INNOVATIVE: Journal Of Social Science Research
Volume 3 Nomor 4 Tahun 2023 Page 680-692
E-ISSN 2807-4238 and P-ISSN 2807-4246
Website: https://j-innovative.org/index.php/Innovative

Peran Direktorat Tindak Pidana Siber (DITTIPIDSIBER) Bareskim Polri Dalam Melakukan Penegakan Hukum Terhadap Kejahatan Pencurian dan Penyalahgunaan Data Pribadi

Gian Wiatma Jonimandala[1✉] , Devy K.G.Sondakh[2] , Jemmy Sondakh[3]
Program Studi Magister Ilmu Hukum, Universitas Sam Ratulangi Manado
Email : gianwj89@gmail.com[1✉]

Abstrak

Direktorat Tindak Pidana Siber (Dittipidsiber) Bareskrim Polri memiliki peran yang sangat penting dalam mengatasi dan menangani kejahatan siber di Indonesia. peran utama Dittipidsiber Bareskrim Polri: Penegakan Hukum Terhadap Kejahatan Siber, Penyelidikan Kasus Kejahatan Siber, Pencegahan dan Pengamanan Cyber, Kolaborasi dengan Pihak Terkait, Penyuluhan dan Edukasi Keamanan Siber, Pengembangan Kemampuan Internal, Menyusun dan Menerapkan Kebijakan Keamanan Siber. Peran Dittipidsiber Bareskrim Polri sangat vital dalam menjaga keamanan siber dan melindungi masyarakat dari ancaman kejahatan siber. Upaya mereka dalam menegakkan hukum, mencegah kejahatan, dan meningkatkan kesadaran akan keamanan siber adalah bagian penting dari perlindungan dan keamanan di dunia maya. Kejahatan pencurian dan penyalahgunaan data pribadi adalah jenis kejahatan siber yang melibatkan akses tidak sah atau pengambilan data pribadi seseorang dengan tujuan yang merugikan individu tersebut atau pihak lain. Dalam konteks kejahatan siber, data pribadi merujuk pada informasi sensitif yang dapat mengidentifikasi individu tertentu. Pencurian data pribadi dapat terjadi melalui berbagai cara, termasuk serangan peretasan atau hacking, serangan phishing, atau akses ilegal ke jaringan atau server yang mengandung data pribadi. Kehadiran dan penggunaan data pribadi dalam dunia digital menimbulkan risiko kejahatan siber yang serius. Oleh karena itu, penting bagi individu dan organisasi untuk meningkatkan kesadaran akan keamanan siber dan mengambil langkah-langkah untuk melindungi data pribadi mereka dari penyalahgunaan atau pencurian.

Kata Kunci : *Dittipidsiber Bareskrim Polri, Kejahatan siber, Pencurian dan penyalagunaan data pribadi.*

Abstract

The Directorate of Cyber Crime (Dittipidsiber) of the Indonesian National Police plays a crucial role in addressing and handling cybercrime in Indonesia. The main roles of Dittipidsiber Bareskrim Polri are: Law Enforcement Against Cyber Crimes, Investigation of Cybercrime Cases, Cybercrime Prevention and Security, Collaboration with Relevant Parties, Education and Awareness on Cyber Security, Internal Capability Development, and Formulation and Implementation of Cyber Security Policies. The role of Dittipidsiber Bareskrim Polri is vital in safeguarding cyber security and protecting the public from cyber threats. Their efforts in law enforcement, crime prevention, and raising awareness of cyber security are crucial aspects of protection and security in the digital realm. Cybercrime involving theft and misuse of personal data is a type of cybercrime that involves unauthorized access or theft of an individual's personal data for malicious purposes. In the context of cybercrime, personal data refers to sensitive information that can identify a specific individual. Personal data theft can occur through various methods, including hacking, phishing attacks, or illegal access to networks or servers containing personal data. The presence and use of personal data in the digital world pose serious cybercrime risks. Therefore, it is essential for individuals and organizations to increase awareness of cyber security and take steps to protect their personal data from misuse or theft.

Keywords: *Dittipidsiber Bareskrim Polri, Cybercrime, Theft and misuse of personal data.*

PENDAHULUAN

Dalam Pasal 28G ayat (1) Undang-Undang Dasar Negara Republik Indonesia Tahun 1945 menyebutkan bahwa 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 manusia. perlindungan diri pribadi sebagaimana disebutkan dalam Pasal 28G ayat (1) Undang-Undang Dasar Negara Republik Indonesia Tahun 1945 di atas erat kaitannya dengan perlindungan terhadap hak-hak pribadi atau hak-hak privat. Perlindungan data juga merupakan hak asasi manusia yang fundamental, sejumlah negara telah mengakui perlindungan data sebagai hak konstitusional atau dalam bentuk "*habeas data*" yakni hak seseorang untuk mendapatkan pengamanan terhadap datanya dan untuk pembenaran ketika ditemukan kesalahan terhadap datanya.

Sejumlah kasus yang mencuat, terutama yang memiliki keterkaitan dengan kebocoran data pribadi seseorang dan bermuara kepada aksi penipuan atau tindak kriminal pornografi, menguatkan wacana pentingnya pembuatan aturan hukum untuk melindungi data pribadi.

Revolusi digital telah menciptakan sebuah inovasi baru dalam kapasitas untuk memperoleh, menyimpan, memanipulasi dan mentransmisikan volume data secara nyata (real time), luas dan kompleks. Oleh karenanya revolusi digital seringkali dianggap identik dengan revolusi data. Perkembangan tersebut telah mendorong pengumpulan berbagai data, tidak lagi tergantung pada pertimbangan data apa yang mungkin berguna di masa depan. Akan tetapi, hampir semua data dikumpulkan, pemerintah dan swasta bersaing untuk memperbesar kapasitas penyimpanan data mereka, dan semakin jarang melakukan penghapusan data. Pada satu sisi, kemajuan teknologi memberikan banyak kemudahan akan tetapi pada sisi lainnya, kemajuan tersebut dapat dimanfaatkan oleh pihak yang tidak bertanggung jawab untuk melakukan tindakan kejahatan.

Direktorat Tindak Pidana Siber (Dittipidsiber) adalah satuan kerja yang berada di bawah Bareskrim Polri dan bertugas untuk melakukan penegakan hukum terhadap kejahatan siber. Secara umum, Dittipidsiber menangani dua kelompok kejahatan, yaitu *computer crime* dan *computer-related crime*. *Computer crime* adalah kelompok kejahatan siber yang menggunakan komputer sebagai alat utama. *Computer-related crime* adalah kejahatan siber yang menggunakan komputer sebagai alat bantu dimana salah bentuk kejahatan di bidang ini yang menjadi ranah dari Direktorat Tindak Pidana Siber (Dittipidsiber) Bareskrim Polri yaitu kejahatan pencurian dan penyalahgunaan data pribadi. Saat ini ada beberapa peraturan perundang-undangan yang telah diterbitkan yang mengatur mengenai perlindungan data pribadi, yaitu : Pasal 31 Peraturan OJK Nomor : 1/POJK.07/2013 tentang Perlindungan Konsumen Sektor Jasa Keuangan. Pasal 77 dan Pasal 79 Undang-Undang Nomor 24 Tahun 2013 tentang Perubahan Atas Undang-Undang Nomor 23 Tahun 2006 tentang Administrasi Kependudukan. Pasal 5 Permen Kominfo Nomor 20 Tahun 2016 tentang Perlindungan Data Pribadi Dalam Sistem Elektronik. Pasal 26 Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik. Pasal 26 Peraturan OJK Nomor 77/POJK.01/2016 tentang Layanan Pinjam Meminjam Uang Berbasis Teknologi Informasi serta Surat Edaran Otoritas Jasa Keuangan Nomor 14/Seojk.07/2014 tentang Kerahasiaan Dan Keamanan Data dan/atau Informasi Pribadi Konsumen hingga yang baru saja disahkan Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi.

Di Indonesia pencurian serta penyalahgunaan terhadap penggunaan data pribadi kerap terjadi, yaitu : pada praktik perbankan, pertukaran data pribadi dilakukan melalui sistem sharing yaitu bertukar informasi tentang data pribadi nasabah di antara sesama card center, mengungkapkan informasi termasuk transaksi yang berhubungan dengan pemegang kartu kredit kepada pihak ketiga atau diperjualbelikan di antara bank sendiri

ataupun melalui pihak ketiga, yaitu baik perorangan maupun perusahaan-perusahaan pengumpul data serta memperjualbelikan data pribadi nasabah. Dalam sektor kesehatan, data pasien diperjualbelikan atau diungkap untuk keperluan asuransi, kesempatan kerja, mendapatkan program bantuan pemerintah tanpa sepengetahuan pasien.

Berdasarkan laporan yang dirilis oleh Bareskrim Polri dalam kurun waktu 4 tahun terakhir 2017-2020, terjadi kenaikan yang signifikan terhadap kejahatan pencurian dan penyalahgunaan data pribadi. Bareskrim Polri mencatat pada 2017 terdapat 47 kasus, 2018 meningkat jadi 88 kasus, dan lonjakan kasus terus terjadi pada 2019-2020 sebanyak 140 kasus. Jenis kasus pencurian dan penyalahgunaan data pribadi bermacam-macam, seperti penipuan, pencemaran nama baik, pornografi, perjudian, hingga mengubah tampilan situs. Sementara itu kasus pencurian dan penyalahgunaan data pribadi juga terjadi di Sulawesi Utara. Kasus yang terjadi yaitu penyalinan data dan informasi kartu ATM nasabah (*skimming*) dimana pelaku *skimming* melakukan penarikan dana di tempat lain. Kasus tersebut ditangani oleh Ditreskrimsus Polda Sulut.

Menurut keterangan Kapolda Sulut Irjen Pol Mulyatno didampingi Direktur Reskrimsus Polda Sulut Kombes Pol Nasriadi menyatakan para pelaku beraksi di 26 lokasi mesin ATM Bank SulutGo di wilayah Kota Manado, pada tanggal 30 Juni 2022, sekitar pukul 00:30 hingga 06:00 WITA. Modus operandinya, para pelaku mengambil uang nasabah dengan cara melakukan transaksi (tarik tunai dan transfer) di mesin-mesin ATM Bank SulutGo dengan menggunakan kartu yang menyerupai kartu ATM (kartu putih yang berisi magnetic stripe). Para pelaku memasang alat skimmer pada mesin-mesin ATM Bank SulutGo yang banyak atau tinggi transaksi perbankannya. Kemudian saat beraksi, sindikat ini terbagi dalam tiga kelompok. Kelompok pertama bertugas memasang alat skimmer, kelompok kedua adalah yang datang untuk mengambil atau bertransaksi memakai kartu putih, sedangkan kelompok ketiga adalah eksekutor yang mengambil uang secara cash dan mentransfer ke rekening lain.

METODE PENELITIAN

Jenis penelitian ini termasuk penelitian hukum normatif yang hanya menggunakan data sekunder. Tipe penelitian hukumnya adalah kajian komprehensif analitis terhadap bahan hukum primer dan bahan hukum sekunder. Hasil kajian dipaparkan secara lengkap, rinci, jelas dan sistematis sebagai karya ilmiah. Penelitian ini merupakan penelitian hukum normatif, dengan metode pendekatan yang digunakan adalah metode yuridis-normatif, karena merupakan penelitian hukum normatif (*legal research*) atau penelitian hukum doktriner, yaitu cara pendekatan yang digunakan untuk memecahkan masalah penelitian dengan meneliti data sekunder. Penelitian ini menggunakan data sekunder yang diperoleh

dari bahan-bahan pustaka. kegiatan utama yang dilakukan dalam melaksanakan penelitian ini, yaitu studi kepustakaan dengan menggunakan teknik dokumenter, yaitu dikumpulkan dari tela'ah arsip atau studi pustaka yang ada pada data sekunder. Metode pengolahan data dalam penelitian ini yaitu dilakukan dengan cara pemeriksaan data terhadap bahan hukum primer, sekunder dan tersier melalui proses (*editing*) yaitu pembenaran apakah data yang terkumpul melalui studi pustaka, dokumentasi sudah dianggap relevan dengan masalah, jelas, tidak berlebihan, dan tanpa kesalahan. Dalam penelitian ini bahan hukum dianalisis secara kualitatif, selanjutnya dideskriptifkan dengan cara menjelaskan, menguraikan dan menggambarkan permasalahan mengenai peran Direktorat Tindak Pidana Siber (Dittipidsiber) Bareskrim Polri dalam melakukan penegakan hukum terhadap kejahatan pencurian dan penyalahagunaan data pribadi.

HASIL DAN PEMBAHASAN

A. Pengaturan Hukum Terhadap Perlindungan Data Pribadi Menurut Peraturan Internasional Dan Nasional Dalam Mencegah Terjadinya Pencurian Dan Penyalahgunaan Data Pribadi

Sebagai sebuah hak yang melekat pada diri pribadi, perdebatan mengenai pentingnya perlindungan terhadap hak atas privasi seseorang mula - mula mengemuka di dalam putusan - putusan pengadilan di Inggris dan kemudian di Amerika Serikat. Hingga kemudian Samuel Warren dan Louis Brandeis menuliskan konsepsi hukum hak atas privasi dalam Harvard Law Review Vol. IV No. 5, 15 Desember 1890. Dalam tulisan tersebut Warren dan Brandeis secara sederhana mendefinisikan hak atas privasi sebagai 'hak untuk dibiarkan sendiri' (*the right to be let alone*). Definisi mereka didasarkan pada dua aras: (i) kehormatan pribadi; dan (ii) nilai - nilai seperti martabat individu, otonomi dan kemandirian pribadi.

Terdapat satu kasus atas perlindungan data pribadi yang menghebohkan publik dunia pada Maret 2018. Amerika Serikat mengalami pelanggaran terhadap data pribadi melalui Cambridge Analytica. Sistem yang dibangun oleh Cambridge Analytica sangat memungkinkan untuk menargetkan kelompok masyarakat yang belum menentukan pilihan pada pemilu dan memiliki tingkat probabilitas yang tinggi untuk memilih, atas dasar itu kampanye yang dilakukan oleh Donald Trump menjadi tepat sasaran. Kumpulan data pribadi tersebut diolah dan dijadikan iklan politik yang dipersonalisasi berdasarkan profil psikologis para pengguna.

Peraturan Internasional yang Mengatur Mengenai Data Pribadi

OECD *Guidelines Governing The Protection Of Privacy and Transborder Flows of Personal Data 1980* Merupakan instrumen internasional pertama yang mengatur tentang privasi atas data pribadi berupa suatu *Guidelines* yang merupakan rekomendasi bagi negara-negara dalam membuat pengaturan cara mengakses, mengelola dan menyebarkan data pribadi. *Guidelines* juga mengatur tentang Prinsip-Prinsip Dasar Penerapan secara Internasional tentang Arus keluar masuk data antar Negara. Untuk mendorong kepastian hukum. OECD mendorong negara-negara untuk mengatur mengenai sanksi yang harus diterapkan bagi pihak-pihak yang telah melanggar privasi khususnya atas data pribadi melalui *e-commerce* (enforcement and redress). *Guidelines* ini, diharapkan akan diadopsi oleh negara anggota ke dalam instrumen nasional masing-masing negara. Ruang lingkup *Guidelines* ini hanya diperuntukkan bagi organisasi Internasional milik pemerintah.

Alasan penggunaan OECD *Guidelines* sebagai pedoman yang disampaikan oleh delegasi Australia karena *Guidelines* tersebut dianggap sebagai salah satu contoh pengaturan privasi secara internasional yang dinilai cukup berhasil mengatur prinsip-prinsip perlindungan privasi yang dikenal secara internasional dan dirasakan masih cukup relevan hingga saat ini.

Peraturan Nasional yang Mengatur Mengenai Data Pribadi Undang-Undang Nomor 27 Tahun 2022 Tentang Perlindungan Data Pribadi

Undang-Undang tentang perlindungan data pribadi (selanjutnya disebut Undang-Undang PDP) ditandatangani oleh Presiden Joko Widodo pada 17 Oktober 2022. Undang-Undang tentang Perlindungan Data Pribadi 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". Undang-undang ini diharapkan menjadi payung hukum yang kuat bagi tata kelola dan perlindungan data personal warga negara dan para penyelenggara pemerintahan.Undang-Undang PDP meliputi 18 bab dan 76 pasal mengatur perihal transfer data pribadi, sanksi administratif, kelembagaan, kerjasama internasional, partisipasi masyarakat, penyelesaian sengketa dan hukum acara, larangan dalam penggunaan data pribadi, ketentuan pidana, hingga ketentuan peralihan dan penutup. Perlindungan diri pribadi ini tercantum dalam Pasal 28G UUD 1945. Perlindungan diri pribadi atau privasi ini bersifat universal, dalam arti diakui banyak negara.

Undang-Undang Nomor 10 Tahun 1998 Tentang Perbankan

Undang-Undang perbankan 1998 yang mengubah Undang-Undang Nomor 7 Tahun 1992, disahkan pada 23 September 1999, merupakan upaya pemerintah untuk memberikan kepastian hukum dalam kegiatan perbankan. Undang-Undang Perbankan 1998, dalam pengaturannya, meliputi masalah-masalah perbankan sebagai lembaga serta aspek kegiatannya: asas, fungsi, dan tujuan bank; rambu-rambu yang harus dipenuhi oleh bank; perilaku petugasnya; hak, kewajiban, tugas, dan tanggung jawab bank; para pelaku serta pihak yang terkait dalam bisnis perbankan; serta hal lain yang berkenaan dengan dunia perbankan tersebut.

Dalam Undang-Undang Perbankan 1998, hak privasi dari nasabah dilindungi dengan diaturnya perihal rahasia bank. Pasal 1 ayat (28) Undang-Undang Perbankan 1998 menyebutkan definisi dari rahasia bank sebagai segala sesuatu yang berhubungan dengan keterangan mengenai nasabah penyimpan dan simpanannya.

Untuk mendukung pengatuaran perlindungan dari data pribadi nasabah tersebut, pengaturan pidana dari pelanggaran rahasia bank juga diatur dalam Pasal 47 ayat (1) dan (2).

Undang-Undang Nomor 36 Tahun 1999 Tentang Telekomunikasi

Undang-Undang Nomor 36 Tagyb 1999 tentang Telekomunikasi (Undang-Undang Telekomunikasi 1999) kemudian disahkan untuk mengganti undang-undang telekomunikasi sebelumnya. Kerahasiaan dari data pribadi maupun informasi pribadi lain milik pengguna jasa telekomunikasi dilindungi dan wajib dijaga kerahasiaannya oleh penyelenggara telekomunikasi. Pasal 42 aya (1) Undang-Undang Telekomunikasi 1999 mewajibkan penyelenggara jasa telekomunikasi untuk merahasiakan informasi yang dikirim dan/atau diterima oleh pelanggan jasa telekomunikasi melalui jaringan da/atau jasa telekomunikasi yang diselenggarakannya. Pengaturan sanksi pidana dari pelanggaran pasal-pasal perlindungan privasi atas data pribadi pengguna jasa telekomunikasi di atas di antaranya terdapat dalam Pasal 56 dan Pasal 57 Undang-Undang Telekomunikasi 1999. Pelanggaran atas pasal-pasal tersebut diancam dengan sanksi pidana, baik berupa denda maupun pidana penjara.

Undang-Undang Republik Indonesia Nomor 8 Tahun 1999 Tentang Perlindungan Konsumen (Undang-Undang Perlindungan Konsumen).

Data informasi yang dijamin oleh Undang-Undang Perlindungan Konsumen adalah informasi mengenai barang dan jasa, bukan informasi mengenai data pribadi kosumen. Promosi sendiri diatur dalam Undang-Undang Perlindungan Konsumen. Pengertian mengenai promosi dijelaskan dalam ketentuan umum yang termuat dalam Pasal 1 ayat (6), Undang-Undang Perlindungan Konsumen tidak melarang promosi yang menggunakan data-data pribadi masyarakat yang didapatkan tanpa persetujuan masyarakat tersebut. Pasal 9 ayat (1) Undang-Undang Perlindungan Konsumen hanya melarang menawarkan, memproduksikan, mengiklankan suatu barang dan/atau jasa secara tidak benar.

Undang-Undang Nomor 39 Tahun 1999 Tentang Hak Asasi Manusia (Undang-Undang HAM 1999)

Dalam Pasal 29 ayat (1) Undang-Undang HAM 1999 diakui hak setiap orang berhak atas perlindungan diri pribadi, keluarga, kehormatan, martabat, dan hak miliknya. Undang-Undang Republik Indonesia Nomor 39 Tahun 1999 tentang Hak Asasi Manusia (Undang-Undang HAM 1999) merupakan landasan hukum yang mengatur tentang pengakuan, perlindungan, dan pemajuan hak asasi manusia di Indonesia.

Peraturang Bank Indonesia Nomor 7/6/PBI/2005 Tentang Transparansi Produk Bank dan Penggunaan Data Pribadi Nasabah (PBI No. 7/6/PBI/2005)

PBI No. 7/6/PBI/2005 merupakan bentuk nyata dari peraturan pelaksana yang dikeluarkan Bank Indonesia demi terlindunginya privasi dari nasabah bank atas data pribadinya. Penetapan PBI No. 7/6/PBI/2005 adalah berdasarkan pertimbangan bahwa transparansi terhadap penggunaan data pribadi yang disampaikan nasabah kepada bank diperlukan untuk meningkatkan perlindungan terhadap hak-hak pribadi nasabah dalam berhubungan dengan bank. Selain daripada penggunaan data pribadi nasabah bank, penggunaan data pribadi oleh bank yang sebelumnya diperoleh pihak lain untuk tujuan komersial juga diatur dalam Pasal 11 PBI No. 7/6/PBI/2005. Pelanggaran oleh bank atas transparansi penggunaan data pribadi oleh bank yang telah diatur dalam PBI No. 7/6/PBI/2005 diancam dengan sanksi administratif serta dijadikan bahan perhitungan dalam komponen penilaian tingkat kesehatan bank pada aspek manajemen bank.

Undang-Undang Nomor 23 Tahun 2006 Tentang Administrasi Kependudukan (Undang-Undang Administrasi Kependudukan 2006)

Hak akses atas data pribadi serta dokumen kependudukan diberikan oleh menteri sebagai penanggung jawab atas hak akses kepada petugas pada penyelenggara dan instansi pelaksana penyelenggaraan administrasi kependudukan sebagaimana disebutkan dalam Pasal 79 ayat (2). Ancaman pidana atas pelanggaran privasi serta penyalagunaan data pribadi dalam administrasi kependudukan selanjutnya diatur dalam Pasal 93, yang mengancam penjara serta denda bagi setiap Penduduk yang dengan sengaja memalsukan surat dan/atau dokumen kepada Instansi Pelaksana dalam melaporkan Peristiwa Kependudukan dan Peristiwa Penting. Undang-Undang Republik Indonesia Nomor 23 Tahun 2006 tentang Administrasi Kependudukan (Undang-Undang Administrasi Kependudukan 2006) merupakan peraturan hukum yang mengatur tentang pendataan dan pengelolaan informasi kependudukan di Indonesia. Tujuan dari Undang-Undang ini adalah untuk menciptakan sistem administrasi kependudukan yang terpadu, akurat, dan terpercaya guna mendukung perencanaan pembangunan dan pelayanan publik yang lebih baik.

Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik (Undang-Undang ITE 2008).

Undang-Undang Republik Indonesia Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (Undang-Undang ITE 2008) adalah peraturan hukum yang mengatur tentang penggunaan teknologi informasi, elektronik, dan transaksi elektronik di Indonesia. Tujuan dari Undang-Undang ini adalah untuk menciptakan lingkungan yang aman dan terpercaya dalam penggunaan teknologi informasi serta mendorong perkembangan transaksi elektronik yang sehat. Undang-Undang ITE 2008 juga mengatur dengan lebih lanjut bahwa mengakses sistem elektronik untuk memperoleh informasi atau dokumen elektronik, intersepsi atau melakukan penyadapan terhadap data atau informasi elektronik, dan memindahkan serta mentransfer informasi elektronik adalah perbuatan yang dilarang dan diancam dengan pidana.

Undang-Undang Nomor 14 Tahun 2008 Tentang Keterbukaan Informasi Publik (Undang-Undang Keterbukaan Informasi Publik)

Pasal 1 ayat (1) Undang-Undang Keterbukaan Informasi Publik mengatur bahwa informasi adalah keterangan, pernyataan, gagasan, dan tanda-tanda yang mengandung nilai, makna, dan pesan, baik data, fakta maupun penjelasannya yang dapat dilihat, didengar, dan dibaca yang disajikan dalam berbagai kemasan dan format

sesuai dengan perkembangan teknologi informasi dan komunikasi secara elektronik ataupun nonelektronik. Perlindungan akan data dan informasi publik yang dihimpun oleh badan publik diatur dalam Pasal 6 ayat (3) Undang-Undang Keterbukaan Informasi Publik. Berdasarkan aturan tersebut, terdapat informasi publik yang tidak dapat diberikan oleh badan publik.

Undang-Undang Nomor 36 Tahun 2009 Tentang Kesehatan (Undang-Undang Kesehatan 2009)

Perlindungan terhadap riwayat kesehatan pasien terdapat dalam Pasal 57 ayat (1) Undang-Undang Kesehatan 2009, yang mengakui hak setiap orang atas rahasia kondisi kesehatan pribadinya yang telah dikemukakan kepada penyelenggara pelayanan kesehatan. Di dalam Undang-Undang Kesehatan 2009, tidak terdapat pengaturan sanksi ataupun hukuman bagi pelanggaran privasi yang dilakukan atas riwayat kesehatan pasien.

Peraturan Presiden Republik Indonesia Nomor 67 Tahun 2011 Tentang Penerapan Kartu Tanda Penduduk Berbasis Nomor Induk Kependudukan Secara Nasional (Perpres KTP 2011)

Perpres KTP 2011 merupakan perubahan kedua dari Peraturan Presiden Nomor 26 Tahun 2009 tentang Penerapan Kartu Tanda Penduduk Berbasis Nomor Induk Kependudukan secara Nasional yang sebelumnya telah diubah dengan Peraturan Presiden Republik Indonesia Nomor 35 Tahun 2010 tentang Perubahan Atas Peraturan Presiden Nomor 26 Tahun 2009 tentang Penerapan Kartu Tanda Penduduk Berbasis Nomor Induk Kependudukan secara Nasional. Di dalam Perpres KTP 2011, tidak terdapat pengaturan yang menyebutkan kewajiban perlindungan terhadap data pribadi milik penduduk yang terdapat dalam KTP dan *database* kependudukan.

Peraturan Menteri Kominfo Nomor 20 Tahun 2016 Tentang Perlindungan Data Pribadi Dalam Sistem Elektronik.

Dalam Permenkominfo 20/2016, cakupan dari perlindungan data pribadi dalam sistem elektronik dilakukan pada proses perolehan dan pengumpulan, pengolahan dan penganalisisan, penyimpanan, penampilan, pengumuman, pengiriman, penyebarluasan, dan/atau pembukaan akses, serta pemusnahan. Ketentuan mengenai perolehan dan pengumpulan data pribadi diatur dalam Pasal 7 sampai Pasal 11 Permenkominfo 20/2016. Kemudian, pengolahan dan penganalisisan data pribadi diatur dalam Pasal 12 dan 13 Permenkominfo 20/2016. Dalam Permenkominfo 20/2016, sanki administratif diberikan oleh menteri atau pimpinan instansi pengawas dan pengatur sektor terkait sesuai dengan

ketentuan peraturan perundang-undangan yang dilakukan setelah berkoordinasi dengan menteri.

Peratutan Pemerintah Nomor 71 Tahun 2019 Tentang Penyelenggaraan Sistem dan Transaksi Elektronik

Adapun regulasi terkait data pribadi dan hak privasi seseorang pada konstitusi Indonesia dan diatur juga dalam Undang-Udnang Nomor 19 Tahun 2016 yang berisi Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik pada Pasal 26. Pasal 26 UU ITE ini mengatur bagaimana setiap informasi elektronik yang mengandung data pribadi itu hanya boleh digunakan atas seizin orang tersebut.

B. Upaya Yang Dilakukan Oleh Direktorat Tindak Pidana Siber (Dittipidsiber) Bareskrim Polri Dalam Melakukan Penegakan Hukum Melalui Penyelidikan Dan Penyidikan Terhadap Kejahatan Pencurian Dan Penyalahagunaan Data Pribadi

Dalam konsep KUHP tindak pidana diartikan sebagai perbuatan melakukan atau tidak melakukan sesuatu yang oleh peraturan perundang-undangan dinyatakan sebagai perbuatan yang dilarang dan diancam dengan pidana. Direktorat Tindak Pidana Siber (Dittipidsiber) Bareskrim Polri mencatat, laporan mengenai pencurian dan penyalahgunaan data pribadi cukup meningkat selama empat tahun terakhir.

Pada tahun 2017 terdapat 47 kasus; kemudian tahun 2018 meningkat menjadi 88 kasus; dan lonjakan kasus terjadi pada tahun 2019 sampai tahun 2020 yakni mencapai 182 kasus. Selain itu, pada 21 Mei 2020, data 2,3 juta warga dan pemilih Indonesia diduga bocor di forum "*Rapid Forums*". Dalam perspektif hukum pidana, terminologi "penegakan hukum" dimaknai sebagai tindakan negara untuk mendeteksi pelanggaran, menghentikannya dan untuk mencegah terjadinya pelanggaran berikutnya dikemudian hari. Tugas dan fungsi Polri dalam mewujudkan penegakan hukum guna terpeliharanya keamanan dan ketertiban pada hakikatnya dapat dilihat sebagai hukum yang hidup (*living law*), karena ditangan Polri itulah hukum menjadi konkret atau mengalami perwujudannya di dalam masyarakat. Direktorat Tindak Pidana Siber (Dittipidsiber) Bareskrim Polri sebagai penjaga pintu gerbang (*gatekeeper*) sistem peradilan pidana memiliki mengemban fungsi represif dalam melakukan penegakan hukum melalui proses penyelidikan dan penyidikan terhadap kejahatan pencurian dan penyalahgunaan data pribadi. Direktorat Tindak Pidana Siber (Dittipidsiber) sendiri dipimpin oleh Brigadir Jenderal (Brigjen).

Berdasarkan Peraturan Kepala Kepolisian Negara Republik Indonesia Nomor 6 tahun 2017 tentang Susunan Organisasi dan Tata Kerja Satuan Organisasi pada Tingkat Markas Besar Kepolisian Negara Republik Indonesia, Direktorat Tindak Pidana Siber (Dittipidsiber) Bareskrim Polri memiliki tugas yakni melaksanakan penyelidikan dan penyidikan tindak pidana khusus yang berkaitan dengan kejahatan siber, tindak pidana informasi dan transaksi elektronik, tindak pidana telekomunikasi yang termasuk di dalamnya kejahatan transnasional terkait dengan kejahatan siber. Sedangkan dalam melaksanakan tugas, Direktorat Tindak Pidana Siber (Dittipidsiber) Bareskrim Polri mempunyai fungsi, antara lain penyelidikan dan penyidikan tindak pidana khusus yang terkait dengan kejahatan siber, termasuk kejahatan transnasional terkait dengan kejahatan siber; dan perumusan kebijakan dalam rangka penyelidikan dan penyidikan tindak pidana siber.

Menurut Undang-Undang No. 2 Tahun 2002 tentang Kepolisian Pasal 1 angka 13 penyidikan adalah serangkaian tindakan penyidik dalam hal dan menurut cara yang diatur dalam undang-undang untuk mencari serta mengumpulkan bukti yang dengan bukti itu membuat terang tentang tindak pidana yang terjadi dan guna menemukan tersangkanya. Dalam memulai penyidikan tindak pidana Polri menggunakan parameter alat bukti yang sah sesuai dengan Pasal 184 KUHAP yang dikaitkan dengan segitia pembuktian / *evidence triangle* untuk memenuhi aspek legalitas dan aspek legitimasi untuk membuktikan tindak pidana yang terjadi.

SIMPULAN

Pengaturan hukum terhadap perlindungan data pribadi diatur baik dalam peraturan internasional dan maupun peraturan nasional. Aturan-aturan ini dibuat untuk mencegah terjadinya pencurian dan penyalahgunaan data pribadi. Khusus untuk peraturan nasional terkait perlindungan data pribadi memberikan suatu landasan hukum bagi Indonesia untuk menjaga kedaulatan negara, keamanan negara, dan perlindungan terhadap data pribadi milik warga negara Indonesia dimanapun data pribadi tersebut berada.

Penegakan hukum terhadap kejahatan pencurian dan penyalahagunaan data pribadi yang dilakukan oleh direktorat tindak pidana siber (dittipidsiber) bareskrim polri dilakukan melalui upaya penyelidikan dan penyidikan, dimana ada tahapan-tahapan dalam proses penyelesaian perkara pencurian dan penyalahgunaan data pribadi , yaitu : tahap pertama : proses penyelesaian perkara pidana dimulai dengan suatu penyidikan oleh penyidik, tahap kedua : proses penyelesaian perkara pidana melalui tahap penangkapan, tahap ketiga : proses penyelesaian perkara pidana melalui tahap penahanan, tahap keempat : proses

pemeriksaan perkara pidana berdasarkan Undang-Undang Nomor 8 Tahun 1981 adalah pemeriksaan di sidang pengadilan.

DAFTAR PUSTAKA

Amrani, Hanafi. 2015. Hukum Pidana Pencucian Uang : Perkembangan Rezim Anti Pencucian Uang dan Implikasinya terhadap Prinsip Dasar Kedaulatan Negaram Yurisdiksi Negara dan Penegakan Hukum. Cetakan Pertama. Yogyakarta : UII Press Yogyakarta.

Bunga, Dewi. Politik Hukum Pidana Terhadap Penanggulangan Cybercrime. Jurnal Legislasi Indonesia Vol 16 No.1 - Maret 2019.

D, Halder & Jaishankar, K. 2011. Cyber crime and the Victimization of Women: Laws, Rights, and Regulations. Hershey, PA, USA: IGI Global.

Djafar, Wahyudi. 2019. Hukum Perlindungan Data Pribadi di Indonesia: Lanskap, Urgensi, dan Kebutuhan Pembaharuan.

Guntara, Bima, Legitimasi Penyebaran Informasi Yang Memiliki Muatan Penghinaan Dan/Atau Pencemaran Nama Baik Dalam Pasal 310 Kuhp Dan Undang-Undang Nomor 19 Tahun 2016 Tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik, Jurnal Surya Kencana Dua: Dinamika Masalah Hukum dan Keadilan, Volume 4 Nomor 2 Desember 2017.

Kobrata D, "RUU Perlindungan Data Pribadi: Sebuah Penantian", Januari 2021, RUU Perlindungan Data Pribadi: Sebuah Penantian (hukumonline.com)

Peraturan Pemerintah No. 82 Tahun 2012 tentang Penyelenggaraan Sistem dan Transaksi Elektronik.

Permen Kominfo Nomor 20 Tahun 2016 tentang Perlindungan Data Pribadi Dalam Sistem Elektronik.

Undang-Undang Nomor 24 Tahun 2013 tentang Perubahan Atas Undang-Undang Nomor 23 Tahun 2006 tentang Administrasi Kependudukan.