JURNAL PENGABDIAN MASYARAKAT BANGSA
e-ISSN : 2987- 0135
Volume 2, No. 5, Tahun 2024
https://jurnalpengabdianmasyarakatbangsa.com/index.php/jpmba/index

Penguatan *Digital Literacy* terkait Informasi dan Transaksi Elektronik (ITE) untuk Pelajar di Desa Hegarmanah, Kabupaten Sumedang

Tomi Setiawan[1], Hilman A. Halim[2]
[1,2] *Fakultas Ilmu Sosial dan Ilmu Politik, Universitas Padjadjaran, Indonesia*

Corresponding Author
Nama Penulis: Tomi Setiawan
E-mail: tomi_setiawan@yahoo.com

Abstrak

Naskah ini memiliki tujuan untuk menggambarkan kegiatan yang telah dilakukan oleh Tim Pengabdian Kepada Masyarakat (PKM) Fakultas Ilmu Sosial dan Ilmu Politik Unpad terkait dengan penguatan literasi digital UU No. 19 Tahun 2016 (juncto UU No. 1 Tahun 2024) Tentang Informasi dan Transaksi Elektronik (ITE) di Desa Hegarmanah, Kabupaten Sumedang. Informasi, transaksi elektronik, dan dunia maya merupakan elemen yang saling berhubungan secara rumit di ranah digital. Ruang siber, sebagai domain yang memiliki banyak sisi, tidak hanya mencakup dampak logis tetapi juga dampak fisik dan kognitif, yang memungkinkan terjadinya operasi siber yang kompleks. Metode kegiatan yang digunakan adalah pemaparan atau sosialisasi dilanjutkan dengan diskusi atau tanya jawab. Secara keseluruhan, pelaksanaan kegiatan literasi ini berlangsung lancar dan peserta memberikan respons positif selama materi diberikan. Dari respons yang diberikan, tampak adanya kebutuhan di lapangan dari para pelajar tentang materi yang diberikan yaitu literasi digital UU No. 19 tahun 2016 tentang Informasi dan Transaksi Elektronik (ITE).

Kata kunci - *informasi, transaksi elektronik, dunia maya*

Abstract

This paper aims to describe the activities carried out by the Community Service Team (Pengabdian Kepada Masyarakat) of the Faculty of Social and Political Sciences Padjadjaran University related to the strengthening digital literacy of Law No. 19 of 2016 (juncto Law No. 1 of 2024) concerning Electronic Information and Transactions (Informasi dan Transaksi Elektronik) in Hegarmanah Village, Sumedang Regency. Information, electronic transactions, and cyberspace are intricately interconnected elements in the digital realm. Cyberspace, as a multi-faceted domain, includes not only logical impacts but also physical and cognitive impacts, allowing for complex cyber operations. The activity method used is exposure or socialization followed by discussion or question and answer. Overall, the implementation of socialization activities went smoothly and participants gave positive responses during the material provided. From the responses given, it appears that there is a need in the field from students about the material provided, namely the digital literacy of Law No. 19 of 2016 concerning Electronic Information and Transactions (Informasi dan Transaksi Elektronik).

Keywords *- information, electronic transactions, cyberspace*

PENDAHULUAN

Regulasi dunia maya merupakan tantangan yang kompleks dan terus berkembang, dengan negara-negara di seluruh dunia mengadopsi berbagai pendekatan untuk mengatasi ancaman dan kejahatan dunia maya. Sifat internasional dunia maya membutuhkan pendekatan multidisipliner, mirip dengan tata kelola area warisan bersama, yang menekankan penggunaan damai dan manfaat bagi seluruh umat manusia (Holder, 2022). Insiden siber baru-baru ini telah mendorong diskusi tentang pengaturan ruang siber, yang mengarah pada proposal untuk konvensi baru di tingkat PBB (Asyari, 2023). Seiring dengan kemajuan teknologi, kebutuhan akan hukum dan peraturan yang diperbarui di dunia maya menjadi sangat penting untuk mengatasi ancaman dunia maya secara efektif.

Hakikat keberadaan dunia maya atau *cyberspace* adalah struktur virtual buatan komputer yang berisi data abstrak yang berperan sebagai realisasi diri. Sebuah forum untuk bertukar pikiran dan sarana untuk memperkuat prinsip-prinsip demokrasi. Dunia maya, seperti yang digambarkan dalam berbagai media, menawarkan platform untuk komunikasi instan tanpa batas fisik, memungkinkan individu untuk terhubung secara global. Anonimitas dan *informalitas* interaksi *online* menciptakan transparansi dan keterbukaan, memungkinkan pengguna untuk terlibat dalam lintas budaya dan usia, menumbuhkan komunitas global di mana individu dapat berbagi pengalaman dan informasi secara *real-time* (van der Linde, 2003). Namun, sifat dunia maya juga menimbulkan kekhawatiran tentang penciptaan identitas baru yang berkelanjutan, karena mengubah isyarat tradisional yang ada dalam interaksi tatap muka, yang berpotensi berdampak pada bagaimana individu memandang dan menampilkan diri mereka secara *online*. Terlepas dari peluang untuk koneksi dan komunikasi, pergeseran ke platform digital menantang gagasan tentang pembentukan identitas dan sosialisasi, menyoroti kompleksitas interaksi manusia di dunia virtual (Whitley, 2013).

Dunia maya menghadapi berbagai tantangan keamanan, termasuk meningkatnya ancaman kejahatan siber, serangan *ransomware*, kerentanan *cloud*, pelanggaran IoT, dan risiko yang terkait dengan penggunaan mata uang *kripto* dan *blockchain* (Kumar, et.al 2022). Sifat serangan siber yang terus berkembang membuat semakin sulit untuk memerangi ancaman yang muncul, sehingga menekankan pentingnya langkah-langkah keamanan siber yang kuat baik di tingkat individu maupun organisasi. Pelanggaran privasi dan risiko keamanan nasional merupakan masalah yang signifikan di dunia maya, dengan ancaman yang canggih dan ditargetkan yang menimbulkan risiko serius bagi individu dan keamanan global (Kopczewski, et.al 2022). Pemerintah, organisasi swasta, dan individu harus terus beradaptasi dengan lanskap ancaman siber yang terus berubah, menggunakan teknik keamanan siber terbaru dan praktik etika untuk melindungi informasi sensitif dan sistem penting.

Memahami sifat dan karakter dunia maya memerlukan peraturan yang disesuaikan dengan perkembangan dan konvergensi teknologi informasi yang dapat digunakan sebagai instrumen kejahatan. Mengenai perbedaan mendasar antara dunia *cyber* dan dunia nyata, menurut (Steinberg & McDowell, 2003) bahwa satu-satunya perbedaan mendasar antara interaksi antara dunia nyata (dunia nyata/dunia fisik) dan dunia *cyber* (*cyberspace*) adalah media yang digunakan. Segala interaksi dan aktivitas di Internet dapat berdampak pada kehidupan manusia di dunia nyata, misalnya melalui transmisi data, penyebaran dan transmisi informasi dan dokumen elektronik, aksesibilitas, dan lain-lain, namun terdapat dampak negatif yang ekstrem dan berskala besar. Ada juga kemungkinan bahwa hal itu akan berdampak di dunia nyata.

Banyak permasalahan terkait dengan aktivitas di dunia maya. Salah satunya terkait dengan kesalahan manusia yang secara signifikan berdampak pada keamanan siber, dengan lebih dari 39%

risiko keamanan dikaitkan dengan faktor manusia. Tantangan yang berpusat pada manusia, seperti kelelahan keamanan dan kelangkaan tenaga profesional berbasis psikologi, berkontribusi pada pelanggaran keamanan, sehingga menekankan perlunya pemahaman holistik tentang faktor manusia dalam keamanan siber (Quchi, Hakimi, & Fazil, 2024). Kebijakan dan pelatihan keamanan siber yang tidak memadai dapat menyebabkan kesalahan manusia yang membuka pintu bagi serangan siber [3]. Interupsi dan peralihan tugas diidentifikasi sebagai sumber kesalahan yang membahayakan keamanan informasi, menyoroti perlunya pekerjaan empiris dalam *cyberpsychology* untuk memandu solusi dalam interaksi manusia-komputer (Yankson, 2023). Kesalahan manusia diakui sebagai ancaman utama terhadap keamanan Teknologi Informasi, menekankan pentingnya mitigasi dan pengendalian kesalahan ini untuk meningkatkan langkah-langkah keamanan siber (Williams, et.al. 2020).. Memahami dan mengatasi kesalahan manusia melalui program pendidikan, pelatihan, dan kesadaran sangat penting dalam mengurangi kemungkinan serangan siber dan memperkuat pertahanan terhadap ancaman yang terus berkembang.

Permasalahan lainya yang sering dilakukan individu dengan data *online* adalah mengabaikan bias, ketidakakuratan, dan batas-batas etika dalam penggunaan data sosial. Selain itu, isu-isu yang terkait dengan pengumpulan data *online*, seperti keterbatasan metodologis dan jebakan, harus dipahami untuk menghindari kesalahan interpretasi hasil (Olteanu, Kiciman, & Castillo, 2018). Sebagai contoh, kerentanan informasi kesehatan pribadi di Amerika Serikat memunculkan risiko yang terkait dengan pelanggaran data dan pentingnya praktik kebersihan data yang baik, seperti mengenkripsi data dan melatih personel tentang perlindungan data. Kesalahan-kesalahan ini dapat menyebabkan hasil yang salah atau tidak tepat, mengorbankan privasi individu dan berpotensi merusak upaya untuk meningkatkan kualitas perawatan kesehatan dan penelitian (Blumenthal, & McGraw, 2015). Oleh karena itu, sangat penting bagi individu dan organisasi untuk menyadari jebakan-jebakan ini dan mengambil tindakan pencegahan yang diperlukan untuk melindungi data online secara efektif.

Landasan pemikiran inilah yang mendasari lahirnya Undang-Undang No 11 tahun 2008 tentang Informasi dan Transaksi Elektronik (selanjutnya disebut UU tentang ITE) yang diundangkan pada tanggal 21 April 2008 yang kemudian diubah dengan UU No. 19 tahun 2016 tentang Informasi dan Transaksi Elektronik (ITE) dan telah diubah kembali dengan UU No. 1 Tahun 2024. Keberadaan UU tentang ITE jika diterapkan dengan benar akan memberikan beberapa manfaat. Berikut beberapa keunggulan UU tentang ITE sebagai undang-undang yang mengatur informasi dan transaksi elektronik di Indonesia: (a) Menjamin kepastian hukum bagi pelaku transaksi elektronik, (b) Mendorong pertumbuhan ekonomi di Indonesia, (c) Salah satu upaya pencegahan kejahatan di Internet, dan (d) Melindungi masyarakat dan pengguna Internet lainnya dari berbagai kejahatan *online*.

Secara umum tujuan pengabdian ini adalah untuk meningkatkan pemahaman pelajar di lingkungan RW 06 Desa Hegarmanah Kecamatan Jatinangor Kabupaten Sumedang tentang pedoman penggunaan Informasi dan Transaksi Elektronik. Dan secara khusus, kegiatan ini mengetahui dengan detail tentang pedoman penggunaan Informasi dan Transaksi Elektronik di kalangan pelajar di RW 06 Desa Hegarmanah Kecamatan Jatinangor Kabupaten Sumedang. Selanjutnya, manfaat kegiatan ini adalah untuk meningkatkan pemahaman pelajar di lingkungan RW 06 Desa Hegarmanah Kecamatan Jatinangor Kabupaten Sumedang khususnya tentang aturan pedoman penggunaan Informasi dan Transaksi Elektronik.

METODE

Sasaran kegiatan ini adalah pelajar dilingkungan RW 06 Desa Hegarmanah Kecamatan Jatinangor Kabupaten Sumedang. Untuk memenuhi tujuan tersebut, kegiatan Pengabdian Kepada Masyarakat (PKM) ini dirancang dalam bentuk literasi digital yang memberikan kesempatan bagi peserta untuk berdiskusi terkait UU No. 19 Tahun 2016 *juncto* UU No. 1 Tahun 2024 tentang Informasi dan Transaksi Elektronik (ITE) yang diberikan oleh pemateri dari Program Studi Administrasi Publik Fakultas Ilmu Sosial dan Ilmu Politik Unpad Dr. (c) Hilman A. Halim, MAP.

PKM dilaksanakan pada tanggal 30 November 2022. Materi yang disampaikan dapat memenuhi tujuan serta hasil yang diharapkan dari kegiatan PKM ini, yaitu mencakup literasi digital terkait UU No. 19 Tahun 2016 *juncto* UU No. 1 Tahun 2024 tentang Informasi dan Transaksi Elektronik (ITE). Pelaksanaan Tim PKM Fakultas Ilmu Sosial dan Ilmu Politik Unpad di RW 06 Desa Hegarmanah Kecamatan Jatinangor Kabupaten Sumedang terlaksana dengan dukungan penuh dari berbagai pihak, khususnya para pelajar yang antusias dalam mengikuti jalannya literasi digital. Selain itu, juga didukung oleh tim tenaga lapangan dalam mempersiapkan absensi, logistik, dokumentasi dan memastikan kelancaran acara.

HASIL DAN PEMBAHASAN

1. Hasil Pelaksanaan Kegiatan

Pelaksanaan Pengabdian Kepada Masyarakat (PKM) ini dilaksanakan pada tanggal 30 November 2022. Secara keseluruhan, pelaksanaan kegiatan literasi digital berlangsung lancar dan peserta memberikan respons positif selama materi diberikan. Dari respons yang diberikan, tampak adanya kebutuhan di lapangan dari para pelajar tentang materi yang diberikan yaitu literasi digital UU No. 19 tahun 2016 *juncto* UU No. 1 Tahun 2024 tentang Informasi dan Transaksi Elektronik (ITE). Adapun kendala yang dihadapi di lapangan pada literasi digital adalah perbedaan tingkat pemahaman awal para pelajar yang beragam tentang Informasi dan Transaksi Elektronik (ITE) itu sendiri.

Tabel 1.

Rangkaian Acara Pelaksanaan Kegiatan

Waktu	Durasi	Acara	PIC
16.00 – 16.05	5′	Persiapan Acara	Divisi Acara
16.05 – 16.10	5′	Pembukaan Acara	MC (Annisa)
16.10 – 16.15	5′	Doa	Razy
16.15 – 16.20	10′	Sambutan dan Penjelasan Kegiatan	Dr. Tomi Setiawan
16.20 – 17.20	60′	Literasi digital / sosialisasi UU tentang ITE, dilanjutkan dengan diskusi (tanya-jawab)	Dr. Hilman A. Halim & Akmal (Moderator)
17.20 – 17.25	5′	Foto bersama	Yoga
17.25 – 17.30	5′	Penutupan acara	MC (Annisa)

Dari pelaksanaan PKM terdapat fakta menarik bahwa pelajar dan masyarakat ini telah sadar akan kebutuhan dalam mempersiapkan diri untuk menggunakan Informasi dan Transaksi Elektronik (ITE) yang baik dan benar. Salah satu cara yang dilakukan adalah dengan mengikutikegiatan literasi digital UU No. 19 tahun 2016 tentang Informasi dan Transaksi Elektronik (ITE). Kebutuhan inilah yang akan dipenuhi oleh tim PKM Fakultas Ilmu Sosial dan Ilmu Politik Unpad sebagai wujud nyata hasil dari pelaksanaan PKM untuk ditawarkan sebagai sebuah solusi bagi masyarakat, khususnya para pelajar di RW 06 Desa Hegarmanah.

Gambar 1.
Foto Bersama Setelah Pelaksanaan Kegiatan Pengabdian

2. Pembahasan

Menjelajahi dunia maya memiliki berbagai risiko yang dapat menimbulkan implikasi yang signifikan. Risiko ini mencakup ancaman keamanan siber dalam sistem-sistem (System of Systems), di mana insiden siber dapat menyebar ke seluruh keamanan siber yang menekankan perlunya langkah-langkah keamanan di tingkat sistem individu dan keamanan siber (Besker, Franke, & Axelsson, 2023). Selain itu, revolusi digital membawa risiko seperti cyberbullying, pelecehan dalam kencan siber, sexting, dandanan daring, dan penggunaan Internet yang bermasalah, yang memengaruhi kesejahteraan remaja dan membutuhkan intervensi untuk mengatasi risiko ini secara kolektif (Nathans, 2022). Memahami risiko-risiko ini sangat penting untuk mengembangkan strategi yang efektif dalam menjelajahi dunia maya dengan aman dan terlindungi.

Dunia maya dapat menumbuhkan permusuhan di antara individu atau kelompok melalui berbagai mekanisme. Kebebasan akses informasi di ranah digital dapat memperburuk konflik laten dengan menyediakan platform untuk penyebaran konten yang memecah belah yang berkaitan dengan masalah suku, adat, ras, dan agama. Selain itu, perluasan ruang berpikir melalui layar dapat menyebabkan hilangnya isyarat hermeneutis, yang berpotensi mengakibatkan salah tafsir dan konflik (Petricini, 2019). Selain itu, bias sikap regional dan polarisasi intraregional dapat berkontribusi pada permusuhan online, terutama ketika individu dengan sikap antarkelompok yang berbeda berinteraksi, yang meningkatkan konflik (Rosenbusch, Evans, & Zeelenberg, 2020). Faktor-faktor ini secara kolektif menggambarkan bagaimana dunia maya secara tidak sengaja dapat memicu permusuhan dan memperburuk ketegangan di antara individu atau kelompok yang berbeda.

Mengatur dunia maya secara efektif merupakan tantangan yang signifikan karena sifatnya yang dinamis dan karakteristiknya yang transnasional. Berbagai negara berinvestasi dalam meningkatkan jaringan informasi dan mengadaptasi hukum untuk memerangi ancaman dunia maya

(Virginia, & Greiman, 2022). Tata kelola internasional ruang siber membutuhkan pendekatan multidisipliner, mirip dengan tata kelola wilayah warisan bersama, untuk memastikan penggunaan yang damai dan bermanfaat bagi seluruh umat manusia. Maraknya serangan siber telah mendorong perlunya hukum dan peraturan yang diperbarui secara global, dengan mempertimbangkan dampak dari teknologi yang berkembang seperti AI, IoT, dan komputasi awan. Namun, kurangnya kerangka kerja internasional yang terpadu menghambat regulasi yang efektif, dengan banyak inisiatif yang masih bersifat nasional atau regional, bukan global (Asyari, 2023). Mengembangkan model regulasi berlapis-lapis, belajar dari domain lain yang telah diatur, dan membina kolaborasi antara sektor publik dan swasta merupakan langkah penting dalam meningkatkan regulasi dunia maya.

Anonimitas di dunia maya memainkan peran penting dalam berkontribusi terhadap permusuhan melalui berbagai mekanisme. Penelitian telah menunjukkan bahwa anonimitas dapat mengarah pada agresi dunia maya dengan memberikan rasa impunitas kepada individu, karena mereka percaya bahwa mereka tidak akan ketahuan dan bahwa konten online tidak bersifat permanen (Michelle, & Wright, 2013). Selain itu, hubungan antara bahasa dan anonimitas sangat kompleks, dengan para ahli berpendapat bahwa kurangnya isyarat sosial dalam komunikasi online dapat menyebabkan permusuhan Jaringan anonimitas, seperti jaringan Tor, telah muncul sebagai alat bagi individu untuk menghindari sensor pemerintah, yang mengarah pada konflik antara pemerintah dan masyarakat atas kontrol pertukaran informasi di dunia maya (Rady, 2013). Temuan-temuan ini menyoroti bagaimana anonimitas dalam interaksi daring dapat mendorong agresi dan konflik, menekankan perlunya penelitian lebih lanjut dan pemahaman tentang implikasinya terhadap perilaku dan dinamika komunikasi .

Individu dapat melindungi data pribadi mereka secara online dengan memanfaatkan teknologi seperti *blockchain* untuk privasi yang terdesentralisasi (Lesjak & Čretnik, 2021). Peraturan Perlindungan Data Umum Uni Eropa memberikan mekanisme kepada individu untuk melindungi data mereka, dengan usia menjadi faktor yang mempengaruhi perilaku dalam perlindungan data. Sebagai contoh, *Decentralized Online Social Networks* (DOSN) menawarkan alternatif dari platform terpusat, memungkinkan pengguna untuk memiliki kontrol yang lebih besar terhadap informasi mereka melalui kerangka kerja kontrol akses berbasis *blockchain*, memastikan perlindungan data yang dapat diaudit dan berbasis pengguna (Rahman et.al (2019). Dengan menyadari pentingnya perlindungan data pribadi, memahami hak-hak yang terkait dengan data pribadi, dan memanfaatkan alat seperti *blockchain* untuk privasi terdesentralisasi dan kontrol akses, individu dapat meningkatkan keamanan informasi pribadi mereka di ranah siber.

Lebih jauh, Kecerdasan Buatan (*Artificial Intelligence* disingkat AI) memainkan peran penting dalam membentuk langkah-langkah keamanan siber di dunia maya dengan meningkatkan deteksi ancaman, kemampuan respons, dan analisis prediktif (Camacho, 2024). Sistem yang digerakkan oleh AI, terutama melalui algoritme pembelajaran mesin, memberdayakan kerangka kerja keamanan untuk beradaptasi secara dinamis terhadap ancaman yang muncul, menganalisis kumpulan data yang sangat besar secara *real-time* untuk mengidentifikasi anomali, mengotomatiskan tugas keamanan rutin, dan memprediksi potensi pelanggaran keamanan berdasarkan data historis dan tren yang muncul. Meskipun AI secara signifikan memperkuat mekanisme pertahanan, AI juga menghadirkan tantangan baru, seperti potensi serangan siber bertenaga AI seperti *malware* dan upaya *phishing deepfake*. Pertimbangan etika, termasuk masalah privasi dan implementasi AI yang bertanggung jawab, sangat penting dalam memastikan pendekatan yang seimbang dan aman untuk memanfaatkan AI dalam

keamanan siber. Secara keseluruhan, integrasi AI di dunia maya sangat penting bagi organisasi untuk memerangi lanskap ancaman siber yang terus berkembang secara efektif dan melindungi aset digital yang penting.

Keamanan siber memainkan peran penting dalam melindungi dunia maya dengan mempertahankan jaringan, program, dan sistem dari serangan digital yang tidak bersahabat. Dengan meningkatnya prevalensi kejahatan siber dan pelanggaran data, organisasi menyadari pentingnya keamanan siber dalam melindungi aset berharga seperti keuangan, informasi, dan aplikasi (Rajabion, 2023). Permintaan akan profesional keamanan siber terus meningkat, terutama di industri yang berurusan dengan data konsumen dalam jumlah besar seperti keuangan, perawatan kesehatan, dan rite. Keamanan siber bertujuan untuk mencegah akses yang tidak sah, perubahan data, atau perusakan, memastikan kerahasiaan, integritas, dan ketersediaan informasi (Mohit, 2022). Seiring dengan kemajuan teknologi, penyerang siber mengembangkan metode mereka, menekankan kebutuhan berkelanjutan akan strategi keamanan siber yang inovatif untuk memerangi ancaman dan kerentanan yang muncul di ranah digital.

Sejak tahun 2008, Indonesia sendiri telah memiliki UU tentang ITE yakni Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik kemudian pada tahun 2016 UU ini diubah menjadi Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (saat ini telah diubah kembali dengan hadirnya Undang-Undang No. 1 Tahun 2024 tentang Perubahan Kedua UU No. 11 Tahun 2008 tentang ITE) yang merinci tindakan apa saja yang dilarang. Pelanggaran terhadap UU tentang ITE dapat mengakibatkan denda dan bahkan hukuman penjara. Berikut beberapa perbuatan yang dilarang dalam UU tentang ITE.

1. *Penyebaran Video Asusila*. Barang siapa melanggar kesusilaan sebagaimana dimaksud dalam Pasal 27 Ayat 1 dipidana dengan pidana penjara dan pidana penjara paling lama 6 tahun atau denda paling banyak Rp1.000.000.000,00 (Rp1 miliar).
2. *Perjudian Online*. Pasal 27(2) UU ITE juga memuat larangan terhadap aktivitas yang berkaitan dengan perjudian. Pelanggaran terhadap hal ini diancam dengan pidana penjara paling lama enam tahun dan/atau denda paling banyak Rp1.000.000.000,00 (Rp1 miliar).
3. *Pencemaran Nama Baik*. Pasal 27(3) UU ITE juga mengatur tentang pencemaran nama baik. Pelanggar yang didakwa berdasarkan bagian ini diancam dengan pidana penjara paling lama empat tahun dan/atau denda paling banyak tujuh ratus lima puluh juta rupiah. Selain itu, dalam perubahan UU Nomor 19 Tahun 2016 dijelaskan ketentuan Pasal 27 Ayat 3 merupakan tindak pidana pemberitahuan umum.
4. *Pemerasan dan Intimidasi*. Orang yang melakukan pemerasan dan intimidasi juga dapat dituntut berdasarkan Pasal 27(4) UU ITE. Ancamannya adalah pidana penjara paling lama 6 tahun dan/atau denda paling banyak Rp1.000.000.000,00 (Rp1 miliar).
5. *Berita Palsu*. Berita palsu juga dilarang dalam Pasal 28 Ayat 1 UU ITE yang mendefinisikan siapa yang dengan sengaja dan tanpa hak menyebarkan berita bohong dan menyesatkan yang merugikan konsumen dalam transaksi elektronik. Siapa pun yang menyebarkan laporan palsu diancam dengan pidana penjara paling lama 6 tahun dan/atau denda paling banyak Rp1.000.000.000,00 (Rp1 miliar).
6. *Ujaran Kebencian*. Ancaman bagi pelaku ujaran kebencian berdasarkan Pasal 28(2) adalah pidana penjara paling lama 6 tahun dan/atau denda paling banyak Rp1.000.000.000,00 (Rp1 miliar).
7. *Terorisme Online*. Sanksi bagi pelaku terorisme online yang mengancam orang lain adalah pidana penjara paling lama empat tahun dan/atau denda paling banyak Rp750.000.000,00

(Rp750 juta).

Dalam pemutakhiran naskah Tim PKM menambahkan sedikit penjelasan tentang perkembangan mutakhir terkait UU tentang ITE adalah hadirnya UU No. 1 Tahun 2024 tentang Perubahan Kedua UU No. 11 Tahun 2008 tentang ITE, untuk memastikan bahwa ruang digital Indonesia tetap bersih, sehat, beretika, produktif, dan berkeadilan, dan untuk memberikan penjelasan tentang berbagai interpretasi dan kontroversi yang muncul di masyarakat. Pasal 13A, 16A, 16B, 18A, 27A, 27B, dan 40A adalah tujuh (tujuh) pasal dari UU No. 11 Tahun 2008 yang ditambahkan pada UU No. 1 Tahun 2024. Di antara pasal baru yang ditambahkan, Pasal 13A mengatur jenis layanan apa yang dapat diberikan oleh Penyelenggara Sertifikasi Elektronik, yang meliputi: (1) Tanda Tangan Elektronik; (2) segel elektronik; (3) penanda waktu elektronik; (4) layanan pengiriman elektronik tercatat; (5) autentikasi situs web; (6) preservasi Tanda Tangan Elektronik dan/atau segel elektronik; (7) identitas digital; dan/atau (8) layanan lain yang menggunakan Sertifikat Elektronik.

Selain itu, UU No. 1 Tahun 2024 mengatur sanksi administratif yang diberikan kepada PSE jika mereka melanggar undang-undang perlindungan anak. Sanksi administratif dapat termasuk: (a) teguran tertulis; (b) denda administratif; (c) penghentian sementara; dan/atau (d) pemutusan akses. Kemudian, Undang-Undang No. 1 Tahun 2024 menetapkan bahwa Penyelenggara Sistem Elektornik (PSE) harus melindungi anak-anak yang menggunakan atau mengakses Sistem Elektronik sebagaimana disebutkan pada Pasal 16A. Untuk mengimplementasikannya, PSE harus menyediakan: (1) informasi mengenai batasan minimum usia anak yang dapat menggunakan produk atau layanannya; (2) mekanisme verifikasi pengguna anak; dan (3) mekanisme pelaporan penyalahgunaan produk, layanan, dan fitur yang melanggar atau berpotensi melanggar hak anak. Dengan disahkan UU No. 1 Tahun 2024, diharapkan dapat menjaga ruang digital Indonesia bersih, sehat, beretika, produktif, dan berkeadilan. Ini dimaksudkan untuk mewujudkan rasa keadilan masyarakat dan kepastian hukum dalam penggunaan ruang digital.

KESIMPULAN

Dunia maya memiliki konsep yang kompleks dan terus berkembang yang tidak memiliki definisi universal dalam hukum internasional. Konsep ini mencakup dunia digital yang diciptakan berdasarkan ruang fisik, sosial, dan pemikiran tradisional, yang membentuk kembali pemahaman dunia maya saat ini menjadi konsep yang lebih komprehensif yang dikenal sebagai ruang siber umum (*general cyberspace*). Ruang siber mengacu pada ranah digital *online* yang saling terhubung dan terpisah dari realitas sehari-hari, yang menghadirkan peluang dan kerentanan, terutama dalam hal keamanan siber. Memahami sifat multidisipliner ruang siber sangat penting untuk mengembangkan kerangka kerja keamanan nasional yang efektif, karena teknologi dan masyarakat saling memengaruhi, berdampak pada proses keamanan di ruang tradisional. Oleh karena itu, konsep utama ruang siber terletak pada interaksi yang rumit antara teknologi, masyarakat, dan hubungan internasional, yang menyoroti perlunya pemahaman yang lebih dalam untuk mengatasi tantangan dan peluang yang dihadirkannya.

Ranah dunia maya yang luas dan saling berhubungan memberikan pengaruh yang cukup besar pada jaringan komunikasi di seluruh dunia dengan melampaui batas-batas negara dan kedaulatan, sehingga menghadirkan tantangan di bidang privasi dan keamanan. Munculnya dunia maya telah menyebabkan munculnya tantangan dan peluang baru bagi para komunikator teknis yang

berurusan dengan "*audiens"* yang memiliki budaya yang beragam secara *online*. Pada akhirnya sistem negara berdaulat dipengaruhi oleh arus informasi di dunia maya, dengan pandangan yang berbeda mengenai implikasi terhadap integritas negara dan kerja sama internasional. Selain itu, pengaruh dunia maya juga meluas ke sumber daya manusia dan keputusan karier, di mana Internet dan jejaring sosial menyediakan data dalam jumlah besar yang dapat mempengaruhi proses pengambilan keputusan. Secara keseluruhan, dampak dunia maya terhadap komunikasi global menggarisbawahi perlunya tata kelola yang beretika, kerja sama internasional, dan intelijen strategis untuk menavigasi kompleksitas dunia digital yang saling terhubung ini.

DAFTAR PUSTAKA

Asyari, H A. (2023). Cyberspace as a Common Heritage of Mankind: Governing Normative Limitations of the Internet by Virtue of International Law. *Acta Universitatis Carolinae. Iuridica*. http://dx.doi.org/10.14712/23366478.2023.56

Besker T., Franke U., & Axelsson J. (2023). Navigating the Cyber-Security Risks and Economics of System-of-Systems. https://doi.org/10.1109/SoSE59841.2023.10178677

Blumenthal, D., & McGraw, D. (2015). Keeping Personal Health Information Safe: The Importance of Good Data Hygiene. JAMA, http://dx.doi.org/10.1001/jama.2015.2746

Camacho N G. (2024). The Role of AI in Cybersecurity: Addressing Threats in the Digital Age. *Journal of Knowledge Learning and Science Technology*. https://doi.org/10.60087/jaigs.v3i1.75

Holder, M. (2022). Cyberspace in a State of Flux: Regulating cyberspace through International Law. *Groningen journal of international law*. https://doi.org/10.21827/GroJIL.9.2.266-280

Kopczewski, M., Ciekanowski Z., Nowicka J., Bakalarczyk-Burakowska, K. (2022). Security threats in cyberspace. *Scientific Journal of the Military University of Land Forces*, doi: 10.5604/01.3001.0016.0040

Kumar, A, Pandey A, Sangam A, Bhatia, M K. (2022). Cyber Security Challenges with Latest Technologies. *International Journal For Science Technology And Engineering*, https://doi.org/10.22214/ijraset.2022.47844.

Lesjak B., & Čretnik M. (2021). How Individuals Care for Personal Data Protection When Using Online Services. *International Journal of Management, Knowledge and Learning*. https://doi.org/10.53615/2232-5697.10.139-148

Michelle F., Wright. (2013). The relationship between young adults' beliefs about anonymity and subsequent cyber aggression.. Cyberpsychology, Behavior, and Social Networking, doi: 10.1089/CYBER.2013.0009 https://doi.org/10.1089/cyber.2013.0009

Mohit, S G. (2022). Significance of Cyber Security in Cyber World. International Journal of Advanced Research in Science, Communication and Technology, doi: 10.48175/ijarsct-5193

Nathans L. (2022). Risks of Cyberspace to Fundamental Rights in the Global Era. http://dx.doi.org/10.1515/ijld-2023-2007

Olteanu A., Kiciman E., & Castillo C. (2018). A Critical Review of Online Social Data: Biases, Methodological Pitfalls, and Ethical Boundaries. https://doi.org/10.1145/3159652.3162004

Petricini, T. (2019). Explorations in the noosphere: Hermeneutic presence and hostility in cyberspace. Explorations in Media Ecology, https://doi.org/10.1386/eme.18.1-2.57_1

Quchi M M., Hakimi M., Fazil, A W. (2024). Human Factors in Cybersecurity: An in Depth Analysis of User Centric Studies. *Jurnal Ilmiah Multidisiplin Indonesia (JIM-ID)*, https://doi.org/10.58471/esaprom.v3i01.3832

Rady, M. (2013). Anonymity Networks: New Platforms for Conflict and Contention. *Social Science Research Network*, https://dx.doi.org/10.2139/ssrn.2241536

Rahman M U., Baiardi F., Guidi F., Ricci L. (2019). Protecting Personal Data using Smart Contracts. *arXiv: Cryptography and Security*. https://doi.org/10.48550/arXiv.1910.12298

Rajabion, L. (2023). Industry 5.0 and cyber crime security threats. In Advanced Research and Real-World Applications of Industry 5.0 (pp. 66-76). IGI Global.

Rosenbusch, H., Evans, A M., & Zeelenberg, M. (2020). Interregional and intraregional variability of intergroup attitudes predict online hostility. European Journal of Personality, https://doi.org/10.1002/per.2301

Steinberg P E.,& McDowell, S D. (2003). Global Communication and the Post-Statism of Cyberspace: a Spatial Constructivist View. *Review of International Political Economy*. https://doi.org/10.1080/0969229032000063207

Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua Undang-Undang No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.

Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.

Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.

van der Linde, G. (2003). The illusion of transparency in cyberspace : article. *Scrutiny*. https://doi.org/10.1080/18125440308566004

Virginia A., Greiman. (2022). Cyber Law and Regulation. https://doi.org/10.1007/978-3-030-91293-2

Whitley, E A. (2013). In Cyberspace All They See Is Your Words: A Review of the Relationship Between Body, Behavior and Identity Drawn From The Sociology Of Knowledge. *Oclc Systems & Services*. https://doi.org/10.1108/10650759710189434

Williams C., et.al. (2020). Human Error in Information Security: Exploring the Role of Interruptions and Multitasking in Action Slips. *Interruptions.* https://doi.org/10.1007/978-3-030-50732-9_80

Yankson, B. (2023). Human Error - A Critical Contributing Factor to the Rise in Data Breaches: A Case Study of Higher Education. *Holistica*. http://dx.doi.org/10.2478/hjbpa-2023-0007