

Edukasi Jaga Jejak Digital, Lindungi Masa Depan

Clerine Clarisa A¹, Olivia Sukmawati², Sunariyo Sunariyo³, Reva Apriliyanti⁴, Jhonatan Rafli⁵, Rofi Adhiatul Ariiqoh⁶

^{1,2,3,4,5,6}Prodi S1 Hukum, Fakultas Hukum, Universitas Muhammadiyah Kalimantan Timur

E-mail: 2311102432040@umkt.ac.id¹, 2311102432019@umkt.ac.id², 2311102432046@umkt.ac.id³, 2311102432047@umkt.ac.id⁴, 2311102432161@umkt.ac.id⁵, Sun487@umkt.ac.id⁶

Article History:

Received: 10 Oktober 2025

Revised: 25 Oktober 2025

Accepted: 29 Oktober 2025

Keywords: Digital, Cyber Crime, Literasi Digital

Abstract: Kegiatan pengabdian kepada masyarakat ini merupakan implementasi Tri Dharma Perguruan Tinggi yang berorientasi pada peningkatan literasi digital pelajar guna menghadapi tantangan era teknologi informasi. Program dilaksanakan di Madrasah Aliyah Negeri (MAN) 1 Samarinda, Provinsi Kalimantan Timur, pada tanggal 9 Oktober 2025, dengan melibatkan 36 siswa/i berusia 16–17 tahun. Tujuan kegiatan ini adalah meningkatkan pengetahuan dan kesadaran pelajar mengenai pengelolaan jejak digital, etika bermedia sosial, perlindungan data pribadi, serta pencegahan kejahatan siber (cybercrime). Metode pelaksanaan menggunakan pendekatan edukatif dan partisipatif melalui ceramah interaktif, diskusi, dan simulasi kasus digital. Materi yang diberikan mencakup literasi digital dasar, pengenalan berbagai bentuk kejahatan siber seperti penipuan daring, peretasan, penyalahgunaan data pribadi, dan cyberbullying, serta strategi pencegahannya. Secara teoretik, kegiatan ini berlandaskan pada Teori Literasi Digital (Paul Gilster), yang menekankan kemampuan berpikir kritis dan etis dalam memanfaatkan teknologi, Teori Pembelajaran Sosial (Albert Bandura), yang menjelaskan pembentukan perilaku digital melalui observasi dan interaksi sosial, serta Teori Tanggung Jawab Hukum (Legal Liability Theory), yang menegaskan bahwa setiap individu yang melakukan perbuatan melawan hukum wajib bertanggung jawab atas akibat perbuatannya. Dalam konteks hukum pidana siber, tanggung jawab ini dapat muncul dari tindakan seperti penyebaran konten hoaks, doxing, pencurian data, atau ujaran kebencian.

PENDAHULUAN

Pengabdian kepada masyarakat merupakan salah satu wujud pelaksanaan Tri Dharma Perguruan Tinggi yang bertujuan memberikan kontribusi nyata bagi pembangunan sosial. Salah

satu bentuk kegiatan pengabdian adalah peningkatan literasi digital bagi pelajar, yang difokuskan untuk meningkatkan pemahaman tentang pentingnya menjaga jejak digital secara bijak dan bertanggung jawab. Kegiatan pengabdian ini dirancang untuk memberikan pemahaman mendalam terkait dampak jangka panjang aktivitas digital, etika bermedia sosial, serta perlindungan data pribadi guna melindungi masa depan generasi muda di era digital.

Pengabdian juga bertujuan untuk meningkatkan kesadaran pelajar mengenai potensi risiko dan bahaya kejahatan siber (cybercrime), serta membantu mereka mengenali berbagai bentuk cybercrime seperti penipuan online, peretasan, penyalahgunaan data pribadi, dan cyberbullying, sekaligus memberikan strategi pencegahannya.

Selain itu, kegiatan ini mendorong partisipasi masyarakat dalam proses edukasi literasi digital dan pembentukan budaya digital yang aman, sehat, dan bertanggung jawab, baik di lingkungan sekolah maupun keluarga. Pengabdian ini dilaksanakan pada tanggal 09 Oktober 2025 di Madrasah Aliyah Negeri 1 Samarinda, diikuti oleh 36 siswa kelas XI B. Metode pengabdian meliputi pemaparan materi, diskusi mengenai permasalahan cybercrime di lingkungan sekolah, studi kasus nyata, serta simulasi penyusunan strategi pencegahan dan penanganan cybercrime di kalangan pelajar. Melalui kegiatan ini, diharapkan peserta dapat memahami pentingnya menjaga jejak digital dan mampu menerapkan langkah-langkah konkret untuk mencegah dan menghadapi kejahatan siber secara efektif.

Pengabdian ini diharapkan dapat membantu proses pembuktian kejahatan siber secara cepat dan akurat dengan mengumpulkan alat bukti yang sah, sehingga dapat diajukan kepada penyidik atau penyidik untuk menetapkan atau menangkap pelaku kejahatan siber. Dengan demikian, diharapkan terjadi penurunan volume kejahatan siber di kalangan mahasiswa maupun masyarakat umum. Selain itu, mahasiswa yang terlibat dalam pengabdian ini dapat berperan aktif dalam mensosialisasikan bahwa beban pembuktian kejahatan siber berada pada korban, sehingga meningkatkan kesadaran hukum masyarakat terhadap pentingnya pemahaman dan perlindungan dalam menghadapi kejahatan siber.

Perkembangan pesat teknologi informasi tidak hanya mengubah pola interaksi sosial dan komunikasi manusia, tetapi juga berdampak signifikan terhadap cara pelaksanaan tindak kejahatan. dengan memanfaatkan teknologi digital dan jaringan internet sebagai media pelaksanaannya. Contoh tindak kejahatan yang memanfaatkan teknologi tersebut antara lain penipuan, pencurian data elektronik, penghinaan, pencemaran nama baik, ujaran kebencian, pelecehan seksual, ancaman, serta berbagai bentuk kejahatan lain yang dilakukan secara maya atau elektronik.

Namun, muncul persoalan mendasar ketika tindak pidana yang dilakukan secara elektronik tersebut belum diatur secara memadai dalam sistem hukum nasional. Tanpa adanya regulasi yang jelas dan komprehensif, aparat penegak hukum akan menghadapi kesulitan dalam melakukan tindakan penegakan hukum karena tidak terdapat dasar legalitas yang sah untuk menangani kejahatan siber tersebut. Oleh karena itu, pengaturan hukum terhadap tindak pidana siber harus meliputi dua aspek utama, yakni aspek materiil dan aspek formil. Aspek materiil mencakup penentuan jenis tindak pidana, unsur-unsur pembentuk tindak pidana, serta kualifikasi dan kuantitas sanksi yang dijatuhkan. Sedangkan aspek formil berfokus pada mekanisme hukum yang digunakan dalam penanganan perkara pidana, termasuk tata cara penyidikan, penuntutan, dan

pembuktian. Salah satu aspek formil yang sangat penting dalam penanganan tindak pidana siber adalah mekanisme pembuktian.

Pembuktian menjadi kunci dalam memastikan proses hukum dapat berjalan secara efektif dan adil, mulai dari tahap penyidikan hingga persidangan di pengadilan. Dalam konteks ini, pembuktian kejahatan siber harus memenuhi ketentuan yang diatur dalam Kitab Undang-Undang Hukum Acara Pidana (KUHAP), khususnya Pasal 184 ayat (1) yang mengatur mengenai alat bukti yang sah dan dapat diterima dalam persidangan. Selain itu, Undang-Undang Nomor 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik (UU ITE) juga memberikan regulasi khusus terkait penggunaan alat bukti elektronik dalam proses pembuktian tindak pidana siber.

Dengan adanya pengaturan hukum yang komprehensif dan terpadu antara KUHAP dan UU ITE, diharapkan penegakan hukum terhadap kejahatan siber dapat dilakukan secara efektif, transparan, dan berdasarkan ketentuan hukum yang jelas. Hal ini sangat penting agar korban kejahatan siber tidak mengalami kesulitan dalam membuktikan alat bukti digital, sehingga proses penegakan hukum tidak terhambat dan pelaku kejahatan dapat segera ditindak secara hukum. Oleh sebab itu, reformasi hukum yang menyentuh aspek pembuktian kejahatan siber menjadi sebuah kebutuhan mendesak dalam menghadapi perkembangan teknologi informasi dan tantangan kejahatan di era digital.

Selain itu, masalah lain yang masih menjadi tantangan dalam sistem hukum di Indonesia adalah keterbatasan pengaturan mengenai alat bukti digital secara menyeluruh. Misalnya, ketentuan tentang alat bukti dalam Kitab Undang-Undang Hukum Acara Pidana (KUHAP), yang menjadi rujukan utama dalam proses peradilan pidana, belum diperbarui secara memadai untuk mengakomodasi penggunaan informasi dan dokumen elektronik sebagai alat bukti yang sah. Hal ini menimbulkan celah hukum yang berpotensi mempersulit proses pembuktian di pengadilan, terutama dalam kasus tindak pidana siber.

Pembahasan terkait validitas alat bukti tersebut akan difokuskan pada konsep dan parameter validitasnya, serta bagaimana peraturan yang ada dapat mendukung penerapan alat bukti elektronik tersebut. Oleh sebab itu, penulis mengangkat tema ini dalam kegiatan pengabdian masyarakat dengan judul: “Edukasi: Jaga Jejak Digital, Lindungi Masa Depan.” Kegiatan ini diharapkan dapat memberikan kontribusi dalam meningkatkan efektivitas penegakan hukum terhadap tindak pidana siber sekaligus menjaga keadilan dan kepastian hukum di era digital.

METODE

Metode pelaksanaan kegiatan pengabdian kepada masyarakat ini dilaksanakan melalui empat tahapan utama yang dirancang agar kegiatan berjalan interaktif, komunikatif, dan efektif dalam menyampaikan pesan edukatif mengenai pentingnya menjaga jejak digital untuk melindungi masa depan dari ancaman cybercrime.

Tahap pertama adalah pembukaan dan pengenalan. Tahap ini bertujuan untuk menciptakan suasana yang akrab dan tidak kaku antara tim pelaksana dan peserta kegiatan. Kegiatan diawali dengan pengenalan anggota tim serta pengenalan singkat mengenai tujuan dan manfaat dari kegiatan pengabdian ini. Metode ini dilakukan agar peserta, khususnya para siswa-siswi, merasa lebih nyaman dan terbuka dalam mengikuti seluruh rangkaian kegiatan.

Tahap kedua bersifat edukatif, yaitu pemaparan materi mengenai konsep jejak digital dan kaitannya dengan kejahatan siber (cybercrime). Pada tahap ini, peserta diberikan penjelasan tentang pengertian jejak digital, bentuk-bentuk dan jenis cybercrime, serta bahaya dan risiko yang dapat timbul akibat kurangnya kesadaran dalam beraktivitas di dunia digital. Materi juga memuat dasar hukum yang berkaitan dengan tindak pidana siber.

Tahap ketiga adalah pemberian contoh kasus yang relevan dengan kehidupan sehari-hari. Contoh kasus yang disajikan meliputi berbagai bentuk pelanggaran digital seperti pencemaran nama baik di media sosial, penipuan daring, penyebaran data pribadi tanpa izin, serta dampaknya terhadap reputasi dan masa depan individu. Penyajian kasus ini bertujuan agar peserta lebih mudah memahami penerapan materi secara nyata dan menyadari pentingnya menjaga perilaku digital.

Tahap keempat adalah sesi diskusi dan tanya jawab. Pada tahap ini, peserta diberikan kesempatan untuk menyampaikan pandangan, pengalaman, maupun pertanyaan seputar isu cybercrime dan keamanan digital. Melalui diskusi ini diharapkan muncul kesadaran kritis dan partisipasi aktif peserta dalam menciptakan budaya digital yang aman, bertanggung jawab, dan beretika.

Dengan keempat tahapan tersebut, kegiatan pengabdian diharapkan tidak hanya memberikan pemahaman teoritis, tetapi juga membangun kesadaran praktis dalam menjaga jejak digital sebagai upaya perlindungan diri dan masa depan dari berbagai ancaman kejahatan siber.

HASIL DAN PEMBAHASAN

Jejak digital merupakan rekaman permanen dari seluruh aktivitas individu di dunia maya, baik yang dilakukan secara sadar maupun tidak, meliputi unggahan di media sosial, riwayat pencarian, transaksi daring, hingga data lokasi. Fenomena ini memiliki implikasi signifikan dalam ranah hukum siber karena dapat dijadikan sebagai bukti autentik dalam kasus kejahatan siber (cybercrime), yang mencakup berbagai bentuk aktivitas ilegal seperti peretasan (hacking), phishing, penyebaran malware, pencurian identitas, cyberbullying, penipuan daring, maupun penyebaran konten ilegal. Secara konseptual, analisis perilaku digital peserta dalam kegiatan ini didasarkan pada Teori Tanggung Jawab Hukum (Legal Liability Theory), yang menegaskan bahwa setiap individu yang melakukan perbuatan melawan hukum wajib bertanggung jawab atas akibat perbuatannya. Dalam konteks hukum pidana siber, tanggung jawab tersebut dapat muncul akibat tindakan seperti penyebaran konten hoaks, doxing, pencurian data, atau ujaran kebencian.

Risiko dari jejak digital yang tidak terkelola dengan baik mencakup pelanggaran privasi, penyalahgunaan data pribadi, kerusakan reputasi, hingga ancaman pelecehan daring yang berdampak pada kehidupan sosial maupun profesional seseorang. Oleh karena itu, kesadaran untuk menjaga jejak digital menjadi hal krusial sebagai bentuk tanggung jawab terhadap keamanan dan etika berinternet. Upaya yang dapat dilakukan meliputi membagikan konten positif, menjaga kerahasiaan data pribadi, menggunakan kata sandi yang kuat, mengatur privasi akun, serta menghapus konten yang berpotensi menimbulkan persepsi negatif.

Studi kasus penusukan pasca sesi live TikTok di Banyuwangi menunjukkan bagaimana komentar daring dapat berujung pada tindak pidana nyata, menegaskan pentingnya bijak dalam berkomunikasi digital. Berdasarkan preskripsi hukum dalam Undang-Undang Informasi dan Transaksi Elektronik (UU ITE), jejak digital seperti pesan, komentar, atau rekaman live dapat dijadikan alat bukti sah sesuai Pasal 5 ayat (1), sementara pelanggaran kesusilaan daring diatur dalam Pasal 27 ayat (1), serta keterlibatan pihak lain dapat dijerat dengan Pasal 55–56 KUHP.

Dengan demikian, kesadaran hukum dan etika digital menjadi kunci utama dalam membangun lingkungan siber yang aman, bertanggung jawab, dan berdaya saing, sekaligus melindungi masa depan individu dari risiko sosial maupun hukum akibat penyalahgunaan teknologi informasi



Gambar 1. Pemaparan Definisi Cyber Crime

Sosialisasi ini juga menjelaskan secara rinci konsep validitas alat bukti yang mencakup dua dimensi: dimensi formil, yang mengutamakan kepatuhan terhadap prosedur hukum dalam memperoleh dan menyajikan alat bukti; dan dimensi materiil, yang menekankan pada keaslian, integritas, legalitas, relevansi, dan keterpercayaan dari isi alat bukti. Pemahaman terhadap kedua dimensi ini menjadi sangat penting, karena alat bukti digital seringkali dipertanyakan keabsahannya, baik dari sisi teknis maupun legal. KUHAP belum memberikan ruang secara eksplisit terhadap pengakuan bukti elektronik, sehingga timbul ketidakpastian hukum dalam praktik peradilan. Dalam konteks inilah, UU ITE memiliki peran penting sebagai pelengkap dan penguat sistem hukum acara pidana. Pasal 5 ayat (1) dan (2) UU ITE secara tegas menyatakan bahwa informasi dan/atau dokumen elektronik serta hasil cetaknya merupakan alat bukti hukum yang sah, selama memenuhi ketentuan dan standar keandalan yang ditentukan.

Dalam pelaksanaan sosialisasi, peserta tidak hanya menerima materi dalam bentuk paparan normatif, tetapi juga dilibatkan secara aktif dalam diskusi interaktif dan kajian kasus konkret. Peserta diajak menganalisis perkara-perkara siber aktual, baik yang berhasil maupun gagal dibuktikan, untuk memahami bagaimana tantangan teknis dan yuridis muncul dalam praktik penegakan hukum. Diskusi ini membuka ruang bagi peserta untuk menggali lebih dalam mengenai prosedur perolehan alat bukti digital, mekanisme menjaga rantai bukti (chain of custody), serta teknik forensik digital yang sah di mata hukum. Simulasi juga dilakukan untuk melatih peserta dalam menyiapkan dan menyusun alat bukti elektronik agar memenuhi prinsip validitas formil dan materiil sehingga dapat dipertahankan dalam proses pembuktian di pengadilan.

Jenis-jenis cyber crime atau kejahatan siber merupakan bentuk penyalahgunaan teknologi digital yang terus berkembang seiring kemajuan internet dan peningkatan aktivitas masyarakat di dunia maya. Oleh karena itu, pemahaman terhadap berbagai bentuk kejahatan siber menjadi hal yang penting, khususnya bagi siswa MAN 1 kelas XI B, sebagai bagian dari upaya peningkatan literasi digital dan kesadaran hukum di era transformasi teknologi informasi.

Salah satu bentuk kejahatan siber adalah hacking, yaitu tindakan ilegal berupa akses tanpa izin terhadap sistem komputer, server, atau data milik pihak lain dengan tujuan mencuri, mengubah, atau mengendalikan informasi tersebut. Tindakan ini melanggar ketentuan Pasal 30 ayat (1) dan (2) Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi

Elektronik (UU ITE) sebagaimana telah diubah dengan Undang-Undang Nomor 19 Tahun 2016, yang menegaskan larangan akses ilegal terhadap sistem elektronik milik orang lain.

Dirancang untuk merusak sistem komputer, mencuri data, atau memantau aktivitas pengguna tanpa sepengetahuan mereka. Contohnya meliputi virus, trojan, spyware, dan ransomware. Perbuatan ini dapat dijerat dengan Pasal 33 UU ITE, yang melarang setiap orang melakukan tindakan yang mengakibatkan gangguan, kerusakan, atau tidak berfungsinya sistem elektronik milik pihak lain.

Kejahatan berikutnya adalah identity theft atau pencurian identitas, yakni tindakan mengambil atau menggunakan data pribadi seseorang seperti nomor identitas, akun media sosial, atau informasi finansial untuk tujuan ilegal seperti membuka akun baru atau melakukan transaksi atas nama korban. Tindakan ini dapat dijerat melalui Pasal 26 ayat (1) UU ITE, yang mengatur perlindungan atas data pribadi dalam penggunaan media elektronik, serta Pasal 378 Kitab Undang-Undang Hukum Pidana (KUHP) tentang penipuan. Selain itu, cyberbullying atau perundungan daring termasuk dalam kategori kejahatan siber karena melibatkan tindakan penghinaan, pelecehan, atau ancaman melalui media digital yang dapat berdampak serius terhadap kesehatan mental dan reputasi korban. Perbuatan ini diatur dalam Pasal 27 ayat (3) UU ITE, yang melarang distribusi atau transmisi informasi elektronik yang bermuatan penghinaan dan/atau pencemaran nama baik.

Online fraud atau penipuan daring merupakan tindakan manipulatif untuk memperoleh keuntungan finansial melalui media digital, misalnya penipuan belanja online, investasi bodong, atau undian palsu. Tindakan ini diatur dalam Pasal 28 ayat (1) UU ITE serta dapat dijerat dengan Pasal 378 KUHP tentang penipuan.



Gambar 2. Pemaparan Jenis-Jenis Kejahatan Cyber

Dengan memahami berbagai bentuk kejahatan siber beserta dasar hukumnya, siswa diharapkan dapat lebih bijak dalam menggunakan teknologi, menjaga keamanan data pribadi, serta menghindari perilaku yang berpotensi menimbulkan konsekuensi hukum di dunia digital. Kesadaran hukum digital menjadi bagian penting dari pembentukan karakter generasi muda yang cerdas, beretika, dan bertanggung jawab dalam berinteraksi di ruang siber.

Selanjutnya, cyber pornography adalah penyebaran atau pembuatan konten pornografi di internet yang bertentangan dengan norma hukum dan moral, termasuk eksploitasi anak secara digital. Tindakan ini diatur dalam Pasal 27 ayat (1) UU ITE dan Undang-Undang Nomor 44 Tahun 2008 tentang Pornografi, yang secara tegas melarang penyebaran konten bermuatan pornografi. Terakhir, DoS/DDoS Attack (Denial of Service / Distributed Denial of Service) merupakan serangan siber yang dilakukan dengan cara membanjiri server menggunakan lalu

lintas palsu sehingga sistem menjadi tidak dapat diakses. Aksi ini termasuk pelanggaran terhadap Pasal 30 ayat (3) dan Pasal 33 UU ITE, karena mengganggu atau menyebabkan sistem elektronik tidak berfungsi sebagaimana mestinya.



Gambar 3. Pemaparan Materi

Bahaya dan risiko jejak digital menjadi isu penting dalam era teknologi informasi yang harus dipahami oleh siswa/i MAN 1 Samarinda sebagai bagian dari literasi hukum dan etika bermedia digital. Jejak digital mencakup seluruh aktivitas seseorang di dunia maya, seperti unggahan, komentar, dan data pribadi yang tersimpan di internet. Ketidakhati-hatian dalam mengelola jejak ini dapat menimbulkan pelanggaran privasi, penyalahgunaan data untuk pencurian identitas, penipuan daring, hingga kerusakan reputasi pribadi dan profesional. Selain itu, jejak digital yang terbuka juga berpotensi dimanfaatkan untuk tindakan cyberstalking, pelecehan daring, serta manipulasi informasi yang dapat memengaruhi keputusan sosial maupun peluang masa depan, termasuk pendidikan dan pekerjaan.

Menurut Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE), sebagaimana telah diubah dengan UU Nomor 19 Tahun 2016, setiap individu memiliki tanggung jawab hukum atas konten digital yang dibuat atau dibagikan. Pasal 27 ayat (3) UU ITE menegaskan bahwa penyebaran informasi yang mencemarkan nama baik atau melanggar kesusilaan dapat dikenakan sanksi pidana, sementara Pasal 28 ayat (1) melarang penyebaran berita bohong yang menimbulkan kerugian. Oleh karena itu, menjaga jejak digital bukan sekadar etika, tetapi juga kewajiban hukum untuk melindungi privasi dan keamanan diri. Siswa/i MAN 1 Samarinda diharapkan mampu bersikap kritis dan bertanggung jawab dalam setiap aktivitas daring dengan berpikir sebelum membagikan informasi, menggunakan media sosial secara positif, serta memahami bahwa setiap jejak digital adalah cerminan karakter dan reputasi diri yang melekat di dunia maya maupun dunia nyata.

Bagian materi ini membahas secara komprehensif bagaimana seseorang dapat menjaga jejak digital secara positif, dilengkapi dengan studi kasus nyata dan landasan hukum yang relevan menurut Undang-Undang Informasi dan Transaksi Elektronik (UU

ITE). Menjaga jejak digital secara positif berarti mengelola aktivitas daring dengan penuh kesadaran, tanggung jawab, serta menjunjung tinggi etika bermedia. Langkah utama yang perlu dilakukan, terutama bagi siswa/i MAN 1 Samarinda sebagai generasi digital, adalah membiasakan diri untuk membagikan konten yang bersifat membangun dan mencerminkan karakter positif, seperti karya pribadi, pencapaian akademik, kegiatan sosial, atau prestasi yang dapat menginspirasi orang lain. Selain itu, penting untuk melindungi data pribadi seperti alamat, nomor identitas, atau informasi finansial agar tidak disalahgunakan. Penggunaan kata sandi yang kuat dan berbeda untuk setiap akun, serta pengaturan privasi di media sosial, menjadi bagian penting dari keamanan digital. Siswa juga disarankan secara berkala melakukan penelusuran terhadap nama mereka di internet untuk memastikan tidak ada informasi yang merugikan atau salah digunakan. Etika berkomunikasi juga menjadi fondasi utama hindari ujaran kebencian, hoaks, maupun perilaku provokatif yang dapat menimbulkan konsekuensi hukum atau sosial di masa depan. Tindakan penghapusan konten lama yang tidak relevan juga termasuk dalam upaya pengelolaan identitas digital yang sehat dan bertanggung jawab.

Studi kasus yang diangkat memperlihatkan relevansi nyata antara aktivitas digital dan akibat hukum di dunia nyata. Kasus yang terjadi di Banyuwangi, misalnya, melibatkan insiden penusukan yang bermula dari komentar tidak pantas di sesi live TikTok. Komentar tersebut memicu emosi dan tantangan antara korban dan kekasih pelaku, yang akhirnya berujung pada tindak kekerasan fisik hingga korban meninggal dunia. Pelaku diketahui telah menyiapkan senjata tajam jenis karambit sebelum pertemuan, dan setelah kejadian sempat berupaya menghilangkan barang bukti serta kabur sebelum akhirnya menyerahkan diri. Dari sisi hukum, kasus ini menunjukkan bahwa aktivitas digital seperti komentar daring dapat menjadi pemicu tindak pidana di dunia nyata, dan seluruh jejak komunikasi digitalnya dapat dijadikan alat bukti sah dalam proses penyidikan. Berdasarkan ketentuan Pasal 5 ayat (1) UU ITE, informasi elektronik seperti chat, komentar, dan rekaman live diakui sebagai alat bukti hukum yang sah. Selain itu, komentar yang mengandung unsur kesusilaan dapat dijerat dengan Pasal 27 ayat (1) UU ITE, sementara pihak lain yang membantu atau turut serta dapat dijerat dengan Pasal 55–56 KUHP. Apabila terbukti terdapat unsur perencanaan dalam tindakan, seperti persiapan senjata atau ajakan pertemuan, maka dapat diterapkan Pasal 340 KUHP tentang pembunuhan berencana. Dengan demikian, studi kasus ini menjadi pembelajaran penting bagi siswa/i MAN 1 Samarinda bahwa perilaku di dunia maya memiliki konsekuensi hukum yang nyata. Segala bentuk komentar, unggahan, dan interaksi digital tidak hanya mencerminkan kepribadian seseorang, tetapi juga dapat menjadi alat bukti yang berpengaruh dalam proses penegakan hukum. Oleh karena itu, bijak dan berhati-hati

dalam beraktivitas di dunia digital adalah wujud nyata dari literasi hukum dan kesadaran etika generasi muda di era siber.



Gambar 4. Foto Bersama Siswa/1 Man 1 Samarinda

KESIMPULAN

Kegiatan pengabdian kepada masyarakat dengan tema “*Edukasi: Jaga Jejak Digital, Lindungi Masa Depan*” di MAN 1 Samarinda merupakan wujud nyata implementasi Tri Dharma Perguruan Tinggi dalam bidang pemberdayaan dan edukasi hukum digital bagi generasi muda. Melalui kegiatan ini, peserta memperoleh pemahaman komprehensif mengenai pentingnya menjaga jejak digital secara bijak, bertanggung jawab, serta berlandaskan etika dan hukum yang berlaku. Hasil kegiatan menunjukkan bahwa siswa memiliki antusiasme tinggi dalam memahami konsep jejak digital, potensi bahaya cybercrime, serta mekanisme perlindungan data pribadi. Edukasi ini juga menumbuhkan kesadaran bahwa setiap aktivitas di ruang siber meninggalkan jejak yang dapat berdampak jangka panjang, baik secara sosial maupun hukum. Dengan memahami dasar hukum yang tertuang dalam Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE) dan Kitab Undang-Undang Hukum Pidana (KUHP), peserta menjadi lebih kritis dalam berperilaku digital serta mampu menghindari pelanggaran yang dapat menimbulkan konsekuensi pidana.

Kegiatan ini tidak hanya meningkatkan literasi digital, tetapi juga memperkuat kesadaran hukum pelajar dalam menghadapi berbagai bentuk kejahatan siber seperti phishing, penipuan daring, pencurian data pribadi, cyberbullying, hingga penyebaran konten ilegal. Peserta juga dilatih untuk mengenali dan mengelola alat bukti digital secara tepat agar dapat berperan aktif dalam mendorong penegakan hukum yang efektif dan adil di era digital. Dengan demikian, kegiatan pengabdian ini berkontribusi dalam membangun budaya digital yang aman, beretika, dan berkeadilan, sekaligus mendukung terwujudnya generasi muda yang cerdas hukum dan tangguh terhadap tantangan era siber. Penguatan kapasitas literasi hukum digital di lingkungan sekolah menjadi langkah strategis untuk menekan angka kejahatan siber dan melindungi masa depan pelajar Indonesia dari dampak negatif perkembangan teknologi informasi. Penerapan Teori Tanggung Jawab Hukum (Legal Liability Theory) menegaskan bahwa setiap individu bertanggung jawab atas konsekuensi dari perbuatan melawan hukum, termasuk di ranah digital.

Dalam konteks edukasi cybercrime, teori ini relevan karena menekankan pentingnya kesadaran hukum sejak dini bagi peserta didik, agar memahami bahwa setiap aktivitas daring meninggalkan jejak hukum yang dapat dipertanggungjawabkan. Melalui pemahaman ini, edukasi literasi digital tidak hanya meningkatkan kemampuan teknis dan etis dalam bermedia sosial, tetapi juga membentuk perilaku digital yang bertanggung jawab, pencegahan pelanggaran hukum, dan penguatan budaya digital yang aman serta berintegritas di kalangan generasi muda.

PENGAKUAN/ACKNOWLEDGEMENTS

Kami menyampaikan apresiasi dan terima kasih yang sebesar-besarnya kepada Program Studi S1 Hukum Universitas Muhammadiyah Kalimantan Timur atas dukungan pendanaan dan fasilitas yang telah diberikan dalam pelaksanaan kegiatan Pengabdian kepada Masyarakat ini. Bantuan tersebut sangat berarti dalam mewujudkan kegiatan sosialisasi hukum dan literasi digital yang bertujuan memperkuat pemahaman masyarakat, khususnya pelajar, mengenai pembuktian tindak pidana siber dan etika bermedia digital.

Kegiatan ini berhasil melibatkan 36 siswa/i MAN 1 Samarinda sebagai peserta aktif yang menunjukkan antusiasme tinggi dalam mengikuti penyuluhan, diskusi interaktif, dan simulasi studi kasus hukum digital. Partisipasi para siswa tidak hanya memperlihatkan peningkatan pengetahuan mengenai dasar hukum dan risiko aktivitas digital, tetapi juga menumbuhkan kesadaran akan pentingnya menjaga jejak digital secara positif dan bertanggung jawab.

Kami berharap kegiatan ini menjadi langkah awal dalam memperkuat kolaborasi antara Program Studi S1 Hukum Universitas Muhammadiyah Kalimantan Timur dan lembaga pendidikan menengah, untuk menciptakan sinergi berkelanjutan dalam pengembangan literasi hukum, penguatan karakter digital, serta kontribusi nyata bagi masyarakat dan penegakan hukum di era teknologi informasi.

DAFTAR REFERENSI

- Erga, Y. (2018). *Kenakalan remaja dan faktor penyebabnya*. Jakarta: Bumi Aksara.
- Kartono, K. (2018). *Psikologi remaja: Teori dan aplikasi dalam pendidikan*. Jakarta: Rajawali Pers.
- Kementerian Pemberdayaan Perempuan dan Perlindungan Anak Republik Indonesia. (2023). *Laporan tahunan perlindungan anak 2023*. Jakarta: KPPPA.
- Komisi Nasional Hak Asasi Manusia Republik Indonesia (Komnas HAM RI). (2020). *Pedoman pendidikan hak asasi manusia di sekolah*. Jakarta: Komnas HAM RI.
- Waani, F. J., Lasut, J. J., & Liedfray, T. (2022). Peran media sosial dalam mempererat interaksi antar keluarga di Desa Esandom Kecamatan Tombatu Timur Kabupaten Minahasa Tenggara. *Jurnal Ilmiah Society*, 2(1), 1–13.
- Butarbutar, R. (2023). Kejahatan siber terhadap individu: Jenis, analisis, dan perkembangannya. *Jurnal Hukum & Pembangunan*, 2(2).
- Ismia. (2022). Kedudukan alat bukti elektronik dalam pembuktian perkara pidana. *Gorontalo Law Review*, 5(1), 179–189.
- Asimah, D. (2021). To overcome the constraints of proof in the application of electronic evidence. *Jurnal Hukum Peratun*, 3(2), 97–110.
- Lasaka, M. (2023). *Ius constituendum* of electronic evidence arrangement in criminal procedure

- law. *Jurnal Legalitas*, 16(2), 154–166.
- Mardiansyah, A. (2008). Mekanisme pembuktian dalam perkara tindak pidana siber (*The verification mechanisms in the event of cyber crime*). *Jurnal Legislasi Indonesia*, 12(4).
- Sari, D. P. (2021). Peran pendidikan kultural dalam penguatan kesadaran HAM di sekolah menengah. *Jurnal Kajian HAM Indonesia*, 4(2), 45–58.
- Republik Indonesia. (1945). *Undang-Undang Dasar Negara Republik Indonesia Tahun 1945*.
- Republik Indonesia. (1999). *Undang-Undang Nomor 39 Tahun 1999 tentang Hak Asasi Manusia*. Lembaran Negara Republik Indonesia Tahun 1999 Nomor 165.
- Republik Indonesia. (2014). *Undang-Undang Nomor 35 Tahun 2014 tentang Perubahan atas Undang-Undang Nomor 23 Tahun 2002 tentang Perlindungan Anak*. Lembaran Negara Republik Indonesia Tahun 2014 Nomor 297.
- Republik Indonesia. (2008). *Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE)*. Lembaran Negara Republik Indonesia Tahun 2008 Nomor 58.
- Republik Indonesia. (2016). *Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik*. Lembaran Negara Republik Indonesia Tahun 2016 Nomor 251.
- Direktorat Jenderal Aplikasi Informatika. (2021). *Keamanan digital untuk remaja*. Jakarta: Direktorat Jenderal Aplikasi Informatika.