Jurnal Pro Hukum:

Jurnal Penelitian Bidang Hukum Universitas GresikVolume 11
Nomor 3, Oktober 2022
pISSN 2089-7146 - eISSN 2615-5567

URGENSI UNDANG-UNDANG PERLINDUNGAN DATA PRIBADI TERHADAP KEJAHATAN PELANGGARAN DATA DI INDONESIA

Edi Saputra Hasibuan[1], **Lia Salsiah**[2]

Dosen Fakultas Hukum Universitas Bhayangkara Jakarta Raya, Indonesia
Email : edi.saputra@dsn.ubharajaya.ac.id, lia.salsiah@dsn.ubharajaya.ac.id

ABSTRAK

Perlindungan oleh negara saat ini tidak hanya dilakukan secara fisik melalui kegiatan yang terjadi di lapangan, namun sudah harus lebih ditingkatkan, mengingat pelanggaran dan tindakan yang melawan hukum kini sudah berkembang pada suatu ruang yang disebut sebagai *cyber space*, dengan mengincar informasi mengenai data, kita dihantui dengan kejahatan yang tidak dapat kita lihat secara langsung. Sekarang ini pelanggaran terhadap keamanan data pribadi sudah menduduki tahap yang jauh berkembang, contohnya saja serangan dalam bentuk *Malware* atau *Phising* (pengelabuhan) aksi dari pelanggaran ini cenderung menyerang pertahanan dari perbankan dan situs dari pemerintahan, motif dari perbuatan pada peretas itu biasanya didasari oleh 2 hal yaitu ekonomi dan kepuasan juga unjuk gigi, selain itu dapat berupa teguran terhadap kinerja pemerintah, misalnya kasus menjelang pemilihan suara untuk pemilihan presiden baru Indonesia pada tahun 2019 lalu, situs dari Komisi Pemilihan Umum (KPU) banyak menerima serangan dari para peretas hebat maupun amatir. Berdasarkan hal ini kemudian membuat penulis tertarik untuk menyoroti mengenai betapa pentingnya undang-undang khusus mengenai perlindungan data.

Kata Kunci: Perlindungan, Data Pribadi, Undang-undang.

ABSTRACT

Protection by the state today is not only carried out physically through activities that occur on the ground, but must be further improved considering that violations and unlawful acts have now developed in a space called cyber space, by eyeing information about data, we are haunted by crimes that we cannot see directly. Currently, violations of the security of personal data have occupied a much developed stage, for example, attacks in the form of Malware or Phishing (phishing) the actions of these violations tend to attack the defenses of banks and sites from the government, the motives of the actions on hackers are usually based on 2 things, namely the economy and satisfaction as well as performances in addition, it can be in the form of a reprimand against the government's performance, for example the case before the election of the vote for Indonesia's new presidential election in 2019, the website of the General Election Commission (KPU) received many attacks from great hackers and amateurs. Based on this, it then makes the author interested in highlighting how important specific laws regarding data protection are.

Keywords: *Protection, Data Privacy Regulation*

PENDAHULUAN

Keterpaduan antara data pribadi, dan teknologi informasi, media, sert telekomunikasi dikelola oleh sistem elektronik, yang memiliki objek yaitu data itu sendiri (Makarim, 2010). Pemaknaan sistem elektronik, merupakan pengembangan sistem informasi dari model e-commerce dengan definisi komputer menurut *Convention on Cyber Crime* (Makarim, 2010). Maksud dari Komputer merujuk pada pasal 1 ayat 5 , Undang–undang Nomor 11 tahun 2008 dirubah menjadi Undang-undang No. 19 tahun 2016 tentang Informasi dan Transaksi Elektronik yaitu sebuah instrumen, untuk menjalankan sistem elektronik, yang berfungsi untuk mengumpulkan mempersiapkan, mengumpulkan, mengolah, menganalisis, menyimpan, menampilkan, mengumumkan, mengirimkan, dan/atau menyebarkan Informasi Elektronik.

Perihal mengenai data pribadi, sejak awalnya manusia itu sendiri memiliki data yang melekat dengan dirinya, yakni biometrik data, ini sudah ada saat Tuhan pertama kali menciptakan manusia (Kindt, 2013). Contoh lainnya sebuah nama sekarang mengalami perkembangan menurut pasal 84 Undang–undang Nomor 23 tahun 2006 tentang Administrasi Kependudukan, selain nama, NIK (Nomor Induk Kependudukan), nomor KK (Kartu Keluarga), tempat dan tanggal lahir, NIK (Nomor Induk Kependudukan) ibu kandung, NIK (Nomor Induk Kependudukan) ayah kandung, keterangan tentang kecacatan fisik dan beberapa isi peristiwa penting. Sangat sederhana sekali pemaknaan data disini.

Pada dasarnya, data pribadi adalah data perseorangan tertentu yang disimpan, dirawat, dan dijaga kebenaran serta dilindungi kerahasiaannya, sesuai dengan pasal 1 ayat 1 Peraturan Menteri Komunikasi dan Informatika Nomor 20 tahun 2016 tentang Perlindungan Data Pribadi. Untuk menjamin keamanan dan keselamatan suatu data perlu disusun dalam pengarsipan yang apik, pasal 3 Undang–undang Nomor 43 tahun 2009 tentang Kearsipan. Adapun definisi lain mengenai data pribadi adalah setiap informasi terkait dengan seseorang yang dapat mengenal orang tersebut, yang merujuk pada nama, nomor identitas, data lokasi, data pengenal dalam jaringan, identitas fisik, psikologis, genetik, mental, ekomomi, atau sosial orang tersebut (Sirait, 2019)

Kejahatan siber yang mengeksploitasi data pribadi ini sontak terlihat, dari laporan ke situs Patroli Siber Polri, dari Januari 2020 sampai dengan 25 Maret 2020, telah terjadi 34 kasus mengenai pencurian data pribadi yang dilaporkan kepada Patroli Siber Polri (Patroli Siber, 2022). Sesuai dengan data ini, setiap bulan setidaknya ada lebih dari 10 kasus yang dilaporkan.

Bahkan baru-baru ini Indonesia sedang menghadapi serangan *hacker* yang menamai dirinya sebagai “Bjorka”, kasus Bjorka ini menjadi perhatian publik oleh karena tindakan yang ia lakukan dengan meretas sejumlah data pemerintah serta melakukan *doxing* terhadap beberapa pejabat publik, ia membagikan sejumlah data pribadi pejabat publik yang berisi nama, Nomor Induk Kependudukan, dan Kartu Keluarga (KK), sampai alamat rumah (Kompas, n.d.)

Oleh karena itu di era maju ini, perlindungan terhadap data pribadi, ditandai dengan standar untuk operasional penyedia sistem elektronik, yang mana, sistem elektronik harus andal, aman serta bertanggung jawab terhadap beroperasinya sistem elektronik sebagaimana mestinya, merujuk pada pasal 15 Undang – undang Nomor 11 tahun 2008 di rubah menjadi Undang - undang No. 19 tahun 2016 tentang Informasi dan Transaksi Elektronik. Ini diartikan agar penyelenggara sistem elektronik, kebal terhadap pembajakan data dan penyerangan dari pencuri.

Selain itu, perlindungan ini terhadap data pribadi sangat penting, karena negara berkewajiban melindungi segenap wilayah dan tumpah darahnya, merujuk pada pasal 2 Undang- undang Nomor 23 tahun 2006 tentang Administrasi Kependudukan, wilayah yang berarti sebagai suatu daerah yurisdiksi dari Indonesia dan darah yang dimaksudkan adalah manusia. Maka negara berkewajiban melakukan perlindungan data pribadi warganya (Indonesia, 2006).

Atas dasar permasalahan tersebut, penulis tertarik dan merasa perlu untuk menjelaskan dan menggali lebih jauh mengenai pentingnya perlindungan data, serta sebagai sebuah pengingat bahwa telah timbul kejahatan baru yang penanganannya juga harus segera dicari solusinya, agar tidak dapat berkembang biak lebih besar lagi.

METODE

Pada penelitian kali ini penulis menggunakan metode penelitian normatif dengan menelaah setiap tulisan, aturan dan penerapannya, serta digabungkan dengan studi kepustakaan atau literatur dengan menganalisis buku, jurnal, *paper*, media cetak, maupun berita online yang terkait dengan perlindungan data. Target data yang dikumpulkan adalah terkait dengan kasus kejahatan siber, perlindungan data, arti, dan aturan terkait.

HASIL DAN PEMBAHASAN

1. Sejarah Perlindungan Data

Pertama kalinya penggunaan kata perlindungan data pribadi itu lahir pada tahun 1970 di negara Jerman dan Swedia, yang dahulu dimaksudkan untuk menghimpun data pribadi masyarakat, yang disimpan dalam komputer. Di dalam data pribadi mencakup fakta-fakta, komunikasi atau pendapat yang berkaitan dengan individu yang merupakan informasi yang sifatnya rahasia, pribadi atau sensitif sehingga pribadi yang bersangkutan ingin menyimpan atau membatasi orang lain untuk mengoleksi, menggunakan atau menyebarkannya kepada pihak lain (Sautunnida, 2018). Keperluan untuk menyimpan data adalah untuk mengetahui berapa jumlah penduduk (sensus penduduk), yang tak disangka ternyata banyak mengalami pelanggaran terhadap penyimpanan data tersebut. Oleh karena pada saat itu pemerintah berinisiatif untuk membuat suatu instrumen perlindungan hukum, yaitu undang – undang perlindungan data pribadi (Dewi, 2009).

Konsep dari sebuah privasi pertama kali dikembangkan oleh Warren dan Brandheis yang menulis sebuah artikel di dalam jurnal ilmiah Sekolah Hukum Universitas Harvard yang berjudul "*The Right to Privacy*" atau hak untuk tidak diganggu. Dalam jurnal tersebut, Warren dan Brandheis menyatakan dengan lahir serta berkembangnya kemajuan dari sebuah teknologi maka timbul suatu kesadaran bahwa orang memiliki hak untuk menikmati hidup atau bahasa lainnya hak untuk tidak diganggu dengan privasinya, baik oleh negara maupun oleh orang lain. Maka dengan itu sebuah hukum seharusnya mengakui dan melindungi hak privasi. Walaupun konsep privasi merupakan hal yang amat sulit untuk didefinisikan, ini dikarenakan setiap orang memiliki batasan yang berbeda (Dewi, 2009).

Menurut Yuwinanto, privasi merupakan konsep abstrak yang mengandung banyak makna. Penggambaran populer mengenai privasi antara lain adalah hak individu untuk menentukan apakah dan sejauh mana seseorang bersedia membuka dirinya kepada orang lain atau privasi adalah

Penggunaan kata untuk menggambarkan data pribadi antara Indonesia dengan negara lain seperti Amerika Serikat, Kanada dan Australia menggunakan kata informasi pribadi, sedangkan negara kita Indonesia menggunakan kata data pribadi sesuai dengan penuangan dalam pasal 26 undang – undang Nomor 11 tahun 2008 diubah menjadi Undang - undang No. 19 tahun 2016 tentang Informasi dan Transaksi Elektronik. Ini sama dengan penggunaan kata di negara – negara Uni Eropa (Latumahina, 2014).

Dalam pembukaan Deklarasi Universal Hak Asasi Manusia (DUHAM) / Universal Declaration of Human Rights (UDHR) menuliskan bahwa hak asasi manusia harus dijamin oleh undang – undang, hak yang ditekankan dalam ini adalah perlindungan atas keprivasian, sesuai dengan pada pasal 12, menyatakan jelas: "*No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honor and reputation. Everyone has the right to the protection of the law against such interference or attacks*." Atau " Tidak seorang pun akan mengalami gangguan sewenang-wenang dengan privasi, keluarga, rumah atau korespondensi, atau serangan terhadap kehormatan dan reputasinya. Setiap orang berhak atas perlindungan hukum terhadap gangguan atau serangan semacam itu (Latumahina, 2014).

Dalam *Black's Law Dictionary* memberikan pengertian dari privasi adalah "*The right to be alone, the right of a person to* hak untuk tidak diganggu. Privasi merujuk padanan dari Bahasa Inggris *privacy* adalah kemampuan satu atau sekelompok individu untuk mempertahankan kehidupan dan urusan personalnya dari publik, atau untuk mengontrol arus informasi mengenai diri mereka (Sautunnida, 2018).

be free from unwarranted public. Term right of privacy is generic term encompassing various rights recognized to be inherent in concept of ordered liberty, and such rights prevents governmental interference in intimate personal relationship or activities, freedom of individual to make fundamental choices involving himself, his family and his relationship with others" atau artinya adalah Hak untuk menyendiri; hak seseorang untuk bebas dari publik yang tidak beralasan. Istilah hak privasi adalah istilah umum yang mencakup berbagai hak yang diakui melekat dalam konsep kebebasan yang diperintahkan, dan hak-hak semacam itu mencegah campur tangan pemerintah dalam hubungan atau kegiatan pribadi yang intim, kebebasan individu untuk membuat pilihan-pilihan mendasar yang melibatkan dirinya, keluarga dan hubungannya dengan orang lain (Sautunnida, 2018)

1. Pentingnya Undang-Undang Khusus Terhadap Perlindungan Data

Mengapa urgensi terhadap lahirnya Undang-undang Perlindungan Data Pribadi harus segera dilakukan? Yang pertama karena hal ini telah menjadi amanat dalam undang-undang Dasar 1945, "Setiap orang berhak atas perlindungan diri pribadi, keluarga, kehormatan, martabat, dan harta benda yang di bawah kekuasaannya, serta berhak atas rasa aman dan perlindungan dari ancaman ketakutan untuk berbuat atau tidak berbuat sesuatu yang merupakan hak asasi.**) Setiap orang berhak untuk bebas dari penyiksaan atau perlakuan yang merendahkan derajat martabat manusia dan berhak memperoleh suaka politik dari negara lain.**).

Menempatkan perlindungan ini menjadi hak dasar bagi hak asasi manusia. Perlindungan atas diri pribadi tidak sebatas melindungi secara fisik saja, melainkan lebih dalam dari itu, seperti hal – hal yang menggambarkan pribadi seseorang. Ini dilakukan untuk meraih kehidupan yang berkualitas (*The right of quality life*), pemaknaan dari hidup berkualitas jauh melebihi hak untuk hidup saja, seperti yang tertulis pada pasal 28A dan 28I sebagaimana hak yang tidak boleh disampingkan atau dikurangi dengan alasan apa pun (*Non Derogable*).

Selain dari undang–undang dasar, Indonesia telah meratifikasi Kovenan internasional tentang hak–hak dan politik, yang ratifikasi menjadi Undang–undang No. 12 tahun 2005 tentang Pengesahan *International Covenant on Civil and Political Rights* (Kovenan Internasional tentang Hak–hak Sipil dan Politik) pokok – pokok dari isi kovenan ini menguatkan pokok – pokok yang ada pada Deklarasi Universal Hak Asasi Manusia (DUHAM), yang mengingatkan untuk negara–negara yang menjadi anggota PBB untuk memajukan dan melindungi hak asasi manusia dan kovenan ini mengakui bahwa hak – hak berasal dari harkat dan martabat yang melekat pada manusia, mengakui bahwa sesuai dengan deklarasi universal hak asasi manusia mengenyam hak–hak sipil dan politik dan juga hak–hak ekonomi. Kaitannya dengan data pribadi dan keprivasian, tertulis pada pasal 6 ayat 1: "Setiap manusia berhak atas hak untuk hidup yang melekat pada dirinya. Hak ini wajib dilindungi oleh hukum. Tidak seorang pun dapat dirampas hak hidupnya secara sewenang-wenang".

Selanjutnya, penulis akan memberikan beberapa contoh kasus yang terjadi akibat pembobolan data, awal bulan Maret 2020 yang lalu, salah satu platform, *e-commerce unicorn* belanja online terbesar di Indonesia yaitu Tokopedia, mengalami pencurian data, sebanyak 15 juta data yang dilaporkan hilang. Dari peretasan ini Tokopedia melanjutkan pemeriksaan dan mendapati tambahan data yang dicuri sebanyak 91 juta data pribadi, dari para pengguna aplikasi mereka, dan lebih dari 7 juta data *merchant* Tokopedia dijual di situs gelap, dibanderol dengan harga 5000 Dollar Amerika, atau setara dengan sekitar Rp. 75 Juta Rupiah pada kurs saat tulisan ini dibuat. Kejadian ini pun dikonfirmasi oleh pihak dari Tokopedia, bahkan kini pelaku belum diketahui siapa yang melakukan (Kompas.com, 2022)

Pada tahun 2014, Komisi Pemilihan Umum juga mengalami serangan pembobolan data seperti ini, bocornya jutaan data kependudukan warga Indonesia milik Komisi Pemilihan Umum (KPU), tersebar di forum komunitas peretas, adapun data yang telah bocor sebesar 2,3 juta Daftar Pemilih Tetap (DPT) pemilu 2014. Data yang bocor tersebut seperti Nama lengkap, Nomor Kartu Keluarga, Alamat Surat Elektronik, Nomor Induk Kependudukan, Tempat dan Tanggal Lahir, Usia, Jenis Kelamin, Status Perkawinan, dan Alamat lengkap penduduk (Kompas, 2022c) Seakan tidak berhenti, lagi-lagi kasus pembobolan data terus terjadi sampai pada kasus yang sedang menjadi bahan perbincangan publik, pembobolan data yang menyebabkan 105 juta data kependudukan bocor dan diperjual belikan di forum *online* "*Breached Forum*" oleh seseorang yang menamakan dirinya "Bjorka", ia menuturkan bahwa data yang ia curi berasal dari KPU, dan bahkan sebelumnya juga menjual data pengguna layanan Indihome, pelaku membuat akun di Twitter dan Telegram dengan maksud untuk memiliki banyak pengikut sehingga tindakannya dapat menjadi perhatian publik juga untuk menawarkan data curian yang ia miliki (Kompas, 2022a)

Bahkan pembobolan terkait data mengenai kesehatan juga tidak luput menjadi sasaran kejahatan ini, Data diri dari pasien pandemi sebanyak 231. 636 berhasil dicuri oleh peretas dan dijual di *Dark Web* dengan harga 300 Dollar Amerika atau setara dengan 4,2 juta rupiah. Data yang berhasil dicuri berupa data sensitif seperti nama, nomor telepon, alamat, terakhir hasil *Polymerase Chain Reaction* (PCR), dan lokasi pasien dirawat. Menurut ahli Ilmu Teknologi (IT) dari Universitas Sebelas Maret Ari Yuana, menjelaskan terjadinya hal ini dikarenakan, adanya celah pada keamanan sisi server, ini dapat terjadi karena *firewall* pada server lemah, juga ada celah keamanan pada *software*, yang mana dalam *software* terdapat *bug* (cacat pemrograman) yang berakibat menjadi celah untuk masuknya peretas (Kompas, 2022b).

Dari deretan panjang kasus pembobolan data di atas, penulis bermaksud untuk menyoroti bahwa sebagai individu, kita saat ini tidak lagi memiliki tempat yang aman, data yang bocor dan selanjutnya dijual oleh pihak yang tidak bertanggung jawab membuat kita mudah mendapat gangguan, seperti penawaran produk yang tiba-tiba masuk ke ponsel kita, telepon, e-mail, *Whats-App* yang masuk tanpa kita kenali nomor penggunanya, hal ini lebih jauh dapat semakin berbahaya ketika data kita digunakan untuk hal-hal yang akan sangat merugikan kita, seperti untuk melakukan kredit, dan pinjaman *online* yang saat ini sedang berkembang.

Sejauh ini penanganan dan hukuman yang diberikan terhadap kasus dari pembobolan data, masih berfokus pada pelaku pembobolan, contohnya Tindakan yang dilakukan oleh peretas, merupakan sebuah tindak pidana yang diatur pada pasal 30 Undang-undang tentang Informasi dan Transaksi Elektronik dengan sanksi pidana berupa penjara dari 6 tahun sampai dengan 8 tahun serta denda Rp. 600.000.000,00 (enam ratus juta rupiah) sampai dengan Rp. 800.000.000,00 (delapan ratus juta rupiah). Pasal ini dijatuhkan jika seseorang melakukan peretasan dengan memasuki sebuah sistem elektronik dan melakukan perbuatan menguntungkan diri sendiri merupakan tindakan yang berlawanan dengan hukum. Pelaku pencurian data itu pada dasarnya merusak atau masuk kepada sistem elektronik hingga mengakibatkan kerugian yang dialami dari penyelenggara sistem elektronik.

Dalam hemat penulis hal ini sangat tidak seimbang mengingat dalam sebuah aplikasi maupun *platform* yang ditawarkan baik oleh swasta maupun oleh lembaga pemerintahan, haruslah bertanggung jawab dengan memiliki sistem elektronik yang kuat, KPU misalnya yang menyimpan data penduduk Indonesia juga harus bertanggung jawab oleh karena sistem mereka yang dapat diretas, sebagai lembaga negara sudah sewajarnya untuk membangun sistem elektronik yang kuat, canggih, dan mumpuni, karena ketika terjadi pembobolan seperti ini, ia bukan hanya mempermalukan lembaga mereka sendiri, namun mempermalukan nama baik negara, terlebih keselamatan data para penduduknya.

Oleh karena itu, urgensi terhadap aturan khusus mengenai perlindungan data sangat penting, karena dalam aturan tersebut nantinya, diharapkan terdapat instrumen yang tidak hanya memberikan hukuman kepada pelaku pencurian data, namun juga memberikan sanksi kepada penyelenggara sistem elektronik, serta memberikan standar yang harus diikuti oleh setiap perusahaan maupun lembaga pemerintahan, seperti penerapan ISO, keamanan sistem manajemen untuk sistem elektronik menurut Kominfo harus memiliki standar ISO 27001. ISO sendiri merupakan kepanjangan dari *International Organization for Standarization*, yang mana adalah sebuah organisasi internasional non-pemerintahan untuk standarisasi. Kominfo juga berharap nantinya penyelenggara sistem elektronik memiliki dokumentasi dan sistem manajemen yang memenuhi standar ini (Prasetya et al., 2015).

SIMPULAN

Berdasarkan pembahasan di atas, dapat ditarik 2 kesimpulan penting. *Pertama*, Mengenai perlindungan data pribadi saat ini di Indonesia dilihat kurang efektif, tentu pernyataan ini didukung dengan minimnya, aturan mengenai perlindungan data pribadi. Kini di Indonesia perihal data pribadi hanya diatur pada pasal 26 Undang -undang No. 11 tahun 2008 yang diubah menjadi Undang–undang No. 19 tahun 2016 tentang Informasi dan Transaksi Elektronik. Setidaknya dari pasal ini, ditulis akibat hukum dari pelanggaran pada data pribadi. Serta dijelaskan juga langkah hukum yang dapat diambil yaitu pengajuan gugatan atas kerugian, walaupun belum jelas dituliskan batas dikatakan sebuah kerugian seperti yang dimaksudkan pada pasal 26 ini. Sejatinya dalam memanfaatkan harus memberikan rasa aman, keadilan dan kepastian hukum.

Kedua, Indonesia sekarang ini masih belum kuat dalam melakukan perlindungan data pribadi, nyatanya hingga sampai kini belum ada undang – undang khusus atau tunggal yang memiliki peran dalam mengatur perlindungan data pribadi, padahal data pribadi sangatlah besar potensinya. Dari kasus yang sudah dijabarkan, kita bisa melihat dampak besar yang terjadi jika data kita dicuri atau bocor ke publik, draft mengenai rancangan Undang-undang tentang Perlindungan Data Pribadi saat ini sudah masuk dalam Program Legislasi Nasional, dan kabarnya akan segera di sahkan, penulis tentu berharap semoga hal ini dapat segera terwujud, dan dapat diterapkan dengan baik.

REFERENSI

Dewi, S. (2009). Cyberlaw Perlindungan Privasi Atas Informasi Pribadi dalam E-Commerce Menurut Hukum Internasional. *Bandung: Widya Padjajaran*.

Indonesia, R. (2006). Undang-Undang Republik Indonesia Nomor 23 Tahun 2006 Tentang Administrasi Kependudukan. *Jakarta, DKI Jakarta, Indonesia*.

Kindt, E. J. (2013). An introduction into the use of biometric technology. In *Privacy and Data Protection Issues of Biometric Applications* (pp. 15–85). Springer.

Kompas. (n.d.). *, "Polri sebut tersangka kasus hacker 'Bjorka' masih bisa bertambah", .*

Kompas. (2022a). *"105 Juta data penduduk bocor, dibantah KPU, tetapi diduga valid"* .

Kompas. (2022b). *"Data pasien Covid-19, dirahasiakan pemerintah, diduga dijual oleh hacker."*

Kompas. (2022c). *"Jutaan data kependudukan di DPT pemilu 2014 milik KPU diduga bocor", .*

Kompas.com. (2022). *"Kasus Kebocoran Data Pribadi di Indonesia dan Nasib Perlindungan Data Pribadi."*

Latumahina, R. E. (2014). *Aspek Hukum Perlindungan Data Pribadi di Dunia Maya*.

Makarim, E. (2010). *Tanggung jawab hukum penyelenggara sistem elektronik*. Rajajawali Pers.

Patroli Siber. (2022). *"Statistik Jumlah Laporan".*

Prasetya, P., Rochim, A. F., & Windasari, I. P. (2015). Desain dan Implementasi Standar Operasional Prosedur (SOP) Keamanan Sistem Informasi Fakultas Teknik Universitas Diponegoro Menggunakan Standar ISO 27001. *Jurnal Teknologi Dan Sistem Komputer*, *3*(3), 387–392.

Sautunnida, L. (2018). Urgensi Undang-Undang Perlindungan Data Pribadi di Indonesia: Studi Perbandingan Hukum Inggris dan Malaysia. *Kanun Jurnal Ilmu Hukum*, *20*(2), 369–384.

Sirait, Y. H. (2019). General Data Protection Regulation (GDPR) dan Kedaulatan Negara Non-Uni Eropa. *Gorontalo Law Review*, *2*(2), 60–71.