

**PERLINDUNGAN HUKUM BAGI KORBAN CYBERCRIME  
PENYEBARAN DATA PRIBADI SECARA ONLINE***(Legal Protection For Cybercrime Victims Of Online Dissemination Of Personal Data)***Muliawansyah Apriandi<sup>1</sup>, Rotua Valentina Sagala<sup>2</sup>, Basuki<sup>3</sup>**<sup>1,2,3</sup>*Program Studi Magister Ilmu Hukum, Pascasarjana Universitas Jayabaya,**E-mail: [2022010262014@pascajayabaya.ac.id](mailto:2022010262014@pascajayabaya.ac.id)***INFO ARTIKEL****Riwayat Artikel:***Received : 25-10-2024**Revised : 13-11-2024**Accepted : 20-11-2024***Kata Kunci:***Legal Protection, Cybercrime Victims, Online Dissemination Of Personal Data.***DOI:** [10.62335](https://doi.org/10.62335)**ABSTRACT**

*The current development of information technology has certainly had a huge influence on social life in Indonesia. With such rapid progress in the field of technology and information, it is like a double-edged sword because apart from having a positive impact, it can also have a negative impact, one of which is the emergence of cybercrime online dissemination of personal data. The research method used is a normative juridical research method, while technical data analysis uses a statutory approach and a case approach, as well as using legal protection theory and punishment theory. The problem formulation taken is how to regulate cybercrime victims disseminating personal data online in Indonesia and what legal protection there is for cybercrime victims disseminating personal data online in Indonesia. The research results showed that legal protection for cybercrime victims of online dissemination of personal data in Indonesia has been regulated based on Law no. 1 of 2024 concerning the Second Amendment to Law Number 11 of 2008 concerning Information and Electronic Transactions (ITE Law), whose criminal sanctions prioritize punishment for the perpetrator only to provide a deterrent effect, and have not provided a direct impact or benefit for the victim. And in order to provide human rights protection for cybercrime victims of online distribution of personal data in Indonesia, apart from being subject to imprisonment and/or fines, perpetrators may also be subject to additional penalties in the form of confiscation of profits and/or assets obtained or proceeds from criminal acts. , and payment of compensation for victims, such as additional criminal sanctions for confiscation of profits and/or assets obtained or proceeds from criminal acts and payment of compensation for victims. Thus, to realize the Integrated Criminal Justice System, law enforcers not only impose prison sanctions and/or fines on perpetrators, but can also impose additional criminal sanctions which can have a direct impact or benefit for victims. And the House of Representatives and the President need to revise the ITE Law, especially by adding additional criminal provisions in the form of confiscation of profits and/or assets obtained or proceeds*

*from criminal acts and payment of compensation. So that this law can really provide better legal protection and can also be felt directly by victims of cybercrime spreading personal data online in Indonesia.*

## **ABSTRAK**

Perkembangan teknologi informasi saat ini tentunya telah membawa pengaruh yang sangat besar bagi kehidupan bermasyarakat di Indonesia Dengan begitu pesatnya kemajuan di bidang teknologi dan informasi tersebut bagaikan pisau bermata dua karena selain memberikan dampak positif juga dapat memberikan dampak negatif yang salah satunya adalah munculnya *cybercrime* penyebaran data pribadi secara online. Adapun metode penelitian yang digunakan adalah metode penelitian yuridis normatif, sedangkan teknis analisis data menggunakan pendekatan perundang-undangan dan pendekatan kasus, serta menggunakan teori perlindungan hukum dan teori pemidanaan. Dengan rumusan masalah yang diambil adalah bagaimana pengaturan terhadap korban *cybercrime* penyebaran data pribadi secara online di Indonesia dan bagaimana perlindungan hukum bagi korban *cybercrime* penyebaran data pribadi secara online di Indonesia. Hasil penelitian yang diperoleh yaitu bahwa pengaturan terhadap korban *cybercrime* penyebaran data pribadi secara online di Indonesia telah diatur berdasarkan Undang-Undang No. 1 tahun 2024 Tentang Perubahan Kedua Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik (UU ITE), yang sanksi pidananya lebih mengedepankan penghukuman kepada si pelaku untuk memberikan efek jera saja, dan belum memberikan dampak atau manfaat langsung bagi korban. Dan dalam rangka memberikan perlindungan hak asasi manusia bagi korban *cybercrime* penyebaran data pribadi secara online di Indonesia, selain dikenakan pidana penjara dan/atau denda, kepada pelaku dapat pula dikenakan pidana tambahan berupa perampasan keuntungan dan/atau harta kekayaan yang diperoleh atau hasil dari tindak pidana, dan pembayaran ganti kerugian bagi korban, seperti adanya sanksi pidana tambahan perampasan keuntungan dan/atau harta kekayaan yang diperoleh atau hasil dari tindak pidana dan pembayaran ganti kerugian bagi korban. Dengan demikian, Untuk mewujudkan *Integrated Criminal Justice System*, para penegak hukum tidak hanya mengenakan sanksi pidana penjara dan/atau denda kepada pelaku, namun dapat pula mengenakan sanksi pidana tambahan yang dapat memberikan dampak atau manfaat langsung bagi korban. Serta Dewan Perwakilan Rakyat dan Presiden perlu melakukan revisi terhadap UU ITE khususnya dengan menambahkan ketentuan pidana tambahan berupa perampasan keuntungan dan/atau harta kekayaan yang diperoleh atau hasil dari tindak pidana dan pembayaran ganti kerugian. Sehingga undang-undang tersebut benar-benar dapat memberikan perlindungan hukum yang lebih baik

dan dapat dirasakan pula secara langsung bagi korban *cybercrime* penyebaran data pribadi secara online di Indonesia.

## 1. LATAR BELAKANG

Perkembangan teknologi informasi saat ini tentunya telah membawa pengaruh yang sangat besar bagi kehidupan bermasyarakat di Indonesia. Dengan kemajuan teknologi informasi ini telah menyebabkan hubungan antara individu yang satu dengan yang lainnya menjadi tanpa batas, tidak mengenal jarak, dan tentunya berdampak pula pada perubahan sosial masyarakat secara signifikan. Akibat dari perkembangan teknologi ini bagaikan pisau bermata dua karena selain memberikan dampak positif memberikan manfaat bagi kesejahteraan dan kemajuan masyarakat, juga dapat memberikan dampak negatif dengan munculnya berbagai macam kejahatan dengan berbagai modus baru yang menggunakan komputer, jaringan, dan/atau perangkat yang terhubung dalam jaringan komputer sebagai media atau alat untuk melakukan kejahatan di dunia maya atau lebih sering dikenal dengan istilah “kejahatan siber” atau “*Cybercrime*”.

*Cybercrime* berasal dari kata *cyber* yang berarti dunia maya atau *internet* dan *crime* yang berarti kejahatan. Dengan kata lain, *cybercrime* adalah segala bentuk kejahatan yang terjadi di dunia maya atau internet. *Cybercrime* merupakan tindak kriminal yang dilakukan dengan menggunakan teknologi komputer sebagai alat kejahatan utama (Agus Rahardjo, 2002). *Cybercrime* yaitu kejahatan yang memanfaatkan perkembangan teknologi komputer khususnya internet. *Cybercrime* didefinisikan sebagai perbuatan melanggar hukum yang memanfaatkan teknologi komputer yang berbasis pada kecanggihan perkembangan teknologi internet (Budi Raharjo, 202). Andi Hamzah dalam bukunya “Aspek-aspek Pidana di Bidang Komputer” mendefinisikan “*kejahatan di bidang komputer secara umum dapat diartikan sebagai penggunaan komputer secara ilegal*” (Andi Hamzah, 1990). Di era modern sekarang ini, segala sesuatu dapat dilakukan dengan mudah melalui media elektronik yang terhubung dengan jaringan internet. Sehingga seseorang akan dengan mudah mengakses berbagai layanan yang tersedia secara online, termasuk diantaranya adalah mengakses layanan judi online ataupun pinjaman online. Seperti dalam :

1. kasus perkara nomor 438/Pid.Sus/2020/PN.Jkt.Utr. pihak korban merasa dirugikan karena data pribadinya telah disalahgunakan oleh pihak terdakwa yang memanfaatkan data pribadi yang disampaikan korban pada waktu mendaftar pinjaman online tersebut antara lain data pribadi seperti nama, alamat tinggal, alamat kantor, nomor telpon, slip gaji, NPWP, kartu keluarga, dan foto diri sendiri (*selfie*) korban dengan memegang KTP agar terlihat wajah korban. Akibat dari perbuatan si terdakwa tersebut, si korban merasa sangat dirugikan karena diharuskan membayar hutang berikut bunga pinjaman yang sangat besar dan diluar kesepakatan awal, diteror, diancam, di intimidasi, serta dipaksa untuk segera melunasi hutangnya tersebut.
2. kasus perkara di Pengadilan Negeri Kotabaru di Kalimantan Selatan Nomor 24/Pid.Sus/2022/PN.Ktb., Nomor 25/Pid.Sus/2022/PN. Ktb., dan Nomor 26/Pid.Sus/2022/PN. Ktb., dimana pelaku juga sama-sama mengintimidasi dan mengancam korbannya akan menyebarkan data pribadi korban secara online

dikarenakan tidak mampu ataupun telat dalam membayar pinjamannya.

3. Kemudian pada kasus perkara Nomor 24/Pid.Sus/2022/PN.Ktb. perbedaan kasus ini dgn yang sebelumnya terletak pada peran pelakunya saja dimana si terdakwa a.n. Donna Uly Novelya B. Sibuea berperan sebagai kepala cabang dari PT. Jasa Mudah Collectindo yang bergerak di bidang usaha jasa penagihan, dan pada perkara Nomor 25/Pid.Sus/2022/PN. Ktb. si terdakwa a.n. Shaun Murphy berperan sebagai penerjemah dan memfasilitasi aplikasi yang berbahasa Indonesia, serta pada perkara Nomor 26/Pid.Sus/2022/PN. Ktb. yang terdakwanya a.n. Kaharuddin berperan sebagai penagih hutang atau *debt collector*. Adapun akibat dari perbuatan para terdakwa tersebut tentunya telah menimbulkan kerugian bagi para korban, karena diharuskan membayar hutang berikut bunga pinjaman yang sangat besar, diteror, diancam, di intimidasi, dipaksa untuk segera melunasi hutangnya tersebut, dengan menyebarkan data pribadi para korban tanpa persetujuan dari para korban.

Sebenarnya masih banyak lagi kasus orang yang terjebak dengan kasus yang serupa, dan malah ada orang yang terjebak jeratan pinjaman online tersebut bermula dari awalnya terjerat judi online. Karena, bagi mereka yang sudah terjerat dan bahkan sudah kecanduan judi online, maka mereka akan menempuh segala cara untuk mendapatkan uang agar dapat bermain judi online tersebut. Dan jika mereka kalah dan kehabisan banyak uang, maka selanjutnya mereka akan lanjut terjebak dengan layanan pinjaman online, karena untuk mendapatkan pinjaman uang secara online tersebut sangat mudah dan tidak sesulit kalau mereka meminjam uang melalui bank. Adapun uang hasil pinjol tersebut bagi mereka yang sudah kecanduan tentunya akan mereka gunakan kembali untuk main judi online tersebut. Perlindungan hukum bagi korban *cybercrime* penyebaran data pribadi secara online sangat diperlukan, karena apabila suatu peristiwa pidana terjadi, aturan hukum sering kali memfokuskan diri untuk menghukum pelaku kejahatan sehingga seringkali korban dari kejahatan tersebut terabaikan. Padahal korban juga patut untuk diperhatikan karena pada dasarnya korban merupakan pihak yang dirugikan dalam suatu tindak pidana. Dampak kejahatan menimbulkan korban dan kerugian. Pada hakikatnya kejahatan haruslah dilihat sebagai sesuatu yang merugikan korban, sehingga pidana yang dijatuhkan kepada pelaku kejahatan juga memperhatikan kepentingan si korban dalam bentuk pemulihan terhadap kerugian yang dideritanya, tidak saja kerugian fisik namun juga kerugian non fisik (Dheny Wahyudi, 2019).

Upaya perlindungan korban sebenarnya sangat penting. Karena di samping dapat mengurangi penderitaan korban atas tindak pidana yang dialaminya, juga dapat mencegah terjadinya korban yang berkelanjutan. Oleh karena itu peneliti tertarik untuk melakukan kajian analisis yuridis terkait dengan pengaturan terhadap korban *cybercrime* penyebaran data pribadi secara online, khususnya dalam memberikan perlindungan hukum bagi para korban yang data pribadinya telah disalahgunakan tersebut.

## 2. KERANGKA TEORI

Teori Perlindungan Hukum, menurut Satjipto Raharjo Perlindungan hukum adalah upaya untuk melindungi kepentingan seseorang dengan mengalokasikan hak asasi manusia kepadanya (Raharjo S. , 2014) dan Teori ppidanaan pada umumnya dapat dikelompokkan

dalam 3 (tiga) golongan besar, yaitu teori absolut atau teori pembalasan (*vergeldings theorien*), teori relatif atau teori tujuan (*doel theorien*), dan teori menggabungkan (*verenigings theorien*) (E. Utrecht, 1958).

### 3. METODE PENELITIAN

Menurut (Ramlani Lina S, 2021) Penelitian (*research*) sesuai dengan tujuannya dapat didefinisikan sebagai usaha untuk menemukan, mengembangkan dan menguji kebenaran suatu pengetahuan. Penelitian dilakukan dengan menggunakan metode-metode ilmiah yang disebut dengan metodologi penelitian. Jenis penelitian yang digunakan adalah metode penelitian hukum normatif melalui data empiris dalam mengkaji dan menganalisis permasalahan hukum atas peraturan Perundang-Undangan yang berlaku (Marzuki, 2005). Teknik pengumpulan data yang dipergunakan melalui studi kepustakaan. Teknik Pengumpulan Bahan Hukum pada penelitian normatif dibatasi pada penggunaan studi dokumen atau bahan pustaka saja yaitu pada data hukum sekunder (Mamudji, 2009).

### 4. ANALISIS DAN PEMBAHASAN

Penelitian ini terdiri dari dua analisis, yakni Analisis tentang pengaturan terhadap korban *cybercrime* penyebaran data pribadi secara online di Indonesia dan Analisis tentang perlindungan hukum bagi korban *cybercrime* penyebaran data pribadi secara online di Indonesia.

#### **Pengaturan Terhadap Korban *Cybercrime* Penyebaran Data Pribadi Secara Online di Indonesia.**

Pengaturan hukum terhadap korban *cybercrime* yang melibatkan penyebaran data pribadi di Indonesia telah berkembang seiring dengan perubahan sosial, teknologi, dan kesadaran akan pentingnya privasi. Secara historis, perlindungan privasi di Indonesia berakar pada Pasal 28G ayat (1) UUD 1945 yang diamanatkan dalam amendemen kedua tahun 2000. Ketentuan ini mengakui hak setiap individu atas perlindungan privasi, kehormatan, martabat, serta rasa aman, yang menjadi landasan konstitusional untuk pembentukan regulasi lebih lanjut.

Langkah konkret pertama untuk menanggulangi kejahatan berbasis teknologi, termasuk penyebaran data pribadi, diwujudkan melalui Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE). Undang-undang ini menjadi tonggak awal dalam regulasi pemanfaatan teknologi informasi di Indonesia, meskipun pada saat itu belum secara eksplisit mengatur perlindungan data pribadi secara rinci. Perkembangan teknologi dan meningkatnya kejahatan siber kemudian mendorong pemerintah untuk memperbaiki UU ITE melalui dua kali revisi, yaitu Undang-Undang Nomor 19 Tahun 2016 dan Undang-Undang Nomor 1 Tahun 2024, yang mempertegas aspek pidana terkait penyalahgunaan data pribadi.

Sebagai respon terhadap kebutuhan perlindungan yang lebih spesifik, Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi (UU PDP) diterbitkan, menjadikan Indonesia lebih sejajar dengan negara-negara yang memiliki regulasi privasi data yang komprehensif, seperti General Data Protection Regulation (GDPR) di Uni Eropa. UU ini tidak hanya memberikan dasar hukum untuk melindungi data pribadi tetapi juga

mengatur sanksi pidana dan administratif terhadap pelanggaran, menjadikannya kerangka hukum yang komprehensif untuk melindungi individu dari penyalahgunaan data pribadi secara online.

Di sisi kebijakan, upaya perlindungan data pribadi juga diintegrasikan dengan kebijakan pembangunan teknologi digital di Indonesia. Program pemerintah seperti "Indonesia Digital 2024" menekankan pentingnya keamanan siber dan perlindungan data sebagai elemen fundamental dalam mendukung transformasi digital. Selain itu, pembentukan lembaga pengawas independen yang diamanatkan oleh UU PDP menjadi tonggak penting dalam memastikan implementasi kebijakan yang efektif dan akuntabel.

Dengan landasan konstitusional dan evolusi regulasi yang terus berkembang, pengaturan hukum terhadap korban cybercrime penyebaran data pribadi di Indonesia menunjukkan adanya komitmen untuk menjawab tantangan era digital. Meski demikian, penerapan di lapangan masih membutuhkan penyempurnaan, terutama dalam hal koordinasi antar-lembaga, pengawasan, serta peningkatan kesadaran publik tentang hak atas perlindungan privasi.

Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (ITE) merupakan tonggak awal dalam pengaturan kejahatan siber di Indonesia, termasuk perlindungan terhadap data pribadi. Perubahan yang dilakukan melalui Undang-Undang Nomor 19 Tahun 2016 dan terakhir dengan Undang-Undang Nomor 1 Tahun 2024 semakin memperkuat landasan hukum dalam menghadapi tantangan cybercrime yang terus berkembang. UU ITE memberikan payung hukum untuk mengatur berbagai aspek teknologi informasi, mulai dari transaksi elektronik hingga perlindungan privasi, yang menjadi isu krusial di era digital.

Pasal 26 ayat (1) dan (2) UU ITE secara tegas mengatur bahwa penggunaan data pribadi melalui media elektronik hanya dapat dilakukan dengan persetujuan dari pemilik data. Ketentuan ini memberikan perlindungan mendasar bagi hak privasi individu, mencerminkan pengakuan hukum atas hak setiap orang untuk menjaga kendali atas informasi pribadinya. Pelanggaran terhadap ketentuan ini bukan hanya melanggar norma hukum, tetapi juga menciptakan dasar hukum bagi korban untuk menuntut ganti rugi atas kerugian yang diderita, baik secara material maupun immaterial.

Regulasi ini juga memberikan mekanisme penyelesaian sengketa melalui jalur hukum, yang mencakup gugatan perdata dan tuntutan pidana terhadap pelaku. Dengan adanya ketentuan ini, korban cybercrime, termasuk penyebaran data pribadi tanpa izin, memiliki akses yang lebih jelas terhadap keadilan dan perlindungan hukum. Hal ini sejalan dengan tujuan UU ITE untuk menciptakan ruang digital yang aman dan menjamin rasa keadilan di tengah pesatnya perkembangan teknologi informasi.

Lebih jauh, penegasan pada persetujuan pemilik data dalam Pasal 26 menunjukkan pentingnya prinsip *consent* sebagai dasar pengelolaan data pribadi. Prinsip ini sejalan dengan standar internasional seperti General Data Protection Regulation (GDPR) di Uni Eropa, menempatkan Indonesia pada jalur yang tepat dalam membangun tata kelola data yang bertanggung jawab. Dalam konteks ini, UU ITE tidak hanya menjadi instrumen hukum, tetapi juga sarana edukasi untuk meningkatkan kesadaran masyarakat tentang pentingnya perlindungan data pribadi.

Namun, meskipun sudah ada landasan hukum yang kuat, implementasi di lapangan memerlukan dukungan dari berbagai pihak, termasuk pemerintah, penegak hukum, dan masyarakat. Penegakan hukum yang konsisten dan penguatan kelembagaan menjadi kunci agar ketentuan Pasal 26 UU ITE benar-benar dapat melindungi individu dari kejahatan siber yang kian kompleks.

Sebagai pelengkap, Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi (UU PDP) secara spesifik mengatur perlindungan data pribadi sebagai bagian dari hak asasi manusia. Dalam konteks teori perlindungan hukum menurut Satjipto Rahardjo, UU PDP mencerminkan upaya negara untuk memberikan perlindungan preventif dan represif. Perlindungan preventif terlihat dari pengaturan mekanisme penyelesaian sengketa melalui jalur non-penal, seperti mediasi, yang bertujuan menyelesaikan konflik secara damai tanpa harus melibatkan proses hukum formal. Sementara itu, perlindungan represif diwujudkan melalui jalur penal dengan ancaman sanksi pidana seperti hukuman penjara hingga lima tahun atau denda maksimal lima miliar rupiah, yang berfungsi untuk memberikan efek jera kepada pelaku dan melindungi korban dari potensi pelanggaran serupa di masa depan. Pendekatan ini selaras dengan pandangan Rahardjo, di mana hukum tidak hanya berfungsi sebagai perangkat aturan, tetapi juga sebagai sarana untuk mencapai keadilan sosial dan melindungi kepentingan individu dalam masyarakat.

Kemudian dalam Undang-Undang Nomor 31 Tahun 2014 tentang Perlindungan Saksi dan Korban memberikan perlindungan khusus bagi korban cybercrime, termasuk mereka yang terkena dampak pelanggaran data pribadi. Hak-hak korban, seperti keamanan pribadi, akses ke proses peradilan, dan bantuan hidup sementara, menunjukkan bahwa hukum tidak hanya fokus pada penghukuman pelaku, tetapi juga pada pemulihan kondisi korban. Dalam perspektif teori pemidanaan menurut E. Utrecht, perlindungan korban ini dapat dipandang sebagai bagian dari tujuan pemidanaan yang mencakup aspek retributif, preventif, dan rehabilitatif. Sanksi terhadap pelaku tidak hanya berfungsi sebagai balasan atas perbuatan melawan hukum (retributif), tetapi juga sebagai langkah preventif untuk mencegah pelanggaran di masa depan dan rehabilitatif untuk membantu korban kembali ke kondisi yang stabil.

Namun, meskipun regulasi ini telah memberikan kerangka hukum dasar, UU ITE dan UU PDP masih memerlukan pengaturan tambahan yang lebih rinci mengenai hak-hak korban cybercrime. Dalam teori perlindungan hukum, ketidakjelasan pengaturan dapat menyebabkan ketimpangan dalam implementasi, yang mengakibatkan perlindungan hukum menjadi tidak optimal. Oleh karena itu, diperlukan revisi dan harmonisasi undang-undang untuk memastikan bahwa perlindungan korban cybercrime, termasuk perlindungan data pribadi, terjamin secara komprehensif.

Implementasi dari ketiga undang-undang ini menunjukkan komitmen pemerintah untuk menciptakan sistem hukum yang adaptif terhadap perkembangan teknologi dan tantangan kejahatan siber. Namun, dalam pandangan E. Utrecht, efektivitas pemidanaan tidak hanya bergantung pada ketegasan hukum, tetapi juga pada bagaimana masyarakat memahami dan mendukung hukum tersebut. Oleh karena itu, kolaborasi antar-lembaga, pelatihan aparat penegak hukum, dan peningkatan kesadaran publik tentang pentingnya perlindungan data pribadi menjadi faktor kunci untuk mewujudkan keadilan substantif.

Dalam jangka panjang, revisi dan harmonisasi undang-undang yang mempertimbangkan aspek perlindungan hukum dan pemidanaan dapat memperkuat kerangka hukum di Indonesia. Hal ini penting untuk menciptakan keadilan bagi korban, meningkatkan efektivitas hukum dalam mencegah kejahatan siber, serta membangun kepercayaan masyarakat terhadap sistem hukum nasional. Dengan demikian, hukum tidak hanya menjadi alat pengendalian sosial, tetapi juga sarana untuk mewujudkan keadilan dan perlindungan bagi semua pihak.

### **Perlindungan Hukum Bagi Korban *Cybercrime* Penyebaran Data Pribadi Secara Online di Indonesia.**

Maraknya kasus penyebaran data pribadi secara online di Indonesia, terutama yang melibatkan pinjaman online ilegal, telah menimbulkan tantangan serius dalam memberikan perlindungan hukum bagi korban. Fenomena ini tercermin dalam berbagai kasus seperti putusan pengadilan Nomor 24/Pid.Sus/2022/PN.Ktb., Nomor 25/Pid.Sus/2022/PN.Ktb., dan Nomor 26/Pid.Sus/2022/PN.Ktb., di mana pelaku penyebaran data pribadi seringkali memanfaatkan ketergantungan masyarakat terhadap layanan digital untuk memanipulasi dan menekan korban. Dengan meningkatnya kebutuhan masyarakat akan pinjaman online selama pandemi, terutama dari platform yang tidak terdaftar secara resmi, pelanggaran data pribadi menjadi isu yang semakin mendesak untuk ditangani.

Korban dari kasus-kasus ini tidak hanya mengalami kerugian materiil berupa biaya yang harus dibayarkan untuk melunasi pinjaman, tetapi juga tekanan mental yang berat. Ancaman penyebaran data pribadi oleh pihak-pihak yang tidak bertanggung jawab menciptakan ketakutan yang mendalam bagi korban dan keluarga mereka. Misalnya, dalam salah satu kasus, korban mengalami intimidasi berupa ancaman distribusi data kontak pribadi kepada orang-orang terdekat jika kewajiban pinjaman tidak dipenuhi. Tindakan ini tidak hanya melanggar privasi tetapi juga memengaruhi stabilitas emosional korban, yang menunjukkan bahwa dampak dari *cybercrime* semacam ini jauh melampaui aspek finansial.

Kasus-kasus tersebut menyoroti kelemahan dalam penegakan hukum terkait perlindungan data pribadi. Meskipun Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) dan Undang-Undang Pelindungan Data Pribadi (UU PDP) telah mengatur ancaman pidana bagi pelaku, hukuman yang dijatuhkan sering kali tidak maksimal. Contohnya, dalam beberapa kasus, pelaku hanya dikenakan hukuman ringan, yang tidak memberikan efek jera. Selain itu, korban jarang menerima pemulihan langsung atas kerugian yang mereka alami, baik dalam bentuk kompensasi materiil maupun dukungan psikologis.

Fenomena ini menegaskan perlunya perlindungan hukum yang lebih komprehensif. Pendekatan yang hanya berfokus pada menghukum pelaku perlu dilengkapi dengan mekanisme pemulihan yang memberikan manfaat langsung kepada korban. Sebagai langkah awal, revisi terhadap UU ITE dapat mencakup penambahan ketentuan pidana tambahan, seperti perampasan keuntungan yang diperoleh pelaku dari tindak pidana dan pembayaran ganti rugi kepada korban, sebagaimana diatur dalam Pasal 69 UU PDP. Hal ini tidak hanya akan memberikan rasa keadilan tetapi juga membantu korban untuk pulih dari dampak kejahatan.

Selain itu, pemerintah dan penegak hukum perlu meningkatkan konsistensi dalam

penegakan aturan. Sistem peradilan pidana yang terpadu dan kolaboratif di antara kepolisian, kejaksaan, dan pengadilan dapat memastikan bahwa pelaku cybercrime menerima hukuman yang sesuai, sementara korban mendapatkan keadilan yang layak. Langkah-langkah ini, jika diterapkan dengan baik, dapat menciptakan efek jera yang lebih kuat sekaligus meningkatkan kepercayaan masyarakat terhadap sistem hukum di Indonesia

Dalam konteks teori perlindungan hukum, negara memiliki tanggung jawab untuk memberikan rasa aman kepada masyarakat melalui pengaturan dan penegakan hukum yang tegas. Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE), bersama dengan perubahan dalam Undang-Undang Nomor 19 Tahun 2016 dan Undang-Undang Nomor 1 Tahun 2024, serta Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi (UU PDP), telah menjadi kerangka hukum utama dalam menangani kasus cybercrime. Ketentuan dalam Pasal 26 UU ITE dan Pasal 65 UU PDP menegaskan bahwa penyebaran data pribadi tanpa persetujuan adalah tindakan melanggar hukum yang dapat dijatuhi sanksi pidana. Namun, sanksi tersebut, seperti pidana penjara hingga enam tahun dan denda maksimal satu miliar rupiah, belum memberikan dampak langsung kepada korban.

Menurut teori pemidanaan, sebagaimana disampaikan oleh Prof. Romli Atmasasmita, tujuan pemidanaan tidak hanya untuk menghukum pelaku tetapi juga untuk memberikan keadilan dan pemulihan bagi korban. Namun, dalam praktiknya, hukuman bagi pelaku cybercrime di Indonesia masih jauh dari optimal. Rata-rata pelaku hanya dijatuhi hukuman penjara di bawah dua tahun dan sering kali tidak dikenakan denda. Hal ini menunjukkan bahwa perlindungan hukum bagi korban belum sepenuhnya terwujud. Idealnya, sanksi pidana harus mencakup pidana tambahan seperti perampasan keuntungan atau harta kekayaan yang diperoleh dari tindak pidana serta pembayaran ganti kerugian bagi korban, sebagaimana diatur dalam Pasal 69 UU PDP.

Selain sanksi pidana, pemerintah juga perlu meningkatkan upaya preventif melalui penyuluhan dan edukasi masyarakat. Kesadaran masyarakat terhadap pentingnya melindungi data pribadi harus ditingkatkan melalui program sosialisasi yang melibatkan berbagai pihak, termasuk pemerintah, media, dan institusi pendidikan. Meskipun program penyuluhan sudah dilakukan oleh dinas terkait, dampaknya masih belum signifikan. Banyak korban yang masih tidak menyadari pentingnya menjaga kerahasiaan data pribadi mereka. Dalam hal penegakan hukum, kolaborasi antar-lembaga penegak hukum sangat diperlukan untuk memastikan keadilan bagi korban. Proses hukum yang konsisten dari penyelidikan hingga vonis pengadilan harus memastikan bahwa pelaku mendapatkan hukuman yang setimpal, sementara korban mendapatkan pemulihan yang adil. Penegakan hukum yang tegas dan transparan tidak hanya akan memberikan efek jera bagi pelaku tetapi juga membangun kepercayaan masyarakat terhadap sistem peradilan.

Ke depan, revisi terhadap UU ITE diperlukan untuk menambahkan ketentuan pidana tambahan yang memberikan manfaat langsung bagi korban. Selain itu, harmonisasi dengan UU PDP dan penerapan sistem peradilan pidana terpadu (Integrated Criminal Justice System) akan memperkuat perlindungan hukum. Dengan langkah ini, diharapkan rasa keadilan dan kepastian hukum bagi korban cybercrime penyebaran data pribadi di

Indonesia dapat tercapai secara lebih optimal.

## 5. PENUTUP / KESIMPULAN

Pengaturan terhadap korban *cybercrime* penyebaran data pribadi secara online di Indonesia telah diatur berdasarkan Undang-Undang No. 1 tahun 2024 Tentang Perubahan Kedua Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik (UU ITE), yang sanksi pidananya lebih mengedepankan penghukuman kepada si pelaku untuk memberikan efek jera saja, dan belum memberikan dampak atau manfaat langsung bagi korban.

Dalam rangka memberikan perlindungan hak asasi manusia bagi korban *cybercrime* penyebaran data pribadi secara online di Indonesia, selain dikenakan pidana penjara dan/atau denda, kepada pelaku dapat pula dikenakan pidana tambahan berupa perampasan keuntungan dan/atau harta kekayaan yang diperoleh atau hasil dari tindak pidana, dan pembayaran ganti kerugian bagi korban.

## SARAN

Untuk mewujudkan *Integrated Criminal Justice System*, para penegak hukum tidak hanya mengenakan sanksi pidana penjara dan/atau denda kepada pelaku, namun dapat pula mengenakan sanksi pidana tambahan yang dapat memberikan dampak atau manfaat langsung bagi korban.

Dewan Perwakilan Rakyat dan Presiden perlu melakukan revisi terhadap UU ITE khususnya dengan menambahkan ketentuan pidana tambahan berupa perampasan keuntungan dan/atau harta kekayaan yang diperoleh atau hasil dari tindak pidana dan pembayaran ganti kerugian

## DAFTAR PUSTAKA

- Abdul Wahid dan Mohammad Labib, *Kejahatan Mayantara (Cyber Crime)*, Refika Aditama, Bandung, 2005.
- Agus Rahardjo, *Cybercrime Pemahaman dan Upaya Pencegahan Kejahatan Berteknologi*, PT. Citra Aditya Bakti, Bandung, 2002.
- Amiruddin dan Zainal Asikin, *Pengantar Metode Penelitian Hukum*, Grafitti Press, Jakarta, 2006.
- Andi Hamzah, *Aspek-aspek Pidana di Bidang Komputer*, Sinar Grafika, Jakarta, 1990.
- Arif Gosita, *Masalah Korban Kejahatan*. Akademika Pressindo, Jakarta, 1993.
- Budi Raharjo, *Memahami Teknologi Informasi*, Elexmedia Komputindo, Jakarta, 2002.
- Budi Raharjo, *Memahami Teknologi Informasi*, Elexmedia Komputindo, Jakarta, 2002.
- Dheny Wahyudi, *Perlindungan Hukum Terhadap Korban Kejahatan Cybercrime Di Indonesia*, Jurnal Ilmu Hukum, 2019.
- E. Utrecht, *Hukum Pidana I*, Universitas Jakarta, Jakarta, 1958.
- G.S. Ramadhani, Arief B.N., & Purwoto, *Sistem Pidana Dan Tindakan "Double Track System" dalam Hukum Pidana Di Indonesia*, Diponegoro Review, Vol. 1, No.4, 2012.
- John M. Echols dan Hassan Shadily, *Kamus Inggris-Indonesia*, Gramedia Pustaka Utama, Jakarta, 2003.
- Josua Sitompul, *Cyberspace, Cybercrimes, Cyberlaw: Tinjauan Aspek Hukum Pidana*, Jakarta,

Rajawali Pers, 2012.

Leonardo Latsiano Dade, Caecilia J. J. Waha, Nurhikmah Nachrawy, *Kajian Yuridis Tentang Tindak Pidana Penyebaran Data Pribadi Melalui Internet (Doxing) Di Indonesia*, Jurnal Fakultas Hukum Universitas Sam Ratulangi Lex Privatum, Vol. 13 No.3 Feb 2024.

Lili Rasjidi dan Ida Bagus Wyasa Putra, *Hukum Sebagai Suatu Sistem*, CV Mandar Maju, Bandung, 2003.

M. Solly Lubis, *Filsafat Ilmu dan Penelitian*, Mandar Maju, Bandung, 2014.

Peter Mahmud Basuki, *Penelitian Hukum*, Kencana, Jakarta, 2011.

Satjipto Raharjo, *Ilmu Hukum*, PT. Citra Aditya Bakti, Bandung, 2014.

Soerjono Soekanto dan Sri Mamudji, *Penelitian Hukum Normatif-Suatu Tinjauan Singkat*, Rajawali Press, Jakarta, 2017.

Soerjono Soekanto, *Pengantar Penelitian Hukum*, Universitas Indonesia Press, Jakarta, 2010, hlm. 122.

Sudarto, *Kapita Selekta Hukum Pidana*, Alumni, Bandung, 1981.

Sugiyono, *Metode Penelitian Kuantitatif dan R&D, Cet. III*, Alfabeta, Bandung, 2007.

#### **Perundangan :**

Undang-Undang Dasar Negara Republik Indonesia Tahun 1945.

Kitab Undang-Undang Hukum Pidana, UU No. 73 Tahun 1958, LN Tahun 1958 No. 127, TLN No. 1660.

Undang-Undang Tentang Kitab Undang-Undang Hukum Pidana, UU No. 1 Tahun 2023, LN Tahun 2023 No. 1, TLN No. 6842.

Undang-Undang Tentang Informasi Dan Transaksi Elektronik, UU No. 11 Tahun 2008, LN Tahun 2008 No. 58, TLN No. 4843.

Undang-Undang Tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik, UU No. 19 Tahun 2016, LN Tahun 2016 No. 251, TLN No. 5952.

Undang-Undang Tentang Perubahan Kedua Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik, UU No. 1 Tahun 2024, LN Tahun 2024 No. 1, TLN No. 6905.

Undang-Undang Tentang Pelindungan Data Pribadi, UU No. 27 Tahun 2022, LN Tahun 2022 No. 196, TLN No. 6820.

Undang-Undang tentang Perubahan Atas Undang-Undang Nomor 13 Tahun 2006 Tentang Perlindungan Saksi Dan Korban, UU No. 31 Tahun 2014, LN Tahun 2014 No. 293, TLN No. 5602.

Undang-Undang Tentang Hak Asasi Manusia, UU No. 39 Tahun 1999, LN Tahun 1999 No. 165, TLN No. 3886.

Peraturan Pemerintah tentang Kompensasi, dan Rehabilitasi Terhadap Korban Pelanggaran Hak Asasi Manusia Yang Berat, PP No. 3 Tahun 2002, LN Tahun 2002 No. 7, TLN No. 4172