PATTIMURA Law Study Review

Volume 4 Nomor 2 Agustus, 2026: h. 166 - 179
E-ISSN: 3025-2245
: 10.47268/palasrev.v4i2.21937

Penegakan Hukum Terhadap Kejahatan Pencurian Data Pribadi di Media Sosial *Facebook*

Muhammad Syaf Nurdin Arey*, Deassy Jacomina Anthoneta Hehanusa[2], Harly Cilford Jonas Salmon

Fakultas Hukum Universitas Pattimura, Ambon, Indonesia.

: syafnurdinarey@gmail.com

ABSTRACT: *The rapid development of information technology has triggered an increase in digital activities, including the collection and storage of personal data. On the other hand, the phenomenon of theft of personal data and personal identity has become rampant and has caused increasingly significant losses, both materially and immaterially. This study aims to examine legal protection against theft of personal data and personal identity in Indonesia and to examine the law enforcement mechanisms and obstacles faced in the process. The research method used is normative juridical, with a regulatory, conceptual, and comparative approach. Data sources come from literature studies of regulations, legal literature, and relevant court decisions. The results of the study show that personal data protection in Indonesia is still in the developing stage, marked by the enactment of Law Number 27 of 2022 concerning Personal Data Protection (PDP). However, there are still limitations to norms in terms of implementation, criminal sanctions, and strong supervisory institutions. In addition, law enforcement against theft of personal data faces various obstacles, including limited authority of law enforcement officers, low public awareness of the importance of protecting personal data, and the complexity of evidence in cases of cross-border cybercrime. International efforts, such as cross-secret cooperation and extradition of perpetrators, are also still not optimal due to differences in legal systems between countries. This study recommends strengthening technical regulations for implementing the PDP Law, increasing the capacity of independent supervisory institutions, educating the public about data security, and increasing international cooperation in combating cybercrime. Effective national legal protection of personal data is an important foundation in maintaining citizens' privacy rights and building trust in the digital ecosystem.*

Keywords: Law Enforcement; Personal Data Protection; Identity Theft.

ABSTRAK: Perkembangan teknologi informasi yang pesat memicu peningkatan aktivitas digital, termasuk pengumpulan dan pemrosesan data pribadi. Di sisi lain, fenomena pencurian data pribadi dan identitas pribadi menjadi semakin marak dan menimbulkan kerugian yang signifikan, baik secara materiil maupun immateriil. Penelitian ini bertujuan untuk mengkaji perlindungan hukum terhadap pencurian data pribadi dan identitas pribadi di Indonesia serta menelaah mekanisme penegakan hukum dan hambatan yang dihadapi dalam prosesnya. Metode penelitian yang digunakan adalah yuridis normatif, dengan pendekatan perundang-undangan, konseptual, dan komparatif. Sumber data berasal dari studi pustaka terhadap peraturan perundang-undangan, literatur hukum, serta putusan pengadilan yang relevan. Hasil penelitian menunjukkan bahwa perlindungan data pribadi di Indonesia masih dalam tahap berkembang, ditandai dengan disahkannya Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi. Namun, masih terdapat kekosongan norma dalam hal implementasi, sanksi pidana, dan kelembagaan pengawasan yang kuat. Selain itu, penegakan hukum terhadap pencurian data pribadi menghadapi berbagai hambatan, antara lain keterbatasan kewenangan aparat penegak hukum, rendahnya kesadaran masyarakat akan pentingnya pelindungan data pribadi, serta kompleksitas pembuktian dalam kasus kejahatan siber lintas negara. Upaya internasional, seperti kerja sama lintas yurisdiksi dan ekstradisi pelaku, juga masih belum optimal akibat perbedaan sistem hukum antarnegara.Penelitian ini merekomendasikan penguatan regulasi teknis pelaksanaan UU PDP, peningkatan kapasitas lembaga pengawas independen, edukasi publik mengenai keamanan data, serta peningkatan kerja sama internasional dalam penanggulangan kejahatan siber. Perlindungan hukum yang efektif terhadap data pribadi merupakan fondasi penting dalam menjaga hak privasi warga negara dan membangun kepercayaan dalam ekosistem digital nasional.

Kata Kunci: Penegakan Hukum; Perlindungan Data Pribadi; Pencurian Identitas.

PENDAHULUAN

Sosial media adalah sebuah media untuk bersosialisasi satu sama lain melalui jaringan internet yang memungkinkan manusia untuk saling berinteraksi dengan mudah serta berpatisipasi, berkomunikasi, berbagi, dan menciptakan berbagai konten tanpa dibatasi ruang dan waktu. Umumnya media sosial dirancang untuk memudahkan seseorang dalam bersosialisasi dan berkomunikasi dengan orang lain. Pengaturan data pribadi dalam sistem perundang-undangan di Indonesia diatur dalam Undang-Undang Nomor 1 tahun 2024 tentang perubahan atas Undang-Undang 19 Tahun 2016 tentang Perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (Selanjutnya disebut UU ITE) dan Peraturan Menteri Komunikasi dan Informatika Nomor 20 tahun 2016 tentang Perlindungan Data Pribadi dalam Sistem Elektronik (Selamjutnya disebut PDPSE).[1]

Diperlukan identitas diri dalam membuat sebuah akun media sosial agar kita bisa dikenali. Hal tersebut juga mengacu kepada Peraturan Menteri komunikasi dan informasi Nomor 5 Tahun 2020 tentang Penyelenggara Sistem Elektronik Lingkup Privat yang mewajibkan seluruh Penyelenggara Sistem Eletronik (selanjutnya disingkat PSE) untuk mendaftarkan diri ke pemerintah.[2] Hadirnya peraturan ini untuk mencegah terjadinya pencurian identitas di media sosial. Indonesia termasuk negara dengan pengguna media sosial terbanyak di dunia, urutan ke-4 terbanyak di bawah China, India, dan Amerika Serikat.

Di Indonesia kurang lebih ada 150 juta pengguna aktif media sosial. Dengan jumlah yang sangat besar itu, memahami kebijakan privasi suatu *platform* media sosial sangat penting agar data pribadi aman. Salah satu syarat menggunakan media sosial dibutuhkan data pribadi yang *valid*.[3] Seiring dengan perkembangan yang sangat pesat itu, banyak situs dan aplikasi pertemanan dan salah satunya adalah *facebook*. Sejak tahun 2007, *facebook* mengalami peningkatan penggunaannya di Indonesia, hingga sekarang. Indonesia menjadi salah satu negara dengan masyarakat pengguna facebook yang terbesar. *Facebook* telah menduduki peringkat pertama jejaring sosial di Indonesia. Tersedianya fasilitas pencarian teman, *chat*, *notes*, dan beragam aplikasi membuat situs pertemanan ini cepat mendapatkan kemudahan dikalangan pengguna internet.

Seiring dengan perkembangan teknologi internet yang makin maju, hal ini searah dengan maraknya model-model kejahatan yang melibatkan teknologi terutama yang berhubungan dengan internet[4]. *Facebook* memiliki peluang lebar untuk disalahgunakan untuk hal-hal negatif, terutama jika digunakan terlalu berlebihan. Pengaruh dari *facebook* dapat kita rasakan sekarang ini terutama bagi orang-orang yang mempunyai intens cukup tinggi dalam menggunakan media internet tidak bisa dipungkiri lagi hampir semua orang mempunyai *account facebook* baik dari kalangan mahasiswa, pelajar, pekerja kantoran, institusi, perusahaan, politisi, hingga masyarakat biasa. Hal ini tidak saja berdampak positif, melainkan dampak negatif. Dampak negatif dari media sosial ini ialah pada data pribadi seseorang, dimana banyak akun yang mengatasnamakan orang lain walaupun bukan dia pemilik akunnya. Hal ini dikategorikan sebagai pencurian data pribadi (*Identity theft).*

---

[1] Muhammad Triadi, "Perlindungan Terhadap Korban Pencurian Data Pribadi Melalui Media Digital", *REUSAM: Jurnal Ilmu Hukum* 11, no. 1 (2023): 45-64.

[2] Andrian pratama taher, https://tirto.id/pekan-depan-platform-medsos-wajib-setor-data-pribadi-ke-pemerintah-ggb2

[3] Endah Pertiwi Dkk, "Analisis Yuridis Terhadap Penyalahgunaan Data Pribadi Pengguna Media Sosial", *Jurnal Rechten: Riset Hukum Dan Hak Asasi Manusia* 2, no. 1 (2020), h. 3

[4] Harly Clifford Jonas Salmon. "Penegakan Hukum Terhadap Kejahatan Penyebaran Konten Porno Balas Dendam (Revenge Porn)", *BACARITA Law Journal* 4, no. 1 (2023): 42-48

Pencurian data pribadi adalah salah satu sisi gelap dari kemajuan teknologi yang mempunyai dampak negatif sangat luas bagi seluruh bidang kehidupan modern saat ini[5] . Pencurian data pribadi sebagai tindak kejahatan murni, dimana orang yang melakukan kejahatan dilakukan dengan sengaja dan terencana untuk melakukan pengerusakkan, pencurian, tindakan anarkis terhadap suatu sistem informasi ataupun sistem informasi atau sistem komputer. Pencurian data pribadi atau pencurian identitas dikenal dengan istilah *Identity theft,* Salah satu ancaman dari *Identity theft* sendiri yaitu serangan *malware, hacking*, dan pencurian identitas. Pencurian data pribadi bisa terjadi tanpa sepengetahuan masyarakat sendiri dan tidak memahami cara melindungi diri sendiri dari kejahatan Pencurian data pribadi dikarekan regulasi dan aturan mengenai Pencurian data pribadi selalu berubah-ubah. Sementara itu pelaku Pencurian data pribadi terus berkembang dan berkeliaran dengan cara terus mengembangkan teknik dan strategi baru.

Berdasarkan hal tersebut, beberapa pengaturan terkait pencurian data pribadi ialah:

1) Pasal 378 Kitab Undang-undang Hukum pidana: (KUHP)

Barang siapa dengan maksud untuk menguntungkan diri sendiri atau orang lain secara melawan hukum, dengan memakai nama palsu atau martabat palsu, dengan tipu muslihat, ataupun rangkaian kebohongan, menggerakkan orang lain untuk menyerahkan barang sesuatu kepadanya, atau supaya memberi hutang maupun menghapuskan piutang diancam karena penipuan dengan pidana penjara paling lama empat tahun.

2) Pasal 67 ayat (1) Undang-undang No. 27 tahun 2022 tentang Perlindungan Data Pribadi:

Setiap Orang yang dengan sengaja dan melawan hukum memperoleh atau mengumpulkan Data Pribadi yang bukan miliknya dengan maksud untuk menguntungkan diri sendiri atau orang lain yang dapat mengakibatkan kerugian Subjek Data Pribadi sebagaimana dimaksud dalam Pasal 65 ayat (1) dipidana dengan pidana penjara paling lama 5 (lima) tahun dan/atau pidana denda paling banyak Rp5.000.000.000,00 (lima miliar rupiah).

Sejalan dengan pengaturan di atas, masih saja terdapat kasus-kasus tentang pencurian data pribadi yang sampai sekarang masih saja belum di atasi. Baru-baru ini, kasus yang sempat viral di media sosial (*facebook*) ialah kasus penipuan berkedok *giveaway* mengatasnamakan Baim Wong yang merupakan manifestasi dari kompleksitas tantangan keamanan digital kontemporer. Fenomena ini mencerminkan bagaimana pelaku kejahatan siber memanfaatkan popularitas seorang publik figur untuk melancarkan aksi penipuan yang terorganisir dan sistematis. Modus operandi yang diimplementasikan oleh pelaku dimulai dengan pembuatan akun media sosial (*facebook*) palsu yang menggunakan identitas digital Baim Wong. Pelaku memanfaatkan momentum popularitas program *giveaway* yang sering dilakukan oleh Baim Wong melalui *channel YouTube* dan media sosialnya.

Dalam praktiknya, pelaku membuat pengumuman palsu tentang program pemberian hadiah atau bantuan sosial yang mengatasnamakan Baim Wong dan tim Baim Paula di media sosial (*facebook*). Teknik manipulasi yang digunakan pelaku melibatkan serangkaian komunikasi yang terstruktur, dimana calon korban diarahkan untuk mengikuti prosedur tertentu untuk dapat mengakses hadiah yang dijanjikan. Pelaku mengeksploitasi antusiasme masyarakat terhadap program *giveaway* dengan mewajibkan korban melakukan

[5] Barda Nawawi Arief, *Tindak Pidana Mayantara: Perkembangan Kajian Cyber crime Di Indonesia*, (Jakarta: RajaGrafindo Persada, 2006), h. 1-2.

transfer sejumlah uang sebagai syarat untuk menerima hadiah yang nilainya jauh lebih besar. Hal ini menandakan bahwa masih lemah pengaturan pidana terkait permasalahan pencurian identitas di media sosial terutama di *facebook*.

METODE PENELITIAN

Metode yang digunakan dalam penelitian ini adalah penelitian hukum normatif dengan pendekatan perundang-undangan, pendekatan kasus, dan pendekatan konseptual. Sumber bahan hukum terdiri dari bahan hukum primer, dan sekunder, dengan Teknik pengumpulan melalui studi pustaka.[6]

HASIL PENELITIAN DAN PEMBAHASAN

A. Mekanisme Penegakan Hukum Kasus Pencurian Data Pribadi

Semakin meningkatnya jumlah pengguna internet, maka semakin bertambah pula kejahatan digital sering terjadi, perkembangan teknologi dan informasi ini tidak saja memberikan manfaat melainkan juga mengakibatkan masalah yang dapat merugikan masyarakat, seperti halnya penyalahgunaan data, pencurian data pribadi, penjualan data pribadi, penipuan dan lain-lain.[7] Maka dari itu payung hukum yang kuat sangat diperlukan, demi terciptanya sebuah keamanan. Dalam hukum internasional sendiri, hak atas privasi data pribadi di atur dalam *Universal Declaration of Human Rights* (selanjutnya disingkat UDCHR) pada pasal 12, yang menyatakan bahwa, setiap orang memiliki hak atas perlindungan hukum terhadap data pribadinya. Indonesia sudah meratifikasi UDCHR, dan dengan hal ini berarti pemerintah harus komitmen dalam menegakkan hukum mengenai hak privasi tersebut. Hukum yang sudah ada diharapkan mampu membawa kebermanfaatan, kepastian hukum, perlindungan, dan juga keadilan bagi seluruh masyaraktnya.[8]

Saat ini pengaturan terhadap perlindungan data pribadi telah diatur dalam peraturan perundang-undangan, yaitu:

1) Peraturan perundang-undang Nomor 27 tahun 2022 Tentang Perlindungan Data Pribadi

Pada 17 Oktober 2022, peraturan ini telah disahkan, mengingat sangat penting bagi pemerintah untuk melakukan upaya pemberian kepastian hukum kepada masyarakat atas data pribadi miliknya. Undang-undang ini juga dijadikan sebagai acuan utama, jika terjadi tindak pelanggaran terhadap data pribadi. Dibuat agar tidak terjadi tumpang tindih peraturan dan menjamin perlindungan bagi masyarakat. Dalam pasal 1 dijelaskan mengenai ketentuan umum, tentang perlindungan data pribadi, Pada bagian pasal 57 menjelaskan sanksi admnisttratif yang akan didapatkan jika pelanggaran jenis ini tetap dilakukan. pada pasal 67 juga membahas mengenai ketentuan pidana dari Tindakan tersebut.

2) Undang-undang Nomor 1 tahun 2024 tentang Perubahan atas Undang- undang Nomor 19 tahun 2016 tentang Informasi dan Transaksi Elektronik

Pengaturan tentang perlindungan data pribadi juga ada didalam UU ITE. Peraturan ini diharapkan dapat menjadi piranti hukum, yang dapat mengkoordinir segala macam bentuk

[6] Deassy J.A. Hehanussa dkk, *Metode Penelitian Hukum*, (Bandung: Widina Bhakti Persada, 2023), h. 40.
[7] Thomas Suyatno dkk, *DasarDasar Perkreditan*, (Jakarta: Gramedia Pustaka Utama, 2017), h. 12
[8] Hanifan Niffari, "Perlindungan Data Pribadi Sebagai Bagian Dari Hak Asasi Manusia Atas Perlindungan Diri Pribadi Suatu Tinjauan Komparatif Dengan Peraturan Perundang-Undangan Di Negara Lain", *Jurnal Hukum Dan Bisnis* (*Selisik*) 6. no. 1 (2020): 1–14

pelanggaran dalam bidang informasi dan teknologi. Dalam peraturan ini juga terdapat ketentuan-ketentuan umum mengenai upaya perlindungan hak privasi seseorang dan apa sanksi yang akan didapatkan, jika tindak pidana tersebut tetap terjadi.[9] Dalam pasal 26 ayat (2) dijelaskan bahwa: "Setiap orang yang dilanggar haknya sebagaimana dimaksud dalam ayat (1) dapat mengajukan gugatan atas kerugian yang di timbulkan berdasarkan undang-undang ini."

Ketentuan dalam pasal di atas merupakan salah satu upaya perlindungan atas data pribadi dalam setiap kegiatan bertransaksi elektronik. Meskipun sudah ada payung hukum yang menaungi, kita sebagai pemilik data haruslah bertangung jawab dan senantiasa waspada atas data pribadi milik kita sendiri.

3) Peraturan Pemerintah Nomor 71 tahun 2019 Tentang Penyelenggaraan Sistem dan Transaksi Elektronik

Dalam PP PTSE ini juga berbicara banyak mengenai perlindungan atas data pribadi milik seseorang, Pada pasal 8 di jelaskan bahwa PSE harus menjamin keamanan, keandalan transakisi elektronik sebagai mana mestinya. Pada pasal 14 juga dijelaskan banyak mengenai prinsip dan kewajiban untuk melindungi data pribadi. Dalam pasal 100 ayat (2) dijelaskan pula sanksi administratif yang akan didapat jika hal tersebut tetap dilanggar, sanksi yang akan didapat antara lain: teguran tertulis, denda, penghentian sementara, pemutusan akses, serta dikeluarkan dari daftar.

4) Pihak yang Berperan dalam Menegakkan Hukum Perlindungan Data Pribadi

Kemajuan teknologi dan informasi saat ini menuntut kita untuk selalu waspada akan kejahatan digital yang selalu menjadi bayang-bayang. Kejahatan peretasan (*cyber crime*) adalah salah satu kejahatan yang tidak pandang bulu. Bahkan orang yang tidak bersalahpun dapat menjadi target dari tindak pidana ini. Maka dari itu perlu adanya peran nyata dari berbagai pihak agar penegakkan pilar hukum dapat ditegakkan sebagaimana mestinya.[10]

a) Pemerintah

Pemerintah sebagai regulator memiliki dua tangung jawab utama dalam hal melindungi informasi dan data pribadi milik warga negaranya. Tugas yang pertama yaitu membuat kerangka hukum yang mengatur perlindungan data pribadi sebagai hak privasi. Tangung jawab yang kedua, yaitu melakukan pengawasan dan penegakkan terhadap regulasi tersebut. Ketika tugas dan perannya berjalan dengan optimal.

b) Pihak Pengontrol atau pemproses data

Dalam melindungi data setiap orang, salah satu pihak yang harus berperan aktif yaitu pengotrol dan pemproses data. Segala kendala apapun yang terjadi, tentunya mereka harus bisa mengatasi dan harus bisa pula memilih langkah-langkah mitigasi resiko yang menjadi bentengan jika terjadi kebocoran data pada sistem yang ada, karena hal demikian adalah tugas dan tangung jawab mereka sebagai pemegang kendali. Merujuk Pengaturan Badan Siber dan Sandi Negara (selanjutnya disebut BSSN) No.8 tahun 2020 Tentang Sistem Pengaman dan Penyelenggaraan Sistem Elektronik, mengharuskan untuk mensertifikasi berdasarkan resiko, baik itu level tertinggi ataupun terendah

[9] M R T R Herryani, "Perlindungan Hukum Terhadap Kebocoran Data Pribadi Konsumen Online Marketace", *Transparansi Hukum* 5, no. 1 (2022): 110–33

[10] Indriana Firdaus, "Upaya Perlindungan Hukum Hak Privasi Terhadap Data Pribadi dari Kejahatan Peretasan", *Jurnal Rechten: Riset Hukum Dan Hak Asasi Manusia* 4, no. 2 (2022), h. 27-30

c) Si pemilik data

Sosok yang berperan penting dalam menjaga privasi terhadap data pribadi yaitu si pemilik data. Ketika bermedia sosial, hendaknya paham betul kode etik dan tata cara dalam menggunakannya, kita juga harus tau tentang apa yang boleh dilakukan dan tidak boleh dilakukan agar hal-hal yang tidak diinginkan tidak terjadi kedepannya. Jangan sampai regulasi dan pihak lain sudah menjalankan perannya, namun si pemilik data malah tidak mematuhi peraturan atau malah menggumbar sendiri data pribadi yang menjadi privasinya.

d) Aparat penegak hukum

Jika kita berbicara mengenai penegakkan hukum, pasti selalu berkaitan erat dengan para aparat penegak hukum itu pula, baik itu polisi, hakim, jaksa, ataupun BSSN. Karena hal tersebut adalah ranah dan tangung jawab mereka. Korelasi antar pihak ini menjadi salah satu kunci untuk menegakkan hukum yang ada. Dari penjelasan di atas, dapat kita Tarik garis lurus bahwa jika segala pihak berperan secara baik dan peka terhadap apa yang menjadi tugas mereka tentulah pelanggaran seperti kejahatan peretasan ini tidak akan terjadi, Perlu adanya kontribusi dan korelasi nyata agar penegakkan hukum ini dapat dilakukan secara optimal dan juga maksimal.

Berdasarkan uraian tersebut di atas, maka penegakan hukum terhadap penyalahgunaan data pribadi selain bergantung kepada penegak hukum dalam melaksanakan penegakan hukumnya tetapi juga bergantung terhadap substansi hukum yang mengaturnya serta kesadaran hukum dalam mencegah dan menanggulangi penyalahgunaan data yang terjadi di masyarakat. Hal ini sebagaimana pendapat Lawrence M. Friedman, yang mengatakan bahwa suatu sistem hukum memiliki tiga bagian atau komponen, yaitu: (1) komponen struktural; (2) komponen substansi; (3) komponen budaya hukum.[11]

B. Pertangung Hambatan Dalam Penegakan Hukum Terhadap Kejahatan Pencurian Data Pribadi

Efektivitas berlakunya aspek pidana dalam Undang-undang Perlindungan Data Pribadi dan Undang-undang informasi dan teknologi elektronik dapat dilihat dari aspek substansi dan struktur hukumnya yang meliputi penegak hukum, sumber aparatur penegak hukum serta peran masyarakat dalam konteks penegakan hukum dan juga harus didukung sarana dan prasarana yang memadai agar penegak hukum dengan teknologi informasi pemerintah terwujud.

Dalam upaya penanggulangan *cyber crime* atau kejahatan di dunia maya oleh aparat penegak hukum terkadang masih mengalami hambatan seperti: 1) Dalam tahap penyidikan banyak kendala ataupun hambatan yang dialami oleh tim penyidik terutama dalam tahap penangkapan tersangka dimana hasil pelacakan paling jauh hanya dapat menentukan *IP Addres*s dari pelaku dan komputer yang digunakan tetapi belum menemukan tersangkanya belum lagi hal ini semakin sulit apabila menggunakan komputer di warnet dan tanpa ada yang mengetahuinya sehingga tidak ada saksi yang mengetahui secara langsung. Tidak hanya itu terkadang data yang disimpan secara digital tersebut tidak diubah oleh tersangka yang dimana akan susah untuk menentukan apakah data tersebut telah dicuri atau tidak; 2) Penyitaan Alat bukti dalam kasus *cyber crime* berbeda dengan alat bukti kejahatan lainnya dimana sasaran atau media *cyber crime* merupakan data-data atau sistem komputer/internet, sehingga apabila pelapor sangat lambat dalam melakukan pelaporan,

[11] Ravena, H. D., *Kebijakan Kriminal: (Criminal Policy)*. (Jakarta: Prenada Media, 2017), h. 176.

hal tersebut membuat jejak pelaku sulit ditemukan dikarenakan adanya program yang telah dibuat oleh tersangka yang digunakan untuk menghapus system yang digunakan tersangka setelah melakukan *hacking*;[12] 3) Faktor lainnya yaitu faktor teknologi juga menjadi hambatan dikarenakan kemajuan teknologi informasi dimana sarana dan prasana serta fasilitas peralatan canggih dan maju yang dibutuhkan ada saat ini khusunya mengenai data elektronik dari suatu pembuktian tindak pidana *cyber crime* dalam bentuk kejahatan terhadap data pribadi; 4) Sulit memperoleh saksi, dimana dalam kasus *cyber crime* berperan sangat penting dimana jarang sekali terdapat saksi dalam kasus *cyber crime* dikarenakan saksi korban yang tidak menyadari adanya kejahatan yang terjadi pada saat itu yang mengakibatkan penyidik sulit untuk melakukan pemeriksaan saksi dan pemberkasan hasil penyelidikan; 5) Kurangnya kemampuan penyidik khususnya pada aparat kepolisian dalam menguasai teknologi komputer

Seperti yang kita ketahui saat ini sangat banyak orang atau masyarakat yang sering mendaftar pada suatu aplikasi atau *website* yang bahkan tidak ketahui apakah aplikasi atau website tersebut aman dan juga banyaknya orang atau masyarakat yang tiba-tiba mendapatkan sebuah notifikasi bahwa mereka telah terdaftar pada suatu aplikasi atau *website* yang mereka sendiri tidak pernah daftar Karena ketidaktahuan masyarakat-lah yang mengakibatkan semakin tinggi kasus *cyber crime* terutama dalam bentuk kejahatan terhadap data pribadi. Sehingga diharapkan kepada pemerintah maupun non pemerintah, aparat penegak hukum dapat membantu masyarakat atau memberikan arahan kepada masyarakat apabila hal tersebut terjadi.

C. Proses Hukum Pidana Apabila Pelaku Pencurian Data Pribadi Berada di Luar Yurisdiksi Negara

1. Pengaturan Hukum Internasional Mengenai Yurisdiksi dalam Menangani Kejahatan Siber (*Cyber crime*)

Setiap negara mempunyai kedaulatan dan aturan hukum yang harus dihormati oleh negara lain atau dengan kata lain setiap negara mempunyai yurisdiksi. Berkaitan dengan arti dan makna kedaulatan, Jean Bodin menyatakan bahwa kedaulatan merupakan atribut dan ciri khusus dari suatu negara. Tanpa adanya kedaulatan, maka tidak akan ada yang dinamakan negara.[13]

Tindak pidana siber merupakan suatu kejahatan yang bersifat *borderless* atau tanpa batasan, artinya yurisdiksi menjadi suatu penghalang bagi penegakan terhadap pelaku tindak pidana siber/*cybercrime*. Skala dari potensi pelaku dari tindak pidana siber ini tidak dapat diklasifikasikan menjadi sebuah kelompok tertentu saja, dikarenakan skala dari kejahatan siber itu sendiri adalah global atau seluruh dunia, selama terjaring atau terkoneksi melalui jaringan internet. Maka dari itu, sebagaimana UU No. 27 Tahun 2022 Tentang Perlindungan Data Pribadi sebagai payung hukum dalam pelindungan data pribadi menyebutkan dalam Pasal 2 bahwa UU PDP tersebut berlaku baik didalam maupun diluar wilayah hukum Indonesia, selama menyangkut warga negara Indonesia.

Kejahatan pencurian data pribadi merupakan salah satu bentuk kejahatan siber yang dapat berkembang menjadi kejahatan transnasional, karena pelaku dapat beroperasi lintas negara dengan memanfaatkan jaringan internet untuk mengakses, menyebarluaskan, atau memperjualbelikan data pribadi tanpa batas yurisdiksi negara. Menurut *United Nations*

[12] Mulqadrin Adam dkk, "Upaya Kepolisian Dalam Penanggulangan Tindak Pidana Kejahatan Dunia Maya (Cyber Crime) Pada Kepolisian Daerah Sulawesi Selatan", *Jurnal of Lex Generalis (JLG)* 2, no. 3 (2021): 1101-1116.

[13] Isjwara Fred, *Pengantar Ilmu Politik*, (Bandung: Binacipta, 996), h. 89

Convention on Transnational Organized Crime tahun 2000, kejahatan dapat dikatakan bersifat transnasional jika terdiri dari:[14] 1) dilakukan di lebih dari satu negara; 2) persiapan, perencanaan, pengarahan dan pengawasan dilakukan di negara lain; 3) melibatkan *organized criminal group* dimana kejahatan dilakukan di lebih satu negara, dan 4) berdampak serius pada negara lain.

Begitu banyak pendapat-pendapat tentang yurisdiksi yang berkembang dan dilontarkan oleh berbagai ahli, namun sedikit sekali yang akhirnya diterima oleh hukum internasional sebagai prinsip. Prinsip-prinsip tersebut adalah:

a. *Subjective Territoriality* (territorialitas subjektif)

Subjective territoriality adalah prinsip yang terpenting di dalam hukum internasional.[15]Menurut prinsip ini, keberlakuan hukum ditentukan berdasarkan tempat perbuatan dilakukan dan penyelesaian tindak pidana dilakukan di negara lain. Mayoritas negara-negara di dunia, mengadopsi prinsip ini ke dalam perundang-undangan pidananya.[16]Namun demikian menurut J.G Starke, sebenarnya asas ini bukan merupakan asas umum hukum internasional, tetapi penggunaannya yang khusus sudah menjadi bagian hukum internasional, sebagai akibat dari dua konvensi yang penting yaitu *Geneva Convention for Supression of Counterfeiting Currency* (1929) dan *Geneva Convention of the Illicit Drug Traffic* (1930).[17]

b. *Objective Territoriality* (teritorialitas objektif)

Objective Territoriality digunakan pada saat suatu tindakan dilakukan oleh pelaku yang berada di luar wilayah suatu negara, akan tetapi justru akibat paling serius yang timbul karena peristiwa itu berada di dalam wilayah negara yang dimaksud.[18]Asas ini dirumuskan oleh Hyde, sebagaimana dikutip oleh J.G Starke[19], sebagai berikut: "*The setting motion outside of a state of a force which produces as a direct consequence an injurious effect therein justifies a territorial sovereign in prosecuting the actor when he enter its domain*." Sebagai contoh, misalnya orang yang sedang berada di perbatasan suatu negara kemudian menembak seseorang yang berada di wilayah negara lain.

c. *Nationality* (nasionalitas aktif)

Nationality adalah prinsip yang didasarkan kepada status kewarganegaraan seseorang. [20]Prinsip ini oleh Starke disebut juga prinsip nasionalitas aktif[21], yaitu negara tidak wajib menyerahkan warga negaranya yang melakukan pelanggaran di luar negeri. Artinya, negara dianggap lebih berwenang mengadili daripada negara lain tempat terjadinya kejahatan. Sebagai ilustrasi, apabila seorang Warga Negara Indonesia (selanjutnya disingkat WNI) berada di luar negeri, kemudian melakukan hubungan denga negara asing dan kemudian meggerakkan kekuatan asing agar melakukan peyerangan kepada Indonesia, maka berdasarkan Pasal 111 ayat (1) KUHP, orang tersebut dapat diadili atau dituntut di pengadilan Indonesia.

d. *Passive Nationality* (nasionalitas pasif)

---

[14] Muladi, *Demokratisasi, Hak Asasi Manusia, dan Reformasi Hukum di Indonesia*, 1st ed. (Jakarta: The Habibie Center, 2002), h. 32
[15] Derrel Menthe, *Jurisdiction in Cyberspace: A Theory of International Spaces*, 4 Mich Tech Review, 1998, h. 2
[16] *Ibid*
[17] J G Starke, *Introduction of International Law*, 9th ed, (London: Butterworths, 2000), h. 184.
[18] Darrel Menthe, *Op. Cit*, 2
[19] J G Starke, *Op. Cit*, h. 187
[20] Darrell Menthe, *Op. Cit*.
[21] J G Starke, *Introduction of International Law*, 9th ed, (London: Butterworths, 2000), h. 211.

Passive Nationality, yaitu asas yurisdiksi berdasarkan kewarganegaraan korban. Asas ini jarang digunakan karena antara lain hukum warga negara asing dianggap tidak memadai untuk melindungi warga negara asing.[22] Prinsip ini sedikit berbeda dengan prinsip nationality. Jika *prinsip nationality* melihat status kewarganegaraan pelaku kejahatan sebagai dasar kewenangan melakukan penuntutan, maka prinsip *Passive Nationality* melihat status kewarganegaraan korban.[23] Pembenaran terhadap prinsip ini adalah bahwa setiap negara berhak melindungi warganegaranya di luar negeri, dan apabila negara territorial tempat pelanggaran itu terjadi tidak menghukum orang yang menimbulkan kerugian itu, maka negara dari korban itu berweang menghukum pelanggar tersebut jika pelaku memasuki wilayahnya.[24]Keberatan terhadap prinsip ini adalah bahwa kepentingan umum negara tidak serta merta terganggu hanya karena salah seorang warganegaranya telah dirugikan.[25] Prinsip nasionalitas pasif ini antara lain termuat dalam undang-undang pidana Mexico, Brazil, Itali dan Indonesia. Sedangkan Inggris dan Amerika Serikat tidak mengadopsi prinsip ini ke dalam undang-undang pidananya.[26]

e. *Protective Principle* (prinsip perlindungan)

Secara etimologi, istilah "*precaution*" berasal dari Bahasa Latin "*prae*" yang berarti "sebelum", dan "*cautio*" yang berarti "*security*" atau "keamanan". Istilah "caution" dalam *Black's Law Dictionary* diartikan sebagai: (1) "*security given to ensure performance of some obligation*"; dan (2) "*the person who gives the security*" Secara umum, *precautionary principle* dapat diartikan sebagai suatu prinsip tindakan kehati-hatian yang dilakukan sebelum timbulnya dampak.[27] Hukum Internasional mengakui bahwa setiap negara berwenang menangai kejahatan yang berkaitan dengan keamanan dan integritas, serta kepentingan ekonomi yang cukup vital.[28]*Protective Principle* inilah yang digunakan sebagai dasar memanifestasikan kewenangan tersebut. Prinsip ini biasanya diterapkan guna melindungi kepentingan negara dari kejahatan yang dilakukan diluar wilayahnya, terutama apabila korban adalah negara atau pemerintah.[29]

Ada dua alasan yang mendasari prinsip ini, yaitu, pertama, akibat kejahatan sangat besar bagi negara yang dirugikan. Kedua, jika kewenangan tidak diterapkan oleh negara yang dirugikan, maka pelaku kejahatan bisa lolos karena di negara tempat perbuatan dilakukan, perbuatan yang dimaksud belum tentu merupakan tindak pidana serta ekstradisi juga ditolak karena alasan-alasan politis.[30] Kelemahan terbesar yang menimbulkan penolakan terhadap *protective principle* ini, yaitu negara (korban) itu sendiri yang menentukan perbuatan mana yang membahayakan keamanan, sehingga dapat menimbulkan kesewenang-wenangan

f. *Universality* (universalitas)

Asas ini seringkali juga disebut sebagai asas "*universal interest jurisdiction*".[31] Dahulu asas ini digunakan sebagai dasar kewenangan untuk menangkap dan menghukum para pelaku bajak laut dan kejahatan perang akan tetapi kemudian asas ini telah diperluas sehingga

[22] Widodo. *Hukum Pidana di Bidang Teknologi Informasi Cybercrime Law*. (Yogyakarta: Aswaja Pressindo, 2013), h. 40
[23] Darrel Menthe, *Op. Cit*, h. 2
[24] J G Starke, *Introduction to International Law*, 9th ed, (London: Butterworths, 2000), h. 211.
[25] *Ibid*
[26] *Ibid*
[27] Garner, Bryan A (Eds). *Black's Law Dictionary*, (Seventh Edition, St. Paul. Minn: West Group, 1999), h. 21
[28] J G Starke, *Introduction to International Law*, 9th ed, (London: Butterworths, 2000), h. 211.
[29] Darrel Menthe, *Op. Cit*, h. 11.
[30] J G Starke, *Op. Cit*, h. 212.
[31] Atmasasmita, Romli, *Pengantar Hukum Pidana Internasional,* (Bandung: Refika Aditama, 2003), h. 20

termasuk pula penyiksaan, genosida, dan pembajakan pesawat udara.[32] Asas *universal interest jurisdiction* ini selayaknya memperoleh perhatian khusus guna penanganan dan penegakkan hukum kasus-kasus *cybercrime*. Hal ini disebabkan karena asas ini memandang kewenangan untuk menangani kejahatan lebih kepada perlindungan terhadap kepentingan-kepentingan tertentu dari negara-negara yang ada di dunia, tanpa perlu mempersoalkan locus delicti dan kewarganegaraan pelaku.[33]

2. Kerjasama Internasional Dalam Mengatasi Konflik Yurisdiksi

Berbagai cara dilakukan oleh negara-negara untuk menyelesaikan permasalahan yurisdiksi, namun apabila pelaku *cybercrime* berada di luar wilayah negara yang terkena dampak paling besar, maka harus dipikirkan bagaimana cara membawa pelaku tersebut ke negara tersebut. Cara yang biasa ditempuh oleh Negara-negara adalah melalui jalur kerjasama internasional. Berikut adalah bentuk kerjasama internasional yang di tempuh negara-negara untuk membawa pelaku *cybercrime* agar dapat diadili di negaranya: [34]

a) Ekstradisi dan Deportasi

Ketika pembahasan mengenai penentuan yurisdiksi negara mana yang berwenang untuk melakukan pentuntutan terhadap pelaku kejahatan maka selanjutnya yang harus dilakukan bagaimana melakukan ekstradisi terhadap pelaku kejahatan tersebut. Indonesia sejak tahun 1979 telah memiliki Undang Undang No 1 tahun 1979 tentang ekstradisi dan telah menjalin hubungan diplomatik dan membuat perjanjian ekstradisi dengan banyak negara yang kemudian disahkan dalam bentuk Undang-Undang. Vattel memandang ekstradisi sebagai suatu kewajiban hukum murni yang dibebankan pada negara- negara oleh hukum internasional dalam hal kejahatan-kejahatan yang serius. Pandangan dari Vattel ini didukung oleh berbagai penulis seperti Heneccius, Rutherford, Schmelzing dan Kent.[35] Menurut J.G Starke bahwa ekstradisi ialah proses di mana berdasarkan perjanjian atau atas dasar resiprositas suatu negara menyerahkan kepada negara lain atas permintaannya seseorang yang dituduh atau dihukum karena melakukan tindak kejahatan yang dilakukan terhadap hukum negara yang mengajukan permintaan[36] . Syarat-syarat permintaan ektradisi tercantum dalam pasal 22 dan 23 Undang-undang Nomor 1 Tahun 1979 yaitu:

Pasal 22: (1) Permintaan ekstradisi hanya akan di pertimbangkan apabila memenuhi syarat-syarat seperti tersebut dalam ayat (2), ayat (3), dan ayat (4): 1) Bahwa telah ada perjanjian ekstradisi sebelumnya atau setidak tidaknya didasarkan hubungan baik dan negara RI menghendakinya (Pasal 2); 2) Yang dapat di ekstradisi adalah tersangka pelaku kejahatan atau tersangka pelaku perbantuan terhadap kejahatan yang di Indonesia maupun di negara peminta perbantuan tersebut dapat dipidana (Pasal 3); 3) Ekstradisi dapat dilakukan terhadap kejahatan yang tekah disebutkan dalam UU No 1 Tahun 1979 atau dalam perjanjian ekstradisi Indonesia dengan negara peminta atau terhadap kejahatan lain yang tidak diatur sebelumnya namun berdasarkan kebijaksanaan negara yang diminta dapat di lakukan ekstradisi (Pasal 4). (2) Surat permintaan ekstradisi harus diajukan secara tertulis melalui sluran diplomatik kepada Menteri Hukum dan HAM Republik Indonesia untuk diteruskan kepada Presiden. (3) Surat Permintaan ekstradisi bagi orang yang

[32] Menthe, Darrel. *Jurisdiction in Cyberspace: A Theory of International Spaces*. 4 Mich Tech Review, 1998 h. 12

[33] E.Y Kanter dan S.R Sianturi, *Asas-asas Hukum Pidana Di Indonesia Dan Penerapannya*, (Jakarta: Storia Grafika, 2002), h. 111

[34] Akbar Kurnia Putra, "Analisis Hukum Yurisdiksi Tindak Kejahatan Siber (Cybercrime) Berdasarkan Convention on Cybercrime", *Jurnal Ilmu Hukum* 7, no. 1 (2016), h. 40

[35] Roeslan Saleh, *Penerapan Lembaga Ekstradisi DalamHubungan Antar Negara*, (Jakarta: Renekacipta, 1992), h. 32.

[36] J G Starke, *Pengantar Hukum Internasional,* (Jakarta: Sinar Grafika, 1989), h. 469

dimintakan ekstrdisinya untuk menjalani pidana harus disertai: a) Lembaran asli atau salina otentik dari putusan pengadilan yang berupa pemidanaan yang sudah mempunyai kekuatan hukum tetap; 2) Keterangan yang diperlukan untuk menetapkan identitas dan kewarganegaraan orang yang dimintakan ekstradisinya; 3) Lembaran asli atau salinan otentik dari surat perintah penahanan yang dikeluarkan oleh pejabat yang berwenang dari negara tersebut. (4) Syarat permintaan ekstradisi bagi orang yang disangka melakukan kejahatan harus disertai: a) Lembaran asli atau salinan otentik dari surat perintah penahanan yang dikeluarkan oleh pejabat yang berwenang dari negara penerima; b) Uraian dari kejahatan yang dimintakan ekstradisi, dengan menyebutkan waktu dan tempat kejahatan dilakukan dengan di sertai bukti tertulis yang diperlukan; c) Teks ketentuan hukum dari negara peminta yang dilanggar atau hal demikian tidak mungkin, isi dari hukum yang diterapkan; d) Keterangan-keternangan saksi di bawah sumpah mengenai pengetahuannya tentang kejahatan yang dilakukan; e) Keterangan yang diperlukan untuk menentukan identitas dan kewarganegaraan orang yang dimintakan ekstradisinya; f) Permohonan penyitaan barang-barang bukti, bila ada dan diperlukan.

Pasal 23: Jika menurut pertimbangan Menteri Kehakiman Republik Indonesia surat yang diserahkan itu tidak memenuhi syarata dalam pasal 22 atau syarat lain yang dutetapkan dalam perjanjian, maka kepada pejabata negara peminta diberikan kesempatan unrtuk melengkapi surat-surat tersebut, dalam jangka waktu yang dipandang cukup oleh Menteri Kehakiman Republik Indonesia.

Apabila Menteri Hukum dan Hak Asasi Manusia (selanjutnya disebut Menteri Hukum Dan HAM) memandang bahwa surat yang dikrimkan tersebut kurang memenuhi syarat Pasal 22 dan 23 maka pejabat yang berwenang dari negara peminta diberikan waktu untuk melengkapinya dan setelah Menteri Hukum dan HAM Republik Indonesia memandang bahwa persyaratannya telah lengkap maka surat permintaan ekstradisi dan kelengkapannya di serahkan ke Kepala Kepolisian Republik Indonesia dan Jaksa Agung Republik Indonesia untuk dilakukan pemeriksaan.

b) Bantuan Timbal Balik (*Mutual Legal Assistance*)

Bantuan Hukum Timbal Balik atau Biasa juga juga dikenal dengan Bantuan Timbal Balik dalam Masalah Pidana (selanjutnya dapat juga disebut Mutual Legal Assistance atau MLA) merupakan satu bentuk kerjasama memerangi kejahatan yang dikenal dari mekanisme hukum yang timbul dalam pergaulan masyaratak internasional. Perserikatan Bangsa-Bangsa (selanjutnya disebutt PBB) melalui lembaganya yaitu *United Nation Office on Drugs and Crime* (selanjutnya disebut UNDOC) memberikan pengertian bahwa MLA adalah prosedur kerjasama internasional dimana Negara-negara mengajukan dan menerima bantuan dalam mengumpulkan alat bukti alat bukti yang akan digunakan dalam penyeldikan dan penuntutan kasus-kasus kejahatan dalam melacak, membekukan dan menyita hasil kejahatan yang diperoleh.[37] Selain memberikan definisi PBB bahkan telah meyusun suatu model perjanjian di bidang Bantuan Timbal Balik dalam Masalah Pidana ini yang dikenal dengan *United Nations Model Treaty* (selanjutnya disebut *UN Model Treaty*). Dalam model tersebut disampaikan pembatasan bahwa bantuan timbal balik bukan berarti bantuan untuk mengadili dan juga bukan bantuan hukum. *UN Model Treaty* menggunakan istilah "*Mutual Assistance*" bukan "*Mutual Legal Assistance*".

[37] Peter Langseth, *United Nations Handbook on Practical Anti Corruption Measures for Prosecutors dan Investigators*, (Vienna; UNDOC, 2004), h. 120.

Atas perbedaan istilah ini, dijelaskan dalam *UN Model Treaty* bahwa kedua istilah tersebut sering digunakan bergantian meskipun dalam sistem hukum tertentu kedua istilah itu bisa berbeda arti. *UN Model Treaty* sendiri menggunakan istilah "*Mutual Assistance*" dalam mamual tersebut, akan tetapi setiap Negara dapat menggunakan istilah manapun yang sesuai dengan sistem hukum mereka. Prinsip-prinsip utama dalam *Mutual Legal Assistance* tercantum dalam UNDOC, *Revised Manuals on the Model Treaty on Extradition and the Model Traety on Mutual Legal Assistance in Criminal Matters* sebagai berikut:

(1). Prinsip Kerjasama

Prinsip kerjasama internasional dalam kasus kasus khusus merujuk pada kerjasama hukum atau peradilan. Prinsip kerjasama biasanya diatur dalam perjanjian atau instrumen legal antara beberapa Negara atau pengaturan khusus dua Negara. Kerjasama yang diatur berbeda-beda, kadang hanya mengatur hal-hal umum, namun tidak menutup kemungkinan mengatur halhal khusus.

(2). Prinsip timbal-balik (resiprositas) atas dasar hubungan baik

Pada umumnya bantuan timbal balik didasarkan pada hukum acara pidana, perjanjian yang dibuat antar Negara, konvensi seta kebiasaan internasional. Namun hal ini tidak selalu dituangkan dalam perjanjian formal, hubungan baik sering dijadikan dasar untuk memberikan bantuan timbal balik walaupun antar kedua Negara belum memiliko perjanjian timbal-balik formal. Menurut Siswanto Sunarso, *Mutual Legal Assistance*, yakni suatu perjanjian yang bertumpu pada permintaan bantuan yang berkaitan dengan penyelidikan, penyidikan, penuntutan, pemeriksaan di depan sidang pengadilan, dan lain-lain, dari Negara Diminta dengan Negara Peminta.[38] Sedangkan menurut Undang-Undang Nomor 1 Tahun 2006 Tentang Bantuan Timbal dalam Masalah Pidana,yang dimaksud Bantuan Timbal Balik Dalam Masalah Pidana adalah: permintaan bantuan kepada negara asing berkenaan dengan penyidikan, penuntutan dan pemeriksaan di sidang pengadilan. Peraturan MLA ini dibuat dengan tujuan untuk memberikan dasar hukum bagi Pemerintah RI dalam meminta dan/atau memberikan bantuan timbal balik dalam masalah pidana dengan Negara asing.

Berdasarkan definisi yang diberikan Undang-Undang tersebut maka dapat diperoleh unsur dari Bantuan Timbal Balik dalam Masalah Pidana yaitu: 1) Bantuan yang diterima maupun yang diajukan adalah bantuan yang terkait kepada hal-hal yang terkait perbuatan kejahatan dalam lingkup hukum pidana; 2) Bantuan terkait kepada prosedur hukum acara pidana di Indonesia (penyidikan, penuntutan, dan pemeriksaan di siding pengadilan); 3) Bantuan harus diajukan dan diterima secara resmi melaui mekanisme hubungan pemerintahan antar Negara (*government to government*); dan 4) Bantuan yang diajukan harus menaati ketentuan hukum Negara yang dimintakan bantuannya.[39]

(3). Pengalihan Perkara (*Transfer of Proceedings*)

Transfer of proceedings atau pengalihan perkara merupakan hal baru dalam sistem peradilan pidana internasional. Cara ini lebih dikenal sebagai pengalihan terhadap perkara dalam sistem peradilan pidana internasional. Dimana praktek mekanisme ini diatur dalam *European Convention on The Transfer of Proceedings in Criminal Matters*. Prosedurnya melibatkan kerjasama internasional dimana suatu negara dapat meminta bantuan dari

[38] Siswanto Sunarso, *Ekstradisi dan Bantuan Timbal Balik dalam Masalah Pidana: Instrumen Penegakan Hukum Pidana Internasional*, (Jakarta: Rineka Cipta, 2009), h. 133

[39] Akbar Kurnia Putra, *Op. Cit*, h. 50

negara lain untuk melakukan proses pengadilan terhadap seseorang yang merupakan tersangka dalam kejahatan yang terjadi di wilayahnya.

Kasus pencurian data pribadi yang menimpa Baim Wong menjadi contoh nyata atas tantangan besar dalam perlindungan data pribadi di Indonesia. Meskipun Indonesia telah memiliki payung hukum yang mengatur perlindungan data pribadi, seperti Undang-Undang Nomor 27 Tahun 2022, kasus ini mengungkap bahwa penerapan hukum tersebut masih menghadapi berbagai kendala. Data pribadi Baim Wong yang disalahgunakan untuk melakukan penipuan menunjukkan rendahnya standar keamanan dan pengelolaan data oleh pihak ketiga yang memiliki akses terhadap data tersebut. Hal ini menegaskan pentingnya tanggung jawab pengendali data dalam menjaga kerahasiaan dan integritas data pribadi.

Selain itu, proses pelacakan pelaku menjadi sulit karena kejahatan ini dilakukan secara anonim dengan teknologi digital yang kompleks, serta pelaku seringkali berada di luar yurisdiksi Indonesia. Kondisi ini menuntut kerja sama internasional yang intensif melalui mekanisme seperti ekstradisi dan bantuan hukum timbal balik (*mutual legal assistance*), namun kendala hukum dan diplomasi antarnegara sering menghambat penegakan hukum tersebut. Kasus ini juga memperlihatkan bahwa figur publik sekalipun sangat rentan terhadap pencurian data pribadi, yang berarti masyarakat umum dengan tingkat kesadaran dan akses hukum yang lebih terbatas menghadapi risiko jauh lebih besar. Oleh karena itu, perlindungan data pribadi harus didukung bukan hanya oleh regulasi yang memadai, tetapi juga oleh kemampuan aparat penegak hukum, kesadaran publik, dan sistem teknologi yang aman serta responsif. Tanpa langkah-langkah tersebut, hukum yang ada hanya akan menjadi sebatas formalitas tanpa efektivitas nyata dalam mencegah dan menindak kejahatan pencurian data pribadi di era digital.

KESIMPULAN

Penegakan hukum terhadap pencurian data pribadi di Indonesia telah memiliki dasar hukum yang cukup kuat melalui Undang-Undang Perlindungan Data Pribadi, Undang-Undang ITE, dan peraturan terkait lainnya. Namun, dalam pelaksanaannya masih menghadapi berbagai hambatan, seperti keterbatasan teknologi, kurangnya kemampuan penyidik, serta sulitnya pelacakan dan pengumpulan alat bukti dalam ranah siber. Sifat kejahatan siber yang lintas batas negara juga menimbulkan tantangan yurisdiksi, sehingga dibutuhkan mekanisme kerjasama internasional yang kuat untuk menegakkan hukum secara efektif.

REFERENSI

Atmasasmita, Romli. *Pengantar Hukum Pidana Internasional*. Bandung: Refika Aditama, 2003.

Firdaus, Indriana. "Upaya Perlindungan Hukum Hak Privasi Terhadap Data Pribadi dari Kejahatan Peretasan." *Jurnal Rechten: Riset Hukum dan Hak Asasi Manusia* 4, no. 2 (2022).

Fred, Isjwara. *Pengantar Ilmu Politik*. Bandung: Binacipta, 1996.

Garner, Bryan A., ed. *Black's Law Dictionary*. 7th ed. St. Paul, MN: West Group, 1999.

Hehanussa, Deassy J. A., dkk. *Metode Penelitian Hukum*. Bandung: Widina Bhakti Persada, 2023.

Herryani, M. R. T. R. "Perlindungan Hukum Terhadap Kebocoran Data Pribadi Konsumen Online Marketplace." *Transparansi Hukum* 5, no. 1 (2022): 110–133.

Kanter, E. Y., dan S. R. Sianturi. *Asas-Asas Hukum Pidana di Indonesia dan Penerapannya*. Jakarta: Storia Grafika, 2002.

Langseth, Peter. *United Nations Handbook on Practical Anti-Corruption Measures for Prosecutors and Investigators*. Vienna: UNODC, 2004.

Menthe, Darrel. "Jurisdiction in Cyberspace: A Theory of International Spaces." *Michigan Technology Law Review* 4 (1998).

Muladi. *Demokratisasi, Hak Asasi Manusia, dan Reformasi Hukum di Indonesia*. Jakarta: The Habibie Center, 2002.

Mulqadrin Adam, dkk. "Upaya Kepolisian dalam Penanggulangan Tindak Pidana Kejahatan Dunia Maya (Cyber Crime) pada Kepolisian Daerah Sulawesi Selatan." *Journal of Lex Generalis (JLG)* 2, no. 3 (2021): 1101–1116.

Nawawi Arief, Barda. *Tindak Pidana Mayantara: Perkembangan Kajian Cyber Crime di Indonesia*. Jakarta: RajaGrafindo Persada, 2006.

Niffari, Hanifan. "Perlindungan Data Pribadi sebagai Bagian dari Hak Asasi Manusia atas Perlindungan Diri Pribadi: Suatu Tinjauan Komparatif dengan Peraturan Perundang-Undangan di Negara Lain." *Jurnal Hukum dan Bisnis (Selisik)* 6, no. 1 (2020): 1–14.

Pertiwi, Endah, dkk. "Analisis Yuridis Terhadap Penyalahgunaan Data Pribadi Pengguna Media Sosial." *Jurnal Rechten: Riset Hukum dan Hak Asasi Manusia* 2, no. 1 (2020).

Putra, Akbar Kurnia. "Analisis Hukum Yurisdiksi Tindak Kejahatan Siber (Cybercrime) Berdasarkan Convention on Cybercrime." *Jurnal Ilmu Hukum* 7, no. 1 (2016).

Ravena, H. D. *Kebijakan Kriminal (Criminal Policy)*. Jakarta: Prenada Media, 2017.

Saleh, Roeslan. *Penerapan Lembaga Ekstradisi dalam Hubungan Antarnegara*. Jakarta: Rineka Cipta, 1992.

Salmon, Harly Clifford Jonas. "Penegakan Hukum Terhadap Kejahatan Penyebaran Konten Porno Balas Dendam (Revenge Porn)." *BACARITA Law Journal* 4, no. 1 (2023): 42–48.

Starke, J. G. *Introduction to International Law*. 9th ed. London: Butterworths, 2000.

Starke, J. G. *Pengantar Hukum Internasional*. Jakarta: Sinar Grafika, 1989.

Sunarso, Siswanto. *Ekstradisi dan Bantuan Timbal Balik dalam Masalah Pidana: Instrumen Penegakan Hukum Pidana Internasional*. Jakarta: Rineka Cipta, 2009.

Suyatno, Thomas, dkk. *Dasar-Dasar Perkreditan*. Jakarta: Gramedia Pustaka Utama, 2017.

Taher, Andrian Pratama. "Pekan Depan, Platform Medsos Wajib Setor Data Pribadi ke Pemerintah." *Tirto*. https://tirto.id/pekan-depan-platform-medsos-wajib-setor-data-pribadi-ke-pemerintah-ggb2.

Triadi, Muhammad. "Perlindungan Terhadap Korban Pencurian Data Pribadi Melalui Media Digital." *REUSAM: Jurnal Ilmu Hukum* 11, no. 1 (2023): 45–64.

Widodo. *Hukum Pidana di Bidang Teknologi Informasi (Cybercrime Law)*. Yogyakarta: Aswaja Pressindo, 2013.