dunia maya perlu dipelajari dari sudut pandang ilmu sosial dan bukan dari sudut pandang teknologi. Cyber Criminology adalah bidang multidisiplin yang mencakup peneliti dari berbagai bidang seperti kriminologi, viktimologi, sosiologi, ilmu internet, dan ilmu komputer. Hubungan antara cybercrime dan kriminologi merupakan hubungan yang rumit dan terus berkembang, yang mencerminkan perubahan yang lebih luas dalam teknologi, perilaku kriminal, dan metodologi yang digunakan untuk memahami dan memerangi kejahatan. Cybercrime menjadi bayangan hitam di Indonesia terkait permasalahan yang belum ditangani secara tuntas dikarenakan minimnya pengetahuan dan edukasi terhadap masyarakat. Minimnya pengetahun tersebut menjadi celah kejahatan oleh pelaku criminal tanpa hambatan ruang dan waktu yang mengakibatkan banyaknya korban dikalangan masyarakat. Jika tidak terkendali, kejahatan siber dapat bermutasi menjadi masalah keamanan nasional yang sangat berbahaya dengan konsekuensi yang berpotensi menimbulkan bencana (Bossler, 2019).

Tantangan yang dihadapi dalam menangani cybercrime atau kejahatan siber telah berkembang menjadi salah satu isu kriminologi yang paling kompleks dan mendesak. Cybercrime mencakup spektrum yang sangat luas dari aktivitas ilegal yang dilakukan melalui atau memanfaatkan teknologi informasi dan komunikasi, seperti peretasan (hacking), phishing, penipuan online, penyebaran malware, ransomware, serta pelanggaran privasi dan pencurian identitas. Keberagaman dan evolusi teknik yang digunakan oleh pelaku cybercrime menggarisbawahi betapa dinamis dan sulitnya menangani kejahatan ini. Salah satu tantangan utama dalam kriminologi terkait cybercrime adalah kecepatan dan skala distribusi informasi yang dimungkinkan oleh kemajuan teknologi. Teknologi digital memungkinkan pelaku untuk melakukan serangan secara bersamaan kepada ribuan, bahkan jutaan, target di seluruh dunia. Selain itu, jaringan global dan infrastruktur internet menciptakan lingkungan yang memungkinkan pelaku kejahatan untuk melakukan aktivitas mereka tanpa batasan geografis, yang seringkali mempersulit otoritas hukum dalam mengidentifikasi dan menangkap pelaku. Anonimitas yang ditawarkan oleh internet dan dark web menambah dimensi baru dalam kejahatan siber, di mana pelaku dapat menyembunyikan identitas mereka dan beroperasi dari lokasi yang jauh dari jangkauan hukum local (Dona, 2022).

Dalam perspektif kriminologi, cybercrime di era digital dianalisis sebagai fenomena kompleks yang melibatkan interaksi antara faktor sosial, ekonomi, dan teknologi. Teori Strain dan Kontrol Sosial menjelaskan bahwa tekanan sosial, seperti kesulitan finansial atau ketidakpuasan hidup, dapat memotivasi individu untuk terlibat dalam kejahatan siber sebagai cara untuk mencapai tujuan yang sulit dicapai dengan cara konvensional, sementara kekurangan ikatan sosial dapat meningkatkan risiko terlibat dalam kejahatan. Selain itu, Teori Rasa Keadilan dan Teori Keuntungan menunjukkan bahwa cybercrime sering dilihat sebagai cara untuk memperoleh keuntungan pribadi dengan risiko yang relatif rendah dibandingkan dengan kejahatan konvensional, serta sebagai bentuk balas dendam terhadap ketidakadilan. Kriminologi sibernetika memfokuskan pada bagaimana teknologi memfasilitasi kejahatan dan bagaimana penegakan hukum dapat menanggapi ancaman baru ini, sedangkan pendekatan preventif menekankan perbaikan sistem keamanan, pendidikan, dan kebijakan untuk mengurangi peluang terjadinya kejahatan siber. Dalam konteks global, cybercrime menunjukkan kompleksitas karena sering melibatkan pelaku dan korban lintas negara, menuntut kerjasama internasional dalam penegakan hukum dan kebijakan keamanan. Dengan memahami cybercrime dari berbagai sudut pandang kriminologi, langkah-langkah yang lebih efektif dapat dikembangkan untuk melawan ancaman ini dan melindungi individu serta organisasi dalam dunia digital (Sabillon, 2016).

METODE PENELITIAN

Metode yang digunakan dalam penelitian ini yaitu Kualitatif dengan pendekatan studi kasus karena memungkinkan penelitian mendalam dankontekstual mengenai fenomena cybercrime yang kompleks. Dengan metode ini, peneliti dapat mengkaji kasus-kasus nyata dari cybercrime secara rinci,memeriksa berbagai aspek dari bagaimana kejahatan siber terjadi, bagaimana pihak berwenang menangani kasus tersebut, dan tantangan spesifik yang muncul dalam proses penanganan. Studi kasus menyediakan pandangan yang kaya tentang teknik yang digunakan oleh pelaku kejahatan siber, respons dari lembaga penegak hukum, serta efektivitas dan kelemahan strategi yang diterapkan. Hal ini memungkinkan peneliti untuk menerapkan teori-teori kriminologi secara langsung dalam konteks praktis, mengevaluasi bagaimana motivasi pelaku dan dinamika kasus mempengaruhi penanganan kejahatan. Dengan menganalisis detail-detail dari berbagai kasus, peneliti dapat mengidentifikasi pola-pola, evaluasi kebijakan, dan memberikan rekomendasi berbasis bukti untuk perbaikan. Pendekatan ini juga membantu menghubungkan teori dengan praktik, menjembatani kesenjangan antara penelitian akademis dan aplikasi dunia nyata, serta memberikan wawasan yang berharga bagi pengembangan strategi pencegahan dan penanganan cybercrime yang lebih efektif di era digital.

HASIL DAN PEMBAHASAN

A. Cybercrime perspektif Kriminologi

Cybercrime adalah istilah yang digunakan untuk menggambarkan berbagai bentuk aktivitas kriminal yang dilakukan dengan menggunakan teknologi informasi dan komunikasi, khususnya internet, sebagai alat atau target. Cybercrime mencakup berbagai jenis kejahatan yang dilakukan secara elektronik dan dapat mempengaruhi individu, organisasi, atau negara secara langsung maupun tidak langsung. Cybercrime dari perspektif kriminologi, merujuk pada kejahatan yang dilakukan dengan memanfaatkan teknologi informasi dan komunikasi, khususnya internet, sebagai alat, medium, atau sasaran. Dalam kajian kriminologi, cybercrime dianggap sebagai manifestasi kejahatan yang bertransformasi mengikuti perkembangan teknologi digital. Ini mencakup berbagai jenis kejahatan seperti hacking, di mana pelaku memasuki sistem komputer tanpa izin; penipuan online, yang melibatkan penggunaan internet untuk menipu korban; pencurian identitas, di mana informasi pribadi dicuri dan disalahgunakan; serta penyebaran malware, yang melibatkan pengembangan dan penyebaran perangkat lunak berbahaya dengan tujuan merusak sistem komputer atau mencuri data (Jaishankar K. , 2011).

Dari sudut pandang kriminologi, cybercrime seringkali dipahami melalui teori-teori yang menjelaskan motivasi pelaku dan dinamika kejahatan dalam konteks digital. Teori strain, misalnya, dapat menjelaskan bagaimana individu yang merasa tertekan secara ekonomi atau sosial mungkin mencari cara ilegal, seperti cybercrime, untuk mencapai tujuan mereka. Teori kontrol sosial dan teori rasionalitas juga relevan, dengan memeriksa bagaimana kurangnya pengawasan sosial dan pertimbangan rasional mengenai risiko dan manfaat dapat mempengaruhi keputusan seseorang untuk terlibat dalam aktivitas ilegal di dunia maya (Dupont, 2021).

Aspek penting dari studi kriminologi tentang cybercrime adalah analisis terhadap dampaknya terhadap individu dan masyarakat. Cybercrime tidak hanya merugikan secara finansial tetapi juga dapat menyebabkan trauma psikologis dan merusak kepercayaan dalam sistem digital yang semakin penting dalam kehidupan sehari-hari. Dampak sosial dari cybercrime juga melibatkan kerusakan reputasi dan implikasi hukum bagi pelaku maupun korban (Stratton, 2017).

B. Penanganan Cybercrime di Era Digital Perspektif Kriminologi

Berdasarkan teori kriminologi, penanganan cybercrime dapat dilihat melalui beberapa perspektif yang membantu memahami dan mengatasi kejahatan siber secara efektif. Salah satu teori utama yang relevan adalah Teori Keseimbangan Sosial (Social Control Theory), yang dikembangkan oleh Travis Hirschi. Teori ini menekankan bahwa hubungan sosial yang kuat dan komitmen terhadap norma-norma sosial berfungsi sebagai penghalang terhadap perilaku kriminal. Dalam konteks cybercrime, pendekatan ini mendorong upaya untuk membangun kesadaran dan kepatuhan terhadap norma-norma keamanan siber melalui edukasi dan pelatihan, baik di kalangan individu maupun organisasi. Dengan memperkuat ikatan sosial yang mendukung perilaku aman di dunia maya, risiko terjadinya cybercrime dapat dikurangi (Jaishankar, 2007).

Teori Pembelajaran Sosial (Social Learning Theory), yang dikemukakan oleh Albert Bandura, juga relevan dalam penanganan cybercrime. Teori ini menyatakan bahwa perilaku kriminal dipelajari melalui interaksi dengan individu lain yang terlibat dalam aktivitas tersebut. Oleh karena itu, penting untuk mengidentifikasi dan mengatasi komunitas atau kelompok yang mempromosikan kejahatan siber. Intervensi dapat dilakukan dengan cara mengurangi akses pelaku ke sumber daya atau pengetahuan yang memungkinkan mereka untuk melanjutkan aktivitas kriminal, serta memberikan alternatif yang lebih positif (Phillips, 2022).

Teori Kesempatan Kriminal (Routine Activities Theory), yang dikembangkan oleh Lawrence Cohen dan Marcus Felson, berfokus pada bagaimana peluang kejahatan muncul dari rutinitas sehari-hari dan situasi. Teori ini menekankan bahwa kejahatan terjadi ketika ada peluang yang terbuka dan adanya pelaku yang berniat jahat serta kurangnya pengawasan. Untuk menangani cybercrime berdasarkan teori ini, langkah-langkah pencegahan seperti memperketat kontrol akses ke sistem, meningkatkan pengawasan jaringan, dan mengurangi celah keamanan yang dapat dimanfaatkan oleh pelaku kejahatan merupakan strategi yang efektif.

Teori Strain (Strain Theory), yang diperkenalkan oleh Robert Merton, menganggap bahwa tekanan dan ketidakpuasan terhadap pencapaian tujuan sosial dapat memicu perilaku kriminal. Dalam konteks cybercrime, ini bisa diterjemahkan sebagai frustrasi atau tekanan yang dirasakan oleh individu yang mungkin merasa terpinggirkan atau tidak memiliki akses yang sama dengan orang lain. Untuk mengatasi cybercrime dari sudut pandang ini, penting untuk menangani faktor-faktor sosial dan ekonomi yang dapat berkontribusi pada perilaku tersebut, seperti meningkatkan kesempatan pendidikan dan ekonomi yang setara (Maimon, 2019).

Teori Kontrol Sosial (Social Control Theory) dari Walter Reckless juga relevan, yang membahas bagaimana kekuatan kontrol sosial baik dari luar maupun dalam individu dapat mempengaruhi perilaku kriminal. Dalam konteks cybercrime, kontrol sosial bisa berupa kebijakan perusahaan yang ketat, pengawasan komunitas online, serta penguatan nilai-nilai etika dalam penggunaan teknologi. Dengan memperkuat kontrol sosial baik di tingkat individu maupun institusi, dapat mengurangi kemungkinan terjadinya kejahatan siber.

Secara keseluruhan, pendekatan berbasis teori kriminologi dalam penanganan cybercrime melibatkan pemahaman tentang penyebab dan motivasi di balik perilaku kriminal, serta penerapan strategi yang sesuai untuk mencegah, mendeteksi, dan menanggulangi kejahatan siber secara efektif. Dalam hal penegakan hukum, penanganan cybercrime memerlukan kerjasama antara berbagai pihak, baik di tingkat domestik maupun internasional. Banyak kejahatan siber melibatkan pelaku yang beroperasi lintas batas negara, sehingga kolaborasi antara lembaga penegak hukum, badan intelijen, dan organisasi internasional sangat diperlukan. Program-program kerjasama internasional seperti INTERPOL dan Europol sering kali memainkan peran penting dalam menangani kasus-kasus lintas negara. Teknik forensik digital juga berperan sentral dalam penyelidikan, dengan analis forensik yang terlatih melakukan pemeriksaan mendalam terhadap perangkat keras dan perangkat lunak untuk mengumpulkan bukti yang dapat digunakan di pengadilan (Holt, 2015).

C. Tantangan Cybercrime di Era Digital Perspektif Kriminologi

Dari perspektif kriminologi, memahami motivasi dan perilaku pelaku cybercrime memerlukan pendekatan yang lebih interdisipliner. Pelaku kejahatan siber sering kali memiliki latar belakang yang bervariasi, mulai dari individu dengan keahlian teknis tinggi yang memanfaatkan pengetahuan mereka untuk keuntungan finansial, hingga kelompok terorganisir yang menggunakan cybercrime sebagai alat untuk spionase atau aksi teroris. Psikologi dan sosiologi berperan penting dalam menganalisis faktor-faktor yang mendorong individu untuk terlibat dalam kejahatan ini, seperti faktor ekonomi, sosial, dan psikologis. Misalnya, beberapa pelaku mungkin terinspirasi oleh dorongan ekonomi atau kemarahan terhadap sistem, sementara yang lain mungkin tertarik pada tantangan intelektual atau status sosial yang terkait dengan kemampuan teknis mereka (Tonellotto, 2020).

Selain itu, dampak sosial dari cybercrime sangat luas dan dapat merusak kepercayaan publik terhadap sistem digital yang menjadi bagian penting dari kehidupan sehari-hari. Kasus-kasus pelanggaran data besar-besaran, seperti kebocoran informasi pribadi atau data perusahaan, dapat menimbulkan kerugian finansial yang signifikan dan dampak jangka panjang terhadap reputasi organisasi serta kesejahteraan individu. Perubahan dalam perilaku manusia yang dipengaruhi oleh teknologi digital, seperti kecenderungan untuk berbagi informasi pribadi secara berlebihan di media sosial, juga meningkatkan kerentanan terhadap serangan siber.

Menangani cybercrime memerlukan kerjasama internasional yang efektif, karena banyak kejahatan siber melintasi batas negara dan memerlukan koordinasi antara berbagai lembaga penegak hukum di berbagai negara. Pengembangan teknologi canggih untuk deteksi dan pencegahan serangan siber, serta peningkatan kemampuan investigasi forensik digital, menjadi sangat penting. Selain itu, pendidikan dan kesadaran masyarakat tentang praktik keamanan siber yang baik harus ditingkatkan untuk melindungi individu dan organisasi dari ancaman digital. Pendekatan yang holistik dan kolaboratif ini sangat diperlukan untuk mengatasi tantangan yang kompleks dan terus berkembang dalam dunia kejahatan siber (Miró-Llinares, 2020).

Tantangan dalam Penanganan Cybercrime

1. Anonimitas dan Yurisdiksi

   Anonimitas : Penjahat dunia maya sering kali menggunakan metode canggih untuk menyembunyikan identitas mereka, seperti enkripsi dan web gelap. Dalam masalah yurisdiksi, Cybercrime sering kali melintasi batas negara, mempersulit proses hukum dan koordinasi antara berbagai negara.

2. Kemajuan Teknologi yang Pesat

   Teknologi berkembang lebih cepat daripada kemampuan lembaga penegak hukum untuk beradaptasi, sehingga sulit untuk mengikuti jenis Cybercrime dan taktik baru.

3. Kompleksitas Cybercrime

   Cybercrime mencakup peretasan, phishing, ransomware, pencurian identitas, dan banyak lagi, yang masing-masing memerlukan pendekatan berbeda. Investigasi yang efektif sering kali menuntut pengetahuan yang sangat terspesialisasi dalam teknologi informasi dan keamanan siber.

4. Pengumpulan dan Pelestarian Bukti

   Bukti digital dapat bersifat tidak stabil dan mudah diubah atau dihancurkan. Memastikan integritas bukti digital merupakan tantangan yang signifikan.

5. Keterbatasan Sumber Daya

   Banyak lembaga penegak hukum tidak memiliki sumber daya yang diperlukan, termasuk personel dengan keterampilan khusus dan teknologi canggih, untuk memerangi kejahatan siber secara efektif.

6. Masalah Privasi

   Menyeimbangkan pemberantasan kejahatan yang efektif dengan menghormati privasi dan kebebasan sipil dapat menjadi tantangan, terutama jika pengawasan dan pengumpulan data terlibat.

SIMPULAN

Cybercrime di era digital merupakan fenomena kompleks yang melibatkan berbagai kejahatan berbasis teknologi informasi, seperti hacking, phishing, dan ransomware. Dari perspektif kriminologi, cybercrime dapat dipahami melalui berbagai teori yang menjelaskan motivasi dan perilaku pelaku. Misalnya, Teori Strain menunjukkan bahwa tekanan sosial atau ekonomi dapat mendorong individu untuk terlibat dalam cybercrime sebagai cara untuk mencapai tujuan yang sulit dicapai dengan cara konvensional. Teori Kontrol Sosial menekankan pentingnya ikatan sosial dan norma-norma untuk mencegah perilaku kriminal, sementara Teori Pembelajaran Sosial menjelaskan bagaimana perilaku kriminal dipelajari melalui interaksi dengan individu lain.

Penanganan cybercrime memerlukan pendekatan berbasis teori, termasuk edukasi, pengawasan, dan kerjasama internasional, serta penerapan teknologi forensik digital. Tantangan utama dalam menangani cybercrime meliputi anonimitas pelaku, kemajuan teknologi yang pesat, kompleksitas kejahatan, pengumpulan bukti, keterbatasan sumber daya, dan masalah privasi. Pendekatan yang holistik dan kolaboratif sangat penting untuk

mengatasi ancaman ini secara efektif.

DAFTAR PUSTAKA

Bossler, A. M. (2019). Introduction: new directions in cybercrime research. Journal of Crime and Justice, 42(5), 495-499.

Dona, R. M. (2022). Legal policy in handling cyber crime for creating personal data security. legal policy in handling cyber crime for creating personal data security, 10(7).

Dupont, B. &. (2021). Enhancing relationships between criminology and cybersecurity. Journal of criminology, 54(1).

Holt, T. &. (2015). Cybercrime in progress: Theory and prevention of technology-enabled offenses. Routledge.

Jaishankar, K. (2007). Establishing a theory of cyber crimes. International Journal of Cyber Criminology, 1(2).

Jaishankar, K. (2011). Cyber criminology: exploring internet crimes and criminal behavior. CRC Press.

Maimon, D. &. (2019). Cyber-dependent crimes: An interdisciplinary review. Annual Review of Criminology, 2(1).

Miró-Llinares, F. &. (2020). Environmental criminology and cybercrime: Shifting focus from the wine to the bottles: In The Palgrave handbook of international cybercrime and cyberdeviance. Cham: Springer International Publishing.

Phillips, K. D. (2022). Conceptualizing cybercrime: Definitions, typologies and taxonomies. Forensic sciences, 2(2).

Sabillon, R. C.-R. (2016). Cybercrime and cybercriminals: A comprehensive study. International Journal of Computer Networks and Communications Security, 4(6).

Stratton, G. P. (2017). Crime and justice in digital society: Towards a'digital criminology'? International Journal for Crime, Justice and Social Democracy, 6(2).

Tonellotto, M. (2020). Crime and victimization in cyberspace: a socio-criminological approach to cybercrime. In Handbook of Research on Trends and Issues in Crime Prevention, Rehabilitation, and Victim Support.