Vol. 5 No. 2 November 2025, hal.41-58.

ISSN 2808-8468 (Online)
sensasi.upnjatim.ac.id

EFEKTIVITAS UNDANG-UNDANG PERLINDUNGAN DATA PRIBADI TERHADAP KEJAHATAN PERETASAN DATA PRIBADI BERBASIS SISTEM ELEKTRONIK DI INDONESIA

Hani Puspita Sari[1], Dwi Irwana Mulyani[2], Melinda Aji Nilamsari[3], Dhaniel Dimas Fajarian Sitorus[4], Yudi Widagdo Harimurti[*5]
*Email: yudi.harimurti@trunojoyo.ac.id

Universitas Trunojoyo Madura[1,2,3,4,5]

Abstrak. Kejahatan dalam sistem elektronik sering kali terjadi dalam bentuk peretasan data pribadi milik orang lain, beberapa dekade terakhir Indonesia mengalami rentetan kasus kejahatan siber berupa kebocoran data nasional, tentu persoalan terkait bagaimana regulasi yang dibentuk mampu untuk mencapai sebagaimana tujuan hukum yaitu kepastian, kemanfaatan dan keadilan, serta dengan analisis deskriptif untuk melihat bagaimana upaya hukum Indonesia terhadap kejahatan peretasan data pribadi dalam sistem elektronik, demikian lebih lanjut penelitian ini mengkaji secara dogmatik dan empiris hukum, penilitian ini menggunakan metode empiris atau non doktrinal guna mengkaji normatif hukum terhadap Undang-Undang perlindungan data pribadi, dari hasil penelitian ini nantinya akan dipergunakan sebagai acuan awal untuk penelitian lebih lanjut.
Keyword: *Kejahatan Cyber, Data Pribadi, System Elektronik*

Abstract. *Crimes in electronic systems often occur in the form of hacking personal data belonging to other people, in the last few decades Indonesia has experienced a series of cybercrime cases in the form of national data leaks, of course the problem is related to how the regulations formed are able to achieve the legal objectives, namely certainty, usefulness and justice, as well as with descriptive analysis to see how Indonesia's legal efforts against the crime of hacking personal data in the system electronic, thus further this study examines the legal dogmatic and empirical method, this research uses empirical or non-doctrinal methods to examine the legal normative of the Personal Data Protection Law, from the results of this study will later be used as an initial reference for further research.*
Keywords: *Cyber Crime, Personal Data, Electronic System*

✉Corresponding author :
Email: yudi.harimurti@trunojoyo.ac.id

Vol. 5 No. 2 November 2025, hal.41-58.
ISSN 2808-8468 (Online)
sensasi.upnjatim.ac.id

LATAR BELAKANG

Kemajuan teknologi memberikan keluasan serta kebebasan antar manusia untuk saling berinteraksi dan membangun hubungan sosial secara intens, kemajuan teknologi beberapa dekade terakhir memberikan wadah dimensi baru bagi manusia untuk saling terhubung, wadah yang dimaksud lebih lazim dikenal dengan sosial, secara prinsip dasar manusia adalah makhluk sosial *"Zoon Politicon"*, artinya manusia perlu serta membutuhkan peranan manusia lainnya untuk saling memenuhi kebutuhan hidupnya masing-masing, mulai dari kebutuhan pangan, sandang, papan bahkan kebutuhan untuk diakui oleh orang lain, transisi kehidupan manusia semenjak mengetahui penggunaan teknologi mendorong peralihan hubungan manusia yang pada mulanya berintraksi secara langsung kini mulai beralih pada interaksi tidak langsung melalui wadah media sosial.

Media sosial juga melalui proses perkembangan secara signifikan, dilansir dari halaman web RRI dalam artikel berjudul ("Six Degrees, Media Sosial Pertama Dalam Sejarah Dunia Digital") menyebutkan sebelum maraknya media sosial yang tren saat ini, Pada bulan Mei 1996, seorang pengusaha bernama Andrew Weinreich menciptakan sebuah platform daring yang mengubah wajah interaksi manusia secara global. Platform tersebut dikenal sebagai *Six Degrees*, yang dianggap sebagai media sosial pertama dalam sejarah.

Perjalanan panjang perkembangan teknologi media sosial hingga akhirnya pada era sekarang banyak sekali platfrom media sosial yang dapat dijumpai, seperti Facebook, Instagram, Whatsapp, serta X. hadirnya media sosial semacam itu memberikan pedoman hidup yang berbeda sebab hubungan antar manusia kini beralih pada dunia maya dimana pola komunikasi yang terjadi dalam media sosial adalah komunikasi tidak langsung *(indirect)*, dimana setiap orang sering kali mendokumentasikan kehidupan sehari-harinya untuk di unggah dalam platform media sosial, bahkan data pribadi seperti KTP, Paspor, bahkan NPWP juga sering dijumpai.

Data pribadi menurut Undang-Undang Nomor 27 Tahun 2022 adalah setiap informasi tentang seseorang yang bisa diidentifikasi secara langsung maupun tidak langsung, artinya data pribadi adalah segala informasi yang mengandung data identitas diri seseorang, secara normatif data pribadi tidak bisa diakses secara umum oleh orang lain, namum pada tataran praktek sosial data pribadi terkadang dijumpai dan berserakan dalam media sosial, hal ini menyebabkan perlunya upaya perlindungan hukum untuk menjaga data pribadi milik seseorang.

Di Indonesia sendiri sering terjadi beberapa kasus kebocoran data pribadi, banyak faktor yang menyebabkan kebocoran data tersebut diantarnya disebabkan hacker yang meretas sistem keamanan *cyber* milik instansi pemeritah maupun pribadi, faktor lainnya adalah kurangnya pemahaman orang untuk menjaga data pribadinya sendiri, hal ini bisa menjadi celah bagi orang lain untuk meretas dan mengetahui data diri milik orang lain.

Beberapa dekade terakhir banyak bentuk kejahatan *cyber* di Indonesia yang terjadi, dalam kurun waktu 3 tahun terakhir telah terjadi peretasan data pribadi skala nasional sejumlah 7 (Tujuh) kali dalam kurun waktu tersebut. Diantaranya pada tahun 2022 terjadi kasus peretasan sebanyak 3 kasus peretasan dan ditahun 2023 terjadi sebanyak 4 kasus peretasan.

Vol. 5 No. 2 November 2025, hal.41-58.
ISSN 2808-8468 (Online)
sensasi.upnjatim.ac.id

Secara rinci data yang didapatkan diantaranya:

1. Pada kuartal III tahun 2022, terdapat 108,9 juta akun di Indonesia yang dibobol,dan berkontribusi sebesar 12% terhadap kebocoran data di dunia.
2. Pada kuartal III tahun 2022, terdapat 108,9 juta akun di Indonesia yang dibobol,dan berkontribusi sebesar 12% terhadap kebocoran data di dunia.
3. Pada November 2022, Bjorka membobol data My Pertamina dan menjual sebesar 44 juta data seharga Rp392 juta melalui situs bitcoin.
4. Pada 12 Maret 2023, sebanyak 18,5 juta data pengguna BPJS Ketenagakerjaan dijual di forum gelap dengan membuka harga sebesar Rp153 juta.
5. Pada 2023, terjadi kebocoran data nasabah Bank Syariah Indonesia (BSI). Yang dilakukan oleh Lockbit, kelompok ransomware asal Rusia, dan mengklaim telah mencuri 1,5 TB data pribadi nasabah BSI
6. Pada 5 Juli 2023, 34 juta data paspor bocor, yang diunggah oleh tangan hacker Bjorka. Data yang bocor berisi nama, nomor paspor, masa berlaku paspor, tanggal lahir, dan gender.
7. Pada 14 Juli 2023, sebanyak 337 juta data Dukcapil yang diunggah di situs BreachForums. Data yang bocor berisi nama, nomor KK, tanggal lahir, alamat, NIK orang tua, nomor akta lahir, nikah, dan agama.

Dari data yang telah dijabarkan diatas maka mejadi suatu kesimpulan bahwa kasus peretasan data pribadi di Indonesia cukup masif dan signifikan, hal demikian juga menjadi bukti konkrit atas kurangnya kesadaran masyarakat untuk melindungi data pribadinya sendiri.

Risiko akan kelalaian dalam menjaga data pribadi akan menimbulkan dampak negatif secara personal ataupun sosial, dampak personal atas kejahatan *cyber* yang demikian yaitu *Carding, carding* sendiri merupakan kejahatan *cyber* yang memiliki resiko serta dampak buruk yang cukup tinggi, carding adalah kejahatan online dimana peretas masuk dalam akun pribadi seseorang untuk kemudian digunakan dalam transaksi illegal. Dampak buruk dari bentuk kejahatan ini adalah kerugian material bagi korban, sebab carding biasa dilakukan terhadap kartu kredit dan ATM milik seseorang.

Pada tahun 2024 telah terjadi peretasan data pribadi yang dilakukan oleh hacker yang menamakan dirinya Bjorka berhasil meretas data NPWP sebanyak 6 juta data NPWP yang bocor diantaranya yaitu NIK, NPWP, Alamat, No Hp, Email dan data lainnya. Diduga 6 Juta Data NPWP yang bocor diperjualkan di *breach forums.* 6 Juta data NPWP tersebut di perjual belikan dengan harga sekitar 150 Juta. Direktorat Penyuluhan, pelayanan, dan hubungan masyarakat Dwi Astuti mengatakan “Dari hasil penelitian pihaknya menyampaikan bahwa data *lo acces* di Direktorat Jendral Pajak dalam 6 tahun terakhir mengalami kebocoran data secara langsung dari sistem informasi di instansinya”.

Maka tentu kesadaran atas perlindungan data pribadi haruslah tertanam secara utuh kepada masyarakat agar kejahatan semacam ini tidak menjadi massif dan kronis di Indonesia, peran pemerintah dalam upaya mitigasi agar upaya peretasan dan kejahatan pencurian data pribadi tidak terjadi berulang kali.

Dari penjabaran diatas maka penulis merumuskan suatu rumusan masalah yaitu, bagaimana penerapan Undang-Undang Nomor 27 Tahun 2022 tentang

Vol. 5 No. 2 November 2025, hal.41-58.
ISSN 2808-8468 (Online)
sensasi.upnjatim.ac.id

perlindugan data pribadi dalam menjamin data pribadi warga negara Indonesia, serta bagaimana upaya hukum yang dilakukan untuk menjamin serta melindungi data pribadi warga negara Indonesia. Dengan adanya beberapa kasus krusial tentang peretasan data pribadi maka penulis dirasa perlu untuk melakukan penelitian lebih lanjut untuk menganalisa kasus-kasus peretasan data pribadi melalui prespektif hukum dan sosial.

METODE PENELITIAN

Metode penelitian yang digunakan adalah metode penelitian hukum empiris, menurut Soerjono Soekanto metode penelitian hukum empiris adalah penelitian yang dilakukan dengan cara mengidentifikasi hukum dan melihat bagaimana hukum dilaksanakan di masyarakat. Penelitian hukum empiris juga disebut sebagai penelitian hukum sosiologis atau penelitian lapangan.

PEMBAHASAN

Dengan munculnya banyak media online perkembangan internet juga mempengaruhi media massa. Hampir semua media massa nasional, baik cetak maupun elektronik. (televisi dan radio) sekarang memiliki media online, atau dengan kata lain telah terjadi konvergensi media. Dengan berkembangnya internet, cara masyarakat menggunakan media juga berubah siapa pun dapat membuat dan mengembangkan media mereka sendiri dengan mudah di akses.

Saat ini, teknologi informasi telah menjadi hal biasa. Teknologi informasi bahkan hampir tidak dapat dipisahkan dari berbagai bidang kehidupan. Media massa telah menjadi salah satu institusi sosial yang penting dalam kehidupan kita, dan mereka tentu membentuk diri mekera sebagai salah satu organisasi yang hidup di tengah masyarakat. Penggunaan internet adalah salah satu teknologi informasi media massa yang tidak dapat dihindari. Tidak hanya orang dewasa, tetapi juga anak-anak dan remaja adalah pengguana internet.

Saat ini kita mengenal internet sebagai sebuah jaringan teknologi komunikasi yang memudahkan kita untuk mengakses informasi. Internet merupakan jaringan yang menghubungkan komputer melalui kabel, telepon, dan satelit. Dengan mengakses situs tertentu setiap orang yang memiliki komputer dapat terhubung ke jaringan internet, yang memungkinkan kita mengakses lautan informasi dan hiburan yang tersebar secara global.

Sejarah perkembangan internet bergantung pada perang dingin yang terjadi setelah Perang Dunia II pada tahun 1945 antara Uni Soviet dengan Amerika Serikat. Perang dingin menyebabkan kedua negara menjadi semakin giat dalam mengembangkan teknologi, dan Amerika kemudian mengikuti jejak Uni Soviet dalam pembangunan teknologi dengan menggunakan kekuatan militer. Ini adalah alasan pembentukan *Advanced Research Project Agency* (ARPA). Tugas pertama yang diemban oleh ARPA adalah mengamankan dan melindungi data-data dan sistem komunikasi yang telah dibangun dan tidak dapat dihancurkan.

Upaya pengamanan informasi dan sistem komunikasi telah mengantarkan terjalinnya kerja sama antara kalangan militer dengan berbagai Universitas di Amerika. Licklider dan W. Clark adalah orang-orang pertama yang membuat paper dengan judul online *"Man computer communication"*. Dengan paper tersebut,

Vol. 5 No. 2 November 2025, hal.41-58.
ISSN 2808-8468 (Online)
sensasi.upnjatim.ac.id

Licklider kemudian menjadi orang pertama yang memimpin Program Penelitian Komputer di Departemen Pertahanan Amerika Serikat setelah karya tersebut.

Maka dengan rentetan sejarah perjuangan dalam mengembangakan teknologi pengetahuan hingga pada akhirnya setiap individu sadar akan peranan prodak teknologi berupa sosial media/media massa membawa arus kehidupan yang mengalami transisi kebiasaan dari komunal primitif hingga kehidupan modern untuk aktif dalam informasi teknologi.

Maka tentu normatifitas hukum di Indonesia haruslah juga mengatur hubungan sosial antara individu dengan individu lainnya dalam komunikasi dan interaksi sosial dalam dunia berbasis internet/online, maka tentu hukum Indonesia haruslah memberikan pengaturan komprehensif terhadap kebiasaan hukum yang hadir dalam dinamika sosial.

Implementasi Undang-Undang Nomor 27 Tahun 2022

Data pribadi merupakan sebuah informasi yang berisikan identitas milik seseorang sehingga data pribadi sangat penting untuk diberikan perlindungan hukum, dengan adanya data pribadi yang berisikan jati diri seseorang maka seseorang tersebut baru dapat melakukan perbuatan hukum dimana suatu perbuatan yang menimbulkan hak dan kewajiban bagi yang berbuat, disisi lain juga data pribadi digunakan untuk melakukan transaksi berupa jual beli online *(e-commerce)*, komunikasi dengan orang lain, menjadi nasabah bank, bahkan data pribadi juga berfungsi untuk memeriksa saksi dalam perkara tertentu.

Dalam Pasal 1 ayat (29) Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggara Sistem dan Transaksi Elektronik menyebutkan bahwa;

> "Data Pribadi adalah setiap data tentang seseorang baik yang teridentifikasi dan/atau dapat diidentifikasi secara tersendiri dan/atau dapat diidentifikasi secara tersendiri atau dikombinasikan dengan informasi lainnya baik secara langsung maupun tidak langsung melalui sistem elektronik dan/atau non-elektronik".

Dalam regulasi hukum di Indonesia juga menjelaskan tentang istilah data pribadi, dalam Pasal 1 Angka 20 Peraturan Mentri Dalam Negeri RI No. 102 Tahun 2019 Tentang Pemberian Hak Akses dan Pemanfaatan Data Kependudukan menyebutkan bahwa;

"Data pribadi adalah data perseorangan tertentu yang disimpan, dirawat, dan dijaga kebenaran serta dilindungi kerahasiaannya".

Dalam pemaknaannya dapat diartikan bahwa data pribadi bersifat sangat rahasia hingga dilindungi secara komprehensif oleh prodak hukum, melihat potensial tindak kejahatan yang berbasis pada peretasan dan penyalahgunaan data pribadi tentu perlindungan akan data pribadi menjadi wajib dan harus untuk memberikan kondisi aman terhadap masyarakat, sebagaimana tujuan hukum yaitu keadilan, kepastian serta kemanfaatan hukum.

Secara global perlindungan data pribadi juga diterapkan oleh beberapa negara anggota PBB, dalam salah satu traktat Internasional yaitu *Universal Declaration of Human Right* menyatakan bahwa;

"no one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks."

Vol. 5 No. 2 November 2025, hal.41-58.
ISSN 2808-8468 (Online)
sensasi.upnjatim.ac.id

Artinya setiap orang dilindungi hukum dan seharusnya tidak mengalami gangguan terhadap privasi, keluarga, rumah atau korespondensi dan setiap orang berhak atas perlindungan hukum terhadap gangguan hak privasi tersebut.

Dalam Undang-Undang Nomor 27 Tahun 2022 Tentang Perlindungan Data Pribadi memberikan dasar hukum terhadap data pribadi, dalam Undang-Undang tersebut juga mengatur tentang mekanisme mitigasi tehadap perlindungan data pribadi warga negara Indonesia, dalam regulasi tersebut juga mengandung asas-asas hukum sebagai bentuk perlindungan hukum data pribadi, merujuk pada Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi, asas perlindungan data pribadi ialah.

a. Asas perlindungan, adalah pemerintah wajib memberikan perlindungan data pribadi warga negaranya baik di dalam maupun di luar negeri.
b. Asas kepentingan umum, adalah bahwa Undang-Undang ini disusun untuk melindungi kepentingan masyarakat secara luas.
c. Asas keseimbangan, adalah keseimbangan antara hak privasi dengan hak negara yang sah berdasarkan kepentingan umum.
d. Asas pertanggungjawaban, adalah penyelengaraan data pribadi harus dapat dipertanggungjawabkan oleh penyelenggara data pribadi.

Dapat diartikan bahwa perlindungan hukum haruslah melibatkan segala pihak, yang paling utama adalah relasi antar pemerintah dan masyrakat dalam menjaga perlindungan data pribadi, peran pemerintah utamanya adalah untuk memberikan upaya perlindungan berupa kebijakan hukum yang mengatur tentang tindak kejahatan *cyber* berupa peretasan dan penyalahgunaan data pribadi seseorang, meningkatkan *cyber security* guna menopang stabilitas keamanan data diri berbasis eletronik nasional, juga pada aspek penegakan hukum.

Menurut Rizky P.P. Karo Karo, S.H.,M.H. menjelaksan tentang berbagai pihak yang terlibat dalam perlindungan data pribadi, diantaranya adalah Pemerintah, Kementrian atau Lembaga, Direktorat Jendral, Instansi Penyelenggara Negara, Penyelenggara Sistem Elektronik, Pengguna Sistem Elektronik, Pengirim dan Penerima, Pelaku Usaha, Pemilik Data Pribadi.

Hal demikian merupakan bukti konkrit dalam hukum normatif bahwa perlindungan atas data pribadi adalah perlu dan harus untuk memberikan kepastian hukum, sebab dalam penafsiran hukum semua orang di anggap tahu akan hukum *(Presumtio Iures de Iure),* maka tentu ikhwal data pribadi menjadi prioritas utama dalam penyelenggaran sistem administrasi dan ketatanegaraan di Indonesia.

Namun dalam prespektif tertentu ada standarisasi tertentu menjadi rasio untuk mengklasifikasikan standar perlindungan data pribadi, dalam standarisasi perlindungan data pribadi sebagaimana diatur dalam Peraturan Pemerintah Perdagangan Melalui Sistem Elektronik (PMSE), berdasarkan Pasal 59 ayat (1), (2) bahwa;

“Pelaku usaha wajib menyimpan data pribadi sesuai standar perlindungan data pribadi sesuai standar perlindungan data pribadi atau kezaliman praktik bisnis yang berkembang”.

Lebih lanjut dijelaskan bentuk standar serta kriteria yang dimaksud dengan perlindungan data pribadi;

Vol. 5 No. 2 November 2025, hal.41-58.
ISSN 2808-8468 (Online)
sensasi.upnjatim.ac.id

a. Data pribadi harus diperoleh secara jujur dan sah dari pemilik data pribadi yang berasangkutan disertai dengan adanya pilihan dan jaminan adanya upaya pengamanan dan pencegahan kerugian pemilik data tersebut.
b. Data pribadi harus dimiliki hanya untuk satu tujuan atau lebih yang dideskripsikan secara spesifik dan sah serta tidak boleh diproses lebih lanjut dengan cara yang tidak sesuai dengan tujuan sendiri.
c. Data pribadi yang diperoleh harus layak, relevan dan tidak terlalu luas dalam hubungannya dengan tujuan pengolahannya sebagaimana disampaikan sebelumnya kepada pemilik data.
d. Data pribadi harus akurat dan harus selalu *up-to-date* dengan memberikan kesempatan kepada pemilik data untuk memuktakhirkan data pribadinya.
e. Data pribadi harus diproses sesuai dengan tujuan, perolehan, dan peruntukannya serta tidak boleh dikuasai lebih lama dari waktu yang diperuntukan.
f. Data pribadi harus diproses sesuai dengan hak subjek pemilik data sebagaimana diatur dalam Peraturan Perundang-undangan.
g. Pihak yang menyimpan data pribadi harus mempunyai sistem pengamanan yang patut untuk mencegah kebocoran atau mencegah setiap kegiatan pemrosesan atau pemfaatan data pribadi secara melawan hukum serta bertanggung jawab atas kerugian yang tidak terduga atau kerusakan yang terjadi terhadap data pribadi terebut.
h. Data pribadi tidak boleh dikirim ke negara atau wilayah lain di luar wilayah Indonesia kecuali jika negara atau wilayah tersebut oleh Menteri dinyatakan memiliki standar dan tingkat perlindungan yang sama dengan Indonesia.

Maka tentu menjadi ikhwal serius dalam menjaga secara penuh data pribadi tersebut.Secara kritis dalam melihat regulasi hukum yang mengatur tentang perlindungan data pribadi dirasa kurang dan tidak teroptimalisasi, dilansir dari Hukum Online menyebutkan bahwa belum ada peraturan pelaksana Undang-Undang Nomor 27 Tahun 2022 lebih jelasnya masih dalam tahap partisipasi publik, kurangnya optimalisasi hukum yang terjadi menyebabkan pada proses penegakan hukum turut serta tidak optimal, tidak berbanding lurus dengan banyaknya praktek perbuatan hukum yang melanggar serta melawan hukum di tengah masyarakat.

Tentu menjadi perhatian serius dalam proses pelaksanaan terhadap payung hukum perlindungan data pribadi, dengan belum terbentuknya peraturan pelaksana Undang-Undang perlindungan data pribadi maka analisa hukum dalam melihat fenomena tersebut menggunakan Peraturan Pemerintah Nomor 71 Tahun 2019 Penyelenggaraan Sistem dan Transaksi Elektronik sebagai dasar hukum untuk suatu perbuatan kejahatan yang bertentangan dengan hukum.

Menurut W. A. Bonger mendefenisikan kejahatan sebagai perbuatan yang antisosial yang memeproleh pertentangan dengan sadar dari negara berupa pemberian penderitaan (baik yang berbentuk hukuman ataupun yang berbentuk tindakan).

Sedangkan kejahatan siber adalah suatu perbuatan melawan hukum dalam dunia elektronik disertai dengan adanya suatu kerugian tertentu bagi orang lain sehingga mendapat pertentangan sosial, kerugian yang dimaksud mencakup

Vol. 5 No. 2 November 2025, hal.41-58.
ISSN 2808-8468 (Online)
sensasi.upnjatim.ac.id

kerugian materil dan esensi seperti harga diri, nilai sesorang dan lain sebagainya. Latar dari kejahatan siber haruslah merujuk pada situasi waktu dan tempat dalam sistem elektronik, sebagimana dalam Pasal 1 ayat (1) Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik menyebutkan bahwa;

> "Sistem Elektronik adalah serangkaian perangkat dan prosedur elektronik yang berfungsi mempersiapkan, mengumpulkan, mengolah, menganalisis, menyimpan, menampilkan, mengumumkan, mengirimkan, dan/atau menyebarkan Informasi Elektronik."

Sehingga dapat dikatakan bahwa segala bentuk peerbuatan kejahatan siber haruslah secara konkrit terjadi dalam dimensi representatif yaitu sistem elektronik, kemudian dalam bentuk pelakasanaan serta upaya perlindungan terhadap kejahatan siber pemerintah membentuk kelembagaan yang memiliki peran dalam perlindungan siber, hal ini didasarkan pada kebiasaan hukum masyarakat yang mulai menggunakan sistem elektronik untuk bertransaksi, bertukar informasi, mencari pengetahuan dan lain sebagainya telah menjadi kebutuhan sehari-hari.

BSSN (Badan Siber dan Sandi Negara) merupakan salah satu lembaga negara yeng berdiri melalui Peraturan Presiden Nomor 28 Tahun 2021, dimana BSSN memiliki peran strategis dan sentral dalam melindungi informasi dalam sistem elektronik seperti data nasional, data rahasia negara, data penduduk, data alutsista negara dan lain sebagianya, disisi lain juga BSSN memiliki fungsi untuk memberikan serta menjamin keamanan sistem elektronik skala nasional maupun regional daerah, lemabaga lainnya yang memiliki peranan dalam perlindungan siber juga ialah KOMINFO (Kementrian Komunikasi dan Informatika) yang memiliki peran dan tugas untuk turut serta untuk menyelenggarakan urusan pemerintah dalam bidang komunikasi dan informatika, tentu KOMINFO juga memiliki peranan yang sama dengan BSSN dimana keduanya juga memiliki peran penting dalam sistem elektronik.

Maka menjadi sebuah kepastian bahwa bentuk perlindungan sistem elektronik haruslah menjadi hal yang sangat perlu diperhatikan, ditambah dengan adanya kejahatan pidana yang berbasis pada sistem elektronik maka menjadi perhatian khusus dalam sistem hukum Indonesia sebab dunia siber memiliki cakupan yang sangat luas hingga masuk ranah global antar negara, maka hal ini menjadi kesulitan tersendiri bagi penegakan hukum perlinndungan siber dalam menegakkan dan menerapkan sanksi pidana terhadap subjek hukum yang melakukan upaya kejahatan siber.

Secara umum bentuk kejahatan dapat diketahui melalui serangkaian perbuatan yang merugikan bagi orang lain, berikut bentuk-bentuk kejahatan berbasis sistem elektronik.

1. Identity theft
   Bentuk kejahatan : pencurian data pribadi berupa no telepon, data diri.
   Contoh : pembobolan akun shopeepay kemudian limit paylater digunakan orang lain.
2. Kejahatan Phishing
   Bentuk kejahatan :berupa akun email untuk verifikasi link palsu.
   Contoh : pembobolan akun m-banking korban melalui verifikasi email.

Vol. 5 No. 2 November 2025, hal.41-58.
ISSN 2808-8468 (Online)
sensasi.upnjatim.ac.id

3. Kejahatan Carding
   Bentuk kejahatan : pembobolan menggunakan kartu kredit orang lain.
   Contoh : nomor kartu kredit dibobol kemudian digunakan untuk berbelanja melalui situs online.
4. Serangan Ransomware
   Bentuk kejahatan : kejahatan malware.
   Contoh : pelaku akan meminta korban berupa uang transferan untuk menghapus ransomware data diri korban.
5. Penipuan Online
   Bentuk kejahatan : berupa pencurian data diri dengan modus foto selfie dengan KTP.
   Contoh : data diri dari aplikasi pinjaman online kemudian data diri tersebut dijual ke pasar gelap yang bertujuan untuk mendapatkan uang.
6. Botnets
   Bentuk kejahatan : berupa botnet (bot) yang menginfeksi computer
   Contoh : apabila ada virus pada komputer maka data yang ada akan hilang dan sistem yang ada akan dijual.
7. *Cyber Espionage* atau mata-mata cyber
   Bentuk kejahatan : peretasan jaringan computer untuk mencuri data-data
   Contoh : kasus sony picture tahun 2009 yang data gaji pegawai dan data film yang belum dirilis di up ke dunia maya
8. Menjiplak Situs Orang Lain
   Bentuk kejhatan : Kejahatan melanggar Hak Atas Kekayaan Intelektual (HAKI) orang lain di internet
   Contoh : kasus rico dwi mahasiswa Unnes tahun 2024
9. SIM SWAP
   SIM Swap merupakan modus kejahatan untuk mengambil ahli nomer posel korban dengan tujuan mengakses perbankan korban dan akibatnya SIM Swap aktif dan bukan lagi milik si korban.
10. Peretasan Situs dan Email
    Peretasan situs dan email yang melibatkan akses tidak sah ke sistem atau email korban dengan meyerang atau mengubah tampilan website, menambahkan konten berbahaya, atau mencuri data sensitif.
11. Kejahatan Skimming
    Kejahatan Skimming merupakan kejahatan perbankan dengan cara mencuri data kartu debit untuk menarik dana di rekening
12. OTP Fraud
    OTP fraud adalah salah satu yang bisa untuk mengakses atau menyelesaikan transaksi. Jika kode OTP sampai diketahui oleh orang lain, bisa berbahaya
13. Pemalsuan Data atau Data Forgery
    Data forgery adalah kejahatan yang di sengaja memalsukan informasi atau data. Tujuannya untuk menipu dan mendapatkan keuntungan yang sah, atau merugikan pihak lain.
14. Kejahtan Konten Ilegal
    Kejahatan konten Ilegal adalah masukkan data atau informasi yang tidak benar, melanggar hukum atau mengganggu ketertiban umum

Vol. 5 No. 2 November 2025, hal.41-58.
ISSN 2808-8468 (Online)
sensasi.upnjatim.ac.id

15. Teroris Dunia Maya atau *Cyber Terorism*
    Cyber Terorism adalah kejahatan yang membuat kerusakan kepada suatu data jaringan komputer. Dengan pelaku yang menawarkan diri kepada korban untuk memperbaiki data untuk disabotase dengan bayaran tertentu.

Tentu segala bentuk perbuatan pastilah memiliki konsekuensi dan bentuk pertanggungjawabannya, dalam prepektif hukum pidana segala bentuk perbuatan yang bertentangan dengan hukum memiliki konsekuensi kausalitas atau sebab akibat, tentu dalam hukum pidana segala hal perbuatan yang melanggar koridor hukum pastilah akan ada konsekuensi sanksi pidana dengan ancaman penjara dan denda ganti rugi, dalam hukum pidana kejahatan dalam sistem elektronik juga telah diatur sebagaimana dalam Pasal 65 ayat (2) Undang-Undang PDP (Perlindungan Data Pribadi) menyebutkan bahwa;
"Setiap Orang dilarang secara melawan hukum mengungkapkan data pribadi yang bukan miliknya."

Narasi verbatim dari pasal tersebut ialah setiap orang tidak diperbolehkan untuk mengakses dan menyebarluaskan data yang bersfiat pribadi milik orang lain, regulasi tersebut juga merupakan masuk dalam koridor *Cyber Law* yang telah diterapkan di Indonesia, penegasan perlindungan data pribadi dalam pasal tersebut telah memberikan payung hukum bagi setiap orang yang menggunakan sistem elektronik untuk tidak melakukan upaya melawan hukum terhadap data pribadi orang lain.

Selanjutnya dalam Pasal 67 ayat (2) Undang-Undang PDP juga memberikan sanksi pidana kepada para pelaku kejahatan peretasan data pribadi milik orang lain, itu merupakan langkah normatif dan prefentif dalam mencegah hal-hal yang dapat memberikan dampak buruk terhadap berlangsungnya penyelenggaraan sistem elektronik di Indonesia, dalam Pasal 67 ayat (2) menyatakan bahwa;
"Setiap Orang yang dengan sengaja dan melawan hukum mengungkapkan data pribadi yang bukan miliknya sebagaimana dimaksud dalam Pasal 65 ayat (2) dipidana dengan pidana penjara paling lama 4 (empat) tahun dan/atau pidana denda paling banyak Rp4.000.000.000,00 (empat miliar rupiah)."

Sanksi pemidanaan telah termaktub secara jelas dan komprehensif dalam pasal tersebut, hal ini mengisyaratkan bahwa dampak dan kerugian dari kejahatan sistem elektronik sangatlah buruk secara signifikan dan meluas, data-data yang diretas oleh pelaku kejahatan berpotensi dapat merugikan baik secara moral, etika, politik, serta sosial.

Analisis dampak kejahatan sistem elektronik membuktikan lemahnya sistem oprasional keamanan siber di Indonesia, disisi lain juga luasnya cakupan sistem elektronik membuat penegak hukum kesulitan dalam menemukan pelaku kejahatan tersebut, aspek sosial berupa kesadaran untuk menjaga data pribadi juga terasa sangat minim dan seringkali diabaikan oleh masyarakat Indonesia.

Analisis Kasus Kebocoran Data Nasional

Pada kasus peretasan yang dilakukan oleh Bjroka pada tahun 2024 telah menjadi bukti konkrit atas lemahnya perlindungan keamanan sistem elektronik di Indonesia, peretasan data yang dilakukan oleh Bjorka sangatlah luas dan signifikan, pada kasus kebocoran data nasional tersebut terjadi pada 23 September 2024 menjadi sorotan masyarakat, sebab hal yang dikhawatirkan adalah kebocoran

Vol. 5 No. 2 November 2025, hal.41-58.
ISSN 2808-8468 (Online)
sensasi.upnjatim.ac.id

tersebut mengenai data NPW (Nomor Pokok Wajib Pajak) masyarakat Indonesia dengan total data yang didapatkan oleh Bjorka sebesar 6 juta data yang berhasil di retas, jumlah tersebut bisa terbilang sangat besar dan signifikan.

NPWP sendiri merupakan salah satu tanda atas identitas seseorang dalam transaksi perpajakan yang dilakukan oleh masyarakat untuk membayar pajak. Pada procedural pembayaran pajak wajib bagi setiap orang untuk menunjukkan NPWP tersebut, dalam NPWP juga tercantum identitas diri seseorang yang terdiri dari nama, alamat serta 9 digit angka pertama yang berisi informasi kode wajib pajak dan 6 digit terakhir merupakan kode administrasi, tentu isi dari NPWP merupakan data pribadi yang bersifat rahasia.

Kasus Bjorka juga tidak luput tersorot oleh dunia internasional sebab bukan hanya kali ini kebocoran data pribadi namun telah terjadi untuk sekian kalinya, dalam kasus Bjorka, dia telah berhasil untuk kedua kalinya melakukan *cheating* terhadap data nasional, mulai dari pelanggan data Indihome, data registrasi SIM card, data KPU (Komisi Pemilihan Umum), data daftar surat kepresidenan Indonesia, serta *doxing* data pejabat publik Indonesia.

Dari rentetan kasus yang dilakukan oleh Bjorka dapat disimpulkan bahwa kasus peretasan data pribadi skala nasional bahka data pribadi presiden dan pejabat publik lainnya bukan hal baru dan perlu adanya perlindungan lebih intens atas data pribadi tersebut.

Dalam kacamata hukum pidana perbuatan Bjorka tentu haruslah mendapat pertanggung jawaban berupa sanksi pemidanaan, sebagiamana yang telah dijelaskan sebelumnya bahwa kejahatan sistem elektronik merupakan kejahatan serius dan dibebankan sanksi pidana sebagai bentuk konsekuensi perbuatannya.

Dalam hukum pidana tentu Bjorka memiliki kedudukan sebagi pelaku kejahatan dan seluruh pihak yang dirugikan atas perbuatan Bjorka merupakan korban atas perbuatannya, tentu menjadi hal pasti bahwa Bjorka harus segera terungkap oleh pihak yang berwenang, sebab hingga saat ini status identitas Bjorka masih belum terungkap secara pasti dan upaya mengungkapan identitas Bjorka hanya masih sebatas dugaan sementara, bahkan upaya pengungkapan identitas Bjroka mengalami kesulitan dan telah menjadi beberapa masyarakat yang diduga sebagai Bjorka ditangkap tanpa dalil pasti, seperti halnya penjual es di Kabupaten Madiun atas nama inisial M.A.H menjadi korban salah tangkap atas dugaan pria tersebut sebagai Bjorka, kasus tersebut bukan hanya terjadi sekali namun beberapa kali korban salah tangkap terjadi di beberapa daerah di Indonesia.

Atas kejahatan sistem elektronik yang dilakukan oleh Bjorka secara hukum pidana haruslah dikenakan sanksi berupa penjara paling lama 4 tahun masa penjara sesuai dengan Pasal 67 ayat (2) Undang-Undang PDP, namun melihat kerugian yang diakibatkan oleh Bjorka yang begitu besar maka secara sanksi pemidanaan penjara harus lebih dari 4 tahun dengan mengganti seluruh kerugian materil atas perbuatannya.

Disisi lain tindak kejahatan peretasan data pribadi juga dapat diajukan dalam gugatan perdata, sebab hukum perdata di Indonesia juga mengatur tentang mekanisme perlindungan data pribadi dalam Pasal 26 ayat (1) Undang-Undang Nomor 19 Tahun 2016 Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik menyebutkan;

Vol. 5 No. 2 November 2025, hal.41-58.
ISSN 2808-8468 (Online)
sensasi.upnjatim.ac.id

> "Kecuali ditentukan lain oleh Peratura Perundang-undangan, penggunaan setiap informasi melalui media elektronik yang menyangkut data pribadi seseorang harus dilakukan atas persetujuan orang yang bersangkutan."

Bunyi Pasal tersebut memberi penjelasan secara jelas dalam proses keperdataan seorang pelaku peretasan data pribadi juga dapat dikenakan sanksi perdata berupa ganti rugi, dalam Pasal yang sama dan ayat (2) selanjutnya dijelaskan bahwa korban dari peretasan data pribadi dapat mengajukan gugatan ganti rugi sebagaimana yang dimaksudkan oleh ayat (1) yang telah disebutkan, bunyi ayat (2) sebagai berikut;

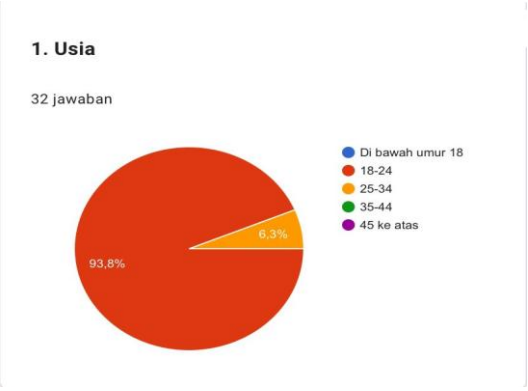
> "Setiap orang yang dilanggar haknya sebagaimana dimaksud pada ayat (1) dapat mengajukan gugatan atas kerugian yang ditimbulkan berdasarkan Undang-Undang ini."

Dari Pasal 26 ayat (1) dan ayat (2) Undang-Undang Nomor 19 Tahun 2016 dapat diartikan bahwa tindak kejahatan siber berupa peretasan data pribadi tidak hanya diatur dalam *cyber law* namun juga diatur dalam hukum pidana dan juga hukum perdata.

Analisis kasus terhadap peretasan data pribadi yang dilakukan oleh Bjorka dapat dilekatkan prinsip-prinsip hukum pidana dan juga perdata serta *cyber law* di Indonesia. Regulasi hukum yang mengatur tentang segala bentuk perbuatan dalam koridor sistem elektronik terbilang sangat signifikan jumlahnya, namun hal ini tidak disertai dengan kesadaran invidu masyarakat dalam menjaga data pribadinya masing-masing, serta kurangnya peran pemerintah untuk meningkatkan keamanan siber pada *high level,* disisi lain peran penegakan hukum cukuplah kurang, terbukti dengan hingga detik ini pelaku kejahatan siber dan peretasan data pribadi yaitu Bjorka belum terungkap identitasnya, sehingga proses penangkapan terkendala dan sulit untuk dilaksanakan.

Hasil Data Kuisioner

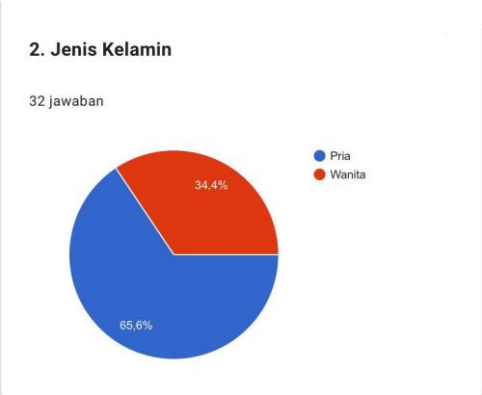
Penelitian ini menggunakan metode empiris, tentu hal utama dalam memperoleh data lapangan, penelitian ini menggunakan metode kuisioner, dengan maksud agar memperoleh data lapangan yang akurat dengan mengajukan pertanyan kepada responden sebanyak 13 buah pertanyaan yang ditujukan kepada masyarakat Indonesia melalui *Google Form*, responden yang menjadi sasaran atas pertanyaan kuisioner tersebut di dapat melalui media sosial berupa WA, FB, IG, dan X. Berikut hasil kuisioner yang di dapatkan daripada responden;



Gambar 1. Rentan usia responden dominan berumur 18-24 tahun dengan persentase

Vol. 5 No. 2 November 2025, hal.41-58.
ISSN 2808-8468 (Online)
sensasi.upnjatim.ac.id

93,8%

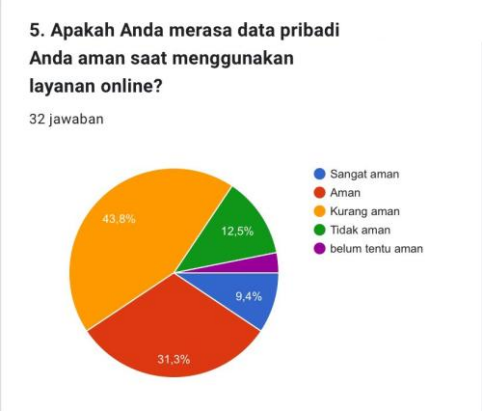


Gambar 2. Jenis kelamin responden dominan laki-laki dengan persentase 65,6%

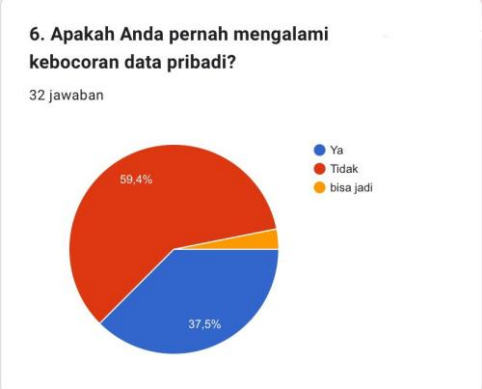
Gambar 3. Pendidikan terakhir responden dominan SMA dengan persentase 78,1%

Gambar 4. Pentingnya perlindungan data pribadi menurut responden sangatlah penting dengan persentase 90,6%

Vol. 5 No. 2 November 2025, hal.41-58.
ISSN 2808-8468 (Online)
sensasi.upnjatim.ac.id

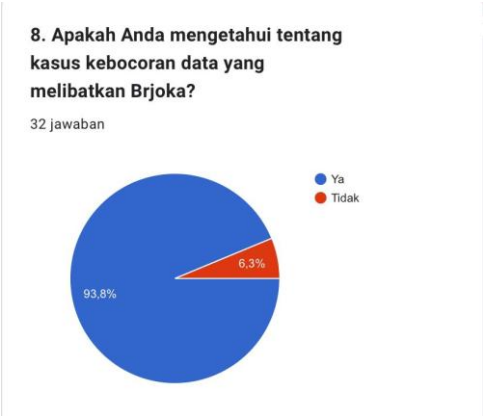


Gambar 5. Data pribadi yang di gunakan saat layanan online dominan kurang aman dengan persentase 43,8%

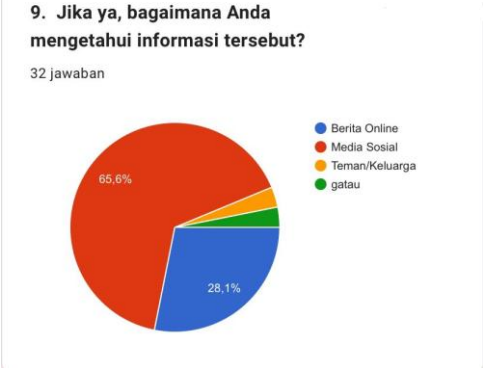


Gambar 6. Responden dominan tidak mengalami kebocoran data pribadi dengan persentase 59,4%

Vol. 5 No. 2 November 2025, hal.41-58.
ISSN 2808-8468 (Online)
sensasi.upnjatim.ac.id



Gambar 7. Responden dominan mengetahui kasus kebocoran data yang melibatkan Brjoka dengan persentase 93,8%



Gambar 8. Responden mengetahui informasi Brjoka melalui media sosial dengan persentase 65,6%

Gambar 9. Dampak pada kasus Brjoka terhadap responden dominan sangatlah besar dengan persentase 43,8%

Vol. 5 No. 2 November 2025, hal.41-58.
ISSN 2808-8468 (Online)
sensasi.upnjatim.ac.id

Gambar 10. Responden bersedia untuk mengikuti sosialisasi perlindungan data pribadi dengan persentase 87,5%

Dari yang telah didapatkan, ada 32 responden serta jawaban, bentuk pertanyaan dalam kuisioner terbagi menjadi 2 yaitu 11 (sebelas) pilihan ganda dan 2 (dua) jawaban terbuka, pertanyan yang diajukan berkaitan dengan peretasan data pribadi oleh Bjorka, data yang didapatkan berguna untuk mendukung penelitian ini lebih lanjut sebagai sumber data tambahan.

Dari data yang telah di cantumkan di atas maka dapat ditarik kesimpulan bahwa msyarakat umum dominan mengetahui kasus peretasan data pribadi yang

Vol. 5 No. 2 November 2025, hal.41-58.
ISSN 2808-8468 (Online)
sensasi.upnjatim.ac.id

dilakukan oleh Bjorka, namun dari jawaban responden terhadap kasus tersebut tidak mengindikasikan kepedulian dan merasa bahwa kasus tersebut adalah lumrah terjadi di Indonesia

Namun disisi lain juga msyarakat secara dominan memiliki kesadaran akan pentingnya menjaga data pribadi secara perorangan dibuktikan dengan data yang didapat yaitu sebesar 90,6% menjawab sangat penting untuk menjaga data pribadi, hal ini di dasarkan pada pengetahuan masyarakat yang mulai adaptif terhadap kemajuan teknologi yang terus berkembang pada penggunaan sistem elktronik, dan sebesar 87,5% masyarakat bersedia untuk mempelajari serta ingin adanya edukasi terkait keamanan data pribadi, itu membuktikan bahwa keinginan masyarakat terhadap perlindungan data pribadi sangatlah tinggi, namun hal tersebut dirasa kurang diimplementasikan oleh pemerintah.

KESIMPULAN

Undang-Undang Nomor 27 tahun 2022 telah memberikan pedoman umum mengenai kehidupan dalam dunia maya, penerapan regulasi tersebut merupakan payung hukum bagi masyarakat agar perbuatan dan tindakannya tidak bertentangan dengan norma-norma sosial dan penyimpangan lainnya, Undang-Undang tersebut juga memberikan jaminan terhadap keberlangsungan *cyber law* di Indonesia, dalam proses penerapan Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi dirasa kurang efektif dalam menjaga keamanan data pribadi, disisi lain juga regulasi tersebut mengalami kesulitan tertentu yang diantarnya proses peraturan pelaksannya masih dalam tahap aspirasi publik, hal ini lah yang menyebabkan kurangnya efektivitas Undang-Undang Nomor 27 Tahun 2022 Tentang Perlindungan Data Pribadi.

Bentuk upaya hukum dalam proses pelaksanaan dan penegakan Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi kurang optimal, sebab kurangnya peran pemerintah pada lini komunal masyarakat kecil dalam melakukan edukasi dan sosialisasi pentingnya keamanan data pribadi, hal ini juga penyebab dan menjadi alasan kurangnya kesadaran masyarakat akan perlindungan data pribadinya masing-masing.

Daftar Pustaka

Adami Chazawi dan Ardi Ferdian. *"Tindak Pidana Informasi & Transaksi Elektronik: Penyerangan Terhadap Kepentingan Hukum Pemanfaatan Teknologi Informasi dan Transaksi Elektronik"*. Malang: Media Nusa Creative, 2015.

Ahmad M. Ramli. *"Cyber Law Dan HAKI: Dalam Sistem Hukum Indonesia"*. Bandung: 2004.

Article 12 Universal Declaration of Human Right.

Budi Suhariyanto. *"Tindak Pidana Teknologi Informasi (Cyber Crime): Urgensi Pengaturan dan Celah Hukumnya"*. Jakarta: Rajawali Pers, 2014.

Dancor, *"Kebocoran Data Indonesia Tertinggi Ke-3"*, diakses pada tanggal (25/09/2024)
https://www.hypernet.co.id/id/2023/03/03/kebocoran-data-indonesia-tertinggi-ke-3/

Indra Lintang, *"10 Kasus Kebocoran Data di Indonesia yang Paling Menggemparkan",* diakses pada tanggal (25/09/2024), https://www.inilah.com/kasus-kebocoran-data-di-indonesia

Karo Karo dan Teguh Prasetyo. *"Pengaturan Perlindungan Data Pribadi Di Indonesia: Perspektif Teori Keadilan Bermartabat"*. Bandung: Nusa Media, 2020.

Kristian dan Yopi Gunawan, *"Penyadapan Dalam Hukum Positif Di Indonesia"*. Bandung: Nuansa Aulia, 2013.

Maskun. *"Kejahatan Siber: Cyber Crime"*. Jakarta: KENCANA, 2013.

Peraturan Mentri Dalam Negeri RI Nomor 102 Tahun 2019 Tentang Pemberian Hak Akses dan Pemanfaatan Data Kependudukan.

Peraturan Pemerintah Nomor 71 Tahun 2019 Tentang Penyelenggaraan Sistem dan Transaksi Elektronik.

Silvana Febriari, *"Deretan Kasus Kebocoran Data Pribadi di Indonesia Sepanjang 2022-2023",* diakses pada tanggal (25/09/2024), https://www.metrotvnews.com/play/NA0CXWqa-deretan-kasus-kebocoran-data-pribadi-di-indonesia-sepanjang-2022-2023

Undang-Undang Nomor 27 Tahun 2022 Tentang Perlindungan Data Pribadi.

Yurizal. *"Penegakan Hukum Tindak Pidana Cyber Crime"*. Malang: Media Nusa Creative, 2018.