Jurnal Serina Abdimas
Vol. 1, No. 2, Mei 2023: hlm 778-788 ISSN-L 2986-6065 (Versi Elektronik)

PENYULUHAN MASYARAKAT MELEK DIGITAL DALAM MEMBANGUN KESADARAN DAN PERLINDUNGAN HUKUM TERHADAP PENIPUAN DAN PENCURIAN DIGITAL

Tundjung Herning Sitabuana[1], Dixon Sanjaya[2] & Shrishti[3]

[1]Fakultas Hukum, Universitas Tarumanagara Jakarta
Email: tundjung@fh.untar.ac.id
[2]Program Studi Magister Hukum, Universitas Tarumanagara Jakarta
Email: dixonsanjaya@gmail.com
[2]Program Studi Sarjana Hukum, Universitas Tarumanagara Jakarta
Emai: shrishti@gmail.com

ABSTRACT

Internet and social media as a result of globalization and technological revolution have become a new media in committing crime. Criminal Investigation Unit in 2022 there were 8,831 cases of cyber crime dominated by authentic data manipulation (3,723 cases) and fraud through electronic media (2,131 cases). Therefore it is necessary to have legal protection from state against security of social media as stated in Article 28C paragraph (1), Article 28F, and Article 28G paragraph (1) of the 1945 Constitution. Community service activities conducted to the people of RT.001/RW.006, Srengseng Village, Kembangan District, West Jakarta, with theme of digital literacy community to build awareness and legal protection against fraud and digital theft. This activity is in the form of legal counseling, with pre-survey stages, socialization, and monitoring and evaluation. This location was chosen because the community was a legal awareness group need to increase public understanding of digital security. The results achieved of legal counseling are the community to know the scope, form, type, mode, and workings of fraud and digital theft, know legal aspects and protection available, as well as efforts that need to be made to avoid fraud and theft digital so that people are expected to be able to literate on digital security. Suggestions to the government to increase socialization concerning institutions that handle fraud and digital theft, and scope of socialization needs to be expanded to increase digital literacy and legal awareness of community.

Keywords: *Fraud and Digital Theft, Legal Counselling, Public Awareness and Protection*

ABSTRAK

Internet dan media sosial sebagai hasil globalisasi dan revolusi teknologi telah menjadi media baru dalam melakukan tindak kejahatan. Badan Reserse Kriminal Kepolisian Republik Indonesia mendata pada tahun 2022 terdapat 8.831 kasus kejahatan dunia maya yang didominasi oleh manipulasi data otentik (3.723 kasus) dan penipuan melalui media elektronik (2.131 kasus). Oleh karenanya diperlukan adanya perlindungan hukum dari negara terhadap keamanan dan kenyamanan bermedia sosial dalam memanfaatkan kemajuan teknologi sebagaimana dinyatakan dalam Pasal 28C ayat (1), Pasal 28F, dan Pasal 28G ayat (1) UUD 1945. Kegiatan Pengabdian Kepada Masyarakat ini dilakukan kepada Masyarakat RT.001/RW.006, Kelurahan Srengseng, Kecamatan Kembangan, Jakarta Barat, dengan tema masyarakat melek digital untuk membangun kesadaran dan perlindungan hukum masyarakat terhadap penipuan dan pencurian digital. Kegiatan ini berupa penyuluhan hukum, dengan tahapan pra survei, sosialisasi, serta monitoring dan evaluasi. Dipilihnya lokasi ini karena masyarakat merupakan kelompok binaan sadar hukum dan perlunya peningkatan pemahaman masyarakat mengenai keamanan digital. Hasil yang dicapai dalam pelaksanaan penyuluhan hukum dalam PKM ini adalah masyarakat mengetahui cakupan, bentuk, jenis, modus, dan cara kerja penipuan dan pencurian digital, mengetahui aspek hukum dan perlindungan yang tersedia, serta upaya-upaya yang perlu dilakukan agar terhindar dari penipuan dan pencurian digital sehingga masyarakat diharapkan dapat melek terhadap keamanan digital. Saran kepada pemerintah untuk meningkatkan sosialisasi mengenai lembaga yang menangani penipuan dan pencurian digital, dan cakupan sosialisasi perlu diperluas untuk meningkatkan literasi digital dan kesadaran hukum masyarakat.

Kata kunci: Kesadaran dan Perlindungan Masyarakat, Penipuan dan Pencurian Digital, Penyuluhan Hukum

1. PENDAHULUAN

Era Globalisasi berkembang sangat pesat melampaui kemampuan untuk mengantisipasi berbagai kemungkinan dampak yang muncul, yang ditandai dengan proses revolusi teknologi dan berbagai bentuk digitalisasi. Pesatnya perkembangan teknologi dipandang sebagai suatu keuntungan bagi

 https://doi.org/10.24912/jsa.v1i2.26056

masyarakat, akan tetapi hal yang terkadang tidak atau belum banyak diperhatikan ialah kekhawatiran bahaya baru yang muncul akibat kemutakhiran teknologi atau biasa disebut kejahatan dunia maya *(cybercrime).* Terdapat 2 (dua) jenis risiko baru yang ditimbulkan, yaitu: (1) risiko siber *(cyberrisk)* terkait dengan kerentanan terhadap jaringan dan integrasi operasional sistem; dan (2) risiko talenta terkait dengan kemampuan sumber daya manusia yang mengoperasikan dan menggunakan perangkat teknologi (Savitri, 2019).

Posisi Indonesia sebagai negara dengan jumlah penduduk mencapai 275 juta jiwa, menjadikannya sebagai pasar yang sangat potensial untuk melakukan berbagai kejahatan dunia maya. Laporan tahunan *We Are Social* yang berjudul, "Digital 2022: Indonesia" mengungkapkan bahwa pada tahun 2022, dari 277 juta penduduk terdapat 370 juta perangkat elektronik terkoneksi dengan 204 juta pengguna internet, dan 69% atau 191,4 juta orang merupakan pengguna aktif media sosial. Adapun *platform* media sosial yang paling banyak digunakan pengguna berusia 16-64 tahun adalah *WhatsApp* (88,7%), *Instagram* (84,8%), *Facebook* (81,3%), *Tiktok* (63,1%), *Telegram* (62,8%), *Twitter* (58,3), dan lainnya (Kemp, 2022). Kondisi-kondisi tersebut menjadi faktor yang mendorong transisi kejahatan konvensional menuju kejahatan digital.

Badan Reserse Kriminal Kepolisian Republik Indonesia mengemukakan bahwa kejahatan siber telah meningkat berkali-kali lipat yaitu pada tahun 2021 terdapat 612 kasus kejahatan siber, dan sepanjang tahun 2022 jumlah tersebut meningkat hampir 14 kali menjadi 8.831 kasus, yang meliputi manipulasi data autentik (3.723), penipuan melalui media elektronik (2.131), *cybercrime* (1.098), pencemaran nama baik secara elektronik (835), mengakses sistem secara tidak sah (358), dan lainnya seperti pengancaman, pornografi, prostitusi, penghinaan hingga ujaran kebencian melalui media elektronik (Pusat Informasi Kriminal Nasional Bareskrim Polri, 2023). Adapun data laporan yang diterima oleh Kementerian Komunikasi, sejak tahun 2017-2022 terdapat 486.000 laporan yang didominasi oleh kasus penipuan transaksi elektronik berkedok investasi dan jual beli (Andreya, 2022).

Pencurian dan penipuan digital merupakan suatu bentuk penggunaan layanan internet atau perangkat lunak *(software)* dengan akses internet untuk menipu atau mengambil keuntungan dari korban, seperti uang, informasi atau identitas pribadi (Amirhardja, Kurnia, & Minggilo, 2022). Dalam buku *Cyber Frauds, Scam, and Their Victims*, Button dan Cross menggunakan istilah "*Cyber Fraud and Scam*", yaitu penipuan yang berusaha untuk menipu seseorang dalam bentuk uang dan/atau informasi secara tidak etis (Button & Cross, 2017). Lebih lanjut, Bruce D. Mandelblit menjelaskan bahwa penipuan dan pencurian digital dengan merujuk penipuan yang menggunakan media internet seperti *chat rooms, email, massage board* atau *website*, untuk melakukan penipuan dengan media lembaga keuangan atau lembaga-lembaga lainnya (Maskun & Meilarati, 2017). Data yang dihimpun oleh Peneliti dari Fisipol UGM bekerjasama dengan PR2Media dan *Center for Digital Society* menunjukkan bahwa dari 1700 responden, 98,3% pernah menerima pesan penipuan. Dari 1.700 responden tersebut, 1.132 responden atau 66,6% pernah menjadi korban penipuan digital (Kurnia, 2022). Hal ini disebabkan karena rendahnya literasi digital masyarakat Indonesia yang menempatkannya rentan menjadi korban penipuan dan pencurian digital. Miskin literasi digital tersebut ditandai dengan kemalasan atau ketidakbiasaan masyarakat untuk memperhatikan, membaca, menyaring, atau memahami informasi atau peringatan yang tersedia di perangkat seluler dan dengan mudah memberikan persetujuan atas akses informasi pribadi secara langsung tanpa membaca isi ketentuan (Anonim, 2023).
Hal yang sama juga terjadi pada warga masyarakat di RT.001/RW.006, Kel. Srengseng, Kec. Kembangan, Jakarta Barat yang menjadi mitra dalam kegiatan Pengabdian Kepada Masyarakat ini di mana tidak semuanya memiliki pemahaman mengenai bentuk dan jenis penipuan dan pencurian

digital dan perlindungan hukum yang diberikan kepada mereka. Atas dasar hal tersebut, diperlukan adanya upaya-upaya untuk meningkatkan kesadaran dan pemberian perlindungan, dari potensi bahaya penipuan dan pencurian digital. Menurut Satjipto Rahardjo, perlindungan hukum diperlukan untuk mengorganisasi berbagai kepentingan dalam masyarakat agar tidak terjadi tubrukan, dan setiap orang dapat menikmati semua hak yang diberikan oleh hukum (Nola, 2016: 40). Hal ini sejalan dengan tujuan bernegara yang terkandung secara *expressive verbis* dalam Alinea IV Pembukaan Undang-Undang Dasar Negara Republik Indonesia Tahun 1945 (UUD 1945), bahwa negara berkewajiban untuk melindungi segenap bangsa Indonesia dan seluruh tumpah darah Indonesia dan untuk memajukan kesejahteraan umum. Lebih lanjut, perlindungan atas keamanan penggunaan teknologi telah dijamin sebagai hak asasi manusia oleh konstitusi, khususnya pada Pasal 28C ayat (1), 28F, dan 28G ayat (1) UUD 1945.

Upaya untuk meningkatkan kesadaran dan perlindungan dari berbagai penipuan dan pencurian digital tersebut memerlukan peningkatan literasi digital sehingga masyarakat memiliki kemampuan analitis, verifikasi, dan evaluasi dengan memahami sebab penipuan digital, jenis, dan cara kerja, kerugian yang ditimbulkan, serta aspek hukum dan aturan yang berlaku. Upaya-upaya tersebut dapat dilakukan melalui beberapa cara, yaitu: (1) Penegakan hukum bagi penanganan penipuan dan pencurian digital; (2) Publikasi kasus dan modus operandi penipuan dan pencurian digital terkini; (3) Edukasi dan pelatihan keamanan digital; (4) Ketersediaan situs tertentu untuk mengecek validitas layanan/informasi; (5) Kampanye publik agar menerapkan prinsip kehati-hatian dan edukasi digital (Kurnia, 2022). Atas dasar hal tersebut, Tim Pengabdian Kepada Masyarakat (Tim PKM) berupaya untuk melakukan edukasi dan advokasi kepada masyarakat. Kegiatan ini ditujukan untuk memberikan pembekalan atau pemahaman dasar terhadap hal-hal yang berhubungan dengan penipuan dan pencurian digital. Kegiatan PKM ini dilaksanakan dengan penyuluhan hukum masyarakat melek digital untuk membangun kesadaran dan perlindungan hukum terhadap penipuan dan pencurian digital.

2. METODE PELAKSANAAN PKM

PKM ini dilaksanakan melalui beberapa tahapan, sebagai berikut:

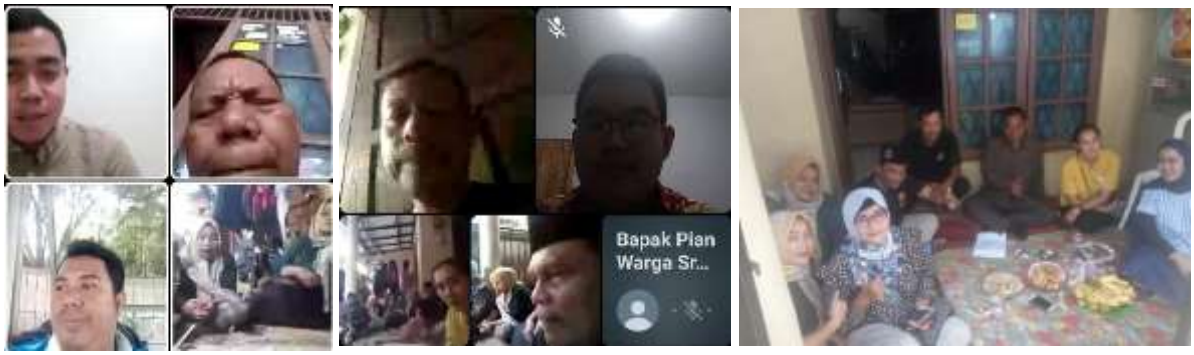
(A) Tahapan Pra-survei. Pada tahap ini dipilih lokasi RT.001/RW.006, Kel. Srengseng (Warga Srengseng), disebabkan faktor, yaitu: (a) Warga Srengseng merupakan mitra atau kelompok binaan sebagai pemodelan masyarakat sadar hukum untuk menyebarluaskan pengetahuan yang diperolehnya kepada masyarakat akar rumput *(grass root society)*; dan (b) Warga Srengseng sangat potensial menjadi korban sehingga diperlukan peningkatan literasi dan edukasi digital.

(B) Tahapan Sosialisasi, kegiatan penyuluhan dilakukan pada hari Sabtu, 11 Maret 2023 pukul 10.00 WIB. Pelaksanaan PKM dilakukan dengan menggunakan media *WhatsApp Video Call* atas permintaan Warga Srengseng agar masyarakat lebih fleksibel untuk mengikuti dan penyuluhan secara daring *(remote).* Tahapan ini terbagi menjadi 2 (dua) sesi, yaitu :

1. Tahapan Pemaparan Materi berupa “Ceramah”, oleh narasumber Bapak Ade Adhari, S.H., M.H., dan Prof. Dr. Tundjung Herning Sitabuana, S.H., C.N., M.Hum., yang merupakan Dosen Fakultas Hukum Universitas Tarumanagara. Adapun judul materi, yaitu: “Masyarakat Melek Digital”. Durasi Penyampaian materi selama 30 menit.

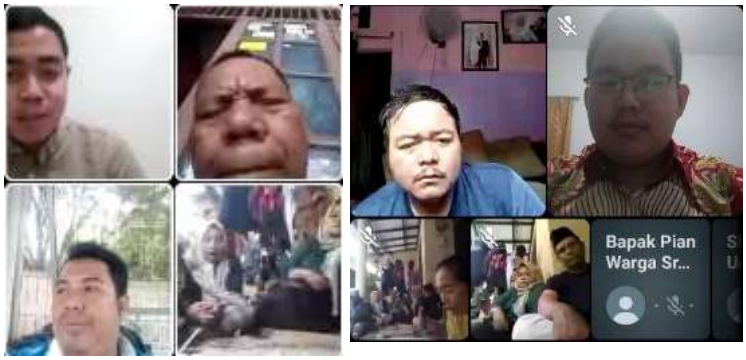
 https://doi.org/10.24912/jsa.v1i2.26056

Gambar 1.
Pemaparan Materi Narasumber



2. Tahapan *Sharing Session* berupa Q & A, dimana Warga Srengseng diberikan kesempatan untuk mengajukan pertanyaan, pernyataan, atau membagikan pengalaman terkait penipuan dan pencurian digital.

Gambar 2.
Sesi Q&A



(C) Tahapan Evaluasi dan Monitoring. Tahapan ini dilakukan sebelum dan pasca penyuluhan untuk menjamin kelancaran dan kesesuaian rencana kegiatan PKM.Proses evaluasi ditujukan untuk merumuskan rekomendasi dan perbaikan kegiatan PKM pada masa mendatang. Proses ini dilakukan secara lisan berupa saran dan masukan dari ketua Tim PKM kepada anggota. Untuk mengetahui kualitas pemahaman masyarakat dilihat dari keaktifan dan partisipasi selama berlangsungnya proses sosialisasi.

3. HASIL DAN PEMBAHASAN

Sebelum menguraikan susbstansi materi yang disampaikan dalam kegiatan ini, perlu dikemukakan beberapa pertanyaan yang diajukan oleh Warga Srengseng selama proses sosialisasi sebagai berikut:

(a) Bagaimana peran pemerintah untuk menjamin keamanan data terkait wacana penerapan kartu tanda penduduk elektronik dan sikap masyarakat?;
(b) Mengapa pengikut dari afiliasi penipuan digital (seperti investasi bodong) dapat dikategorikan sebagai korban sementara mereka telah mengetahui risikonya?; dan
(c) Apakah hukum mengatur perjudian *online*? masih banyak situs perjudian *online* dan bagaimana peran pemerintah mengatasi perjudian *online* tersebut?

Berbagai pertanyaan dan diskusi yang dilakukan bersama dengan masyarakat berlangsung dengan dinamis. Beberapa pertanyaan yang dikemukakan menunjukan bahwa perkembangan teknologi

sangat erat dengan kehidupan masyarakat seperti wacana KTP elektronik/digital, penipuan investasi dan pinjaman online, hingga pembahasan mengenai fenomena perjudian *online.* Untuk menjawab berbagai pertanyaan dan pengalaman masyarakat tersebut, perlu terlebih dahulu disadari bahwa dinamika perkembangan teknologi yang sangat cepat khususnya di tengah revolusi industri 4.0 menuju 5.0 ditandai dengan transformasi elektronik dan digitalisasi di semua lini kehidupan bermasyarakat, berbangsa, dan bernegara. Hal ini menjadi tantangan bagi hukum untuk mampu mengakomodasi perkembangan demi melindungi masyarakat sebagai *adressat* dari hukum dan teknologi itu sendiri sebagaimana sebuah ungkapan hukum menyatakan "*het recht hink achter de feiten ann*" bahwa hukum selalu berjalan tertatih-tatih di belakang suatu peristiwa dalam masyarakat. Oleh karenanya ranah digital harus diintegrasikan ke dalam sistem hukum, dan sistem hukum nasional harus mampu merespon berbagai perubahan dari proses digitalisasi khususnya dampak-dampak negatif yang ditimbulkan daripadanya. Sebagaimana telah dijelaskan bahwa kemajuan teknologi mendorong pula berbagai bentuk kejahatan baru di dunia maya *(cybercrime).* Direktorat Tindak Pidana Siber membedakan 2 (dua) kelompok besar kejahatan siber, yaitu: (Pusat Informasi Kriminal Nasional Bareskrim Polri, 2023)

(a) *Computer Crime*, yaitu kejahatan yang menggunakan komputer sebagai alat utama, berupa peretasan sistem elektronik *(hacking),* intersepsi atau penyadapan ilegal, pengubahan tampilan situs web *(web defacement),* gangguan sistem *(system interference),* dan manipulasi data *(data manipulation).*
(b) *Computer Related Crime*, yaitu kejahatan yang menggunakan komputer sebagai alat bantu berupa pornografi dalam jaringan *(online pornography),* perjudian *online,* pencemaran nama baik, pemerasan *online*, penipuan dalam jaringan *(online fraud),* ujaran kebencian, pengancaman *online*, akses ilegal, dan pencurian data *(data theft)*

Dalam praktiknya, kedua bentuk kejahatan siber tersebut termanifestasikan ke dalam berbagai bentuk penipuan dan pencurian digital, yaitu berupa: (1) *Account Take Over;* (2) *Scamming;* (3) *ID Theft;* (4) *Pharming;* (5) *Malware;* (6) *Videoscam dan Scareware;* (7) *Vishing;* (8) *Keylogging Viruses;* (9) *Koobface;* (10) *Cyber Espionage;* (11) *Cyber Sabotage dan Extortion;* dan (12) *Infringement of Privacy* (Cross *et.al*., 2014, Dam, Klausner, & Schrittwieser, 2020, Maskun & Meilarati, 2017). Penipuan dan pencurian digital dalam bentuk-bentuk tersebut dijalankan dengan serangkaian modus operandi yang paling umum menggunakan cara, yaitu:

(a) Menggunakan *email,* pesan media sosial, ataupun nomor palsu (anonim) yang mengatasnamakan orang tertentu atau organisasi/lembaga tertentu (seperti teman, keluarga, bank, lembaga asuransi, dan sebagainya) untuk menipu korban untuk memperoleh data pribadi;
(b) Menggunakan email, pesan media sosial ataupun nomor palsu (anonim) untuk menyebarkan dan mendistribusikan *malware* atau virus ke perangkat seluler sehingga memungkinkan pelaku meretas atau mengakses detail informasi pribadi korban melalui penyusupan jaringan atau sistem elektronik tertentu.

Cara-cara tersebut digunakan untuk melakukan penipuan dan pencurian digital dengan melekatkannya pada konteks yang bisa berupa pinjaman *online,* pengiriman video atau tautan situs tertentu, investasi, tawaran pekerjaan, kurir paket *e-commerce,* hadiah undian, asmara, undangan, ataupun bentuk rayuan lainnya yang mana telah mengandung virus atau *malware* atau sistem tertentu untuk meretas dan mengakses perangkat seluler korban. Sarana yang paling umum digunakan melalui pesan singkat (SMS), media sosial, *email* hingga penggunaan telepon secara langsung. Modus penipuan dan pencurian digital yang terjadi ditujukan untuk menyasar informasi atau data pribadi korban seperti kode *one time password* (OTP), *password,* nomor induk kependudukan, nomor telepon, alamat kantor, jabatan maupun nama ibu kandung. Informasi

 https://doi.org/10.24912/jsa.v1i2.26056

pribadi tersebut dapat digunakan untuk kepentingan finansial seperti melakukan pemerasan atau pembobolan rekening bank korban (Nurdiani, 2020).

Kerentanan untuk menjadi korban dari berbagai bentuk penipuan dan pencurian digital tersebut dapat dipengaruhi oleh setidak-tidaknya 3 (tiga) faktor utama, yaitu: (Salsabilah, Mulyadi, & Agustianti, 2021)

1. Faktor umur, di mana kematangan usia akan mempengaruhi kemampuan berpikir (rasionalitas), kewaspadaan, dan kehati-hatian dalam menilai informasi;
2. Faktor jenis kelamin, di mana laki-laki dan perempuan memiliki titik lemah tersendiri untuk menjadi korban penipuan dan pencurian digital;
3. Faktor Pendidikan, di mana pengetahuan dan intelegensia seseorang mempengaruhi kemampuan mengolah, memverifikasi, dan bersikap atas suatu informasi.

Kondisi-kondisi demikian telah menimbulkan keresahan dan kekhawatiran dalam masyarakat bahkan mengancam keamanan dan merugikan kesejahteraan masyarakat sehingga hukum sebagai panglima dalam negara hukum Indonesia berperan penting dalam memberikan perlindungan-perlindungan hukum. Sebagaimana hukum memiliki tujuan mencapai ketertiban, keamanan, keharmonisan, dan ketenteraman dalam masyarakat. Hukum juga menjadi alat atau sarana untuk mencapai tujuan bernegara *(staatsidee)* yang terkandung dalam Pembukaan UUD 1945 yaitu melindungi segenap bangsa Indonesia dan seluruh tumpah darah Indonesia serta memajukan kesejahteraan umum, termasuk dalam pemanfaatan teknologi media sosial. Dengan mengingat hukum sebagai suatu sistem sebagaimana dikemukakan oleh Lawrence M. Friedman, maka perlindungan hukum kepada masyarakat tidak dapat dilepaskan dari subsistem-subsistem yang ada, sebagai berikut:

Pertama, sub sistem substansi hukum *(legal susbstance)*, bahwa perlindungan hukum bagi masyarakat diatur dalam sejumlah peraturan perundang-undangan dan kebijakan pemerintah. Keberadaan Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi (UU PDP), dan Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik beserta perubahannya (UU ITE) merupakan pelengkap dalam upaya memberikan perlindungan hukum secara normatif dari bahaya penipuan dan pencurian data pribadi melalui media-media digital. Pasal 65 dan 66 UU PDP secara jelas menyatakan larangan … yang secara melawan hukum untuk mengumpulkan data pribadi yang bukan miliknya untuk keuntungan sendiri atau orang lain yang mengakibatkan kerugian pada subjek data pribadi, mengungkap data pribadi, menggunakan data pribadi milik orang lain, dan membuat data pribadi palsu atau memalsukan data pribadi (data pribadi dalam hal ini meliputi data dan informasi kesehatan, biometric, genetika, catatan kejahatan, data anak, keuangan pribadi, nama lengkap, jenis kelamin, kewarganegaraan, agama, status perkawinan, dan data yang mengidentifikasikan seseorang), yang pelanggarannya dapat diancam dengan pidana penjara sebagaimana diatur dalam Pasal 67 dan 68 disertai dengan perampasan keuntungan dan/atau harta kekayaan yang diperoleh dari hasil tindak pidana dan pembayaran ganti kerugian sebagaimana ditentukan dalam Pasal 69. Dalam Pasal 70 juga diatur sanksi terhadap tindakan yang dilakukan oleh korporasi yang dapat ditambah dengan adanya pidana tambahan. Selain itu, pengaturan yang lebih luas mengenai penyalahgunaan teknologi juga diatur dalam Pasal 30-34 UU ITE yang pada pokoknya mengatur mengenai larangan untuk secara melawan hukum mengakses, mengintersepsi, mentransmisikan, mengubah, menambah, merusak, menghilangkan, memindahkan, mengurangi, menyembunyikan, melakukan tindakan yang dapat merusak atau menyebabkan berpindahnya informasi dan/atau dokumen elektronik oleh atau kepada sistem elektronik milik orang lain. Pelanggaran atas ketentuan ini juga diancam dengan sanksi pidana sebagaiman diatur dalam Pasal 46-50 UU ITE. Beberapa peraturan teknis dan sektoral

mengamanatkan kewenangan pemerintah menyelenggarakan sistem elektronik yang aman, andal, dan bertanggung jawab.

Kedua, sub sistem struktur hukum *(legal structure).* berkaitan dengan aparatur penegak hukum telah terbentuk lembaga atau kesatuan yang bertugas mengatasi berbagai bentuk penipuan dan pencurian digital. Misalnya Amerika Serikat telah membentuk *Computer Emergency Response Team*, *Computer Crime Squad*, dan *Internet Fraud Council* yang berwenang untuk melacak, mengumpulkan data, dan menghalangi kegiatan penipuan secara *online.* Di London Inggris, Kepolisian London bersama dengan *London National Intelligence Bureae* bekerja sama dalam mengelola laman pelaporan penipuan digital, sedangkan di Singapura *Monetary Authority of Singapore, Association of Banks in Singapore, Info-communications Media Development Authority*, dan *National Crime Prevention Council* bekerja sama dalam memberantas aksi *phising* melalui SMS yang menargetkan nasabah bank, dan ada pula badan *CaseTrust* untuk sertifikasi praktik-praktik bisnis *(online)* (Maskun dan Meilarati: 2017: 90-92, Kurnia *dkk*., 2022: 126). Sementara di Indonesia, upaya penanganan dan pencegahan penipuan dan pencurian digital dilakukan oleh:

1. Kementerian Komunikasi dan Informasi dengan membentuk "Badan Regulasi Telekomunikasi Indonesia" yang berperan memproses laporan atau pengaduan penyalahgunaan jasa telekomunikasi yang diindikasikan sebagai penipuan. Langkah-langkah bagi masyarakat untuk melapor yaitu melalui situt *website* resmi Kominfo (Aduan BRTI) dengan mengisikan data diri dan menguraikan isi aduan dilengkapi dengan lampiran bukti. Kemudian aduan akan dianalisis dan diverifikasi. Apabila terbukti, Kominfo melalui SMART PPI akan mengirimkan notifikasi perintah blokir ke *provider* atau penyelenggara jasa telekomunikasi (Kementerian Komunikasi dan Informatika, 2018).
2. Kepolisian Republik Indonesia melalui Direktorat Tindak Pidana Siber Badan Reserse Kriminal (Dirtippid Siber Bareskri Polri) ayng merupakan unit kerja yang bertugas untuk melakukan penegakan hukum terhadap kejahatan siber. Tim ini juga membentuk *website* patroli siber yang berfungsi sebagai layanan informasi dan peningkatan penyuluhan hukum (Kepolisian Republik Indonesia, 2023). Selain itu, Kepolisian Republik Indonesia bekerja sama dengan Ombudsman, Kementerian Dalam Negeri, Kantor Staf Presiden, dan Kementerian Komunikasi dan Informasi juga mengembangkan aplikasi dan *website* Layanan Aplikasi dan Pengaduan Online Rakyat (Lapor), yaitu suatu sistem pengelolaan pengaduan layanan publik yang terintegrasi dalam satu pintu. Layanan ini dibentuk atas dasar Peraturan Presiden Nomor 76 Tahun 2013 tentang Pengelolaan Pengaduan Layanan Publik, dan Peraturan Menteri Pemberdayaan Aparatur Negara dan Reformasi Birokrasi Nomor 3 Tahun 2015 tentang Roadmap Pengembangan Sistem Pengelolaan Pengaduan Pelayanan Publik Nasional. Sampai dengan 2019 telah terintegrasi 34 kementerian, 96 lembaga, dan 493 pemerintahan daerah di Indonesia, dengan jumlah 570 laporan per hari, dan sejak dijalankan tahun 2012 telah menerima 1.389.891 laporan (Kepolisian Republik Indonesia, 2019).

Selain itu, terdapat pula lembaga yang tidak memiliki kewenangan penindakan melainkan kewenangan preventif yaitu Indonesia *Security Incident Response Team on Internet and Infrastructure/Coordination Center* (Id-SIRTII/CC), yang diprakarsai oleh beberapa lembaga seperti Direktorat Jenderal Pos dan Telekomunikasi, Kepolisian Republik Indonesia, Kejaksaan Agung, Bank Indonesia, Asosiasi Pengelola Jasa Internet Indonesia, Asosiasi Warung Internet Indonesia, Asosiasi Kartu Kredit Indonesia, dan Masyarakat Telematika Indonesia pada tahun 2005. Badan ini berada di bawah Badan Siber dan Sandi Negara yang berdasarkan Peraturan Badan Siber dan Sandi Negara Nomor 10 Tahun 2020 tentang Tim Tanggap Insiden Siber, Badan ini memiliki ruang lingkup, yaitu:

 https://doi.org/10.24912/jsa.v1i2.26056

1. Menyelenggarakan layanan Tim Tanggap Insiden Siber sesuai dengan kebutuhan penanganan Insiden Siber tingkat nasional;
2. Menjadi pusat koordinasi penanganan Insiden Siber tingkat nasional;
3. Merumuskan panduan teknis penanganan Insiden Siber tingkat nasional;
4. Melaksanakan registrasi Tim Tanggap Insiden Siber;
5. Menyediakan fasilitas dan mekanisme kerja untuk menerima laporan penanganan Insiden Siber dari pihak yang menerima layanan;
6. Membangun dan mengelola pangkalan data Insiden Siber dari seluruh Tim Tanggap Insiden Siber yang teregister, dan informasi mengenai Insiden Siber di tingkat nasional;
7. Memberi bantuan atau mengoordinasikan bantuan yang diperlukan dari pihak yang menerima layanan dalam hal penanganan Insiden Siber.

Tugas pokok dari badan ini berkaitan dengan sosialisasi keamanan sistem informasi pemantauan, pendeteksian, dan peringatan dini terhadap jaringan telekomunikasi dalam tindakan pengamanan pemanfaatan jaringan, membantu asistensi dan pendampingan untuk meningkatkan keamanan dan keandalan sistem informasi instransi atau lembaga strategis, serta menyelenggarakan penelitian dan pengembangan di bidang pengamanan teknologi informasi atau sistem informasi (Maskun dan Meilarati, 2017: 92-96).

Ketiga, sub sistem budaya hukum *(legal culture)* merupakan kemampuan masyarakat untuk mengantisipasi dan menghindar dari berbagai bentuk penipuan dan pencurian digital. Budaya hukum erat kaitannya dengan kesadaran hukum yaitu faktor di mana seseorang atau masyarakat mengetahui, memahami, dan mentaati hukum yang berlaku. Selo Soemardjan memaknai kesadaran hukum sebagai cara-cara di mana orang memahami hukum dan institusi hukum, yang berkaitan erat dengan faktor-faktor: (1) usaha-usaha menanamkan hukum dalam masyarakat agar masyarakat mengetahui, menghargai, mengakui, dan mentaati hukum; (2) reaksi masyarakat yang didasarkan pada sistem nilai yang berlaku; dan (3) jangka waktu penanaman hukum diharapkan dapat memberikan hasil (Apriandhini, Santi, & Widhi, 2021: 77). Dalam menghadapi berbagai bentuk penipuan dan pencurian digital, maka setidaknya ada 3 (tiga) kemampuan yang harus dimiliki masyarakat, yaitu: (Amirhardja, Kurnia, dan Monggilo, 2022: 108).

(a) Kemampuan kognitif, yaitu pengetahuan masyarakat untuk aman menggunakan segala media digital;
(b) Kemampuan afektif, yaitu sikap masyarakat untuk menjaga keamanan digital;
(c) Kemampuan behaviour, yaitu perilaku sehari-hari masyarakat yang memperhatikan keamanan digital.

Keamanan digital yang dimaksud dalam hal ini meliputi keamanan terhadap perangkat digital (misalnya pengamanan perangkat seluler menggunakan *password*, kata sandi, tanda pengenal wajah atau sidik jari, dan lainnya), pengamanan identitas pribadi maupun identitas digital, mewaspadai penipuan *online (online fraud),* dan memahami rekam jejak digital. Proses pelaksaan PKM ini berupaya mendorong dan meningkatkan kemampuan digital masyarakat. Warga Masyarakat secara aktif dan partisipatif mengikuti rangkaian sosialisasi. peningkatan pemahaman dan kesadaran masyarakat tercermin dari beberapa hal, yaitu: (1) masyarakat memperoleh pengetahuan dasar mengenai regulasi dan lembaga yang tersedia; (2) masyakarat merespon narasumber dengan mengajukan pertanyaan yang dihadapi dalam kehidupan sehari-hari; (3) masyarakat memperoleh tanggapan dan mengetahui tindak lanjut atas masalah yang dihadapi; (4) masyarakat saling merespon dan menanggapi beberapa pertanyaan yang diajukan. Proses ini sejalan dengan upaya membangun kesadaran dan kemampuan masyarakat terkait keamanan digital yang menjadi fokus dari pemerintah berdasarkan "Peta Jalan Literasi Digital 2021-2024" yang disusun oleh Kementerian Informasi dan Komunikasi dalam Kurikulum Literasi Digital, dengan

mendorong tercapainya 10 kompetensi kemampuan literasi digital dalam masyarakat, yang meliputi: (Kominfo, Siberkreasi & Delloite, 2020: 10, Kurnia *dkk*., 2020: 21)

1. Kemampuan untuk memastikan akses perangkat digital dan platform yang digunakan aman;
2. Kemampuan bersikap selektif saat menerima atau mencari informasi;
3. Kemampuan memahami berbagai peluang dan ancaman di media digital;
4. Kemampuan mengasah keterampilan analisis terhadap berbagai situasi;
5. Kemampuan untuk memverifikasi;
6. Kemampuan mengevaluasi informasi-informasi yang diterima;
7. Kemampuan mendistribusikan informasi yang dipastikan tidak akan membahayakan diri sendiri atau orang lain;
8. Keterampilan untuk memproduksi konten yang tidak membahayakan diri sendiri dan tidak membahayakan orang lain;
9. Kemampuan berpartisipasi dalam konteks keamanan digital melalui ikut melakukan pengawasan konten, melakukan pelaporan atau sekadar aktif dalam upaya sosialisasi keamanan digital; dan
10. Kemampuan berperan aktif sebagai kolaborator dalam menciptakan suasana yang aman dan nyaman dalam menggunakan media digital

Beberapa informasi yang telah dikemukakan pada saat PKM tersebut, Warga Masyarakat memperoleh pengetahuan dan pemahaman mengenai berbagai bentuk, jenis, dan modus penipuan dan pencurian digital, peraturan dan kebijakan yang berlaku, bentuk perlindungan hukum, dan upaya untuk menghindari dan mengatasi penipuan dan pencurian digital melalui lembaga negara yang tersedia. Kegiatan PKM ini ditujukan untuk mendorong peningkatan kemampuan masyarakat dalam rangka mencapai masyarakat melek digital yang ditandai dengan peningkatan kesadaran dan literasi digital serta mampu berpartisipasi secara aktif dalam menghindari, mengatasi, dan berperan serta dalam memberantasi berbagai bentuk penipuan dan pencurian digital melalui program-program kampanye publik, advokasi, hingga bermitra dengan instansi dan lembaga pemerintah untuk melakukan patroli siber di media sosial.

4. KESIMPULAN DAN SARAN

Kejahatan berbasis digital telah berkembang sedemikian rupa melalui bentuk-bentuk *virus*, *malwave*, *video*, situs tautan *(link)*, aplikasi hingga dokumen-dokumen tertentu yang dengan mudah disebarkan melalui media sosial seperti *WhatsApp, Instagram, Telegram, Twitter*, hingg *Short Message* (SMS). Kejahatan tersebut memungkinkan pelaku untuk memperoleh data dan informasi korban. Berbagai modus digunakan baik berupa pinjaman *online*, undangan, kurir pengantar paket, jual beli, video dengan judul *clickbait*, maupun hadiah undian. Kerentanan tersebut dipengaruhi oleh faktor di antaranya faktor usia, gender, maupun pendidikan. Untuk mengantisipasi penipuan dan pencurian digital telah menerbitkan undang-undang khususnya UU ITE dan UU PDP, membentuk Id-SIRTII/CC yang bersifat preventif untuk mengantisipasi potensi ancaman dan gangguan siber dalam jaringan, dan memberdayagunakan Dirtippid Siber Bareskrim Polri (melalui layanan "LAPOR"), dan Kemenkominfo (melalui layanan "Aduan BRTI") untuk melakukan penindakan penipuan dan pencurian digital. Kesulitan dalam penanganan pencurian dan kejahatan siber dapat terjadi karena dominasi tingkat kemampuan literasi digital masyarakat yang rendah. Literasi terhadap keamanan digital ditandai dengan kemampuan kognitif, afektif, dan behaviour di mana masyarakat memiliki pemahaman, kemampuan mengelola dan memverifikasi informasi, serta menerapkan prinsip kehati-hatian dalam bermedia sosial.

Melalui Kegiatan PKM kepada warga masyarakat di RT.001/RW.006, Kelurahan Srengseng, Kecamatan Kembangan, Jakarta Barat ini masyarakat memiliki pemahaman dan pengetahuan mengenai berbagai bentuk, jenis, modus, dan cara terjadinya penipuan dan pencurian digital,

 https://doi.org/10.24912/jsa.v1i2.26056

peraturan dan kebijakan yang berlaku, bentuk perlindungan hukum, cara kerja sistem hukum, dan lembaga yang memberikan perlindungan hukum serta cara mengakses perlindungan hukum yang diberikan kepada masyarakat. PKM melalui penyuluhan ini dilakukan dalam rangka mewujudkan kesadaran hukum atas berbagai perkembangan bahaya penipuan dan pencurian digital. Dengan demikian masyarakat diharapkan dapat terhindar dari bahaya penipuan dan pencurian digital serta mampu berpartisipasi aktif menyebarluaskan pengetahuan yang dimilikinya guna mengatasi berbagai bentuk pencurian dan penipuan digital. Upaya-upaya edukasi dan advokasi (kampanye publik) perlu semakin diperluas cakupan dan muatannya, dan pemerintah dapat mensosialisasikan layanan pengaduan yang tersedia sehingga semakin luas lagi kesadatan hukum yang terbangun.

Ucapan Terima Kasih *(Acknowledgement)*

Kegiatan PKM ini dapat terlaksana dengan bantuan pihak-pihak yang terlibat, Tim PKM mengucapkan terima kasih kepada Bapak Ade Adhari, S.H., M.H., sebagai narasumber dan pemateri dalam kegiatan PKM, Warga Masyarakat RT.001/RW.006, Kel. Srengseng, Jakarta Barat, dan Lembaga Penelitian dan Pengabdian Masyarakat Universitas Tarumanagara yang telah mendanai dan mendukung pelaksanaan PKM.

REFERENSI

Amirhardja, S., Kurnia, N., dan Monggilo, Z.M.Z (Ed). (2022). *Lentera Literasi Digital Indonesia: Panduan Literasi Digital Kaum Muda Indonesia Timur.* Malang: Tiga Serenda

Andreya, E. (2022, Oktober 22). Upaya Kominfo Berantas Aksi Penipuan Transaksi Elektronik. Diakses 2023, 7 Oktober. https://aptika.kominfo.go.id/2022/10/upaya-kominfo-berantas-aksi-penipuan-transaksi-online/.

Anonim. (2023, 29 Januari). Kewaspadaan Hindari Pencurian Data Pribadi. *Media Indonesia*

Apriandhini, M., Santi, Y., & Widhi, E.N. (2021). Kesadaran dan Kepatuhan Hukum Terhadap Penerapan Protokol Kesehatan Masa Pandemi Covid-19 di UPBJJ Samarinda. *Jurnal Hukum, Humaniora, Masyarakat, dan Budaya*, 1(1), 75-83. Doi: https://doi.org/ 10.33830/humaya.v1i1.1869.2021

Button, M., & Cross, C. (2017). *Cyber Frauds, Scams and Their Victims.* London: Routledge

Cross, C., *et.al.* (2014). *Challenges of Responding to Online Fraud Victimisation in Australia*. *Trends & Issue in Crime and Criminal Justice,* No. 474, 1-6. https://www.aic.gov.au/ publications/tandi/tandi474

Dam, T., Klausner, L. D., & Schrittwieser, S. (2020). *Typosquatting for Fun and Profit: Cross Country Analysis of Pop-Up Scam. Journal of Cyber Security and Mobility,* 9(2), 265-300. Doi: https://doi.org/10.13052/jcsm2245-1439.924

Kementerian Komunikasi dan Informatika, Siberkreasi, & Deloitte. (2020). *Roadmap Literasi Digital 2021-2024.* Jakarta: Kominfo, Siberkreasi, & Deloitte

Kementerian Komunikasi dan Informatika. (2018). Ayo! Laporkan Gangguan Telekomunikasi Kepada Kami. Diakses 2023, 6 Mei. https://layanan.kominfo.go.id /microsite/aduan-brti

Kemp, S. (2022, Februari 15). Digital 2022: Indonesia. Diakses 2023, 6 Maret. https://datareportal.com/ reports/digital-2022-indonesia

Kepolisian Republik Indonesia. (2023). Tentang Kami: Direktorat Tindak Pidana Siber Bareskrim Polri. Diakses 2023, 6 Maret. https://siber.jatim.polri.go.id/page/tentang-kami

Kepolisian Republik Indonesia. (2019). Apa Itu Lapor?. Diakses 2023, 6 Maret. https://polri.lapor.go.id/tentang

Kurnia, N., *dkk.* (2022). *Penipuan Digital di Indonesia: Modus, Medium, dan Rekomendasi.* Yogyakarta: Magister Ilmu Komunikasi FISIPOL UGM

Kurnia, N., *dkk.* (2020). *Kolaborasi Lawan (Hoaks) Covid-19: Kampanye, Riset, dan Pengalaman Japelidi di Tengah Pandemi.* Yogyakarta: Magister Ilmu Komunikasi UGM

Maskun dan Meilarati, W. (2017). *Aspek Hukum Penipuan Berbasis Internet.* Bandung, Keni Media

Nurdiani, I. P. (2020). Pencurian Identitas Digital Sebagai Bentuk *Cyber Related Crime*. *Jurnal Kriminologi Indonesia,* 16 (2), 1-10.

Pusat Informasi Kriminal Nasional Bareskrim Polri. (2023, Januari 5). Kejahatan Siber di Indonesia Naik Berkali-Kali Lipat. Diakses 2023, 6 Maret. https://pusiknas.polri.go.id /detail_artikel/kejahatan_siber_di_indonesia_naik_berkali-kali_ lipat

Salsabilah, T., Mulyadi, dan Agustianti, R. D. (2021). Tindak Pidana *Romance Scam* Dalam Situs Kencan *Online di* Indonesia. *Jurnal Kertha Semaya,* Vol. 9(3), 387-403. Doi: https://doi. org/10.24843/KS.2021.v09.i03.p02

Savitri, A. (2019). *Revolusi Industri 4.0: Mengubah Tantangan Menjadi Peluang di Era Distrupsi 4.0.* Yogyakarta: Genesis