JIM: Jurnal Ilmu Multidisiplin
E-ISSN: 2829-4580
P-ISSN: 2829-4599
GREENATION PUBLISHER
+62 812 1046 7572 http://greenpub.org greenation.info@gmail.com
DOI: https://doi.org/10.38035/jim.v4i4

Menilai Kesiapan Implementasi Kebijakan dalam Mengatasi Fenomena Cybercrime di Kota Pekanbaru

Rifki Amanda[1], Mhd. Suhaidi[2], Dwi Septiyaningsih[3], Aisyah Yulfitri[4], M. Rafi[5]
[1]Universitas Riau, Pekanbaru, Indonesia, rifki.amanda6804@student.unri.ac.id
[2]Universitas Riau, Pekanbaru, Indonesia, mhd.suhaidi4073@student.unri.ac.id
[3]Universitas Riau, Pekanbaru, Indonesia, dwi.septiyaningsih0083@student.unri.ac.id
[4]Universitas Riau, Pekanbaru, Indonesia, aisyah.yulfitri1743@student.unri.ac.id
[5]Universitas Riau, Pekanbaru, Indonesia, rafy060611@lecturer.unri.ac.id

Corresponding Author: rifki.amanda6804@student.unri.ac.id[1]

Abstract: *The increasing phenomenon of cybercrime in Pekanbaru City poses a serious threat to the digital security of the community and highlights the importance of local government preparedness in dealing with it. This study aims to assess the readiness of the Pekanbaru City government in implementing cybercrime prevention policies through an analysis of the content of the policies and the context of their implementation. The research uses qualitative methods with data collection techniques such as interviews and literature studies, including books, journals, and several related legal sources. The results show that the local government has made various efforts, such as forming a Cyber Unit team for law enforcement, but there are still significant obstacles in the form of limited human resources, a lack of technical equipment, and the absence of local regulations that specifically regulate the handling of cybercrime. Furthermore, inter-agency coordination has not been optimal, thereby hampering the effectiveness of case handling. The study concludes that the readiness of the Pekanbaru City government still needs to be strengthened through technical capacity building, the formulation of more adaptive local policies, and increased collaboration between institutions to create a more responsive digital protection system.*

Keyword: *Cybercrime, Policy Implementation, Government.*

Abstrak: Fenomena kejahatan *cyber* yang terus meningkat di Kota Pekanbaru menimbulkan ancaman serius terhadap keamanan digital masyarakat dan mendorong pentingnya kesiapan pemerintah daerah dalam menanganinya. Penelitian ini bertujuan menilai kesiapan pemerintah Kota Pekanbaru dalam mengimplementasikan kebijakan penanggulangan kejahatan *cyber* melalui analisis terhadap isi kebijakan dan konteks pelaksanaannya. Penelitian menggunakan metode kualitatif dengan teknik pengumpulan data berupa wawancara, dan studi literatur seperti buku, jurnal, dan beberapa sumber hukum terkait. Hasil penelitian menunjukkan bahwa pemerintah daerah telah melakukan berbagai upaya seperti pembentukan tim Unit *Cyber* untuk penegakan hukum, namun masih terdapat hambatan signifikan berupa keterbatasan sumber daya manusia, minimnya perangkat teknis, serta belum adanya regulasi daerah yang secara khusus mengatur penanganan kejahatan *cyber*.

Selanjutnya, koordinasi lintas instansi juga belum berjalan optimal sehingga menghambat efektivitas penanganan kasus. Penelitian menyimpulkan bahwa kesiapan pemerintah Kota Pekanbaru masih perlu diperkuat melalui penguatan kapasitas teknis, penyusunan kebijakan daerah yang lebih adaptif, serta peningkatan kolaborasi antar lembaga untuk menciptakan sistem perlindungan digital yang lebih responsif.

Kata Kunci: *Cybercrime*, Implementasi Kebijakan, Pemerintah.

PENDAHULUAN

Isu yang berkaitan dengan fenomena *cybercrime* telah banyak diteliti oleh berbagai keilmuan. Fenomena *cybercrime* itu sendiri merupakan suatu kejatan yang dilakukan oleh suatu individu atau kelompok melalui perangkat elektronik seperti komputer, jaringan teknologi informasi, serta kejahatan lainnya yang difasilitasi oleh jaringan internet atau teknologi informasi (Phillips et al., 2022). Kemudian, *Association of Chief Police Officers of England* (ACPO) dan *The U.S. Department of Justice* (DOJ) menjelaskan bahwa *cybercrime* merupakan sebagai segala bentuk kejahatan yang dilakukan dengan perangkat komputasi elektronik (Ch et al., 2020). Saat ini, perkembangan teknologi modern memberikan peluang besar dalam komunikasi lintas batas dan menghadirkan risiko baru berupa kerentanan keamanan data serta potensi peretasan. Berdasarkan catatan *Cybersecurity Ventures* kerugian global akibat *cybercrime* mencapai sekitar USD 3 triliun pada tahun 2015 dan meningkat menjadi USD 6 triliun pada tahun 2021 (Boskovic, 2022). Melihat fenomena di atas, *cybercrime* telah menjadi sebuah ancaman dari kemajuan teknologi informasi. Selanjutnya, upaya dalam mengatasi ancaman dari *cyber* ini telah dibentuk berbagai regulasi dan aturan oleh pemerintah di seluruh dunia, sehingga peraturan keamaan *cyber* ini bertujuan untuk mendorong praktik manajemen risiko, melindungi data pribadi, dan menegakkan hukum terhadap pelaku kejahatan *cyber* (Kristianti & Kurniasi, 2024).

Di Indonesia, landasan hukum utama dalam menanggulangi kejahatan *cyber* adalah Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) yang mengatur aktivitas digital dan memberikan dasar penegakan hukum terhadap pelanggaran seperti peretasan, penipuan, maupun pelanggaran hak cipta. Saat ini, UU ITE dianggap sebagai suatu terobosan hukum yang mampu mendorong perkembangan Informasi dan Teknologi (IT) serta mampu merespon tindak pidana penipuan yang mengikuti kemajuan perkembangan zaman (Junaidi, 2020). Selanjutnya, hukum menjadi peran penting dalam pencegahan dan penanggulangan kejahatan, sehingga hukum harus menciptakan regulasi yang responsif terhadap kejahatan *cyber* dengan membutuhkan bantuan lintas sektor seperti pemerintah, swasta, dan masyarakat. Oleh karena itu, terciptanya kerangka hukum yang adaptif dan kelengkapan teknologi keamanan *cyber* menjadi hal yang krusial dalam mengatasi kejatahan *cyber* yang terus berkembang (Soesanto et al., 2023). Timbulnya kejahatan *cyber* ini diakibatkan oleh cepatnya akses internet sehingga kondisi ini sering dimanfaatkan oleh oknum yang tidak bertanggung jawab untuk mencari keuntungan finansial melalui kejahatan virtual atau dunia maya. Dalam situasi saat ini, kejahatan virtual tidak hanya merugikan pribadi seseorang melainkan juga berpotensi merugikan organisasi dan pemerintah, walaupun di satu sisi dapat meningkatkan efektifitas tetapi disisi lain kejahatan *cyber* juga semakin meningkat disebabkan oleh akses internet yang berkembang pesat dan lebih cepat (Butarbutar, 2023).

Berdasarkan kasus dan keadaan *cybercrime* di Indonesia melahirkan ancaman serius, sehingga kejahatan *cybercrime* ini menjadi salah satu kejahatan tertinggi di dunia (Habibi & Liviani, 2020). Dalam kondisi saat ini, perkembangan akses yang begitu pesat dan cepat mengakibatkan fenomena *cybercrime* ini merambat ke tinggal lokal. Akses internet yang lebih cepat dan jumlah layanan perbankan elektronik yang lebih banyak di beberapa wilayah seperti Kota Pekanbaru, sehingga membuka jalan bagi kejahatan *cyber* seperti penipuan

online, *hacking*, dan pelanggaran data pribadi. Hal ini benar-benar mengganggu tingkat kepercayaan masyarakat terutama dalam hal transaksi finansial dan membuat pengguna layanan digital merasa tidak aman dan kerentanan. Beberapa kasus menunjukkan bahwa pelaku lokal dan jaringan internasional melakukan kejahatan ini. Dalam kondisi saat ini, kejahatan *cyber* telah banyak terjadi pada tingkat lokal seperti yang ditemukan Polresta Pekanbaru yaitu sindikat penipuan internet yang terdiri dari warga Nigeria pada Februari 2025. Meskipun dia harus mentransfer sejumlah uang terlebih dahulu,korban dijanjikan hadiah ATM sebesar USD 30.000. dalam kasus ini, pelaku dijerat dengan Pasal 28 ayat (1) UU ITE dan Pasal 378 KUHP dan korban mengalami kerugian sebesar Rp. 365 juta (FNIndonesia.com, 2025). Selain itu, ada kasus penipuan yang terjadi pada September 2024 di mana seorang penduduk Indragiri Hilir ditipu hingga Rp. 170 juta karena menjual mobil melalui platform Facebook, metode penipuan ini menggunakan pihak ketiga yang berpura-pura melakukan transaksi tetapi setelah uang dikirim penjualpun menghilang (Haluanriau.co, 2024).

Studi literatur menunjukkan bahwa *cybercrime* merupakan fenomena yang memerlukan kesiapan dari pemerintah lokal dalam mengatasi penipuan berbasis online. Setiap kasus penipuan atau pencurian data menjadi tantangan tersendiri bagi pemerintah lokal terhadap sistem digital. Sehingga, hal ini menjadi poin penting untuk dianalisis dengan menggunakan model Grindle (1997) yang menekankan bahwa kesiapan pemerintah lokal dipengaruhi oleh dua variabel besar, yakni isi kebijakan *(content of policy)* yang terdiri atas sub indikator yaitu *interest affected, type of benefits, extent of change envisioned, site of decision making, program implementors, resources committed* dan konteks implementasi *(context of implementation)* yang terdiri atas sub indikator yaitu *power, interest, and strategies of actors involved, institutions and regimecharacte ristics, compliance and responsiveness*. Variabel dalam teori ini membahas kepentingan kelompok sasaran atau target group termuat dalam isi kebijakan, jenis manfaat yang diterima oleh target group, sejauhmana perubahan yang diinginkan dari sebuah kebijakan (Grindle, 2017).

Berdasarkan Fenomena di atas secara fundamental kasus-kasus tersebut memiliki konsekuensi yang jelas, korban mengalami kerugian finansial yang signifikan dan dapat mengancam stabilitas keuangan keluarga. Tidak hanya itu, rasa percaya diri terhadap layanan digital dan lembaga keuangan juga menurun. kemudian, situasi saat ini menunjukkan bahwa kejahatan internet bukan hanya pelanggaran hukum tetapi juga masalah sosial dan ekonomi. Oleh karena itu, mengatasi permasalahan ini perlu memberikan perlindungan dan keamanan kepada penduduk Kota Pekanbaru dari kerentanan digital, edukasi masyarakat, penguatan regulasi, serta peningkatan kemampuan penegakan hukum harus bekerja sama untuk mengatasi permasalahan *cybercrime* yang muncul di wilayah lokal seperti Kota Pekanbaru.

Peran pemerintah lokal sangat dibutuhkan dalam mengatasi permasalahan *cybercrime* demi menjaga kepercayaan masyarakat terhadap keamanan data serta menjamin keamanan transaksi digital. Pemerintah Kota Pekanbaru turut menyiapkan regulasi seperti Peraturan Walikota Nomor 13 Tahun 2023 tentang Penyelenggaraan Sistem Pemerintahan Berbasis Elektronik Di Lingkungan Kota Pekanbaru, akan tetapi regulasi ini hanya mencakup menyelenggaraan pemerintah berbasis elektronik bukan untuk mengatasi permasalahan fenomena *cybercrime* di Kota Pekanbaru. Melihat kondisi tersebut, penelitian ini menjadi penting untuk dilakukan agar dapat diketahui terkait kesiapan pemerintah lokal dalam menghadapi fenomena *cybercrime* di Kota Pekanbaru. Oleh karena itu, penelitian ini bertujuan untuk menjelaskan sejauh mana kesiapan pemerintah lokal dalam meningkatkan kepercayaan publik kepada fenomena *cybercrime* di Kota Pekanbaru.

METODE

Penelitian ini menggunakan metode penelitian kualitatif dengan subjek penelitian pada Kepala Kepolisian Resor (Kapolres) Kota Pekanbaru dan Dinas Komunikasi dan

Informatika Kota Pekanbaru. Pada esensinya metode penelitian kualitatif merupakan penelitian yang berlandaskan pada filsafat postpositivisme digunakan untuk meneliti pada kondisi objek alamiah dimana peneliti sebagai instrumen kunci sehingga hasil penelitian kualitatif lebih menekankan makna dari pada generalisasi (Nurrisa et al., 2025). Metode penelitian ini digunakan karena fokus kajian mengarah pada analisis kesiapan Pemerintah Kota Pekanbaru dalam mengatasi fenomena *cybercrime*. Instrumen penelitian yang digunakan meliputi wawancara bersama polresta dan *cyber* kominfo, dan dokumen serta studi literatur seperti buku, jurnal, dan beberapa sumber hukum terkait. Hasil data yang diperoleh kemudian dianalisis secara deskriptif untuk memberikan pemahaman yang mendalam mengenai kesiapan pemerintah daerah dalam menghadapi fenomena tersebut.

HASIL DAN PEMBAHASAN

Seiring dengan laju perkembangan teknologi, peran kebijakan pada tingkat pemerintah lokal sangat dibutuhkan dalam mengatasi permasalahan *cybercrime,* hal ini bertujuan demi terciptanya keamanan data serta menjamin keamanan transaksi digital. Kemudian, terciptanya keamanan data dan transaksi digital membutuhkan kesiapan dari pemerintahan lokal seperti regulasi yang mengatur tentang *cybercrime* sehingga regulasi ini bisa menjadi tindak lanjut pemerintahan lokal dalam mengatasi perkembangan kasus *cybercrime* di tingkat lokal. Selanjutnya, kurangnya perencanaan kebijakan secara proaktif menjadi penanda kurangnya kesiapan pemerintahan lokal dalam mengatasi fenomena *cybercrime.* Hal ini menciptakan lingkungan digital yang lebih aman dan terlidungi membutuhkan kebijakan yang kuat untuk mengatasi fenomena *cybercrime* (Anastasya & Kansil, 2024).

Jika ditelusuri kembali, dalam konteks pemerintahan lokal khususnya pemerintah Kota Pekanbaru membutuhkan bantuan dari semua pihak untuk mengatasi permasalahan *cybercrime* seperti Organisasi Perangkat Daerah (OPD) dan instansi-instansi terkait. Oleh sebab itu, satuan Reserse Kriminal (Satreskrim) Polresta Pekanbaru telah membentuk tim *cyber* untuk memantau aktivitas di internet selama 24 jam penuh. Fokus utama tim ini yaitu menemukan dan memantau berita bohong atau hoaks yang dapat menyebabkan konflik atau perpecahan di masyarakat (Mediacenter.riau.go.id, 2024). Kemudian, pada Juni 2024 serangan hacker mengganggu jaringan layanan Kementerian Komunikasi dan Informatika (Kemkominfo) sehingga serangan ini menyebabkan website pemerintah di 30 kementerian lembaga, 15 provinsi, 148 kabupaten, dan 48 kota, termasuk Kota Pekanbaru. Menindak lanjuti fenomena tersebut, Diskominfo Kota Pekanbaru segera melakukan perbaikan pada layanan pusat data daerah untuk memulihkan kembali seluruh aplikasi layanan perangkat daerah yang terganggu oleh serangan hacker dengan metode *ransomware*. Kemudian, pemerintah Kota Pekanbaru juga telah membentuk tim *Computer Security Incident Response Team* (CSIRT), tim ini bertanggung jawab untuk mencegah, menanggulangi, dan menanggapi insiden keamanan *cyber* (Pekanbaru.go.id, 2024).

Dengan demikian, penanganan kejahatan *cybercrime* bukanlah hal yang mudah untuk diatasi. Dalam hal ini, sifat dari kejahatan *cybercrime* yang susah untuk di atasi dan undang-undang yang ada di Indonesia belum dapat menangani perkembangan kejahatan maya sehingga ini mejadi tantangan dalam mengatasi fenomena *cybercrime* yang terus berkembang (Sari, 2021). Selanjutnya, mengatasi permasalahan fenomena *cybercrime* sampai ke tingkat lokal membutuhkan kebijakan di tingkat lokal sebagai tindak lanjut mengatasi permasalahan perkembangan fenomena *cybercrime* yang semakin berkembang seiring dengan berjalannya waktu. Berkitan dengan kebijakan di tingkat lokal yang menjadi penanda kesiapan pemerintah lokal model Grindle (1997) yang menekankan bahwa kesiapan pemerintah lokal dipengaruhi oleh dua variabel besar, yakni isi kebijakan *(content of policy)* dan konteks implementasi *(context of implementation)*, sehingga model ini dapat mengambarkan sejauhmana perubahan yang diinginkan dari sebuah kebijakan (Grindle, 2017).

A. Content Of Policy

Isi kebijakan keamanan *cyber* di Kota Pekanbaru memperlihatkan bagaimana substansi kebijakan nasional diterjemahkan ke dalam konteks lokal. Dalam kerangka Grindle, dimensi *content of policy* menyoroti sejauh mana tujuan, strategi, dan sumber daya kebijakan dijalankan oleh aktor-aktor pelaksana di tingkat daerah. Implementasi kebijakan ini melibatkan dua lembaga utama, yaitu Diskominfo Pekanbaru sebagai pelaksana teknis dan Polresta Pekanbaru sebagai penegak hukum, yang keduanya berupaya menjaga ruang digital dari ancaman kejahatan *cyber*. Berdasarkan hal tersebut, penelitian ini akan dibahas dengan merujuk pada dua variabel besar, yakni isi kebijakan *(Content of Policy)* dan lingkungan implementasi *(Context of Implementation)* yang merupakan dua variabel utama dalam penelitian ini. Selanjutnya, menurut Merilee S. Grindle (1980) isi kebijakan *(content of policy)* terdiri atas beberapa sub indikator yaitu *interest affected, type of benefits, extent of change envisioned, site of decision making,* dan *program implementors,* serta *resources committed.*

1. *Interest Affected* (Kepentingan yang Mempengaruhi)

Kepentingan yang terpengaruh dalam konteks penelitian ini merupakan faktor yang memiliki pengaruh signifikan terhadap pelaksanaan kebijakan. Kepentingan tersebut dapat memengaruhi hubungan sosial, politik, maupun ekonomi masyarakat dalam merespons kebijakan yang diterapkan. Menurut Grindle (1980), *interest affected* dalam implementasi kebijakan selalu melibatkan berbagai aktor dengan kepentingan yang berbeda-beda, dan sejauh mana kepentingan tersebut berperan akan menentukan efektivitas pelaksanaan kebijakan itu sendiri.

Dalam konteks pelaksanaan kebijakan pelaporan kejahatan *cyber* di Kota Pekanbaru, dinamika kepentingan terlihat dalam proses pengambilan keputusan dan koordinasi antarinstansi. Masyarakat dapat melaporkan kasus kejahatan *cyber* melalui *Computer Security Incident Response Team* (CSIRT) sebagai unit khusus yang menangani insiden *cyber* di tingkat daerah di bawah koordinasi Dinas Komunikasi, Informatika, Statistik, dan Persandian Kota Pekanbaru**.** Keberadaan CSIRT menjadi representasi kepentingan pemerintah daerah dalam melindungi keamanan informasi publik sekaligus memastikan respons cepat terhadap laporan masyarakat. Namun, apabila kasus tersebut tidak dapat diselesaikan di tingkat kota, penanganannya akan diteruskan secara berjenjang hingga ke tingkat pemerintahan pusat. Mekanisme pelaporan berlapis ini mencerminkan adanya koordinasi vertikal antarlevel pemerintahan serta keterlibatan berbagai kepentingan, baik dari masyarakat, pemerintah daerah, maupun pemerintah pusat, dalam penanggulangan kejahatan *cyber* di Indonesia.

2. *Type of Benefits* (Tipe Manfaat)

Suatu kebijakan publik pada dasarnya harus memiliki manfaat nyata bagi masyarakat, memberikan dampak positif, serta mampu menghasilkan perubahan ke arah yang lebih baik melalui penyelesaian permasalahan yang dihadapi publik. Dalam konteks kebijakan penanggulangan kejahatan *cyber* di Kota Pekanbaru, rancangan dan implementasi kebijakan harus berorientasi pada kebermanfaatan bagi masyarakat, khususnya dalam upaya meminimalkan terjadinya kasus-kasus *cybercrime* di wilayah tersebut. Oleh karena itu, efektivitas kebijakan dapat diukur dari sejauh mana kebijakan tersebut mampu menekan angka kejahatan *cyber* serta meningkatkan rasa aman masyarakat dalam menggunakan teknologi digital.

Implementasi penanganan kejahatan *cyber* di lingkungan Kepolisian Resor Kota (Polresta) Pekanbaru dilaksanakan dengan berpedoman pada landasan hukum yang kuat, yaitu Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (ITE)**,** Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan atas Undang-Undang ITE**,** serta Undang-Undang Nomor 1 Tahun 2022 tentang Hubungan Keuangan antara Pemerintah

Pusat dan Pemerintahan Daerah**.** Ketiga regulasi tersebut berfungsi sebagai dasar normatif dalam menetapkan bentuk tindak pidana serta prosedur penyelidikan terhadap kasus-kasus kejahatan cyber seperti *cyberbullying*, penipuan daring, maupun pencemaran nama baik di media sosial. Kebijakan ini pada hakikatnya dirancang untuk memberikan perlindungan hukum bagi masyarakat dari berbagai ancaman di ruang digital, sehingga masyarakat pengguna internet menjadi kelompok yang memperoleh manfaat langsung dari implementasinya. Adapun pelaksanaan kebijakan dilakukan oleh Unit *Cyber* Satreskrim Polresta Pekanbaru yang bertugas melakukan penyelidikan, klarifikasi laporan, dan memberikan edukasi publik mengenai literasi digital serta keamanan *cyber*. Dengan demikian, keberadaan unit ini tidak hanya memperkuat aspek penegakan hukum terhadap tindak pidana *cyber*, tetapi juga mencerminkan peran strategis kepolisian dalam membangun kesadaran masyarakat terhadap pentingnya keamanan informasi di era transformasi digital.

3. *Extent of Change Envisioned (Deraajat Perubahan yang Diinginkan)*

Kebijakan yang dirancang dalam menangani kasus *cybercrime* di Kota Pekanbaru perlu memiliki target yang jelas dan terukur agar dapat mencapai tujuan yang diharapkan. Penetapan sasaran kebijakan menjadi penting untuk memastikan bahwa setiap program yang dijalankan mampu memberikan hasil nyata dalam mengurangi tingkat kejahatan *cyber* di masyarakat. Semakin luas dan besar perubahan yang diinginkan melalui kebijakan tersebut, maka semakin kompleks pula tantangan yang dihadapi dalam implementasinya. Oleh karena itu, perumusan kebijakan penanggulangan kejahatan *cyber* harus mempertimbangkan kapasitas sumber daya, tingkat koordinasi antarinstansi, serta kesiapan teknis dari lembaga pelaksana.

Dalam konteks ini, pelaksanaan program *Computer Security Incident Response Team* (CSIRT) di Kota Pekanbaru masih menghadapi sejumlah hambatan yang berpengaruh terhadap efektivitas implementasinya. Salah satu kendala utama adalah keterbatasan sumber daya manusia (SDM) di bidang teknologi informasi, yang menyebabkan proses penanganan insiden *cyber* belum dapat berjalan secara optimal. Selain itu, tingkat pemahaman terhadap penggunaan perangkat elektronik dan sistem keamanan digital di masing-masing Organisasi Perangkat Daerah (OPD) juga masih bervariasi. Kondisi tersebut menuntut adanya peningkatan kapasitas melalui pelatihan dan pendampingan teknis bagi OPD agar memiliki pemahaman yang lebih baik mengenai keamanan *cyber* serta mampu menyediakan IT *Support* di setiap instansi.

Sebagai langkah penguatan implementasi kebijakan, pemerintah daerah berupaya melakukan pelatihan secara berkelanjutan serta menambah jumlah SDM yang kompeten guna mempercepat proses penanganan kasus kejahatan *cyber* di wilayah Kota Pekanbaru. Upaya ini juga didukung oleh inisiatif Kepolisian Resor Kota (Polresta) Pekanbaru**,** yang menjalin kerja sama lintas sektor dengan Dinas Komunikasi, Informatika, Statistik, dan Persandian serta pihak perbankan melalui penyusunan nota kesepahaman **(***Memorandum of Understanding*/MoU**).** Kolaborasi ini diharapkan dapat memperluas akses informasi, memperkuat koordinasi antarinstansi, dan meningkatkan efektivitas penegakan hukum terhadap tindak pidana *cyber*. Dengan demikian, sinergi antara pemerintah daerah, aparat penegak hukum, dan lembaga keuangan menjadi faktor strategis dalam memperkuat sistem keamanan *cyber* di Kota Pekanbaru. Kebijakan yang terintegrasi dan berbasis kolaborasi tersebut diharapkan mampu meningkatkan ketanggapan pemerintah terhadap ancaman kejahatan *cyber* sekaligus membangun budaya keamanan digital di lingkungan masyarakat.

4. *Site of Decision Making* (Letak Pengambilan Keputusan)

Pengambilan keputusan dalam suatu kebijakan memegang peranan penting dalam menentukan keberhasilan implementasinya. Proses pengambilan keputusan menjadi titik krusial yang menunjukkan sejauh mana kebijakan yang dirancang telah ditempatkan secara

tepat dalam struktur organisasi dan mekanisme pelaksanaannya. Kejelasan posisi dan alur pengambilan keputusan akan berpengaruh langsung terhadap efektivitas kebijakan yang dijalankan, khususnya dalam konteks pengelolaan isu-isu strategis seperti keamanan *cyber* di tingkat pemerintah daerah.

Dalam konteks pelaksanaan kebijakan di Kota Pekanbaru, proses pengambilan keputusan pada Dinas Komunikasi, Informatika, Statistik, dan Persandian dilakukan melalui sistem pelaporan internal yang dikelola oleh Pekanbaru *Computer Security Incident Response Team* (CSIRT)**.** Melalui mekanisme ini, setiap laporan insiden *cyber* dimonitor secara langsung oleh Kepala Dinas untuk kemudian ditindaklanjuti oleh tim teknis pada masing-masing unit perangkat daerah (UPD). Apabila kasus kejahatan *cyber* yang ditangani tidak dapat diselesaikan di tingkat kota, maka laporan tersebut akan diekskalasi ke tingkat yang lebih tinggi, yaitu pemerintah provinsi atau pemerintah pusat. Pola kerja ini menunjukkan bahwa pengambilan keputusan dalam implementasi kebijakan keamanan *cyber* di Pekanbaru bersifat desentralistik**,** di mana kewenangan dan tanggung jawab dibagi secara berjenjang antara pemerintah daerah dan pusat. Model ini mencerminkan adanya koordinasi vertikal yang adaptif, sekaligus memperlihatkan peran penting pemerintah daerah dalam mendeteksi, merespons, dan menindaklanjuti kasus kejahatan *cyber* secara cepat dan terarah.

5. *Program Implementors* (Pelaksana Program)

Dalam konteks implementasi kebijakan publik, aspek pelaksana program (*program implementer*) memiliki kedudukan yang sangat penting karena keberhasilan suatu kebijakan sangat bergantung pada sejauh mana para pelaksana memahami, menguasai, dan melaksanakan kebijakan tersebut sesuai dengan ketentuan yang berlaku. Salah satu hal yang perlu diperhatikan adalah kejelasan dalam penentuan aktor pelaksana, karena sebuah kebijakan yang tidak secara rinci menyebutkan implementornya berpotensi menimbulkan tumpang tindih kewenangan dan lemahnya koordinasi antarlembaga. Pelaksanaan kebijakan penanganan *cybercrime* di Kota Pekanbaru disimpulkan bahwa struktur implementor kebijakan penanganan *cybercrime* di Pekanbaru masih bersifat terpusat dengan pola koordinasi lintas lembaga. Kondisi ini menunjukkan bahwa meskipun Diskominfo telah berperan aktif melalui pembentukan CSIRT, namun masih dibutuhkan kebijakan daerah yang lebih operasional agar peran pelaksana di tingkat lokal dapat berjalan lebih optimal dan responsif terhadap dinamika kejahatan *cyber* di wilayahnya.

6. *Resources Committed* (Sumber Daya yang Digunakan)

Sumber daya yang tersedia merupakan salah satu faktor utama yang menentukan keberhasilan pelaksanaan suatu kebijakan publik. Sumber daya tersebut mencakup tenaga kerja, keahlian, anggaran, serta sarana dan prasarana pendukung. Ketersediaan dan kapasitas sumber daya yang memadai akan sangat memengaruhi efektivitas implementasi kebijakan, karena tanpa dukungan sumber daya yang cukup, kebijakan yang dirancang dengan baik sekalipun berpotensi tidak mencapai tujuannya secara optimal.

Dalam konteks kebijakan penanganan *cybercrime* di Kota Pekanbaru, keterbatasan sumber daya masih menjadi kendala utama yang menghambat efektivitas implementasi di lapangan. Kesiapan Satuan Reserse Kriminal (Satreskrim) Polresta Pekanbaru, misalnya, masih terbatas dalam hal sumber daya manusia, ketersediaan alat digital forensik, serta dukungan regulasi teknis yang memadai. Kondisi tersebut berdampak pada lambatnya proses penyelidikan dan penanganan kasus *cybercrime*, terutama karena koordinasi dan komunikasi antarinstansi belum berjalan secara optimal. Sementara itu, Dinas Komunikasi, Informatika, Statistik, dan Persandian (Diskominfo) Kota Pekanbaru juga menghadapi tantangan serupa. Hambatan yang paling menonjol meliputi keterbatasan sumber daya manusia yang kompeten di bidang teknologi informasi, keterbatasan anggaran operasional, serta minimnya peralatan teknis yang diperlukan dalam mendukung keamanan sistem informasi daerah. Struktur

organisasi Diskominfo yang masih berada pada level "seksi" turut menambah beban kerja yang tinggi dan membatasi fleksibilitas dalam penanganan insiden *cyber*. Selain itu, keterlambatan pencairan dana untuk pengadaan alat pendukung juga menjadi faktor penghambat dalam mempercepat respons terhadap insiden *cybercrime* yang terjadi.

B. Context Of Implementation

Konteks pelaksanaan kebijakan keamanan *cyber* di Pekanbaru menunjukkan bahwa keberhasilan implementasi tidak hanya ditentukan oleh isi kebijakan, tetapi juga oleh lingkungan birokrasi, sosial, dan politik yang mengitarinya. Dimensi *context of implementation* dalam teori Grindle menekankan pentingnya kondisi pelaksana dan dukungan struktural yang memungkinkan kebijakan bekerja secara efektif. Selanjutnya, menurut Merilee S. Grindle (1980) isi kebijakan *(context of implementation)* terdiri atas beberapa sub indikator yaitu *Power, Interest, and Strategy of Actor Involved, Institution and Regime Characteristic dan Compliance and Responsiveness.*

1. *Power, Interest, and Strategy of Actor Involved* (Kekuatan, Kepentingan Kepentingan, dan Strategi dari Aktor yang Terlibat)

Pencapaian tujuan dalam fase implementasi kebijakan sangat dipengaruhi oleh kekuatan dan kepentingan aktor yang terlibat. Dalam konteks implementasi kebijakan publik, aktor pelaksana (*implementor*) memiliki peran strategis karena mereka merupakan pihak yang paling berpotensi memengaruhi arah dan hasil pelaksanaan kebijakan di lapangan. Serangkaian kegiatan yang terjadi selama implementasi memperlihatkan dinamika kekuatan dan strategi yang dimainkan oleh berbagai aktor kepentingan, di mana setiap pihak menunjukkan perannya melalui tindakan yang mencerminkan posisi dan kepentingannya masing-masing.

Di Kota Pekanbaru, pembentukan regulasi yang secara khusus mengatur penanganan *cybercrime* pada tingkat daerah belum terwujud. Penanganan fenomena ini masih berpedoman pada kebijakan nasional, yaitu Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (ITE), yang menjadi landasan utama dalam pelaksanaan berbagai kegiatan penegakan hukum di bidang kejahatan *cyber*. Namun demikian, meningkatnya kompleksitas kasus *cybercrime* di tingkat lokal menunjukkan perlunya kebijakan daerah yang lebih adaptif terhadap konteks dan kebutuhan wilayah, misalnya dalam bentuk Peraturan Daerah (Perda) yang secara spesifik mengatur tentang penanganan kejahatan *cyber* di Kota Pekanbaru. Dalam praktiknya, strategi dan kepentingan aktor terlihat dari upaya sinergi antarinstansi dalam memperkuat kapasitas dan memperluas jangkauan kebijakan penanganan *cybercrime*. Kepolisian Resor Kota (Polresta) Pekanbaru, misalnya, berinisiatif menjalin kerja sama dengan pemerintah daerah melalui Dinas Komunikasi, Informatika, Statistik, dan Persandian (Diskominfo), serta bekerja sama dengan pihak perbankan, Otoritas Jasa Keuangan (OJK), dan Pusat Pelaporan dan Analisis Transaksi Keuangan (PPATK). Kerja sama tersebut direncanakan akan diformalkan melalui nota kesepahaman *Memorandum of Understanding* (MoU) sebagai dasar hukum koordinasi lintas lembaga dalam memperkuat sistem pengawasan dan investigasi kasus *cybercrime*.

Di sisi lain, Diskominfo Kota Pekanbaru berfokus pada peningkatan kapasitas internal dengan melaksanakan pelatihan kepada berbagai Organisasi Perangkat Daerah (OPD). Langkah ini bertujuan agar setiap OPD memiliki kemampuan *IT support* yang memadai untuk menjaga keamanan sistem informasi masing-masing. Selain itu, Diskominfo juga berencana menambah jumlah sumber daya manusia (SDM) yang kompeten di bidang teknologi informasi guna memperkuat kemampuan teknis dalam mempercepat proses penanganan insiden *cyber* di lingkungan pemerintahan daerah. Dengan demikian, dapat dilihat bahwa implementasi kebijakan penanganan *cybercrime* di Kota Pekanbaru melibatkan berbagai aktor dengan peran dan kepentingan yang saling melengkapi. Polresta Pekanbaru

berperan dalam penegakan hukum dan koordinasi lintas sektor, sementara Diskominfo berperan dalam penguatan kapasitas kelembagaan serta perlindungan sistem informasi publik. Sinergi antara kedua lembaga tersebut menjadi faktor kunci dalam membangun sistem keamanan *cyber* yang lebih adaptif dan responsif di tingkat daerah.

2. *Institution and Regime Characteristic* (Karakteristik Lembaga yang Sedang Berkuasa)

Implementasi suatu program kebijakan publik sering kali menimbulkan potensi konflik di antara kelompok-kelompok yang kepentingannya terdampak. Konflik ini muncul karena adanya perbedaan orientasi, prioritas, dan kepentingan antaraktor yang terlibat dalam pelaksanaan kebijakan. Dalam konteks pemerintahan daerah, Dinas Komunikasi, Informatika, Statistik, dan Persandian (Diskominfo) Kota Pekanbaru telah membentuk kebijakan *Computer Security Incident Response Team* (CSIRT) sebagai langkah strategis dalam menjaga keamanan informasi di lingkungan pemerintahan daerah.

Kebijakan ini secara substansial difokuskan pada perlindungan dan pengamanan data serta sistem informasi internal pemerintah Kota Pekanbaru. Artinya, ruang lingkup kebijakan CSIRT masih terbatas pada pencegahan dan penanganan serangan *cyber* terhadap situs-situs dan jaringan pemerintahan, bukan pada penanganan langsung terhadap kasus-kasus *cybercrime* yang dialami masyarakat umum. Hal ini terjadi karena penanganan *cybercrime* yang menyasar warga atau entitas nonpemerintah merupakan kewenangan lembaga kepolisian, khususnya melalui Unit *Cyber* Satreskrim Polresta Pekanbaru. Dalam konteks ini, peran Diskominfo lebih bersifat teknis dan pengawasan, yaitu sebagai pelaksana yang memastikan keamanan sistem informasi pemerintahan tetap terjaga dan terhindar dari ancaman serangan *cyber*. Pembentukan CSIRT menjadi kebijakan utama yang merepresentasikan upaya preventif pemerintah daerah dalam memperkuat sistem pertahanan digital dan meningkatkan kesiapan institusional terhadap potensi ancaman di ruang *cyber*

Dengan demikian, dapat dipahami bahwa kebijakan CSIRT di Kota Pekanbaru merupakan langkah penting dalam memperkuat tata kelola keamanan informasi pemerintah daerah. Keterbatasan cakupan kewenangan dalam penanganan *cybercrime* terhadap masyarakat menunjukkan perlunya sinergi yang lebih erat antara pemerintah daerah dan aparat penegak hukum. Kolaborasi lintas lembaga ini menjadi penting untuk menciptakan sistem perlindungan *cyber* yang komprehensif, meliputi baik aspek kelembagaan pemerintahan maupun kebutuhan keamanan digital masyarakat luas.

3. *Compliance and Responsiveness* (Tingkat Kepatuhan dan Adanya Respon dari Pelaksana)

Grindel (1997) mengungkapkan bahwa dalam proses pelaksanaan suatu kebijakan perlu adanya kepatuhan daya tangkap para pelaksana, maka yang hendak dijelaskan pada sub indikator ini adalah sejauh mana tingkat kepatuhan dan respon para pelaksana dalam menanggapi suatu kebijakan. Pada intinya dibutuhkan komitmen dari semua *stakeholder*, karena sebuah kebijakan tidak akan berjalan dengan baik apabila orang orang yang terkait didalamnya tidak mematuhi atau menjalankan kebijakan tersebut sesuai dengan aturan yang berlaku, maka dibutuhkan kesadaran yang tinggi bukan ego sektoral maupun mementingkan kepentingan kelompok tertentu saja.

Berdasarkan pada sub indikator tersebut, hasil penelitian ini menunjukkan bahwa secara kelembagaan, hubungan antara Diskominfo dan Polresta Pekanbaru masih bersifat fungsional dan belum memiliki mekanisme koordinasi formal yang mengikat. Diskominfo berperan menjaga keamanan sistem dan jaringan pemerintah daerah, sementara Polresta menangani aspek hukum ketika pelanggaran digital terjadi. Namun, ketiadaan payung koordinasi yang jelas membuat penanganan kasus sering terhambat, terutama ketika melibatkan data lintas instansi atau sektor perbankan.

KESIMPULAN

Berdasarkan penjelasan diatas, penelitian ini menunjukkan bahwa kesiapan Pemerintah Kota Pekanbaru dalam menghadapi fenomena *cybercrime* masih menghadapi berbagai keterbatasan, baik dari sisi kebijakan, kapasitas sumber daya, maupun koordinasi antarinstansi. Meskipun pemerintah daerah telah memiliki suatu kebijakan dari diskominfo Kota Pekanbaru yaitu *Computer Security Incident Response Team* (CSIRT), namun kebijakan ini hanya diperuntukkan untuk menangani kasus *cybercrime* di situs pemerintah bukan untuk permasalahan *cybercrime* di masyarakat. Kemudian, Polresta Pekanbaru telah membentuk Unit *Cyber* untuk penegakan hukum, namun regulasi khusus di tingkat daerah yang secara komprehensif mengatur penanganan *cybercrime* belum tersedia karena ditingkat lokal hanya berpedoman kepada regulasi nasional yaitu UU ITE. Ketergantungan pada kebijakan nasional serta minimnya pedoman operasional di tingkat lokal membuat pelaksanaan penanganan kasus sering terhambat, terutama ketika melibatkan aktor lintas sektor dan membutuhkan pertukaran data secara cepat.

Selain itu, faktor sumber daya seperti sumber daya manusia, perangkat teknis, maupun anggaran turut menjadi tantangan besar dalam mendukung efektivitas implementasi kebijakan. Variasi pemahaman keamanan digital di setiap OPD, keterbatasan alat forensik, serta belum optimalnya koordinasi antara Diskominfo dan Polresta memperlihatkan bahwa sistem keamanan *cyber* di Pekanbaru masih perlu diperkuat. Oleh karena itu, peningkatan kapasitas teknis, pengembangan regulasi daerah yang lebih adaptif, serta sinergi antara pemerintah daerah, aparat penegak hukum, sektor perbankan, dan masyarakat menjadi langkah penting untuk meningkatkan perlindungan digital serta mengurangi risiko kejahatan *cyber* di Kota Pekanbaru.

REFERENSI

Anastasya, V., & Kansil, C. S. T. (2024). Efektivitas Hukum dan Kebijakan Publik dalam Menghadapi Ancaman Cyber terhadap Keamanan Negara. *Jurnal Multidisiplin Indonesia*, *3*(2), 1710–1716.

Butarbutar, R. (2023). Kejahatan Cyber Terhadap Individu: Jenis, Analisis, Dan Perkembangannya. *Jurnal Hukum & Pembangunan*, *2*(2). https://doi.org/10.21143/telj.vol2.no2.1043

Ch, R., Gadekallu, T. R., Abidi, M. H., & Al-Ahmari, A. (2020). Computational system to classify Cyber Crime offenses using machine learning. *Jurnal Sustainability*, *12*(10). https://doi.org/10.3390/SU12104087

Edy Soesanto, Achmad Romadhon, Bima Dwi Mardika, & Moch Fahmi Setiawan. (2023). Analisis dan Peningkatan Keamanan Cyber: Studi Kasus Ancaman dan Solusi dalam Lingkungan Digital Untuk Mengamankan Objek Vital dan File. *Jurnal Penelitian Bisnis Dan Manajemen*, *1*(2), 172–191. https://doi.org/10.47861/sammajiva.v1i2.226

FNIndonesia.com. (2025). *Polresta Pekanbaru Berhasil Ungkap Sindikat Kasus Penipuan Online, WNA Nigeria Diamankan*. https://fn-indonesia.com/berita/detail/polresta-pekanbaru-berhasil-ungkap-sindikat-kasus-penipuan-online-wna-nigeria-diamankan#gsc.tab=0

Grindle, M. S. 1980. P. A. A. I. I. T. T. W. N. J. : P. U. (2017). *Politics and Policy Implementation in the Third World*. Princeton University Press.

Habibi, M. R., & Liviani, I. (2020). Kejahatan Teknologi Informasi (Cyber Crime) dan Penanggulangannya dalam Sistem Hukum Indonesia. *Jurnal Pemikiran Dan Pembaharuan Hukum Islam*, *23*(2), 400–426. https://doi.org/10.15642/alqanun.2020.23.2.400-426

Haluanriau.co. (2024). *Kasus Penipuan Jual Beli Mobil Online, Kasat Reskrim Pekanbaru Imbau Masyarakat Waspada*. Haluanriau.Co. https://riau.harianhaluan.com/daerah/1113608966/kasus-penipuan-jual-beli-mobil-

online-kasat-reskrim-pekanbaru-imbau-masyarakat-waspada

Kristianti, N., & Ririn Kurniasi. (2024). Peraturan dan Regulasi Keamanan Cyber di Era Digital. *Jurnal Ilmu Hukum*, *7*(1), 297–310.

Matić Bošković, M. M. (2022). Cybercrime Money Laundering Cases and Digital Evidence. *Jurnal Strani Pravni Život*, *16*(4), 451–167. https://doi.org/10.56461/spz_22406kj

Mediacenter.riau.go.id. (2024). *Polresta Pekanbaru Intensifkan Patroli Cyber Cegah Hoaks Selama Pilkada*. https://mediacenter.riau.go.id/read/88347/polresta-pekanbaru-intensifkan-patroli-cyber-.html

Muhammad Junaidi, Kadi Sukarna, B. S. (2020). Pemahaman Tindak Pidana Transaksi Elektronik Dalam Undang- Undang No 19 Tahun 2016 Tentang Informasi Dan Transaksi Elektronik. *Jurnal BUDIMAS*, *02*(02), 109–118. https://www.golder.com/insights/block-caving-a-viable-alternative/

Nurrisa, F., Hermina, D., & Norlaila. (2025). Pendekatan Kualitatif dalam Penelitian : Strategi , Tahapan , dan Analisis Data. *Jurnal Teknologi Pendidikan Dan Pembelajaran (JTPP)*, *02*(03), 793–800.

Pekanbaru.go.id. (2024). *Diskominfo Pekanbaru Ajak Semua OPD Optimalkan Layanan Pusat Data Pemerintah*. https://www.pekanbaru.go.id/p/news/diskominfo-pekanbaru-ajak-semua-opd-optimalkan-layanan-pusat-data-pemerintah#

Phillips, K., Davidson, J. C., Farr, R. R., Burkhardt, C., Caneppele, S., & Aiken, M. P. (2022). Conceptualizing Cybercrime: Definitions, Typologies and Taxonomies. *Forensic Sciences*, *2*(2), 379–398. https://doi.org/10.3390/forensicsci2020028

Sari, U. I. P. (2021). Kebijakan Penegakan Hukum Dalam Upaya Penanganan Cyber Crime Yang Dilakukan Oleh Virtual Police Di Indonesia. *Jurnal Hukum*, *2*(1). https://studialegalia.ub.ac.id/index.php/studialegalia/article/view/7%0Ahttps://studialegalia.ub.ac.id/index.php/studialegalia/article/download/7/6