



PERLINDUNGAN HUKUM TERHADAP KONSUMEN KORBAN PENYALAHGUNAAN DATA PRIBADI PADA PERDAGANGAN ELEKTRONIK

Affifah Dwi Kusuma Ningtyas¹, Revie Kurnia Katjong², Andi Annisa Nurlia Mamonto³

Fakultas Hukum, Universitas Yapis Papua. Indonesia

Email: affifahkusuma03@gmail.com¹, reviekatjong@gmail.com²,

annisanurliamamonto1@gmail.com³

Corresponding author: Affifahkusuma03@gmail.com

ABSTRAK

Perlindungan hukum terhadap konsumen yang menjadi korban penyalahgunaan data pribadi dalam perdagangan elektronik dibagi menjadi dua macam yaitu Bentuk perlindungan Hukum Preventif dan Represif. Bentuk perlindungan hukum Preventif adalah Perlindungan yang diberikan pemerintah dengan tujuan untuk mencegah sebelum terjadinya pelanggaran, Bentuk perlindungan hukum Represif adalah bentuk perlindungan yang diberikan kepada konsumen setelah terjadi pelanggaran atau penyalahgunaan data pribadi. Upaya hukum tersebut dibagi menjadi non-litigasi (di luar pengadilan) dan litigasi (melalui pengadilan). Upaya Hukum Non-Litigasi dengan cara Pengaduan ke Pelaku Usaha atau Platform, Pengaduan ke Kementerian Komunikasi dan Informatika (Kominfo), Pengaduan ke Lembaga Pengawas Data Pribadi (LPDP), Pengaduan ke Badan Perlindungan Konsumen Nasional (BPKN), Penyelesaian Sengketa di Badan Penyelesaian Sengketa Konsumen (BPSK). Upaya Hukum Litigasi dengan cara Gugatan Perdata (Perbuatan Melawan Hukum), Laporan Pidana ke Kepolisian, Class Action (Gugatan Kelompok).

Kata kunci: *Perlindungan Konsumen; Penyalahgunaan Data Pribadi; Perdagangan Elektronik.*

ABSTRACT

Legal protection for consumers who become victims of personal data misuse in e-commerce is divided into two types: Preventive and Repressive. Preventive legal protection is provided by the government to prevent violations before they occur. Repressive legal protection is provided to consumers after a violation or misuse of personal data has occurred. These legal remedies are divided into non-litigation (outside the court) and litigation (through the court). Non-litigation legal remedies include filing complaints with business actors or platforms, complaints with the Ministry of Communication and Information Technology (Kominfo), complaints with the Personal Data Supervisory Agency (LPDP), complaints with the National Consumer Protection Agency (BPKN), and dispute resolution with the Consumer Dispute Resolution Agency (BPSK). Litigation legal remedies include civil lawsuits (for unlawful acts), criminal reports to the police, and class actions.

Keywords: *Consumer Protection; Personal Data Misuse; E-Commerce;.*

I. PENDAHULUAN

Sistem teknologi informasi memungkinkan penerapan konsep perlindungan data yang menegaskan bahwa individu memiliki hak untuk menentukan apakah mereka akan bergabung dengan komunitas tertentu. Individu tersebut memiliki kewenangan untuk memutuskan apakah akan membagikan atau bertukar data pribadi mereka, serta menetapkan syarat-syarat yang mereka anggap layak dalam proses tersebut. Pada masa kini, hak privasi telah mengalami perkembangan yang signifikan, sehingga mencakup perumusan hak untuk melindungi data pribadi secara lebih komprehensif.

Perlindungan data pribadi telah menjadi aspek yang sangat krusial dan tidak dapat diabaikan dalam konteks perdagangan elektronik. Dalam era digital yang semakin berkembang pesat ini, di mana transaksi dan interaksi bisnis sering kali dilakukan secara daring, pentingnya menjaga kerahasiaan dan keamanan informasi pribadi pengguna menjadi semakin mendesak. Hal ini tidak hanya berkaitan dengan kepatuhan terhadap regulasi yang ada, tetapi juga berhubungan erat dengan kepercayaan konsumen terhadap platform perdagangan elektronik.

Perdagangan elektronik adalah suatu kegiatan bisnis yang dilakukan melalui jaringan internet yang melibatkan beberapa pihak seperti pedagang, konsumen, manufaktur dan penyedia layanan. Perdagangan Elektronik atau E-Commerce” adalah istilah yang digunakan untuk menggambarkan perdagangan yang didukung oleh kemajuan teknologi. Sejak berkembangnya perdagangan elektronik atau e-commerce orang-orang dapat menjual barang atau jasa melalui website atau blog. Transaksi melalui internet memberikan kemudahan, kenyamanan, dan efisiensi waktu bagi pengguna, yang semuanya berkontribusi pada pertumbuhan pesat industri perdagangan elektronik di Indonesia.

Perdagangan elektronik, juga dikenal sebagai e-commerce, adalah salah satu kemajuan yang dihasilkan oleh pertumbuhan ekonomi digital. Penjual dan pembeli dapat melakukan transaksi apa pun tanpa perlu bertemu secara tatap

muka melalui e-commerce. Kegiatan jual beli dapat dilakukan di mana saja asalkan terhubung ke jaringan internet. Hal ini tentu saja memberikan kontribusi untuk meningkatkan efisiensi waktu pada kehidupan manusia serta mengurangi biaya barang dan/atau jasa.

Meskipun demikian, terdapat masalah besar terkait perlindungan data pribadi pada perdagangan elektronik. Beberapa undang-undang tentang perlindungan data pribadi telah dibuat oleh pemerintah, sistem implementasi dan penegakan masih perlu diperbaiki. Salah satu faktor utama yang menyebabkan risiko keamanan data pribadi adalah kurangnya pengetahuan masyarakat dan keamanan data pribadi, terutama dalam hal transaksi e-commerce. Hal ini disebabkan oleh banyaknya orang yang tidak tahu tentang hak-hak konsumen saat melakukan transaksi online dan risiko yang terkait dengan perlindungan data pribadi. Dengan kata lain, mereka lebih rentan terhadap penyalahgunaan data pribadi oleh pihak yang tidak bertanggung jawab, seperti pelaku kejahatan siber. Oleh karena itu, diperlukan kesadaran yang lebih besar tentang perlindungan data pribadi dan hak konsumen dalam perdagangan elektronik (e-commerce).

Menurut Pasal 1 Peraturan Pemerintah No. 71 Tahun 2019 mengenai Penyelenggaraan Sistem dan Transaksi Elektronik, "data pribadi merupakan beberapa macam data perseorangan yang dapat teridentifikasi secara sendiri atau dikombinasi dengan informasi yang lain, baik itu secara langsung maupun tidak melalui system elektronik dan/atau non elektronik." Penyalahgunaan data pribadi pada suatu perdagangan elektronik saat ini semakin sering terjadi. Penyalahgunaan data pribadi sering kali terjadi dalam bentuk penjualan informasi kepada pihak ketiga tanpa adanya persetujuan yang jelas, serta kebocoran data yang disebabkan oleh kelalaian dalam sistem pengamanan. penyalahgunaan data pribadi tersebut dapat terjadi karena para pengendali atau pemroses data pribadi lebih memperhatikan fitur kemudahan pengaksesan oleh pengguna daripada keamanan sehingga memperbesar kesempatan terjadinya peristiwa kebocoran data pribadi. Data pribadi konsumen yang bocor dapat menimbulkan kerugian terhadap konsumen.

Kerugian pertama yang mungkin dialami oleh konsumen adalah kerugian finansial, yang dapat mencakup kehilangan uang serta bentuk kerugian lainnya. Kerugian kedua yang signifikan adalah kehilangan privasi, yang

merujuk pada situasi di mana privasi konsumen terganggu akibat kebocoran data pribadi mereka.

Pada Pasal 4 huruf a Undang-Undang Nomor 8 Tahun 1999 mengenai Perlindungan Konsumen dijelaskan bahwa konsumen memiliki hak mutlak yaitu hak agar terjaminnya rasa kenyamanan, tingkat keamanan dan keselamatan diri konsumen ketika mengkonsumsi atau menggunakan suatu barang atau jasa. Yang berarti, jika terjadi penyalahgunaan data pribadi maka konsumen yang jadi korban penyalahgunaan data pribadi telah dilanggar haknya selama atau setelah proses perdagangan elektronik. Atas ancaman kejadian tersebut, diperlukan perlindungan hukum yang melindungi kerahasiaan data pribadi milik para konsumen, dikarenakan data pribadi konsumen sangat rentan mengalami kebocoran dan disalahgunakan oleh para pihak tidak bertanggung jawab untuk melakukan tindakan ilegal yang pada akhirnya hanya akan menimbulkan kerugian untuk konsumen.

Perlindungan data pribadi konsumen dalam transaksi e-commerce sangat penting untuk melindungi hak konsumen, dan meningkatkan kepercayaan konsumen terhadap sistem perdagangan elektronik. Kepercayaan ini sangat penting untuk pertumbuhan dan keberlanjutan industri e-commerce di Indonesia. Tanpa kepercayaan dari konsumen, perkembangan e-commerce bisa terhambat, sehingga potensi ekonominya akan terbatas. Penting untuk diingat bahwa data pribadi konsumen meliputi informasi sensitif seperti nama, alamat, nomor telepon, dan informasi keuangan. Konsumen dapat menjadi korban penipuan, pencurian identitas, dan berbagai jenis kejahatan siber lainnya jika data ini masuk ke tangan orang yang tidak berwenang. Oleh karena itu, penting bagi peraturan yang ada harus didukung oleh mekanisme penegakan hukum yang efektif. Selain itu, masyarakat harus dididik tentang pentingnya menjaga kerahasiaan data pribadi. Dengan pemahaman yang lebih baik tentang risiko-risiko yang terkait dengan keamanan data dan langkah-langkah yang dapat diambil untuk mengurangi risiko tersebut, masyarakat akan menjadi lebih proaktif dalam menjaga privasi mereka.

Penelitian terdahulu yang telah dilakukan oleh Alfrida Sylfia, I Gusti Ngurah Adyana, Mohammad Fahrial Amrullah, dan Hendra Djaja, Fakultas Hukum, Universitas Merdeka Malang dengan judul: "Tanggungjawab Yuridis PT. Tokopedia atas Kebocoran Data Pribadi dan Privasi Konsumen dalam

Transaksi Online” inti pembahasan pada penelitian ini adalah hubungan hukum antara pelaku usaha (yang dalam hal ini adalah Tokopedia) dengan konsumen muncul karena adanya perbuatan yang dijanjikan dan dijalankan oleh kedua belah pihak dan dikarenakan adanya kebocoran data pribadi dan privasi konsumen PT. Tokopedia harus meningkatkan sistem keamanan secara berkala dan wajib melakukan pengecekan rutin sehingga diharapkan tidak lagi terjadi kasus serupa di kemudian hari. Sesuai dengan Pasal 19 Undang-Undang Perlindungan Konsumen Tokopedia wajib memberikan ganti rugi administratif terhadap konsumen atas pelanggaran yang terjadi. Selain itu, sesuai dengan Peraturan Pemerintah Nomor 80 Tahun 2019 tentang Perdagangan Melalui Sistem Elektronik, Tokopedia akan dikenakan sanksi peringatan tertulis, setiap pergerakannya akan diawasi, masuk ke dalam blacklist, pemblokiran layanan penyelenggara perdagangan baik itu dalam atau luar negeri oleh instansi yang berwenang dan/atau dilakukan pencabutan izin usaha. Sementara penelitian yang dilakukan oleh Yudha Sri Wulandari, Fakultas Hukum, Universitas Kutai Kertanegara yang berjudul “Perlindungan Hukum bagi Konsumen terhadap Transaksi Jual- Beli e-commerce” Penelitian yang dilakukan tersebut menyimpulkan bahwa Undang-Undang Perlindungan Konsumen dan Undang-Undang Informasi dan Transaksi Elektronik telah cukup memberikan perlindungan untuk konsumen dalam kegiatan jual- beli secara online, serta upaya-upaya bagi konsumen apabila terjadi wanprestasi atau pelanggaran hak konsumen selama proses jual-beli secara elektronik.

Berdasarkan Latar Belakang Masalah diatas, Maka penulis tertarik meneliti dan menulis dengan judul “Perlindungan Hukum Terhadap Konsumen Korban Penyalahgunaan Data Pribadi Pada Perdagangan Elektronik.

II. METODE PENELITIAN

Jenis Penelitian yang digunakan adalah penelitian normatif, Pengumpulan informasi dengan cara Penelitian Kepustakaan (*Library Research*). Jenis data yang digunakan dalam penelitian ini adalah data kualitatif dengan pendekatan hukum normatif. Dimana penelitian ini dilakukan berdasarkan bahan hukum utama dengan cara menelaah teori-teori, konsep-konsep asas-asas hukum serta peraturan perundang-undangan yang relevan dengan penelitian ini. Teknik

analisis data yang digunakan dalam penelitian ini menggunakan metode kualitatif. Penelitian kualitatif adalah penelitian yang dilakukan di lingkungan alam dengan metode manusia yang berfokus pada konteks fenomena, mengikuti pemahaman yang evolusioner dan interpretatif secara fundamental.

III. HASIL DAN PEMBAHASAN

A. Perlindungan Hukum Terhadap Konsumen Korban Penyalahgunaan Data Pribadi Pada Perdagangan Elektronik

Perkembangan teknologi informasi dan komunikasi telah mendorong pertumbuhan perdagangan elektronik secara pesat. Perdagangan Elektronik tidak hanya memberikan kemudahan bagi konsumen, tetapi juga meningkatkan risiko penyalahgunaan data pribadi. Oleh karena itu, perlindungan hukum terhadap konsumen menjadi aspek penting dalam memastikan keamanan dan kepercayaan dalam ekosistem digital.

Data pribadi konsumen merupakan informasi yang bersifat rahasia dan melekat pada identitas seseorang, seperti nama, alamat, nomor identitas, nomor telepon, email, hingga informasi keuangan. Dalam konteks *e-commerce* atau perdagangan elektronik, data ini dikumpulkan, diproses, dan disimpan oleh pelaku usaha sebagai pengendali data. Penyalahgunaan data tersebut, seperti dijual kepada pihak ketiga tanpa persetujuan atau diretas, berpotensi menimbulkan kerugian baik materiil maupun immateriil.

Data pribadi yang seharusnya dijaga kerahasiaannya sering kali disalahgunakan oleh pelaku usaha atau pihak ketiga, baik untuk kepentingan komersial, penipuan, hingga kejahatan digital lainnya.

Untuk itu, penting untuk mengidentifikasi faktor-faktor penyebab terjadinya penyalahgunaan data pribadi pada perdagangan elektronik.

Penyalahgunaan data pribadi dapat disebabkan oleh berbagai faktor, baik dari dalam maupun luar sistem. Beberapa faktor penyebab utama meliputi serangan siber, kelemahan sistem keamanan, kesalahan manusia (*human error*), dan ancaman dari dalam (*insider threats*). Selain itu, kurangnya kepatuhan terhadap regulasi akan keamanan data juga turut berkontribusi.

Faktor-faktor penyebab terjadinya penyalahgunaan data pribadi pada perdagangan elektronik:

1. Serangan Siber:
 - a. Serangan *Phising*

Penjahat siber menggunakan email atau pesan palsu untuk menipu pengguna agar memberikan informasi pribadi.
 - b. *Malware*

Perangkat lunak berbahaya yang dapat mencuri data pribadi dari perangkat yang terinfeksi.
 - c. Peretasan (*Hacking*)

Upaya untuk mengakses sistem atau data secara tidak sah.
2. Kelemahan Sistem Keamanan:
 - a. Sistem yang Tidak Aman

Celah dalam sistem keamanan memungkinkan peretas untuk masuk dan mencuri data.
 - b. Konfigurasi yang Buruk

Kesalahan dalam pengaturan sistem dapat menciptakan titik lemah yang dapat dimanfaatkan.
 - c. Aplikasi yang Tidak Aman

Aplikasi yang tidak diperbarui atau memiliki kerentanan keamanan dapat menjadi pintu masuk bagi penyerang.
3. *Human Error*

Kelalaian pengguna dalam menjaga kerahasiaan data, seperti menggunakan kata sandi yang lemah, mengklik tautan mencurigakan, atau membagikan informasi pribadi secara sembarangan, dapat menyebabkan kebocoran data.
4. Ancaman Dari Dalam

Karyawan atau pihak internal yang memiliki akses ke data juga dapat menjadi sumber kebocoran data jika mereka menyalahgunakan akses tersebut.
5. Kurangnya Kepatuhan Regulasi

Kurangnya pemahaman dan kepatuhan terhadap peraturan perlindungan data pribadi dapat meningkatkan risiko penyalahgunaan data.

Sistem dan Transaksi Elektronik menyatakan pengertian data pribadi adalah “setiap data tentang seseorang baik yang teridentifikasi dan/atau dapat diidentifikasi secara tersendiri atau dikombinasi dengan informasi lainnya baik

secara langsung maupun tidak langsung melalui Sistem Elektronik dan/atau non-elektronik.” Oleh sebab itu, data pribadi penting untuk mendapatkan perlindungan karena berisikan fakta-fakta dari seseorang. Perlindungan pada suatu data pribadi milik seseorang merupakan suatu perlindungan mutlak yang dilakukan secara tertentu terkait bagaimana hukum melindungi data pribadi semua warga negara saat dikumpulkan, disimpan, didistribusikan, dan digunakan.

Dalam menjalankan dan memberikan perlindungan hukum dibutuhkan suatu tempat atau wadah dalam pelaksanaannya yang sering disebut dengan bentuk perlindungan hukum. Bentuk perlindungan hukum dibagi menjadi dua macam yang dapat dipahami, sebagai berikut:

1. Bentuk Perlindungan Hukum Preventif

Perlindungan yang diberikan pemerintah dengan tujuan untuk mencegah sebelum terjadinya pelanggaran. Hal ini terdapat dalam peraturan perundang-undangan dengan maksud untuk mencegah suatu pelanggaran serta memberikan rambu-rambu atau batasan-batasan dalam melakukan suatu kewajiban. Peraturan perundang-undangan yang relevan meliputi:

- a. Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi yang secara khusus mengatur prinsip-prinsip pemrosesan data pribadi, termasuk persetujuan eksplisit, keabsahan pemrosesan, dan hak-hak subjek data sekaligus kewajiban kepada pelaku usaha sebagai pengendali data. Dalam Pasal 5-9 Undang-Undang Perlindungan Data Pribadi disebutkan bahwa setiap orang berhak atas perlindungan data pribadinya, termasuk hak untuk memperoleh informasi, mengakses, memperbaiki, menghapus, dan menolak pemrosesan data. Ini berarti konsumen memiliki kontrol terhadap data pribadinya dan dapat meminta pertanggungjawaban apabila datanya disalahgunakan.
- b. Undang-Undang Nomor 8 Tahun 1999 tentang Perlindungan Konsumen. Pasal 4 huruf a Undang-Undang Perlindungan Konsumen menyebutkan:
"Konsumen berhak atas kenyamanan, keamanan, dan keselamatan dalam mengkonsumsi barang dan/atau jasa."

Dalam konteks penyalahgunaan data pribadi, hak ini dilanggar ketika pelaku usaha lalai dalam menjaga kerahasiaan data konsumen.

Melalui peraturan-peraturan tersebut, pelaku usaha diwajibkan untuk:

- 1) Memberikan informasi yang benar, jelas, dan jujur mengenai identitas, hak, dan kewajiban;
- 2) Menyediakan kebijakan perlindungan data;
- 3) Menjamin keamanan sistem penyimpanan data;
- 4) Mendapatkan persetujuan sebelum mengumpulkan dan memproses data pribadi konsumen.

Jika data pribadi konsumen digunakan tanpa izin dalam transaksi online, maka konsumen telah kehilangan rasa aman dan kenyamanan dalam bertransaksi, yang merupakan hak konsumen sebagaimana dijamin oleh Undang-Undang Perlindungan Konsumen. Dalam hal ini, penyalahgunaan data pribadi menjadi bentuk pelanggaran hak konsumen.

2. Bentuk Perlindungan Hukum Represif

Perlindungan hukum represif diberikan kepada konsumen setelah terjadi pelanggaran atau penyalahgunaan data pribadi. Perlindungan ini mencakup:

- a. Lembaga yang berwenang seperti Lembaga Pengawas Data Pribadi (LPDP) dapat memberikan sanksi administratif kepada pelaku usaha yang melanggar. Sesuai Pasal 57-58 Undang-Undang Perlindungan Data Pribadi Bentuk sanksi meliputi:
 - a. Peringatan tertulis,
 - b. Denda administratif,
 - c. Penghentian sementara layanan.
- b. Sanksi pidana bagi pihak yang dengan sengaja mengungkapkan data pribadi tanpa hak sebagaimana diatur dalam Pasal 67 Undang-Undang Perlindungan Data Pribadi, dengan ancaman pidana maksimal 5 tahun dan/atau denda hingga Rp5 miliar.
- c. Hak untuk mendapatkan ganti rugi, Pasal 19 Undang-Undang Perlindungan Konsumen, yang mewajibkan pelaku usaha memberikan ganti rugi kepada konsumen melalui jalur perdata.

Perlindungan ini bertujuan memberikan efek jera kepada pelaku dan memberikan keadilan bagi konsumen sebagai korban.

Akan tetapi, implementasi perlindungan hukum ini masih menghadapi tantangan. Banyak pelaku usaha yang belum sepenuhnya patuh terhadap ketentuan Undang-Undang Perlindungan Data Pribadi, terutama pelaku usaha skala kecil dan menengah yang minim infrastruktur keamanan siber. Selain itu, banyak konsumen yang belum memahami hak-haknya atas data pribadi.

Kesadaran konsumen terhadap pentingnya data pribadi masih rendah. Banyak di antara mereka yang sembarangan memberikan data kepada *platform digital* tanpa membaca atau memahami kebijakan privasi yang ditawarkan. Hal ini memperbesar kemungkinan penyalahgunaan data tanpa sepengetahuan mereka.

Perlindungan hukum terhadap konsumen juga membutuhkan keterlibatan aktif dari pemerintah dalam memberikan edukasi dan sosialisasi mengenai hak atas data pribadi serta risiko-risiko penyalahgunaan yang mungkin terjadi. Pemerintah perlu menjadikan literasi digital sebagai bagian dari upaya perlindungan konsumen.

Di sisi lain, perlu juga dibangun hukum yang tegas dan responsif terhadap pelanggaran. Penegakan hukum yang lemah akan membuat pelaku penyalahgunaan data tidak jera, dan kepercayaan publik terhadap ekosistem digital pun menurun.

Konsumen sebagai subjek data juga perlu didorong untuk aktif melakukan kontrol terhadap datanya. Hak untuk mengakses dan memperbaiki data, serta hak untuk menarik persetujuan, harus dipermudah oleh pelaku usaha. Jika tidak, maka konsumen menjadi subjek pasif yang tidak memiliki kuasa terhadap informasi pribadinya sendiri.

B. Upaya Hukum Yang Bisa Konsumen Lakukan Jika Menjadi Korban Penyalahgunaan Data Pribadi Pada Perdagangan Elektronik

Undang-undang memberikan suatu jaminan terhadap upaya untuk perorangan atau badan hukum yang pada suatu hal tertentu untuk melawan suatu putusan yang telah diputuskan oleh hakim yang dianggap tidak

memenuhi asas keadilan atau merugikan salah satu pihak disebut dengan upaya hukum. Konsumen yang mengalami penyalahgunaan data pribadi dalam aktivitas perdagangan elektronik memiliki hak hukum yang dijamin oleh berbagai instrumen peraturan perundang-undangan di Indonesia. Upaya hukum tersebut dibagi menjadi non-litigasi (di luar pengadilan) dan litigasi (melalui pengadilan).

1. Upaya Hukum Non-Litigasi

a. Pengaduan ke Pelaku Usaha atau Platform

Langkah pertama yang dapat dilakukan oleh konsumen adalah mengajukan pengaduan langsung kepada pelaku usaha atau platform e-commerce terkait. Biasanya, pelaku usaha memiliki mekanisme internal untuk menerima, memproses, dan menyelesaikan keluhan konsumen, termasuk yang berkaitan dengan penyalahgunaan data pribadi.

b. Pengaduan ke Kementerian Komunikasi dan Informatika (Kominfo)

Konsumen dapat melapor ke Kominfo atas penyalahgunaan data pribadi oleh pelaku usaha. Berdasarkan Pasal 58 ayat (1) Undang-Undang No. 27 Tahun 2022 tentang Pelindungan Data Pribadi, Kominfo berwenang untuk menjatuhkan sanksi administratif seperti peringatan tertulis, penghentian sementara aktivitas pengolahan data, hingga denda administratif.

Kementerian Komunikasi dan Informatika Republik Indonesia (Kominfo) berperan penting dalam pengawasan dan penegakan hukum terhadap perlindungan data pribadi, terutama dalam ranah digital dan perdagangan elektronik. Jika konsumen merasa data pribadinya disalahgunakan, maka pengaduan ke Kominfo dapat menjadi jalur penyelesaian administratif dan investigatif.

Penyelesaian penyalahgunaan data pribadi oleh kominfo sebagai berikut:

- 1) Penerimaan dan Verifikasi Laporan
- 2) Penyelidikan dan Klarifikasi
- 3) Pencarian Bukti dan Pembentukan Tim
- 4) Tindakan Hukum
- 5) Mediasi dan Penyelesaian Sengketa

c. Pengaduan ke Lembaga Pengawas Data Pribadi (LPDP)

Undang-Undang Perlindungan Data Pribadi membentuk lembaga pengawas independen yang memiliki kewenangan dalam menyelesaikan

sengketa perlindungan data pribadi dan melakukan mediasi antara konsumen dengan pelaku usaha.

d. Pengaduan ke Badan Perlindungan Konsumen Nasional (BPKN)

Badan Perlindungan Konsumen Nasional merupakan lembaga yang dapat memberikan advokasi dan mediasi kepada konsumen. Hal ini didasarkan pada Pasal 31 Undang-Undang No. 8 Tahun 1999 tentang Perlindungan Konsumen.

e. Penyelesaian Sengketa di Badan Penyelesaian Sengketa Konsumen (BPSK)

Konsumen dapat menempuh penyelesaian sengketa secara alternatif di Badan Penyelesaian Sengketa Konsumen, melalui mediasi, konsiliasi, atau arbitrase sebagaimana diatur dalam Pasal 52–58 Undang-Undang Nomor 8 Tahun 1999 Tentang Perlindungan Konsumen.

2. Upaya Hukum Litigasi

a. Gugatan Perdata (Perbuatan Melawan Hukum)

Konsumen dapat mengajukan gugatan ke pengadilan berdasarkan Pasal 1365 KUH Perdata, yang menyatakan bahwa setiap perbuatan yang melanggar hukum dan menimbulkan kerugian pada orang lain mewajibkan pelakunya mengganti kerugian tersebut. Gugatan perdata dilakukan dengan tujuan memulihkan kerugian yang harus diderita oleh konsumen atau korban dengan sanksi atau hukuman berupa ganti kerugian/denda dan sanksi tersebut nantinya akan dijatuhkan pada pengendali data pribadi apabila terbukti bersalah. Konsumen dapat mengambil tindakan selaku korban penyalahgunaan data pribadi adalah sebagai berikut:

- 1) Memperkarakan permasalahan atas dasar perbuatan melawam hukum ke Pengadilan Negeri.
- 2) Dalam hal upaya banding, konsumen atau korban dapat mengajukan upaya banding tersebut ke Pengadilan Tinggi.
- 3) Untuk upaya kasasi dan peninjauan kembali, konsumen dapat mengajukan upaya tersebut ke Mahkamah Agung.

b. Laporan Pidana ke Kepolisian

Jika unsur pidana terpenuhi, konsumen dapat melaporkan ke aparat penegak hukum. Penyalahgunaan data pribadi dapat dijerat pidana berdasarkan:

- 1) Pasal 67–69 Undang-Undang Perlindungan Data Pribadi, yang mengatur ancaman pidana penjara dan/atau denda terhadap pelaku

penyalahgunaan data pribadi. Dengan ancaman pidana maksimal 5 tahun dan/atau denda hingga Rp5 miliar.

Berdasarkan Undang-Undang Perlindungan Data Pribadi, Proses penyelesaiannya:

- a) Melakukan pelaporan ke kepolisian setempat sesuai dengan cakupan wilayahnya.
 - b) Mengajukan tuntutan ke Pengadilan Negeri untuk upaya tingkat pertama.
 - c) Jika putusan pada upaya tingkat pertama di Pengadilan Negeri dirasa tidak sesuai dan memberatkan maka konsumen dapat mengajukan upaya banding ke Pengadilan Tinggi.
 - d) Jika kemudian putusan dari upaya banding masih dirasa tidak adil atau tidak sebanding dengan kerugian-kerugian yang telah diderita atau dialami. Maka konsumen selaku korban di sini bisa melakukan upaya kasasi dan peninjauan kembali di Mahkamah Agung.
- c. Class Action (Gugatan Kelompok)

Jika pelanggaran data berdampak pada banyak konsumen, maka dapat dilakukan gugatan kelompok (class action). Hal ini diatur dalam Peraturan Mahkamah Agung (PERMA) No. 1 Tahun 2002 tentang Acara Gugatan Perwakilan Kelompok.

IV. PENUTUP

4. Kesimpulan

1. Penyalahgunaan data pribadi dapat disebabkan oleh berbagai faktor, baik dari dalam maupun luar sistem. Beberapa faktor penyebab utama meliputi serangan siber, kelemahan sistem keamanan, kesalahan manusia (*human error*), dan ancaman dari dalam (*insider threats*). Selain itu, kurangnya kepatuhan terhadap regulasi akan keamanan data juga turut berkontribusi. Perlindungan hukum terhadap konsumen yang menjadi korban penyalahgunaan data pribadi dalam perdagangan elektronik dibagi menjadi dua macam yaitu Bentuk perlindungan Hukum Preventif dan Represif. Bentuk perlindungan hukum Preventif adalah Perlindungan yang diberikan pemerintah dengan tujuan untuk mencegah sebelum terjadinya pelanggaran, Bentuk perlindungan hukum Represif adalah

bentuk perlindungan yang diberikan kepada konsumen setelah terjadi pelanggaran atau penyalahgunaan data pribadi.

2. Upaya hukum tersebut dibagi menjadi non-litigasi (di luar pengadilan) dan litigasi (melalui pengadilan):
 - a. **Upaya Hukum Non-Litigasi**
 - 1) Pengaduan ke Pelaku Usaha atau Platform
 - 2) Pengaduan ke Kementerian Komunikasi dan Informatika (Kominfo)
 - 3) Pengaduan ke Lembaga Pengawas Data Pribadi (LPDP)
 - 4) Pengaduan ke Badan Perlindungan Konsumen Nasional (BPKN)
 - 5) Penyelesaian Sengketa di Badan Penyelesaian Sengketa Konsumen (BPSK)
 - b. **Upaya Hukum Litigasi**
 - 1) Gugatan Perdata (Perbuatan Melawan Hukum)
 - 2) Laporan Pidana ke Kepolisian
 - 3) Class Action (Gugatan Kelompok)

DAFTAR PUSTAKA

- Abdul Halim Barkatullah, *Hukum Transaksi Elektronik*, Bandung: Nusa Media, 2017.
- A.S Hornby, Gen.Ed, dan Zulham, *Hukum Perlindungan Konsumen*, Jakarta, Kencana Prenada Media Group, 2013.
- Sinta Dewi Rosadi, *Cyber Law: Aspek Data Privasi Menurut Hukum Internasional, Regional, dan Nasional*, Bandung, Refika Aditama, 2015.
- Undang-Undang Dasar Negara Republik Indonesia Tahun 1945
- Undang-Undang Nomor 8 Tahun 1999 Tentang Perlindungan Konsumen.
- Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi.
- Undang-Undang Nomor 1 Tahun 2024 tentang Informasi dan Transaksi Elektronik atau UU ITE.
- Peraturan Mahkamah Agung (PERMA) Nomor 1 Tahun 2002 tentang Acara Gugatan Perwakilan Kelompok.
- . Alfrida Sylfia, et.al, *Tanggung jawab Yuridis PT. Tokopedia Atas Kebocoran Data Pribadi dan Privasi Konsumen dalam Transaksi Online*. Bhirawa Law Journal, vol. 2, no. 5 (2021).

Anna Inao, Ni Made Ari Yulianti Griadhi, *Perlindungan Hukum Terhadap Kebocoran Data Konsumen E-Commerce*. Kertha Semaya: Jurnal Ilmu Hukum, vol. 10, no. 11 (2022).

Ni Kadek Darmayanti, Yuwono, *Upaya Perlindungan Hukum Terhadap Konsumen Online di Indonesia*. Kertha Semaya: Jurnal Ilmu Hukum, vol. 2, no. 2 (2014).