JTIK (Jurnal Teknologi Informasi dan Komunikasi)
p-ISSN : 2087-0868 (media cetak); e-ISSN : 2598-9707 (media online)
Vol. 16, No. 2, September 2025
http://ejurnal.provisi.ac.id/index.php/JTIKP

PENGELOLAAN INFORMASI DIGITAL DALAM MENANGANI PERJUDIAN ONLINE DI INDONESIA

Muhammad Zaenal Muhajir[1], Eka Yulyana[2], Lina Aryani[3]
[1,2,3] Department of Government, Universitas Singaperbangsa Karawang, Indonesia

Article Info

Article history:

Received May 25, 2025
Revised June 11, 2025
Accepted August 29, 2025

Keywords:

Managing Online Gambling,
Digital Information,
Cybersecurity

ABSTRACT

Online gambling has become a serious problem in Indonesia, with an increase in gambling content reaching 5,128,871 pieces in the 2017-2024 period, of which 67.4% was addressed by 2024. This study aims to evaluate and analyze digital information management strategies used to address the problem of online gambling in Indonesia. This study applies a qualitative methodology through a single case study approach at the Directorate of Informatics Application Control (APTIKA) of the Ministry of Communication and Digital. Data collection was carried out through four main methods: observation, in-depth interviews, documentation, and literature study. Data analysis uses the Miles and Huberman model with the Defense In Depth information security theory from Coole & Brooks (2011) which consists of four aspects: governance, people, process, and technology. The results show that digital information management has been implemented with a strong operational structure through the implementation of regulations from the ITE Law, the PDP Law, and the PP PSTE, human resource capacity development through continuous training, the implementation of comprehensive SOPs with encryption technology and strict access control, and the use of advanced technology for monitoring and detection. Furthermore, there are still significant obstacles, particularly significant gaps in public communication and accessibility of information to the public, limited prevention education programs, and challenges in dealing with technological developments used by cybercriminals.

Corresponding Author:

Muhammad Zaenal Muhajir,
Government Department, Faculty of Social & Politics, Universitas Singaperbangsa Karawang
Jl. HS. Ronggowaluyo, Telukjambe Timur, Karawang - 413630, Indonesia.
Email: 2110631180102@student.unsika.ac.id

OPEN ACCESS

1. INTRODUCTION

Pengelolaan informasi di era digital menjadi tantangan besar bagi pemerintah. Pesatnya kemajuan teknologi informasi menyebabkan volume data yang dihasilkan setiap hari tumbuh secara drastis. *International*

Data Corporation (IDC), melaporkan bahwa lebih dari 90% semua data online yang dihasilkan dua tahun terakhir akan melonjak tinggi, dan diperkirakan volumenya akan meningkat dari 33 zettabyte (ZB) pada tahun 2018 menjadi 175 zettabyte pada tahun 2025 (Molitor et al., 2024).

Peningkatan volume data ini menimbulkan beragam masalah, salah satu masalah utama yang perlu disoroti lebih mendalam adalah maraknya perjudian online. Fenomena ini merupakan salah satu permasalahan sosial yang telah berlangsung sejak lama (Anita, 2024), Pada sekitar abad ke-5 Masehi, daerah Indonesia (Kepulauan) masih terbagi menjadi berbagai kerajaan. Permainan taruhan yang paling populer pada waktu itu adalah pertarungan hewan seperti sabung ayam, jangkrik, domba, dan kerbau. Seiring dengan kemajuan peradaban dan zaman, permainan judi juga telah berkembang menjadi lebih modern. (Mulya, 2024). Jika zaman dahulu aktivitas perjudian dilakukan dengan pertemuan langsung secara tatap muka. Saat ini situasinya sudah berubah, perjudian tidak lagi membutuhkan interaksi secara langsung, bahkan sekarang sistem perjudian bersifat global (Susanti, 2021).

Perjudian online di Indonesia dapat dianggap sebagai salah satu bentuk dari *Cybercrime*, karena tindakan ini berlangsung di dunia maya dan memanfaatkan kemajuan teknologi yang dialami oleh masyarakat secara luas. (Satrya, Nugroho, & Supolo, 2022), baik melalui platform media sosial, hiburan, konten digital, bahkan hingga merambah ke media pesan singkat dalam lingkungan pribadi (Hakim, Marini, & Basyarudin, 2024). Pertumbuhan situs dan aplikasi perjudian online tidak terlepas dari banyaknya iklan yang mempromosikan konten negatif yang menyertakan unsur perjudian online, sehingga hal ini memberikan keleluasaan bagi kelompok penjudi serta masyarakat secara umum untuk mengakses berbagai jenis permainan judi daring (Hendarto & Handayani, 2024).

Beberapa penelitian sebelumnya telah mengeskplorasi isu judi online dalam berbagai konteks. Susilo, (2022) dalam artikelnya "Pengamanan Informasi Digital Terhadap Konten Negatif Guna Mewujudkan Ketahanan Nasional" menyoroti bahwa Metode perlindungan, pengawasan, dan pemblokiran terhadap informasi yang mengandung unsur negatif belum dapat dilakukan dengan optimal. Hal ini disebabkan oleh keadaan fasilitas yang dimiliki Kemenkomdigi maupun Kepolisian RI, berupa peralatan pencari belum memiliki kemampuan mengawasi maupun memblokir akses serta penyebaran konten negatif dengan menggunakan teknologi VPN. Naila Ainaiya & dkk, (2024 Pendekatan hukum pidana mengenai perjudian online tercantum dalam pasal 27 ayat (2) Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik. Pemerintah mempertimbangkan kepentingan publik, keberlanjutan, dan konsekuensi jangka panjang dari pilihan yang diambil. Disisi lain, Rival Pahrijal & dkk, (2024) menekankan bahwa Indonesia menghadapi tantangan yang berat dalam memberantas praktik perjudian online di tengah-tengah larangan hukum yang sudah mengakar dan kemajuan teknologi.

Penelitian ini memiliki relevansi yang kuat dengan disiplin ilmu pemerintahan karena pemerintah serta aparat penegak hukum perlu melakukan upaya yang efektif untuk menangani kejahatan yang berhubungan dengan perjudian daring, demi melindungi masyarakat dan menjaga keamanan di dunia maya. Negara bertanggung jawab untuk menjamin kepastian hukum, terutama dalam mengatasi setiap tindakan kriminal yang bertentangan dengan norma dan nilai-nilai Pancasila, termasuk perjudian daring yang dilarang di Indonesia. Namun, sampai saat ini, usaha untuk memberantas kejahatan judi online masih belum berjalan dengan optimal (Fanani, A. F., & Tritasyah, R. P., 2023).

Adapun keterbaruan penelitian ini menggunakan pendekatan kualitatif dan metode studi kasus tunggal untuk menganalisis strategi dan hambatan yang dihadapi oleh Direktorat Pengendalian Aplikasi Informatika (APTIKA) dalam menanggulangi fenomena ini. Penelitian ini memberikan perspektif baru yang dapat memperkuat upaya pengelolaan informasi digital. Selain itu, penelitian ini tidak hanya memberikan wawasan tentang bagaimana strategi dan regulasi dapat dioptimalkan, tetapi juga menyoroti pentingnya kolaborasi antara pemerintah dan masyarakat dalam menciptakan ekosistem digital yang aman. Pertanyaan penelitian yang diangkat dalam studi ini adalah Bagaimana pengelolaan informasi digital dalam menangani perjudian online di Indonesia?

Penelitian ini bertujuan untuk mengevaluasi dan menganalisis strategi pengelolaan informasi digital yang digunakan untuk mengatasi permasalahan judi online di Indonesia. Studi ini memberikan kontribusi terhadap pendalaman wawasan terkait hambatan-hambatan dan alternatif solusi dalam manajemen informasi

digital. Dengan demikian, temuan dari penelitian ini diharapkan mampu menyajikan saran-saran yang berguna bagi para pemangku kebijakan dan stakeholder terkait dalam rangka upaya pemberantasan aktivitas judi online di Indonesia.

2. METHOD

Penelitian ini menerapkan metodologi kualitatif melalui pendekatan studi kasus tunggal. Metode studi kasus adalah teknik riset yang mengeksplorasi suatu permasalahan dengan parameter yang terdefinisi dengan jelas, melaksanakan pengumpulan data secara menyeluruh, serta menggunakan berbagai macam sumber informasi. Kasus yang diteliti dapat berbentuk kejadian, kegiatan, prosedur, atau program tertentu (Creswell, 2017). Pendekatan ini memungkinkan peneliti untuk mendalami secara mendetail satu kasus tertentu sesuai dengan isu yang diangkat. Permasalahan yang diangkat oleh peneliti berkaitan dengan fenomena judi online yang mengalami pertumbuhan signifikan dewasa ini, dimana masyarakat terlibat dalam aktivitas perjudian secara digital melalui platform online seperti website atau aplikasi yang terhubung dengan jaringan internet (Chintya Siringoringo et al., 2024). Adapun penelitian ini menggunakan teori dari Coole & Brooks (2011), teori ini memiliki 4 elemen penting seperti *governance*, *people, process,* dan *technology*. Peneliti melakukan penelitian di salah satu lembaga pemerintahan pusat, yaitu di Direktorat Pengendalian Aplikasi dan Informatika. Penelitian dimaksudkan untuk menganalisis strategi dan upaya pemerintah pusat dalam membasmi perjudian online di Indonesia.

Pengambilan data dilaksanakan melalui empat cara utama, yakni observasi, wawancara mendalam, dokumentasi, dan studi kepustakaan (Sugiyono, 2014). Observasi dilakukan untuk mengkaji serta melakukan pencatatan secara teratur terkait perilaku individu atau kelompok dengan cara mengamati langsung di lapangan. Wawancara mendalam dilakukan dengan informan kunci, termasuk Tim Aduan Konten Kementerian Komunikasi dan Digital, Professional Analis Data, dan Masyarakat untuk menggali perspektif mereka terkait penggelolaan informasi digital dalam menangani perjudian online. Dokumentasi mencakup analisis dokumen-dokumen resmi, seperti laporan program, peraturan menteri, dan hasil evaluasi terkait penanganan perjudian di Indonesia. Studi kepustakaan memiliki peran penting dalam penelitian, karena setiap penelitian tidak terlepas dari literatur ilmiah. Data dalam penelitian ini diperoleh dari berbagai sumber yang relevan dengan permasalahan yang diteliti, seperti buku, jurnal, artikel, media internet dan hasil penelitian sebelumnya. Data Informasi yang diperoleh dianalisis menggunakan model Miles dan Huberman. Keabsahan data dijamin melalui triangulasi sumber data dan metode, serta berdiskusi dengan para ahli untuk memastikan interpretasi data yang tepat.

3. RESULT AND DISCUSSION

Direktorat Jenderal Aplikasi Informatika (Ditjen Aptika) yang pada awalnya Ditjen Aplikasi Telematika (Ditjen Aptel) didirikan dalam rangka pengembangan Information and Communication Technology (ICT) yang efektif di Indonesia. ICT tidak dapat dilepaskan dari unsur 3C, yakni Communication, Computer, dan Content yang selanjutnya dirancang sebagai logo Kemkominfo yang terdiri dari tiga huruf C dengan gradasi warna biru.

Direktorat Jenderal Aplikasi Informatika (Ditjen Aptika) didirikan berdasarkan mandat Peraturan Menteri Kominfo Nomor 12 Tahun 2021 mengenai Struktur Organisasi dan Tata Kerja Kementerian Komunikasi dan Informatika. Ditjen Aptika bertugas untuk merumuskan dan melaksanakan kebijakan dalam pengelolaan aplikasi informatika.

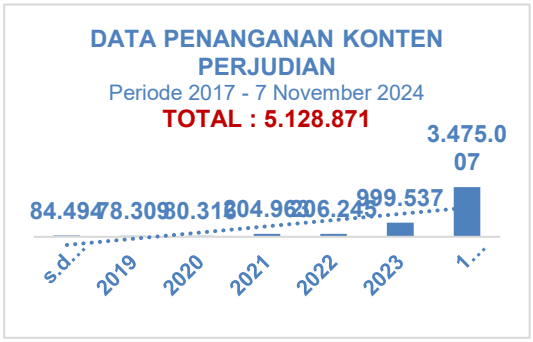
Direktorat Jenderal Aplikasi Informatika memiliki tanggung jawab dalam merumuskan dan melaksanakan kebijakan berkaitan dengan pengelolaan aplikasi informatika.

Dalam menjalankan tugasnya, Ditjen Aptika melaksanakan fungsi:

a. Penyusunan kebijakan mengenai pengelolaan layanan aplikasi pemerintah dan ekonomi digital, penguatan informatika, serta pengawasan aplikasi informatika;

b. Pelaksanaan kebijakan dalam sektor pengelolaan layanan aplikasi informatika pemerintah dan ekonomi digital, pemberdayaan teknologi informasi, serta pengendalian aplikasi informatika;
c. Penyusunan norma, standar, prosedur, dan kriteria dalam pengelolaan layanan aplikasi informatika pemerintahan;
d. Pelaksanaan penyediaan bimbingan teknis dan pengawasan di sektor penatakelolaan layanan aplikasi informatika pemerintahan;
e. Pelaksanaan evaluasi dan pelaporan di bidang penatakelolaan layanan aplikasi informatika pemerintahan dan ekonomi digital, pemberdayaan informatika, dan pengendalian aplikasi informatika;
f. Pelaksanaan administrasi Direktorat Jenderal Aplikasi Informatika; dan
g. Pelaksanaan Pelaksanaan tugas lain yang ditugaskan oleh Menteri.

Sejak tahun 2017 hingga 7 November 2024, Kemkomdigi telah menangani total sebanyak 5.128.871 konten terkait perjudian. Dari jumlah tersebut, sebanyak 3.457.007 konten berhasil diatasi hanya dalam rentang waktu 1 Januari hingga 7 November 2024. Periode ini mencatatkan angka penanganan tertinggi sepanjang sejarah pengelolaan konten perjudian oleh Kemkomdigi. Angka ini mewakili sekitar 67,4% dari total konten yang diproses sejak 2017, yang menunjukkan peningkatan dramatis dalam jumlah konten perjudian digital yang beredar dan peningkatan penegakan peraturan digital. Fenomena ini menunjukkan bahwa aktivitas perjudian daring merajalela dan memerlukan respons regulasi yang lebih komprehensif. Hal ini juga menunjukkan bahwa sistem pengawasan digital yang diterapkan Kemkomdigi telah meningkatkan kemampuan dan efektivitasnya dalam mengidentifikasi dan menangani konten ilegal di dunia maya Indonesia. Gambar 1 di bawah ini memperlihatkan data penanganan konten perjudian di Indonesia:



Gambar 1. Data Penanganan Konten Perjudian
Sumber: Olahan Peneliti dari Komdigi 2024

Total konten yang tersebar melalui situs web dan alamat IP berjumlah 4.414.740. Dari jumlah tersebut, sebanyak 541.226 konten diunggah oleh pelaku melalui platform Meta, 126.995 melalui layanan berbagi file, serta 27.505 melalui Google atau YouTube. Selain itu, terdapat 17.296 konten yang diunggah melalui akun X (Twitter), 986 melalui akun Telegram, 74 melalui TikTok, 26 melalui Snack Video, 14 melalui App Store, 6 melalui Line, dan 3 melalui Hello App. Data menunjukkan bahwa situs web dan alamat IP merupakan pemain utama dalam penyebaran konten perjudian, dengan total 4.414.740 konten atau setara dengan 86,1%. Angka yang sangat tinggi ini menunjukkan bahwa perjudian daring di Indonesia tidak lagi bersifat rahasia, tetapi telah berkembang menjadi industri digital yang terorganisasi dan berteknologi maju. Operator game telah banyak berinvestasi dalam menciptakan platform web khusus dengan antarmuka yang mudah digunakan, sistem pembayaran terintegrasi, dan layanan pelanggan yang komprehensif. Penemuan ini memiliki tiga implikasi penting. Pertama, perjudian digital telah menjadi industri yang matang dan terorganisasi dengan baik, dengan operator yang menjalankan operasi sepenuhnya digital, bukan operasi amatir. Kedua, penegakan menjadi sangat rumit karena situs web dan alamat IP dapat dengan mudah dipindahkan atau disalin, serta menggunakan teknik pengaburan yang canggih seperti jaringan pengiriman konten (CDN), server proxy, dan rotasi IP dinamis untuk menghindari deteksi dan pemblokiran. Ketiga, sebagian besar pendapatan masih terkonsentrasi pada model bisnis perjudian berbasis situs web tradisional, karena platform daring dapat menyediakan pengalaman

pengguna yang lengkap, perpustakaan permainan yang kaya, dan sistem keuangan terintegrasi, yang sulit dicapai pada platform media sosial dengan fungsi terbatas. Gambar 2 di bawah ini memperlihatkan data penyebaran konten perjudian di Indonesia:



Gambar 2. Data Penanganan Konten Perjudian Sumber: Komdigi 2024

Berdasarkan hasil penelitian, peneliti menggunakan teori keamanan informasi (pertahanan berlapis) yang dikemukakan oleh Coole & Brooks (2011). Terdiri dari empat (4) elemen/aspek yaitu pemerintahan, sumber daya manusia, proses dan teknologi. Elemen-elemen ini digunakan untuk melakukan analisis komprehensif terhadap ancaman keamanan umum dalam perjudian online, termasuk yang berikut ini (Wijaya et al., 2015):

3.1. Aspek *Governance* (Pemerintahan)

Komponen ini mengacu pada kerangka kerja manajemen yang digunakan untuk mengawasi dan mengoordinasikan orang, proses, dan teknologi, termasuk: manajemen risiko, keamanan informasi, dan penyelarasan kebijakan. Di zaman digital sekarang ini, informasi pribadi seseorang tersebar di berbagai platform online mulai dari jejaring sosial hingga aplikasi berbelanja. Informasi seperti nama, alamat, nomor telepon, gambar, dan pola belanja memiliki nilai ekonomi yang signifikan. Tanpa regulasi yang tegas, data pribadi dapat disalahgunakan untuk penipuan, pencurian identitas, atau diperjualbelikan kepada pihak-pihak yang tidak bertanggung jawab. Sehubungan dengan itu, Direktorat Aptika sebagai badan yang mengawasi informasi dan komunikasi memerlukan peraturan yang ketat untuk menjaga data masyarakat.

Pengaturan pengelolaan data di Direktorat Aptika berlandaskan pada tiga peraturan utama yang saling mendukung. UU ITE, atau Undang-Undang Informasi dan Transaksi Elektronik, merupakan dasar utama untuk pengaturan data dalam dunia digital di Indonesia. Undang-undang ini menetapkan prinsip yang sederhana tetapi krusial bahwa data milik orang lain tidak boleh digunakan tanpa izin. Dalam pelaksanaannya, saat suatu aplikasi ingin memperoleh akses ke kontak telepon, lokasi, atau foto Anda, mereka harus meminta izin terlebih dahulu melalui pop-up atau pemberitahuan. Apabila perusahaan memanfaatkan data tanpa izin dan menyebabkan kerugian, pemilik data berhak untuk mengajukan tuntutan ganti rugi melalui proses hukum. Misalnya, jika sebuah toko online memanfaatkan data pelanggan untuk mengirimkan spam atau menjual informasi pribadi kepada pihak ketiga tanpa persetujuan, pelanggan dapat mengajukan gugatan sesuai dengan UU ITE.

Regulasi kedua adalah UU PDP atau Undang-Undang Perlindungan Data Pribadi yang merupakan ketentuan yang lebih terperinci dan menyeluruh dalam menjaga data pribadi. Peraturan ini diterapkan kepada semua pihak, termasuk lembaga pemerintah dan perusahaan swasta yang menangani data pribadi masyarakat. UU PDP memberikan berbagai hak kepada pemilik data seperti hak untuk mengetahui jenis data yang dikumpulkan, hak untuk mengakses serta memperbaiki data pribadi, hak untuk menghapus data atau yang dikenal sebagai right to be forgotten, hak untuk memindahkan data ke platform lain, dan hak untuk menolak pemrosesan data untuk tujuan tertentu.

Regulasi ketiga adalah PP PSTE atau Peraturan Pemerintah mengenai Sistem dan Transaksi Elektronik yang berperan sebagai pedoman teknis yang menguraikan secara mendetail cara pengelolaan data dalam sistem elektronik. PP PSTE memberikan panduan praktis untuk pelaksanaan UU ITE dan UU PDP, mencakup aspek persetujuan mengenai cara meminta izin yang sah termasuk format persetujuan yang jelas dan tidak menyesatkan, aspek pemrosesan yang mengatur prosedur pengolahan data yang aman termasuk enkripsi dan batasan akses, aspek penyimpanan yang menetapkan standar keamanan untuk menyimpan data termasuk cadangan dan pemulihan, serta aspek penghapusan yang mengatur cara menghapus data secara permanen saat tidak diperlukan lagi atau atas permintaan pemilik data.

Berdasarkan penjelasan tersebut dapat ditarik kesimpulan bahwa bahwa peraturan sudah diterapkan, namun pelaksanaannya masih mengalami kesulitan karena banyak orang yang belum sepenuhnya menyadari hak-hak mereka mengenai data pribadi. Kemajuan teknologi terbaru seperti kecerdasan buatan dan *Internet of Things* juga memerlukan penyesuaian regulasi yang berkelanjutan.

3.2. Aspek *People* (Sumber Daya Manusia)

Komponen ini menjelaskan definisi, pemeliharaan, serta penegakan peran dan tanggung jawab keamanan untuk karyawan dan vendor baik internal maupun eksternal. Elemen keamanan individu meliputi penjabaran, pengelolaan, dan pelaksanaan tugas serta kewajiban yang mesti dilaksanakan oleh semua karyawan dan penyedia layanan, baik yang berasal dari dalam maupun luar organisasi.

Menuru hasil penelitian yang telah dilakukan, Direktorat Aplikasi dan Informatika (Aptika) telah menunjukkan dedikasi yang tinggi dalam memperbaiki dan mengembangkan kapasitas sumber daya manusia di sektor teknologi informasi dan keamanan siber. Komitmen ini terlihat melalui usaha terencana yang dilakukan untuk memperbaiki keterampilan teknis dan pemahaman keamanan data di antara karyawan. Walaupun begitu, selama proses tersebut, Direktorat Aptika tetap menghadapi sejumlah tantangan penting yang berkaitan dengan keselarasan pemahaman antara unit kerja dan peningkatan kolaborasi antar sektor yang lebih efisien.

Dalam pengembangan kapasitas SDM, tim Direktorat Aptika telah menunjukkan komitmen yang layak dihargai melalui keterlibatan aktif dalam berbagai program peningkatan kemampuan. Sesuai dengan hasil penelitian yang ada, tim secara teratur mengikuti pelatihan dan program peningkatan kesadaran keamanan data yang diadakan oleh pihak internal maupun bersama Badan Siber dan Sandi Negara (BSSN) serta lembaga terkait lainnya. Pendekatan ini mencerminkan pemahaman yang baik mengenai signifikansi pembelajaran berkelanjutan dalam menghadapi perubahan teknologi yang sangat dinamis. Program pelatihan yang dilaksanakan tidak hanya menitikberatkan pada aspek teknis saja, tetapi juga mencakup peningkatan kesadaran mengenai pentingnya keamanan data dan privasi dalam setiap kegiatan operasional. Kolaborasi dengan BSSN sebagai lembaga otoritas keamanan siber nasional juga mencerminkan usaha untuk mengimplementasikan praktik terbaik dan standar keamanan yang telah teruji di tingkat nasional.

Kerja sama di dalam departemen pada struktur Direktorat Aptika telah berjalan dengan cukup baik dan menunjukkan pola koordinasi yang teratur. Studi menunjukkan bahwa kerjasama antar departemen sangat krusial dan dilakukan secara intensif, khususnya antara tim analisis data, unit keamanan siber, dan divisi hukum. Kerjasama antara ketiga unit ini sangat penting karena kompleksitas tantangan yang dihadapi dalam era digital saat ini memerlukan pendekatan lintas disiplin. Tim analis data berfungsi dalam menemukan pola dan kecenderungan dari big data yang telah dikumpulkan, unit keamanan siber memiliki tanggung jawab untuk menjaga infrastruktur dan sistem informasi dari berbagai ancaman, sedangkan bagian hukum menawarkan perspektif regulasi dan kepatuhan terhadap aturan yang berlaku. Kerjasama yang mendalam ini memungkinkan proses pengambilan keputusan yang lebih menyeluruh dan didasarkan pada analisis mendetail dari berbagai perspektif.

Di luar itu, terutama terkait dengan pendidikan masyarakat, masih ada celah yang cukup besar dalam sosialisasi dan kampanye peningkatan kesadaran publik. Temuan studi menunjukkan bahwa pendidikan mengenai risiko perjudian online di sekitar masih sangat terbatas, dengan keluhan bahwa kampanye atau sosialisasi langsung mengenai bahaya perjudian online kepada masyarakat hampir tidak pernah dilakukan. Keadaan ini menunjukkan adanya ketidaksesuaian antara upaya internal Direktorat Aptika dalam

mengembangkan kapasitas SDM dengan program outreach untuk mendidik masyarakat. Namun, keberhasilan dalam melawan kejahatan siber dan menjaga data pribadi tidak hanya tergantung pada kemampuan internal organisasi, tetapi juga pada tingkat kesadaran dan kewaspadaan masyarakat sebagai pengguna akhir teknologi digital.

Berdasarkan penjelasan tersebut dapat ditarik kesimpulan bahwa Keterbatasan dalam pendidikan masyarakat ini dapat berpengaruh terhadap bertambahnya jumlah korban kejahatan siber, termasuk perjudian daring, yang pada akhirnya akan menambah beban tugas Direktorat Aptika dalam menangani kasus dan penegakan hukum. Masyarakat yang kurang memahami risiko dan bahaya dari aktivitas online tertentu cenderung lebih mudah menjadi korban, sehingga dibutuhkan strategi komunikasi publik yang lebih efisien dan jangkauan yang lebih luas. Ini membutuhkan kolaborasi dengan berbagai pemangku kepentingan, termasuk media, organisasi masyarakat sipil, institusi pendidikan, dan platform media sosial agar pesan edukasi dapat disampaikan dengan cara yang menarik dan mudah dimengerti oleh berbagai kelompok masyarakat.

3.3 Aspek *Processes* (Proses)

Direktorat Aplikasi dan Informatika (Aptika) telah berhasil menciptakan struktur operasional yang teratur dengan baik melalui penerapan Prosedur Operasional Standar (SOP) yang jelas dan menyeluruh. Struktur operasional yang kuat ini menunjukkan komitmen organisasi dalam melaksanakan tugas dan fungsinya dengan cara yang profesional dan terukur. Namun, di pihak lain, penelitian juga menunjukkan adanya perbedaan yang cukup besar dalam aspek sosialisasi dan akses informasi kepada masyarakat. Situasi ini menghasilkan sebuah paradoks di mana walaupun Direktorat Aptika memiliki kemampuan teknis dan operasional yang memadai, efek dan keuntungan yang diharapkan belum dapat dirasakan secara maksimal oleh masyarakat umum akibat kurangnya komunikasi dan edukasi publik.

Dalam pengelolaan data, Direktorat Aptika telah menunjukkan tingkat profesionalisme yang tinggi dengan menerapkan prosedur verifikasi dan validasi data yang ketat, serta memanfaatkan teknologi enkripsi dan kontrol akses yang ketat. Penerapan teknologi enkripsi mencerminkan kesadaran lembaga mengenai perlunya menjaga integritas dan kerahasiaan data yang dikelola, mengingat sifat sensitif informasi yang ditangani oleh Direktorat Aptika meliputi data pribadi masyarakat dan informasi strategis mengenai keamanan siber nasional. Pengawasan akses yang ketat juga menunjukkan adanya sistem otorisasi berlapis, di mana hanya staf yang memiliki wewenang dan kebutuhan tertentu yang diperbolehkan mengakses data sesuai dengan prinsip need-to-know dan least privilege. Prosedur verifikasi dan validasi data yang ketat juga mencerminkan komitmen untuk menjamin akurasi dan keandalan data yang digunakan sebagai landasan dalam pengambilan keputusan operasional dan strategis.

Walaupun struktur operasional internal sudah terorganisir dengan baik, penelitian menunjukkan adanya ketidaksesuaian yang signifikan antara kapasitas internal organisasi dan kesadaran publik serta aksesibilitas. Dari sudut pandang masyarakat, ada keterbatasan akses informasi yang cukup mencemaskan, di mana mayoritas masyarakat mengakui bahwa mereka tidak memahami rincian proses pelaporan dan mekanisme yang ada. Pernyataan masyarakat bahwa mereka "mungkin bisa melapor ke polisi atau menggunakan website pemerintah, tetapi saya sendiri belum pernah mencobanya" mencerminkan ketidakpastian dan keraguan mengenai prosedur yang harus dilalui saat menghadapi masalah terkait kejahatan siber atau pelanggaran data pribadi. Keadaan ini menunjukkan bahwa walaupun Direktorat Aptika memiliki sistem dan prosedur yang baik, informasi mengenai layanan dan mekanisme tersebut tidak disampaikan kepada masyarakat secara efektif.

Berdasarkan penjelasan tersebut dapat ditarik kesimpulan bahwa kesenjangan dalam komunikasi publik ini memiliki pengaruh yang signifikan terhadap keberhasilan program dan kebijakan yang dilaksanakan oleh Direktorat Aptika. Ketika masyarakat kurang mendapatkan informasi terkait prosedur pelaporan, mereka cenderung tidak melaporkan peristiwa yang dialami, sehingga banyak kasus yang tidak terpantau oleh sistem pemantauan. Hal ini dapat mengakibatkan penilaian yang kurang terhadap ukuran masalah yang sebenarnya

dan berisiko mengganggu ketepatan data yang digunakan dalam perencanaan strategis. Di samping itu, individu yang tidak menyadari risiko serta cara-cara kejahatan siber akan lebih mudah menjadi korban, yang pada gilirannya akan menambah tekanan pada sistem penegakan hukum dan berpotensi merugikan perekonomian nasional.

3.4. Aspek *Technology* (Teknologi)

Direktorat Aplikasi dan Informatika (Aptika) telah meraih tingkat kecanggihan yang tinggi dalam penerapan teknologi untuk mendukung operasional pengawasan dan penegakan hukum di ranah digital. Penerapan teknologi canggih ini menunjukkan pemahaman organisasi terkait kompleksitas tantangan keamanan siber saat ini yang membutuhkan pendekatan teknologi yang sama-sama canggih. Penerapan beragam platform teknologi canggih ini tidak hanya mencerminkan komitmen terhadap modernisasi operasional, tetapi juga menandakan penyesuaian terhadap lanskap ancaman digital yang terus berubah dengan cepat. Namun, di sisi lain, penelitian juga menunjukkan realitas paradoksal di mana teknologi yang sama yang diterapkan untuk penegakan juga menjadi pendorong bagi aktivitas ilegal yang ingin dicegah, menciptakan perlombaan senjata teknologi antara regulator dan pelaku kejahatan siber.

Dari sudut pandang masyarakat, data penelitian menunjukkan pengaruh besar teknologi dalam proliferasi perjudian online, di mana kemudahan akses internet, tingginya iklan di media sosial, dan kesederhanaan transaksi digital menciptakan situasi ideal yang memudahkan orang untuk tergoda mencoba perjudian online. Kenyataan ini menggambarkan sifat dua sisi dari kemajuan teknologi, di mana teknologi yang menawarkan kenyamanan dan konektivitas juga menimbulkan kerentanan serta peluang untuk aktivitas ilegal. Meningkatnya kemudahan akses internet melalui smartphone dan koneksi broadband yang semakin luas secara signifikan mengurangi hambatan untuk masuk ke dunia perjudian daring. Iklan media sosial yang canggih dengan kemampuan micro-targeting memungkinkan operator perjudian untuk menjangkau demografis tertentu dengan pesan yang sangat personal dan meyakinkan. Sistem pembayaran digital yang mulus dan masyarakat yang semakin tanpa uang tunai juga mengurangi hambatan dalam transaksi perjudian, memudahkan perjudian impulsif dan berpotensi lebih adiktif.

Walaupun teknologi berfungsi sebagai fasilitator perilaku judi yang bermasalah, data juga menunjukkan bahwa masyarakat mendukung penggunaan teknologi untuk tujuan pencegahan dan pendidikan. Dukungan terhadap pemanfaatan aplikasi atau platform digital sebagai langkah pencegahan menunjukkan kesadaran masyarakat bahwa teknologi bisa menjadi pedang bermata dua yang bisa digunakan untuk tujuan baik atau buruk. Inisiatif komunitas untuk menyebarluaskan informasi tentang risiko perjudian online melalui media sosial menunjukkan adanya gerakan akar rumput yang bisa dimanfaatkan dan diperkuat melalui kolaborasi dengan kampanye resmi dari pemerintah. Pendekatan kesadaran yang bersumber dari kerumunan ini dapat menjadi sangat kuat karena komunikasi antar teman sering kali memiliki kredibilitas dan keterkaitan yang lebih tinggi dibandingkan dengan pesan resmi dari pemerintah.

Namun, penggunaan teknologi untuk pencegahan dan pendidikan juga menghadapi tantangan yang signifikan. Kesenjangan digital yang masih ada di Indonesia menunjukkan bahwa tidak semua segmen masyarakat memiliki akses yang setara terhadap alat pencegahan dan konten edukasi yang tersedia secara daring. Di samping itu, kelebihan informasi di ruang digital membuat pesan edukasi harus bersaing dengan jumlah konten lain yang sangat besar, termasuk iklan perjudian yang sering kali memiliki nilai produksi dan anggaran pemasaran yang jauh lebih tinggi. Misinformasi dan disinformasi juga dapat melemahkan upaya pencegahan resmi, terutama jika terdapat pesan yang bertentangan atau teori konspirasi yang beredar di platform media sosial.

Berdasarkan penjelasan tersebut dapat ditarik kesimpulan bahwa untuk pemanfaatan teknologi dalam upaya pencegahan dapat dioptimalkan, namun diperlukan strategi yang lebih canggih dan berlapis. Ini mencakup pengembangan aplikasi mobile yang ramah pengguna untuk pelaporan dan pendidikan, penerapan teknologi blockchain untuk transparansi dalam aliran dana, pemanfaatan analitik big data untuk pemodelan prediktif terhadap populasi berisiko, serta penerapan chatbot bertenaga AI untuk memberikan dukungan dan informasi segera kepada individu yang memerlukan bantuan. Kerjasama dengan perusahaan teknologi dan platform media sosial juga penting untuk memastikan bahwa pesan pencegahan memperoleh visibilitas dan

jangkauan yang memadai, mungkin melalui penyesuaian algoritmik yang mengutamakan konten edukatif daripada iklan perjudian untuk demografi atau konteks tertentu.

4. CONCLUSION

Berdasarkan temuan dari penelitian yang berjudul Pengelolaan Informasi Digital Dalam Menangani Perjudian Online di Indonesia, dengan memanfaatkan teori Keamanan Informasi (Defence In Depth) yang diusulkan oleh Coole & Brooks (2011) yang terdiri dari empat aspek/elemen yaitu *governance, people, process*, dan *technology,* dapat disimpulkan sebagai berikut:

1. Aspek *Governance* (Pemerintahan)
   Regulasi pengelolaan data di Direktorat Aptika bukan hanya sejumlah aturan yang kompleks, melainkan juga merupakan perlindungan yang nyata untuk hak-hak digital masyarakat Indonesia. Dengan mengetahui dan menggunakan regulasi ini, masyarakat dapat merasakan kenyamanan teknologi digital sekaligus tetap melindungi keamanan dan privasi data pribadi. Setiap orang memiliki tanggung jawab krusial dalam melindungi keamanan data, mulai dari mempelajari kebijakan privasi secara seksama hingga melaporkan dugaan pelanggaran kepada pihak berwenang. Akhirnya, peraturan ini ditujukan untuk membangun ekosistem digital yang aman, transparan, dan bertanggung jawab demi kemajuan teknologi yang berkelanjutan di Indonesia.
2. Aspek *People* (Manusia)
   Direktorat Aptika telah memperlihatkan komitmen dan kemajuan yang baik dalam pengembangan kapasitas SDM serta kolaborasi internal, tetap diperlukan usaha yang lebih terencana dan menyeluruh untuk menangani tantangan-tantangan yang ada. Keberhasilan melaksanakan misi Direktorat Aptika tidak hanya tergantung pada kapasitas internal organisasi, tetapi juga pada kemampuan untuk menciptakan ekosistem keamanan siber yang melibatkan semua pemangku kepentingan, termasuk masyarakat umum. Investasi dalam pengembangan sumber daya manusia, pembenahan sistem dan prosedur internal, serta peningkatan program edukasi publik adalah kunci untuk mencapai tujuan jangka panjang dalam menciptakan ruang siber yang aman dan terpercaya bagi seluruh masyarakat Indonesia.
3. Aspek *Processes* (Proses)
   Direktorat Aptika sudah memiliki struktur operasional yang kuat dengan SOP yang lengkap, teknologi mutakhir, dan prosedur yang ketat, tantangan besar masih ada dalam aspek komunikasi publik dan akses informasi. Keterbatasan ini dapat mengurangi efektivitas program dan kebijakan yang sudah direncanakan dengan baik, serta dapat berdampak pada tingkat kepercayaan dan partisipasi masyarakat. Karena itu, investasi dalam pengembangan strategi komunikasi publik yang efisien dan peningkatan aksesibilitas informasi menjadi prioritas utama untuk memaksimalkan dampak positif dari kemampuan operasional yang sudah ada. Keberhasilan dalam menghadapi tantangan ini akan mempengaruhi apakah Direktorat Aptika dapat merealisasikan tujuannya dalam menciptakan ruang siber yang aman dan dapat dipercaya bagi seluruh masyarakat Indonesia.
4. Aspek *Technology* (Teknologi)
   Penerapan teknologi mutakhir di Direktorat Aptika telah mencapai tingkat yang mengesankan dengan integrasi berbagai sistem canggih untuk pemantauan, deteksi, dan analisis. Namun, perlombaan senjata teknologi dengan penjahat siber dan operator perjudian memerlukan inovasi dan adaptasi yang berkelanjutan. Di sisi lain, dukungan publik terhadap pencegahan berbasis teknologi menunjukkan peluang untuk pendekatan kolaboratif yang dapat memperkuat efektivitas upaya penegakan hukum resmi. Tantangan di masa depan ialah bagaimana memaksimalkan dampak positif dari teknologi sambil mengurangi konsekuensi negatif, serta memastikan bahwa solusi teknologi dapat diakses dan bermanfaat bagi seluruh lapisan masyarakat Indonesia tanpa memperburuk kesenjangan digital yang sudah ada.

ACKNOWLEDGEMENTS

Penulis mengucapkan terima kasih yang sebesar-besarnya kepada semua pihak yang telah memberikan dukungan dalam penyelesaian penelitian ini. Penelitian ini didukung oleh Universitas Singaperbangsa Karawang melalui Departemen Sosial dan Politik yang telah menyediakan fasilitas dan akses penelitian. Penulis menyampaikan apresiasi yang tinggi kepada Direktorat Jenderal Aplikasi Informatika (Ditjen Aptika) Kementerian Komunikasi dan Digital Republik Indonesia yang telah memberikan akses data dan informasi yang sangat berharga untuk penelitian ini. Terima kasih khusus disampaikan kepada Tim Aduan Konten Kementerian Komunikasi dan Digital, Professional Analis Data, dan seluruh informan kunci yang telah bersedia memberikan wawasan mendalam mengenai pengelolaan informasi digital dalam menangani perjudian online. Ucapan terima kasih juga disampaikan kepada Badan Siber dan Sandi Negara (BSSN) yang telah memberikan perspektif keamanan siber yang memperkaya analisis penelitian ini. Kolaborasi dengan berbagai lembaga terkait telah memberikan pemahaman yang komprehensif mengenai kompleksitas tantangan pengelolaan informasi digital di era modern.

Penulis juga mengakui kontribusi dari masyarakat yang telah berpartisipasi sebagai responden dalam penelitian ini, memberikan gambaran nyata mengenai dampak dan tantangan perjudian online dari perspektif pengguna. Masukan mereka sangat berharga dalam memahami aspek sosial dari permasalahan yang diteliti. Terakhir, penulis menyampaikan terima kasih kepada seluruh rekan peneliti dan akademisi yang telah memberikan saran, kritik konstruktif, dan dukungan moral selama proses penelitian berlangsung. Meskipun mereka mungkin tidak setuju dengan semua interpretasi atau kesimpulan dalam penelitian ini, kontribusi dan wawasan mereka telah sangat membantu dalam memperkaya kualitas penelitian. Semoga penelitian ini dapat memberikan kontribusi yang berarti bagi pengembangan kebijakan pengelolaan informasi digital dan upaya penanggulangan perjudian online di Indonesia.

REFERENCES

[1] Annisa Laras, Najwa Salvabillah, Cindy Caroline, Jusini Delas H, Farra Dinda, & Mic Finanto. (2024). Analisis Dampak Judi Online di Indonesia. Concept: Journal of Social Humanities and Education, 3(2), 320–331. https://doi.org/10.55606/concept.v3i2.1304

[2] Chintya Siringoringo, A., Yunita, S., Negeri Medan, U., William Iskandar Ps, J. V, Percut Sei Tuan, K., Deli Serdang, K., & Utara, S. (2024). Tren Perjudian Online di Kalangan Mahasiswa: Dampak dan Upaya Pencegahannya. Journal on Education, 06(02), 10948–10956.

[3] Coole, M., P., & Brooks, D., J. (2011). Mapping the organizational relations within physical security's body of knowledge: A management heuristic of sound theory and best practice. Proceedings from the fourth Australian security and intelligence conference. Perth. Western Australia. Retrieved from: http://ro.ecu.edu.au/cgi/viewcontent.cgi?article=1013&context=asi Cyber threats and ongoing efforts to protect the nation, 1-7 (2011).

[4] Doi, , Poltak, H., & Rianto Widjaja, R. (2024). Local Engineering Journal of Local Architecture and Civil Engineering-NC-SA 4.0 DEED) license (https://creativecommons.org/licenses/by-nc-sa/4.0/) Pendekatan Metode Studi Kasus dalam Riset Kualitatif. 2(1). https://doi.org/10.59810/localengineering.

[5] Hendarto, D. H., & Handayani, R. S. (2024). Pencegahan Kejahatan Siber Terkait Distribusi Perjudian Online di Indonesia dalam Rangka Mewujudkan Keamanan dan Ketertiban Masyarakat. Pencegahan Kejahatan Siber Terkait Distribusi Perjudian Online Di Indonesia Dalam Rangka Mewujudkan Keamanan Dan Ketertiban Masyarakat, 5(5), 1542–1558.

[6] Institute, S. (2001). Defense in depth. Retrieved from SANS Institute InfoSec Reading Room.

[7] Malian, D. (2024). Penanganan Dan Tantangan Cybercrime Di Era Digital Perspektif Kriminologi. INNOVATIVE: Journal Of Social Science Research, 7048-7056

[8] Molitor, D., Saharia, A., Raghupathi, V., & Raghupathi, W. (2024). Exploring the Characteristics of Data Breaches: A Descriptive Analytic Study. Journal of Information Security, 15(02), 168–195. https://doi.org/10.4236/jis.2024.152011.

[9] Mulya, A. S. (2024). Tinjauan Kriminologi Terhadap Tindak Pidana Judi Online Studi Kasus Omzet Jaringan Judi Online Capai Rp 2,2 Milyar di Batam. Proceedings Series on Social Sciences & Humanities, 17, 97–102. https://doi.org/10.30595/pssh.v17i.1121.

[10] Naila Ainaiya, Alya Hadziqo Sae Saiffy, & Revienda Anita Fitrie. (2024). Analisis Pengambilan Keputusan Kebijakan Dalam Penanganan Perjudian Online. Eksekusi : Jurnal Ilmu Hukum Dan Administrasi Negara, 2(2), 505–518. https://doi.org/10.55606/eksekusi.v2i2.1225.

[11] Raharjo S. (2022). Pengamnan Informasi Digital Terhadap Konten Negatif Guna Mewujudkan Ketahanan Nasional. http://lib.lemhannas.go.id/public/media/catalog/0010-112200000000101/swf/7548/PPRA%2064%20-%2088%20S.pdf.

[12] Satrya, A., Nugroho, B., & Supolo, S. (2022). Tindak Pidana Pencucian Uang Terhadap Perjudian Online. AL-MANHAJ: Jurnal Hukum Dan Pranata Sosial Islam, 4(2), 287–296. https://doi.org/10.37680/almanhaj.v4i2.1863.

[13] Susanti, R. (2021). JUDI ONLINE DAN KONTROL SOSIAL MASYARAKAT PEDESAAN (Online Gambling and Social Control of Rural Communities). ETNOREFLIKA: Jurnal Sosial Dan Budaya, 10(1), 86–95. https://doi.org/10.33772/etnoreflika.v10i1.1094

[14] Wijaya, A., Gultom, R. A., Studi Peperangan Asimetris, P., & Strategi Pertahanan Unhan, F. (2015). INFORMATION SECURITY STRATEGY TO COUNTER CYBER THREATS IN ELECTRONIC PROCUREMENT SYSTEMS (STUDY OF HACKER ATTACKS IN SPSE PROVINSI LAMPUNG 2015).

[15] Zulfikar, R. dkk (2024). Academica: Jurnal Pengabdian Kepada Masyarakat Edukasi Menghadapi Era Digital Dan Resiko Teknologi Terhadap Kasus Judi Online dan Pinjaman Online dalam Upaya Penegakan dan Perlindungan Hukum bagi Masyarakat Desa Banyusari Article Info. https://doi.org/10.5281/zenodo.13358062

[16] Zurohman, A., Marhaeni, T., Astuti, P., Tjaturahono, D., & Sanjoto, B. (2016). Journal of Educational Social Studies Dampak Fenomena Judi Online terhadap Melemahnya Nilai-nilai Sosial pada Remaja (Studi di Campusnet Data Media Cabang Sadewa Kota Semarang). http://journal.unnes.ac.id/sju/index.php/jess.

[17] Lexy J Moleong. (2016). *Metode Penelitian Kualitatif.* PT. Remaja Rosdakarya : Bandung.

[18] Sugiyono. (2017). *Metode Penelitian Pendidikan (Pendekatan Kuantitatif, Kualitatif dan R & D).* Alfabeta : Bandung.

[19] Patria N, dkk. (2024). *Satu Dekade Pembagunan Digital Indonesia.* Jakarta : Kementerian Kominfo/Direktorat Jenderal Aplikasi dan Informatika RI, PT Sarana Ecommerce Nusantara.

[20] Novali Panji Nugroho, PPATK: Umur Pemain Judi Online Cenderung Rambah Usia Kurang dari 10 Tahun, https://www.tempo.co/hukum/ppatk-umur-pemain-judi-online-cenderung-rambah-usia-kurang-dari-10-tahun-1164743. (akses 11 Februari 2025).