Volume 10 Issue 1, 2024
P-ISSN: 2442-8019, E-ISSN: 2620-9837

PENGETAHUAN MAHASISWA FH UKI ANGKATAN 2023 TERHADAP PENYERAHAN DAN PENGAKSESAN PASSWORD PONSEL TANPA IZIN

Kezia Heliane Morselinda[1], L. Elly AM Pandiangan[2*], Nanin Koeswidi Astuti[3]

[1] Fakultas Hukum, Universitas Kristen Indonesia, Indonesia.
[2*] Fakultas Hukum, Universitas Kristen Indonesia. Indonesia.E-mail: elly.pandiangan@uki.ac.id
[3] Fakultas Hukum, Universitas Kristen Indonesia. Indonesia.
**Corresponding Author*

Abstract: *This article analyzes the knowledge of UKI Law Faculty students Class of 2023 regarding the protection of personal data, especially regarding the act of handing over passwords and accessing cellphones without permission. The aim is for FH students to become prospective legal professionals who will play an important role in ensuring compliance with the law and protecting individual rights. The method used is empirical juridical with a qualitative approach. Findings from the results of distributing questionnaires to 100 students showed that 56% of students were aware of the existence of the Personal Data Protection Law and/or had read and studied the contents of the Personal Data Protection Law, but 99% of students were aware that Personal Data is the right of every living creature. , and must be protected, while 30% have, whether intentionally or not, violated other people's privacy rights in the form of content or other information and 25% of students have had their rights harmed by individuals who have violated human rights in protecting personal data. UKI FH students must know that the protection of personal rights is an inseparable part of the law. Knowledge and understanding of personal data protection will be able to prepare them to handle the challenges of personal data protection legal issues in the future.*

Keywords: *Personal Data; Cell Phone Access Without Permission; Personal Data Protection.*

How to Site: Kezia Heliane Morselinda, L. Elly AM Pandiangan, Nanin Koeswidi Astuti (2024). Pengetahuan Mahasiswa FH UKI Angkatan 2023 Terhadap Penyerahan dan Pengaksesan *Password* Ponsel Tanpa Izin. Jurnal hukum *to-ra*, 10 (1), pp 56-72. DOI. 10.55809/tora.v10i1.328

Introduction

Data pribadi mengandung informasi yang sensitive karena berkaitan dengan privasi seseorang. Data pribadi ini seringkali dikumpulkan oleh lembaga-lembaga pemerintah dan non pemerintah untuk beragam keperluan, seperti pembuatan KTP, KK, pajak, peduli lindungi yang sekarang menjadi satu sehat, BPJS, pembukaan rekening Bank, pinjaman online dan sebagainya. Informasi data pribadi ini dikumpulkan secara online, hal ini rentan disalah gunakan. Perlindungan data pribadi penting dilindungi agar privasi seseorang tetap terjaga. Data pribadi seperti nama, Alamat, no identitas dan informasi seseorang yang dapat digunakan sebagai tujuan identifikasi, jika jatuh ke tangan yang

salah maka rentan terjadi pencurian identitas, penipuan dan tindakan kriminal lainnya yang dapat merugikan keuangan dan juga immaterial, seperti manipulasi opini publik atau penggunaan informasi pribadi untuk tujuan kriminal.

Perlindungan data pribadi merupakan dasar dari adanya kepercayaan masyarakat terhadap institusi atau lembaga atau organisasi dan layanan yang mengumpulkan dan mengelola data pribadi seseorang tersebut, jika data pribadi tidak dilindungi dengan baik akan menyebabkan kepercayaan publik dan menyebabkan hubungan seseorang dan pihak yang mengumpulkan dan mengelola data menjadi hilang. Perlindungan data pribadi juga berkontribusi pada pembangunan lingkungan yang mendukung inovasi dan pengembangan teknologi yang bertanggung jawab. Dengan memastikan bahwa data pribadi terlindungi, individu lebih cenderung untuk berbagi informasi dan berpartisipasi dalam penggunaan teknologi baru tanpa takut akan penyalahgunaan atau pelanggaran data pribadi.

Kasus pelanggaran data pribadi di Indonesia sejak tahun 2019 ada 79 kasus. Sejak Januari hingga Juni 2023 tercatat ada 35 kasus pelanggaran data pribadi. Pada tahun 2022, data SIM card masyarakat Indonesia yang dijual pada saat itu diklaim sebagai ulah hacker Bjorka. Bahkan, kabarnya ada 1,3 miliar data pendaftar SIM card. Data yang bocor termasuk NIK, nomor telepon provider, sampai tanggal pendaftaran yang mencapai 87 GB. Data-data ini dihargai senilai Rp743,5 juta. Sementara pada tahun 2023, terdapat kasus kebocoran data nasabah Bank Syariah Indonesia (BSI). Sebelum data bocor, terdapat keluhan gangguan layanan transaksi pada 8 Mei 2023. Lockbit mengklaim serangan terhadap BSI ada 1,5 TB data pribadi berhasil dicuri dalam kasus pencurian data ini. Lockbit adalah salah satu kelompok ransomware asal Rusia. Lockbit sempat bernegosiasi dengan pihak BSI dan meminta tebusan sebesar Rp296 miliar. Karena tak kunjung ditebus, Lockbit menyebarkan data tersebut di pasar gelap pada 16 Mei 2023. Tahun 2023 juga terjadi 34 juta data paspor bocor yang dilakukan oleh hacker Bjorka. Data yang bocor yaitu nama, nomor paspor, masa berlaku paspor, tanggal lahir, dan gender. Data-data itu dijual seharga Rp150 juta. Pada 14 Juli 2023, terjadi kebocoran 337 juta data Dukcapil di unggah di situs BreachForums yang mengklaim adalah RRR. Data-data yang bocor yaitu nama, nomor KK, tanggal lahir, alamat, NIK orang tua, nomor akta lahir, nikah, dan agama.

Pengetahuan dan kesadaran masyarakat akan keamanan digital menjadi semakin penting dalam era teknologi informasi saat ini. Di tengah perkembangan teknologi yang pesat, masalah keamanan, seperti pengaksesan data pribadi dan pelanggaran privasi semakin merebak. Salah satu aspek yang menjadi sorotan adalah praktik penyerahan data pribadi, memahami bahwa penyalahgunaan akses ke perangkat ponsel dapat mengakibatkan dampak negatif bagi masyarakat. Sebagai bagian dari masyarakat,

mahasiswa Fakultas Hukum Universitas Kristen Indonesia (FH UKI) angkatan 2023 tentu saja, tidak terkecuali menghadapai tantangan dan risiko terkait dengan keamanan digital. Mereka adalah bagian dari generasi Z yang tumbuh dalam ketergantungan pada teknologi, salah satunya adalah penggunaan smartphone yang menjadi bagian dari kehidupan sehari-hari mereka. Namun tidak dipungkiri, seiring dengan penggunaan teknologi yang semakin meningkat, menyebabkan kemungkinan terjadinya penyalahgunaan dan pelanggaran privasi juga semakin meningkat.

Salah satu permasalahan yang menjadi sorotan dalam pengetahuan mahasiswa FH UKI angkatan 2023 adalah praktik penyerahan password dan akses terhadap penggunaan ponsel tanpa izin. Penyalahgunaan password dan akses ke perangkat ponsel dapat terjadi dalam berbagai bentuk, seperti tindakan mengintip pesan pribadi hingga mengakses data sensitif pengguna tanpa seizin pemiliknya. Tindakan semacam ini tidak hanya melanggar privasi individu, tetapi juga dapat memiliki dampak yang merugikan secara hukum dan moral. Oleh karena itu, pemahaman yang kuat tentang pentingnya menjaga keamanan digital, termasuk praktik penyerahan password ponsel tanpa izin, menjadi sangat penting bagi mahasiswa FH UKI angkatan 2023. Mereka perlu diberikan pemahaman yang mendalam tentang risiko yang terkait dengan tindakan pelanggaran data pribadi, serta pentingnya menghormati data pribadi dan hak-hak digital orang lain.

Dengan pemahaman yang kuat tentang isu-isu keamanan digital ini, mahasiswa FH UKI angkatan 2023 dapat menjadi agen perubahan yang proaktif dalam mempromosikan budaya penggunaan teknologi yang bertanggung jawab dan etis. Dengan demikian, mereka tidak hanya akan menjadi pengguna teknologi yang mahir, tetapi juga individu yang sadar akan tanggung jawab moral dan hukum yang melekat dalam penggunaan teknologi informasi dan komunikasi. Data pribadi bagi setiap individu adalah hak asasi manusia yang dilindungi oleh konstitusi. Tujuan perlindungan data pribadi adalah menjamin hak warga negara atas perlindungan data pribadi dengan menumbuhkan kesadaran masyarakat, serta menjamin pengakuan dan penghormatan atas pentingnya perlindungan data pribadi.

Penelitian Spyros E. Polykalas and George N. Prezerakos mengenai perlindungan data pribadi pada aplikasi seluler yang ada di di Google Play Store dan kesesuaian dengan prosedur dan ketentuan di UE. Hasil penelitian menunjukan bahwa sebagian besar aplikasi seluler yang diperiksa memerlukan akses ke data pribadi secara luas. Selain itu, ditemukan bahwa aplikasi seluler gratis meminta akses ke pribadi data dalam tingkat yang lebih tinggi dibandingkan dengan permintaan relevan dari aplikasi berbayar, yang

menunjukkan dengan jelas bahwa model bisnis aplikasi seluler gratis didasarkan pada eksploitasi data pribadi.[1]

Penelitian Matina Tsavli, Pavlos S. Efraimidis, Vasilios Katos dan Lilian Mitrou mengenai masalah privasi dan keamanan yang muncul dari model perizinan di sistem operasi Android, beserta kekurangan yang belum ditangani secara layak. Hasil penelitian menunjukkan bahwa, sistem opetasi smartphone sangat mengkhawatirkan karena tidak menyediakan tingkat perlindungan yang memadai untuk data pribadi pengguna yang memiliki akses ke semua data pribadi namun memiliki kerentanan dalam keamanan.[2]

Penelitian Nanin Koeswidi Astuti dan Robertus Nugroho Perwiro Atmojo mengenai perlindungan konsumen atas keamanan informasi dalam transaksi e-commerce menunjukan bahwa untuk mengatasi risiko keamanan dalam traksaksi e-commerce dengan cara menggunakan mekanisme check and balance, khususnya bagi transaksi dengan nilai obyek perjanjian bernilai puluhan bahkan ratusan juta, sekaligus dapat melindungi rahasia, integritas dan bank data.[3]

Oleh karena itu artikel ini bermaksud ingin membahas pengetahuan mahasiswa FH UKI Angkatan tahun 2023 terkait tindakan pelanggaran data pribadi khususnya permintaan password dan/atau mengakses ponsel tanpa izin. Penelitian ini merupakan penelitian hukum empiris yang dilakukan dengan cara meneliti data primer yaitu data yang diperoleh secara langsung dari masyarakat, berkaitan dengan ilmu-ilmu sosial yang lain yang melihat fenomena atau gejala hukum di masyarakat sebagai obyek kajiannya.[4] Pendekatan yang digunakan adalah pendekatan kualitatif yaitu suatu cara analisis hasil penelitian yang menghasilkan data deskriptif analisis yaitu data yang dinyatakan oleh responden secara tertulis atau lisan serta tingkah laku yang nyata yang diteliti dan dipelajari sebagai sesuatu yang utuh. Oleh karena itu peneliti harus dapat menentukan data mana yang diharapkan atau diperlukan dan relevan dengan materi penelitian, sehingga dalam analisis dipentingkan kualitas data karena peneliti tidak semata-mata bertujuan mengungkap kebenaran tapi memahami kebenaran tersebut.[5]

[1] Polykalas, S. E. and Prezerakos, G. N. (2019). When the mobile app is free, the product is your personal data. Journal Digital Policy, Regulation and Governance, vol. 21 no. 2. Page.89-101. https://doi.org/10.1108/DPRG-11-2018-0068
[2] Tsavli, M., Efraimidis, P. S., Katos, V. and Mitrou, L. (2015). Reengineering the user: privacy concerns about personal data on smartphones. Journal Information & Computer Security, vol. 23 no. 4. Page.394-405. https://doi.org/10.1108/ICS-10-2014-0071
[3] Astuti, N. K dan Atmojo, R.N.P. (2022). PERLINDUNGAN KONSUMEN ATAS RISIKO KEAMANAN INFORMASI DALAM TRANSAKSI E-COMMERCE. Journal Honeste Vivere, Volume 32 Issue 2, 2022. Hlm. 98-107. https://doi.org/10.55809/hv.v32i2.135
[4] Irwansyah, Penelitian Hukum: Pilihan Metode & Praktik Penulisan Artikel, Edisi Revisi, Yogyakarta: Mirra Buana Media, 2021, hlm.43.
[5] Fajar, M. dan Achmad, Y. Dualisme Penelitian Hukum Normatif & Empiris, Yogyakarta: Pustaka Pelajar, 2010, hlm.192.

Discussion

Tujuan dan Pengaturan Perlindungan Data Pribadi

Perlindungan terhadap data privasi individu diatur dalam Undang-Undang Dasar 1945 tentang perlindungan hak privasi tercantum di Pasal 28G ayat (1), yakni "Setiap orang berhak atas perlindungan diri pribadi, keluarga, kehormatan, martabat dan harta benda yang dibawah kekuasaannya, serta berhak atas rasa aman dan perlindungan dari ancaman ketakutan untuk berbuat atau tidak berbuat sesuatu yang merupakan hak asasi".[6] Presiden Joko Widodo, dalam pidato kenegaraan menegaskan pentingnya Indonesia bersiap menghadapi fenomena kolonialisme digital (dengan konsep data sebagai minyak baru) melalui pernyataan tegas bahwa data merupakan kekayaan baru bagi bangsa kita. Saat ini, data memiliki nilai lebih tinggi daripada minyak, sehingga menurut Presiden Joko Widodo, Indonesia perlu mewujudkan kedaulatan data (*data sovereignty*). Setiap hak warga negara harus dilindungi oleh legislasi dalam adaptasi kebiasaan baru sebagai amanat kedaulatan virtual".[7]

Tujuan utama perlindungan data pribadi adalah untuk menjaga privasi individu, termasuk informasi pribadi seperti nama, alamat, nomor identitas, riwayat medis, dan informasi sensitif lainnya. Perlindungan data pribadi bertujuan untuk mencegah informasi ini jatuh ke tangan yang salah dan digunakan untuk tujuan yang tidak diinginkan, seperti penyalahgunaan untuk upaya penipuan dan kegiatan kriminal lainnya. Perlindungan data pribadi juga bertujuan untuk membangun dan mempertahankan kepercayaan publik terhadap organisasi atau lembaga yang mengumpulkan dan mengelola data pribadi. Dengan menunjukkan komitmen untuk melindungi privasi individu, organisasi dapat memperoleh kepercayaan dari masyarakat. termasuk memastikan kepatuhan terhadap peraturan dan regulasi yang berkaitan dengan pengumpulan, penyimpanan, dan penggunaan data pribadi. Ini mencakup peraturan seperti General Data Protection Regulation (GDPR) di Uni Eropa dan Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi (UU PDP). Sebelum ada UU PDP, pengaturan data pribadi tersebar di dalam beberapa peraturan perundang-undang yaitu UU No.7 tahun 1971 tentang Ketentuan-ketentuan Pokok Kearsipan, UU No.8 tahun 1997 tentang Dokumen Perusahaan, UU No.39 tahun 1999 tentang HAM, UU No.10 tahun 1998 tentang Perbankan, UU No.23 tahunn1992 tentang Kesehatan dan UU No.36 tahun 1999 tentang Telekomunikasi.

[6] Undang-Undang Dasar Republik Indonesia Tahun 1945, https://jdih.mkri.id/mg58ufsc89hrsg/UUD_1945_Perubahan.pdf
[7] Hummel, P. et.al., "Sovereignty And Data Sharing", ITU Jurnal: ICT Discoveries, Special Issue No. 2, 23 November 2018, https://www.researchgate.net/publication/330555591_Sovereignty_and_Data_Sharing

UU Kearsipan terdapat pengaturan aspek publik yang diselenggarakan oleh Pemerintah dalam rangka penyelenggaraan administrasi negara, termasuk juga data dan/atau informasi pribadi seseorang. Dimana tujuan kearsipan ditegaskan di Pasal 3 yaitu untuk menjamin keselamatan bahan pertanggungjawaban nasional tentang perencanaan, pelaksanaan dan penyelenggaraan kehidupan berbangsa serta menyediakan bahan pertanggungjawaban tersebut bagi kegiatan pemerintah.UU Kearsipan ini juga mengatur ancaman pidana terhadap siapapun yang memiliki data secara melawan hukum dan/atau menyimpan dan dengan sengaja menyebarkan isi arsip kepada pihak ketiga.[8]

UU Dokumen Perusahaan mengatur mengenai catatatan atau keterangan yang dibuat dan diterima oleh perusahaan dalam rangka pelaksanaan kegiatan perusahaan baik tertulis di kertas maupun dalam bentuk media rekaman yang dapat dilihat, dibaca dan didengar. Dokumen perusahaan terdiri dari dokumen keuangan dan dokumen lain yang berisi keterangan yang mempunyai nilai guna bagi perusahaan, seperti data pelanggan, data karyawan yang termasuk dalam klasifikasi data atau informasi pribadi.[9] UU HAM mengatur mengenai kebebasan untuk berkomunikasi dan mendapatkan informasi secara pribadi sekaligus jaminan terhadap privasi, salah satunya adalah hak mengembangkan diri untuk mencari, memperoleh, menyimpan, mengolah dan menyampaikan informasi dengan menggunakan segala jenis sarana yang tersedia.[10] UU Perbankan mengatur mengenai kewajiban bank untuk merahasiakan keterangan mengenai nasabah penyimpan dan simpanannya, kecuali untuk kepentingan perpajakan, penyelesaian piutang bank, untuk kepentingan peradilan dalam perkara pidana dan atas permintaan, persetuan dan kuasa dari ahli wariscnasabah penyimpan telah meninggal dunia.[11]

UU Telekomunikasi mengatur kerahasiaan informasi yaitu larangan setiap orang melakukan perbuatan tanpa hak, tidak sah atau manipulasi terhadap akses ke jaringan telekomunikasi atau akses ke jasa telekomunikasi dan akses ke jaringan telekomunikasi khusus dengan adanya ancaman pidana 6 tahun dan denda maksimal Rp.600 juta. Selain itu diatur larangan setiap orang melakukan penyadapan atas informasi yang disalurkan melalui jaringan telekomunikasi dalam bentuk apapun dengan ancaman pidana 15 tahun bagi pelanggarnya. UU ini juga mengatur kewajiban penyelenggara jasa telekomunikasi untuk merahasiakan informasi yang dikirim dan diterima pelanggan jasa telekomunikasi yang diselenggarakannya dengan acaman pidana 2 tahun dan denda maksimal Rp.200 juta. Dalam kasus pidana penyelenggara jasa telekomunikasi wajib

[8] Undang-Undang Nomor 7 Tahun 1971 tentang Ketentuan -Ketentuan Pokok Kearsipan, LN.RI Tahun 1971.No.32.
[9] Undang-Undang Nomor 8 Tahun 1997 tentang Dokumen Perusahaan, LN.RI Tahun 1997 No.18, TLN.RI No.3674.
[10] Undang-Undang Nomor 39 tahun 1999 tentang Hak Asasi Manusia, LN.RI Tahun 1999 No.165, TLN.RI No.36.
[11] Undang-Undang Nomor 10 tahun 1998 tentang Perbankan, LN.RI Tahun 1998 No.182, TLN.RI No.3790.

merekam informasi untuk keperluan proses peradilan pidana atas permintaan Jaksa Agung atau Kepala Kepolisian Republik Indonesia untuk tindak pidana dengan ancaman diatas 5 tahun, seumur hidup atau mati.[12]

UU PDP hadir sebagai bentuk perlindungan negara terhadap hak privasi dan keamanan informasi setiap individu, meliputi data spesifik yang mencakup informasi tentang kesehatan, biometrik, genetika, catatan kejahatan, data anak, data keuangan, dan/atau data lainnya sesuai dengan ketentuan peraturan perundang-undangan dan data umum yang mencakup informasi tentang nama lengkap, jenis kelamin, kewarganegaraan, agama, status perkawinan, dan/atau data pribadi yang dikombinasikan mengidentifikasi seseorang. Hak-hak ini dilindungi dari potensi penyalahgunaan dari kejahatan keuangan seperti pemerasan, penipuan, pengajuan pinjaman, pengajuan online (pinjol), transaksi uang illegal, mengaku sebagai orang lain untuk mendapatkan bantuan sosial, layanan kesehatan, program tenaga kerja, spam dan phishing via email, messenger, telpon, dan sebagainya.[13]

Jenis Data Pribadi

Pelindungan data pribadi merupakan salah satu hak asasi manusia yang merupakan bagian dari pelindungan diri pribadi maka perlu diberikan landasan hukum untuk memberikan keamanan atas data pribadi, berdasarkan Undang-Undang Dasar Negara Republik Indonesia Tahun 1945. pelindungan data pribadi ditujukan untuk menjamin hak warga negara atas pelindungan diri pribadi dan menumbuhkan kesadaran masyarakat serta menjamin pengakuan dan penghormatan atas pentingnya pelindungan data pribadi. Hadirnya UU PDP merupakan amanat dari Pasal 28G ayat (1) Undang-Undang Dasar Negara Republik Indonesia Tahun 1945 yang menyatakan bahwa, "Setiap orang berhak atas perlindungan diri pribadi, keluarga, kehormatan, martabat, dan harta benda yang di bawah kekuasaannya, serta berhak atas rasa aman dan pelindungan dari ancaman ketakutan untuk berbuat atau tidak berbuat sesuatu yang merupakan hak asasi". Persoalan Felindungan Data Pribadi mtrncul karena keprihatinan akan terhadap Data Pribadi yang dapat dialami oleh orang dan/atau badan hukum. Pelangaran tersebut dapat menimbulkan kerugian materiel dan non-materiel.[14]

[12] Undang-Undang Nomor 36 tahun 1999 tentang Telekomunikasi, LN.RI Tahun 1999 No.154, TLN.RI No.3881.
[13] Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data pribadi, LN.RI Tahun 2022 No.196, TLN.RI No.6820.
[14] *Ibid.*

UU PDP membagi data pribadi dalam 2 klasifikasi yaitu:

1. Data Pribadi yang bersifat spesifik, yaitu data pribadi yang apabila dalam pemrosesannya dapat mengakibatkan dampak lebih besar kepada subjek data pribadi, antara lain tindakan diskriminasi dan kerugian yang lebih besar subjek data pribadi, meliputi:
    a. Data dan Informasi Kesehatan, yaitu catatan atau keterangan individu yang berkaitan dengan kesehatan fisik, kesehatan mental, dan/atau pelayanan Kesehatan;
    b. Data Biometrik, yaitu data yang berkaitan dengan fisik, fisiologis, atau karakteristik perilaku individu yang memungkinkan identifikasi unik terhadap individu, seperti gambar wajah atau data dektiloskopi. Data biometrik juga menjelaskan pada sifat keunikan dan/atau karakteristik seseorang yang harus dijaga dan dirawat, namun tidak terbatas pada rekam sidik jari, retina mata, dan sampel DNA;
    c. Data Genetika, yaitu semua data jenis apa pun mengenai karakteristik suatu individu yang diwariskan atau diperoleh selama perkembangan prenatal awal;
    d. Catatan Kejahatan, merupakan catatan tertulis tentang seseorang yang pernah melakukan perbuatan melawan hukum atau melanggar hukum atau sedang dalam proses peradilan atas perbuatan yang dilakukan, antara lain catatan kepolisian dan pencantuman dalam daftar pencekalan atau penangkalan;
    e. Data Anak;
    f. Data Keuangan Pribadi, yaitu termasuk namun tidak terbatas kepada data jumlah simpanan pada bank, termasuk tabungan, deposito, dan data kartu kredit;
    g. Data lainnya sesuai dengan ketentuan Peraturan Perundang-undangan.[15]
2. Data Pribadi yang bersifat umum, meliputi:
    a. Nama Lengkap;
    b. Jenis Kelamin;
    c. Kewarganegaraan;
    d. Agama;
    e. Status Perkawinan;
    f. Data Pribadi Yang Dikombinasikan Mengidentifikasi Seseorang.[16]

[15] Danrivanto Budhijanto. Hukum Perlindungan Data Pribadi Di Indonesia Cyberlaw & Cyberseccurity. Bandung: PT. Refika Aditama, 2023, hlm. 32-33.
[16] *Op.cit*, Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data pribadi, Pasal 4 ayat (3).

Tindakan Memaksa, Menyerahkan Dan Mengakses Data Pribadi

Tindakan memaksa, menyerahkan, dan mengakses data pribadi tanpa izin merupakan bentuk pelanggaran serius terhadap privasi individu dan berpotensi menyebabkan dampak negatif yang merugikan. Hal ini merujuk pada situasi di mana individu atau entitas menggunakan kekuatan atau tekanan untuk memaksa individu lain untuk menyerahkan data pribadi mereka. Seperti adanya ancaman fisik, pemerasan, atau penipuan untuk mendapatkan informasi sensitif dari seseorang. Hal ini dapat terjadi saat seseorang secara sukarela atau karena tekanan menyerahkan informasi pribadi mereka kepada pihak lain tanpa izin. Hal ini terjadi karena kurangnya kesadaran tentang pentingnya menjaga privasi atau karena manipulasi dari pihak lain.

Tindakan yang melibatkan akses ilegal atau tidak sah ke data pribadi seseorang tanpa izin. Ini bisa terjadi melalui peretasan, penggunaan perangkat lunak berbahaya, atau eksploitasi celah keamanan dalam sistem atau jaringan. Semua tindakan ini merugikan individu yang data pribadinya disalahgunakan. Dampaknya bisa sangat merugikan, termasuk pencurian identitas, penipuan keuangan, penyebaran informasi yang sensitif, dan pelanggaran privasi yang meluas. Oleh karena itu, penting bagi individu dan organisasi untuk mengambil langkah-langkah untuk melindungi data pribadi mereka dan menghindari terlibat dalam tindakan memaksa, menyerahkan, atau mengakses data pribadi orang lain tanpa izin yang sah. Ini termasuk memperkuat keamanan informasi, meningkatkan kesadaran tentang risiko keamanan digital, dan mengikuti praktik terbaik dalam manajemen data pribadi.

Salah satu cara yang dilakukan dalam pencurian identitas dikenal dengan *social engineering* yaitu teknik manipulasi yang bisa membahayakan keamanan data kita. Oknum pelaku rekayasa sosial atau *social engineering* akan menyisipkan virus, melakukan breach dan tindak kejahatan *cyber* lainnya tanpa izin. *Social engineering* juga sering kali sukar dideteksi sehingga data kamu bisa saja dicuri tanpa kamu sadar. Tujuannya adalah untuk memanfaatkan aspek psikologis dari perilaku manusia untuk mendapatkan keuntungan yang tidak sah. Berikut adalah beberapa contoh teknik social engineering yang umum digunakan:

1. *Phishing*: Penyerang mencoba untuk mendapatkan informasi sensitif seperti nama pengguna, kata sandi, atau informasi keuangan dengan menyamar sebagai entitas tepercaya melalui email, pesan teks, atau situs web palsu;
2. *Pretexting:* Penyerang menciptakan cerita palsu atau situasi untuk mendapatkan informasi dari target. Mereka bisa menyamar sebagai seseorang yang berwenang atau memiliki kebutuhan mendesak untuk informasi tersebut;

3. *Baiting:* Penyerang menawarkan sesuatu yang menarik kepada target, seperti file musik atau film gratis, tetapi file tersebut sebenarnya berisi malware yang dapat memberikan akses ke sistem target;
4. *Quid Pro Quo*: Penyerang menawarkan bantuan atau imbalan tertentu kepada target dalam pertukaran untuk informasi sensitif atau akses ke sistem mereka;
5. *Tailgating*: Penyerang mengikuti seseorang yang sah ke dalam gedung atau area terlarang dengan berpura-pura menjadi bagian dari mereka, sehingga mereka dapat mendapatkan akses yang tidak sah;
6. *Dumpster Diving*: Penyerang mencari informasi sensitif dari sampah fisik, seperti dokumen yang terbuang, yang dapat memberikan wawasan tentang sistem atau kebiasaan kerja target.[17]

Social engineering dapat menjadi ancaman yang serius terhadap keamanan informasi, karena seringkali target yang dibujuk atau dimanipulasi tidak menyadari bahwa mereka telah menjadi korban. Oleh karena itu, penting bagi individu dan organisasi untuk meningkatkan kesadaran tentang teknik *social engineering*, serta mengadopsi kebijakan dan tindakan keamanan yang dapat melindungi mereka dari serangan semacam itu. Ini termasuk pelatihan karyawan, implementasi protokol keamanan yang kuat, dan penggunaan alat teknologi untuk mendeteksi dan mencegah upaya *social engineering*.

Pengetahuan Mahasiswa FH UKI Angkatan 2023 Terhadap Pelanggaran Data Pribadi

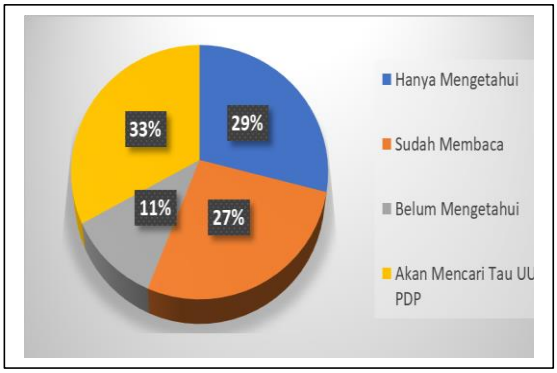
Untuk mengetahui pengetahuan mahasiswa FH UKI Angkatan 2023, peneliti melakukan survei kepada 100 Mahasiswa, dengan mengajukan jumlah pertanyaan survei 18 (delapan belas) soal mengenai pendapat, pemahaman, dan pengalaman mahasiswa Fakultas Hukum Universitas Kristen Indonesia yang dijadikan 4 (empat) pertanyaan krusial yaitu:

1. Mahasiswa FH UKI yang sekedar mengetahui UU PDP ada 29%;
2. Mahasiswa FH UKI yang sudah membaca isi dari UU PDP ada 27%;
3. Mahasiswa FH UKI yang belum sama sekali mengetahui dan membaca dari UU PDP ada 11%, dan;
4. Mahasiswa FH UKI yang akan mencari tau mengenai UU PDP ada 33%.

[17] Team, (2023). Apa Itu Social Engineering: Jenis, dan Prosesnya. Online. https://codingstudio.id/blog/social-engineering-adalah/. Diakses pada 29 Februari 2024.

Dari pertanyaan mengenai UU PDP dapat diperoleh hasil seperti dalam gambar di bawah ini:

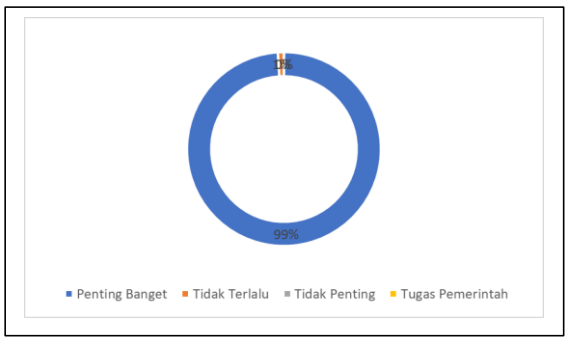
Gambar 1: Pengetahuan Mahasiswa FH UKI Angkatan 2023 terhadap UU PDP.



Dari pertanyaan mengenai urgensi pentingnya data pribadi dilindungi, diperoleh hasil sebagai berikut:

1. Pengetahuan terhadap mahasiswa FH UKI mengenai hak data pribadi yang harus dilindungi dengan hasil 99%;
2. Mahasiswa Fakultas Hukum Universitas Kristen Indonesia sadar betul bahwa Data Pribadi merupakan hak setiap makhluk hidup, dan harus dilindungi.

Gambar 2: Pengetahuan Mahasiswa FH UKI terhadap Hak-Hak Data Pribadi Yang Harus Dilindungi

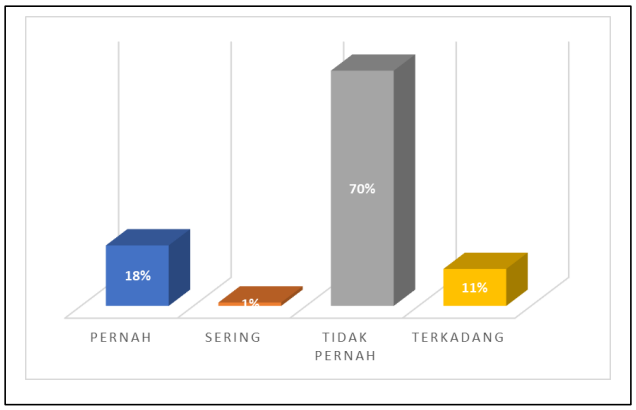


Dari pertanyaan mengenai pengalaman mahasiswa Fakultas Hukum Universitas Kristen Indonesia mengenai pelanggaran yang mereka pernah lakukan dalam penyebaran informasi maupun konten, dengan hasil sebagai berikut:

1. Mahasiswa FH UKI yang pernah melakukan penyebarluasan data pribadi ada 18%;

2. Mahasiswa FH UKI yang sering melakukan penyebaran konten maupun informasi mengenai data pribadi ada 1%;
3. Mahasiswa FH UKI yang terkadang melakukan penyebaran konten maupun informasi mengenai data pribadi tetapi hanya dimoment dan orang tertentu ada 11%;
4. Mahasiswa FH UKI yang tidak pernah sama sekali melakukan penyebaran informasi dan memilih tetap menjaga data pribadi orang lain dalam bentuk apapun ada 7%.

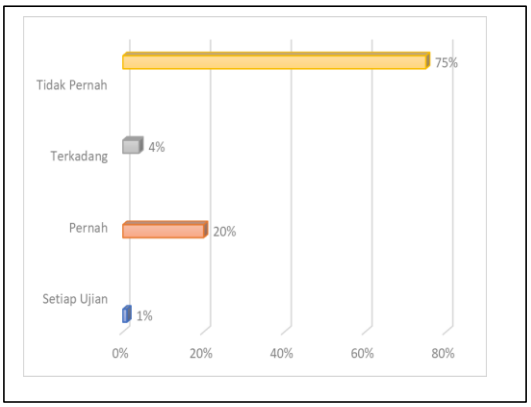
Gambar 3: Pengalaman Mahasiswa FH UKI Dalam Melanggar Perlindungan Data Pribadi Orang lain



Dari pertanyaan mengenai pengalaman mahasiswa FH UKI yang pernah mengalami penyitaan alat komunikasi dan atau diaksesnya alat komunikasi serta data pribadinya, diperoleh hasil sebagai berikut:

1. Mahasiswa FH UKI yang pernah mengalami penyitaan alat komunikasi dan diaksesnya alat komunikasi serta data pribadinya ada 20%;
2. Mahasiswa FH UKI yang pernah mengalami mengalami penyitaan alat komunikasi dan diaksesnya alat komunikasi serta data pribadinya pada saat ujian ada 1%;
3. Mahasiswa FH UKI yang pernah mengalami diaksesnya alat komunikasi serta data pribadinya ada 4%;
4. Mahasiswa FH UKI yang tidak pernah sama sekali mengalami pengaksesan atau penyitaan alat komunikasi ada 75% orang;

Gambar 4: Pengalaman Mahasiswa FH UKI Yang Pernah Mengalami Penyitaan Alat Komunikasi Dan/Atau Diaksesnya Alat Komunikasi Serta Data Pribadinya



Dari hasil penyebaran kuesioner pada mahasiswa FH UKI Angkatan 2023 dengan pendekatan kualitatif terkait ketaatan mahasiswa FH UKI terhadap UU PDP dikaitkan dengan masalah budaya membaca mahasiswa dan kepeduliannya terhadap hak-hak privasinya. Pendekatan ini memastikan setiap kebijakan hukum terkait perlindungan data pribadi mendapatkan pemahaman yang utuh, tepat dan komprehensif atas hal-hal yang diatur sehingga kebijakan yang diambil oleh Pemerintah dan diterapkan seadil mungkin bagi setiap warga negara dan mencegah timbulnya risiko yang tidak diharapkan.

Pengetahuan mahasisa FH UKI Angkatan tahun 2023 terhadap perlindungan data pribadi terkait tindakan penyerahan password dan pengaksesasn ponsel tanpa izin dilihat dari teori Lawrence M. Friedman tentang efektivitas hukum dapat diketahui, bahwa efektif dan berhasil tidaknya penegakan hukum tergantung tiga unsur sistem hukum, yakni struktur hukum (*struktur of law*), substansi hukum (*substance of the law*) dan budaya hukum (*legal culture*).

Struktur hukum menyangkut aparat penegak hukum, substansi hukum meliputi perangkat perundang-undangan dan budaya hukum merupakan hukum yang hidup (*living law*) yang dianut dalam suatu masyarakat. Mengenai struktur hukum Friedman berpendapat bahwa sistem hukum memiliki struktur yang terdiri dari unsur-unsur seperti: jumlah dan ukuran pengadilan; yurisdiksinya, struktur juga berarti bagaimana badan legislative terorganisir…prosedur apa yang diikuti oleh departemen kepolisian, dan sebagainya. Struktur, dengan kata lain, adalah semacam persilangan dari sistem hukum.[18] Aspek lain dari sistem hukum adalah substansinya. Yang dimaksud dengan ini adalah aturan sebenarnya, norma, dan pola perilaku orang-orang di dalam sistem

[18] Lawrence M. Friedman, System Hukum Dalam Perspektif Ilmu Sosial, The. Legal System: A Sosial Science Perspektive, Bandung: Nusa Media, 2009, hlm. 24.

hukum yang hidup, bukan hanya aturan-aturan dalam buku-buku hukum.[19] Sedangkan mengenai budaya hukum, Friedman berpendapat sikap masyarakat terhadap hukum dan sistem hukum yang mereka yakini .Dengan kata lain, merupakan puncak pemikiran sosial dan kekuatan sosial yang mana menentukan bagaimana hukum digunakan, dihindari, atau disalahgunakan. [20] Kultur hukum atau budaya hukum menyangkut budaya hukum yang merupakan sikap manusia (termasuk budaya hukum aparat penegak hukumnya) terhadap hukum dan sistem hukum. Sebaik apapun penataan struktur hukum untuk menjalankan aturan hukum yang ditetapkan dan sebaik apapun kualitas substansi hukum yang dibuat tanpa didukung budaya hukum oleh orang-orang yang terlibat dalam sistem dan masyarakat maka penegakan hukum tidak akan berjalan secara efektif.[21]

Dilihat dari substansi hukum Friedman maka keberadaan UUD PDP (UU No. Nomor 27/2022) memberikan perlindungan hukum yang kuat terhadap privasi individu dengan menetapkan standar yang jelas tentang bagaimana data pribadi boleh dikumpulkan, disimpan, digunakan, dan diungkapkan. Hal ini membantu mencegah penyalahgunaan data pribadi oleh pihak yang tidak berwenang. Dengan adanya UU Perlindungan Data Pribadi, terdapat landasan hukum yang jelas untuk menegakkan kepatuhan dan mengambil tindakan hukum terhadap pelanggaran perlindungan data. Ini mencakup sanksi bagi organisasi yang melanggar ketentuan dalam UU tersebut, seperti denda atau sanksi lainnya. Mahasiswa FH UKI Angkatan tahun 2023 sejumlah 29% yang mengetahui dan 27% yang sudah membaca UU PDP menunjukan bahwa UU PDP ini belum tersosialisasi pada masyarakat, khususnya generasi Z yang paling banyak menggunakan smartphone dalam kesehariannya dalam berselancar di dunia siber.

Dilihat dari struktur hukum Friedman Struktur hukum, keberadaan undang-undang perlindungan data pribadi terdapat pendekatan minimalis, dimana pemerintah hanya campur tangan sejauh yang diperlukan untuk mencegah penyalahgunaan data pribadi, jika seseorang melanggar privasi seseorang mereka dapat dikenai sanksi ancaman pidana.

Dilihat dari budaya hukum friedman maka lebih dari setengah mahasiswa FH UKI Angkatan tahun 2023 yang tidak melakukan penyebarluasan data pribadi orang lain, berarti mahasiswa fakultas hukum memahami tindakan yang tidak seharusnya dilakukan diluar dari peraturan maupun beretika dalam mengambil sikap yang bijak dalam menggunakan internet maupun dalam menggunakan alat komunikasi. Hal tersebut terlepas dari sudah dibaca atau belumnya peraturan perundang-undangan

[19] *Ibid*, hlm.25.
[20] *Ibid*, hlm.27.
[21] Leden Marpaung, Asas Teori Praktek Hukum Pidana, Jakarta: Sinar Grafika, 2005, hlm.62.

oleh mahasiswa FH UKI. Begitu juga denga pengalaman mahasiswa yang pernah mengalami diaksesnya alat komunikasi, maupun dimintanya password ponsel masih tergolong lumayan banyak yaitu 25% dari total 100 mahasiswa FH UKI. Kasus tersebut terbagi dari banyak kalangan, ada yang mengalami dari lingkungan sekolah, pertemanan, orangtua, pasangan, maupun keluarga.

Conclusion

Pentingnya pengetahuan bagi mahasiswa FH UKI dan mahasiswa pada prodi lain tentang pentingnya perlindungan hak pribadi, karena mereka sebagai calon praktisi hukum yang belajar mengenai sistem hukum dan peraturan yang berlaku. Mahasiswa FH UKI harus mengetahui bahwa perlindungan hak pribadi adalah bagian tidak terpisahkan dari hukum. Pengetahuan dan pemahaman akan perlindungan data pribadi akan dapat mempersiapkan mereka dalam menangani tantangan isu hukum perlindungan data pribadi di masa mendatang. Mahasiswa FH UKI sebagai agen perubahan yang akan memegang peran penting dalam memastikan kepatuhan terhadap hukum dan melindungi hak-hak individu dan proaktif mendidik masyarakat tentang pentingnya privasi dan hak-hak individu.

References

Book

Astuti, N. K dan Atmojo, R.N.P. (2022). PERLINDUNGAN KONSUMEN ATAS RISIKO KEAMANAN INFORMASI DALAM TRANSAKSI E-COMMERCE. Journal Honeste Vivere, Volume 32 Issue 2, 2022. Hlm. 98-107. https://doi.org/10.55809/hv.v32i2.135

Danrivanto Budhijanto. Hukum Perlindungan Data Pribadi Di Indonesia Cyberlaw & Cyberseccurity. Bandung: PT. Refika Aditama, 2023, hlm. 32-33.

Fajar, M. dan Achmad, Y. Dualisme Penelitian Hukum Normatif & Empiris, Yogyakarta: Pustaka Pelajar, 2010.

Hummel, P. et.al., "Sovereignty And Data Sharing", ITU Jurnal: ICT Discoveries, Special Issue No. 2, 23 November 2018, https://www.researchgate.net/publication/330555591_Sovereignty_and_Data_Sharing

Irwansyah, Penelitian Hukum: Pilihan Metode & Praktik Penulisan Artikel, Edisi Revisi, Yogyakarta: Mirra Buana Media, 2021.

Friedman, L. M. System Hukum Dalam Perspektif Ilmu Sosial, The. Legal System: A Sosial Science Perspektive, Bandung: Nusa Media, 2009.

Marpaung, L. Asas Teori Praktek Hukum Pidana, Jakarta: Sinar Grafika, 2005.

Polykalas, S. E. and Prezerakos, G. N. (2019). When the mobile app is free, the product is your personal data. Journal Digital Policy, Regulation and Governance, vol. 21 no. 2. Page.89-101. https://doi.org/10.1108/DPRG-11-2018-0068

Team, (2023). Apa Itu Social Engineering: Jenis, dan Prosesnya. Online. https://codingstudio.id/blog/social-engineering-adalah/. Diakses pada 29 Februari 2024.

Tsavli, M., Efraimidis, P. S., Katos, V. and Mitrou, L. (2015). Reengineering the user: privacy concerns about personal data on smartphones. Journal Information & Computer Security, vol. 23 no. 4. Page.394-405. https://doi.org/10.1108/ICS-10-2014-0071

Regulation

Undang-Undang Dasar Republik Indonesia Tahun 1945, https://jdih.mkri.id/mg58ufsc89hrsg/UUD_1945_Perubahan.pdf

Undang-Undang Nomor 10 tahun 1998 tentang Perbankan, LN.RI Tahun 1998 No.182, TLN.RI No.3790.

Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data pribadi, LN.RI Tahun 2022 No.196, TLN.RI No.6820.

Undang-Undang Nomor 36 tahun 1999 tentang Telekomunikasi, LN.RI Tahun 1999 No.154, TLN.RI No.3881.

Undang-Undang Nomor 39 tahun 1999 tentang Hak Asasi Manusia, LN.RI Tahun 1999 No.165, TLN.RI No.36.

Undang-Undang Nomor 7 Tahun 1971 tentang Ketentuan -Ketentuan Pokok Kearsipan, LN.RI Tahun 1971.No.32.

Undang-Undang Nomor 8 Tahun 1997 tentang Dokumen Perusahaan, LN.RI Tahun 1997 No.18, TLN.RI No.3674.