

## **KEBOCORAN DATA PRIBADI MELALUI FITUR STICKER DI DALAM PLATFORM INSTAGRAM**

*Adetya Firnanda<sup>1</sup>, Revita Pirena Putri<sup>2</sup>, Mriya Afifah Furqania<sup>3</sup>*

*Program Studi Ilmu Hukum, Fakultas Hukum, Universitas 17 Agustus 1945 Surabaya*

*e-mail: [1adafira616@gmail.com](mailto:1adafira616@gmail.com), [2rpirena27@gmail.com](mailto:2rpirena27@gmail.com), [3mafifah67@gmail.com](mailto:3mafifah67@gmail.com)*

### **Abstrak**

*Penelitian ini bertujuan untuk mengetahui aturan-aturan yang berkaitan dengan perlindungan data pribadi dan sistem elektronik serta mencari tahu mengenai upaya-upaya penyelenggara sosial media sebagai penyelenggara sistem elektronik untuk melindungi data pribadi penggunanya. Kebaruan yang ditawarkan dalam penelitian ini adalah pencarian upaya penyelenggara sosial media untuk memberikan perlindungan data pribadi terhadap fitur-fitur yang disediakan dengan menggunakan metode studi kepustakaan dengan meneliti beberapa peraturan perundang-undangan dan didukung dengan bahan sekunder dari banyak referensi. Penelitian ini beranjak dari adanya kasus penyalahgunaan data pribadi melalui fitur yang disediakan di salah satu media sosial yaitu Instagram. Fitur tersebut digunakan untuk mencari data pribadi penggunanya seperti gambar diri, nama panggilan, dan data penting lainnya yang kemudian dicuri dan disalahgunakan oleh pihak ketiga. Terlihat dalam beberapa peraturan perundang-undangan salah seperti Undang-Undang No. 11 Tahun 2008 jo Undang-Undang No 19 Tahun 2016 mengenai Informasi dan Transaksi Elektronik dan peraturan pelaksanaannya mengisyaratkan adanya perlindungan data pribadi baik dari pencurian maupun penyalahgunaan serta kewajiban baik penyelenggara maupun pengguna sistem elektronik. Berdasarkan hal tersebut maka dibutuhkan sebuah upaya khususnya dari penyelenggara media sosial sebagai penyelenggara sistem elektronik untuk mengaktifkan fitur-fitur tertentu yang dapat melindungi para penggunanya seperti pengaktifan fitur anti cuplikan layar hingga verifikasi data.*

**Kata kunci: Perlindungan Data Pribadi, Fitur Sosial Media, Pertanggungjawaban Hukum**

### **1. PENDAHULUAN**

Indonesia sebagai negara dengan populasi penduduk terbesar keempat di dunia sekira 272 juta penduduk per Juni 2021 tentu menjadi sebuah negara yang sangat potensial sebagai tempat untuk mengembangkan dan mempopulerkan suatu sistem elektronik yang dikenal sebagai media sosial. Hal ini terbukti dengan jumlah pengguna aktif media sosial di Indonesia yang mencapai 170 Juta orang per Januari 2021 menurut data yang dilansir oleh Hootsuite.com. Ini menunjukkan betapa besarnya pangsa pasar Indonesia bagi media sosial untuk mengembangkan produknya disini.

Namun demikian bukan berarti penggunaan media sosial di Indonesia terlepas dari permasalahan. Sering kali permasalahan mengenai terjadinya kebocoran data pribadi pengguna kepada pihak ketiga. Data pribadi yang bocor ini sering kali digunakan untuk berbagai tindakan yang merugikan seperti penipuan, dan berbagai kejahatan-kejahatan yang berkaitan dengan penggunaan data pribadi untuk melancarkan aksinya.

Terutamanya ditengah kondisi pandemic Covid-19 yang melanda dunia, mengakibatkan adanya pembatasan kegiatan di dunia nyata maka banyak kegiatan manusia dialihkan secara daring termasuk pula untuk bersosialisasi. Sebagai contoh adalah perbandingan peningkatan pengguna media sosial Instagram di Indonesia. Menurut data Hootsuite.com, jumlah pengguna Instagram di Indonesia per Januari 2021 mencapai 85 juta pengguna. Sedangkan menurut laporan dari Napoleon Cat, per Oktober 2021 pengguna Instagram di Indonesia mencapai jumlah 91 juta orang. Dapat dilihat bahwa dalam jangka waktu tersebut terdapat peningkatan jumlah pengguna sebesar 6 juta pengguna. Besarnya jumlah pengguna Instagram di Indonesia tentunya menjadi suatu fakta yang kemudian menimbulkan kekhawatiran mengenai bagaimana keamanan data pribadi pengguna di Indonesia terhadap kemungkinan kebocoran data pribadi kepada pihak ketiga.

Pada bulan November 2021, muncul suatu tren di Instagram melalui fitur sticker yaitu “Add Yours” dimana penggunanya dapat mengikuti atau memulai sebuah tantangan atau *challenge*. Tantangan ini kemudian dilanjutkan oleh pengguna Instagram lainnya. Adapun tantangan tersebut berupa berbagi informasi apa pun dalam bentuk teks maupun foto. Informasi yang lazim dijadikan sebagai tantangan atau *challenge* adalah nama panggilan, di mana kota lahir, foto masa kecil, dan lain sebagainya. Dan, siapa saja bisa mengikuti dan memulai tantangan atau *challenge* ini.

Namun, dari tren penggunaan fitur stiker “Add Yours” ini kemudian menimbulkan suatu permasalahan dimana data pribadi yang ada dalam tantangan atau *challenge* ini kemudian disalahgunakan oleh pihak ketiga. Dikutip dari Antara, akun Twitter @ditamoechtar\_ berbagi kisah temannya yang ditelepon pelaku *phising*. Pelaku memanggil orang itu menggunakan nama panggilan dekat. Rupanya, sang teman secara tidak sadar mengikuti tren “Add Yours Instagram” dengan menyebutkan “variasi nama panggilanmu”. Kasus yang muncul ini hanya merupakan satu kejadian yang kemudian disampaikan ke publik dan masih banyak lagi kasus-kasus yang kemudian mungkin tidak disampaikan atau mendapatkan perhatian dari publik.

Kemudian jika menilik dari aturan hukum yang ada di Indonesia dalam hal ini adalah Undang-Undang No. 11 Tahun 2008 jo Undang-Undang No 19 Tahun 2016. Dalam undang-undang ini belum mengatur mengenai bagaimana perlindungan terhadap data pribadi dan pertanggungjawaban hukum oleh penyedia layanan media sosial yang kemudian mengakibatkan terjadinya kebocoran data pribadi kepada pihak ketiga dengan menggunakan fitur-fitur yang disediakan penyedia layanan media sosial itu sendiri. Juga berdasarkan fakta bahwa penduduk Indonesia, terutama pengguna layanan media sosial masih belum seluruhnya sadar akan pentingnya untuk menjaga kerahasiaan data pribadi yang dimilikinya.

Perbandingan penelitian pertama menghasilkan jawaban bahwa Di Indonesia terkait perlindungan hukum terhadap data pribadi masih dipandang belum optimal, hal tersebut dapat dilihat dari masih banyaknya penyalahgunaan data pribadi seseorang tanpa sepengetahuan dari pemiliknya yang diakibatkan kurang ketatnya pengamanan dan pengawasan dari pihak-pihak pengguna data. Upaya pengaturan terkait hak privasi atas data pribadi merupakan perwujudan atas pengakuan dan perlindungan hak-hak dasar manusia. Oleh karenanya, penyusunan Rancangan Undang-Undang tentang Perlindungan Data pribadi mempunyai landasan filosofis yang kuat serta dapat dipertanggungjawabkan. Landasan filosofis yang dimaksud adalah Pancasila yang merupakan *rechtsidee* (cita hukum) serta gagasan untuk mewujudkan hukum kepada yang dicita-citakan. (Situmeang, 2021).

Kemudian pada penelitian yang kedua yang masih relevan dengan penelitian penulis memberikan jawaban bahwa Indonesia belum memiliki peraturan perundang-undangan yang secara khusus mengatur mengenai perlindungan data pribadi. Pemerintah Indonesia dituntut untuk melindungi masyarakat dan mengatur masalah perlindungan atas data pribadi dan menyiapkan berbagai bentuk perlindungan hukum. Selain itu, dalam Undang-Undang Nomor 17 Tahun 2007 tentang Rencana Pembangunan Jangka Panjang 2005-2025 juga telah ditentukan bahwa untuk mewujudkan bangsa yang berdaya saing harus meningkatkan pemanfaatan ilmu pengetahuan dan teknologi. Salah satunya melalui peraturan yang terkait dengan privasi. Dalam konteks model pengaturan perlindungan data pribadi di Indonesia, dapat diterapkan khususnya dengan melihat model pengaturan di Uni Eropa melalui *EU General Data Protection Regulation* (EU GDPR) yang meliputi ruang lingkup: (1) pengaturan prinsip, (2) adanya pembagian/klasifikasi data pribadi umum dan khusus, (3) Hak-Hak pemilik Data Pribadi, (4) Pengendali dan pemroses data pribadi, (5) Kode Etik dan sertifikasi, (6) Transfer data pribadi ke negara lain atau organisasi internasional, (7) Otoritas pengawas yang Independen, dan (8) Ganti Rugi dan Pertanggung jawaban, sanksi (Niffari, 2020).

Selanjutnya pada penelitian yang ketiga memunculkan jawaban bahwa hakikat dari hak privasi terhadap data pribadi adalah hak konstitusional warga negara Indonesia yang telah diatur dalam UUDNRI Tahun 1945 khususnya pada pasal 28 huruf G ayat (1). Bentuk perlindungan hukum terhadap data pribadi sebagai privasi di Indonesia saat ini menerapkan beberapa pasal yang tersirat mengatur mengenai data pribadi. Indonesia belum memiliki peraturan perundang – undangan khusus yang menjadi dasar hukum perlindungan data pribadi sehingga saat ini Indonesia memiliki kekosongan norma. (Kusnadi and Wijaya, 2021)

Berdasarkan penelitian – penelitian yang masih relevan yang peneliti gunakan, maka peneliti merumuskan satu rumusan masalah yakni bagaimana perlindungan dan pertanggungjawaban hukum terhadap data pribadi yang bocor kepada pihak ketiga melalui fitur-fitur yang disediakan oleh penyedia layanan media sosial.

## 2. METODE PENELITIAN

Menggunakan penelitian normatif dan konseptual dengan menggunakan peraturan perundang-undangan sebagai bahan hukum primer yang ditunjang dengan studi kepustakaan terhadap bahan hukum sekunder untuk menemukan konsep-konsep yang relevan dengan penelitian ini (Marzuki, 2017).

### 3. HASIL PENELITIAN DAN PEMBAHASAN

#### 3.1 Perlindungan dan Pertanggungjawaban dalam Kasus Perlindungan Data Pribadi

Berkaca dari kasus yang tengah viral di Instagram bahwa adanya penyalahgunaan data pribadi yang dicuri melalui salah satu fitur Instagram, maka negara wajib memberikan perlindungan terhadap masyarakat dengan membuat aturan-aturan mengenai perlindungan data pribadi dan sistem elektronik. Dasar dari peraturan perundang-undangan yang telah ada yaitu Undang-Undang Dasar Negara Republik Indonesia Tahun 1945 Pasal 28G Ayat (1) yang menyatakan bahwa diri pribadi, keluarga, kehormatan, dan harta benda yang ada dibawah kekuasaannya merupakan hak yang perlu dilindungi. Setiap orang juga berhak atas rasa aman dan perlindungan dari ancaman ketakutan untuk berbuat atau tidak berbuat sesuatu yang merupakan hak asasi. (Niffari) Bunyi dari pasal tersebut mengisyaratkan untuk mengadakan peraturan perundang-undangan lain agar perlindungan terhadap data pribadi dapat berjalan dengan semestinya.

Adapun peraturan yang mengatur mengenai kewajiban penyelenggara sistem elektronik dalam melindungi data pribadi yaitu pada Undang-Undang No. 11 Tahun 2008 jo Undang-Undang jo 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik (UU ITE) serta peraturan pelaksanaannya adalah Peraturan Pemerintah No. 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik (PP PSTE) dan Peraturan Menteri Komunikasi dan Informatika No. 20 Tahun 2016 tentang Perlindungan Data Pribadi (Permen PDP). Undang-Undang ITE mengisyaratkan tentang adanya persetujuan orang yang bersangkutan terhadap penggunaan sistem informasi dan bila terjadi hal-hal yang tidak diinginkan maka penyelenggara sistem elektronik wajib menghapus informasi/dokumen elektronik. Lebih lanjut mengenai pelaksanaannya disebutkan dalam PP PSTE Pasal 12 bahwa untuk mencegah terjadinya penyalahgunaan data maka penyelenggara sistem elektronik wajib menerapkan manajemen resiko terhadap kerugian yang akan timbul. Manajemen resiko ini harus dilaksanakan penyelenggara sistem elektronik dengan menganalisis resiko dan menanggulangi ancaman atau kerugian yang akan terjadi.

Upaya untuk mencegah ini dapat pula dilakukan dengan kewajiban penyelenggara sistem informasi untuk memberikan edukasi kepada pengguna sistem elektronik. Salah satu edukasi yang perlu dilakukan adalah untuk tidak menyebarkan data pribadi yang sangat penting mereka dan berhati-hati dalam memilah data yang akan mereka sebar. Edukasi juga bisa mengenai berbagai modus kejahatan dalam dunia *cyber* bilamana mereka menyebarkan data pribadi mereka secara tidak aman. Kewajiban ini disebutkan dalam PP PSTE Pasal 28. Edukasi yang dimaksud termasuk pula hak, kewajiban tanggung jawab seluruh pihak terkait serta prosedur pengajuan komplain.

Adapun kewajiban penyelenggara sistem yang disebutkan dalam Pasal 30 Ayat (1) PP PSTE yaitu kewajiban untuk menyediakan fitur sesuai dengan karakteristik sistem elektronik demi melindungi hak ataupun kepentingan pengguna sistem elektronik. Lebih lanjut dikatakan bahwa fitur-fitur ini paling sedikit menerapkan fasilitas yang ada dalam Ayat (2) salah satunya untuk melakukan koreksi. Tak hanya pencegahan, namun juga terdapat aturan mengenai penanggulangan. Pun dalam Pasal 14 disebutkan bahwa penyelenggara sistem elektronik mempunyai kewajiban untuk melaksanakan prinsip perlindungan data pribadi yaitu salah satunya dalam memproses data pribadi harus dilakukan dengan melindungi keamanan data dari penyalahgunaan data pribadi.

Dalam PP PSTE disebutkan mengenai kewajiban penyelenggara sistem elektronik untuk menghapus dan mengeluarkan dari mesin pencari bilamana informasi/dokumen elektronik tersebut tidak relevan. Tidak relevan yang dimaksud terjadi bilamana diperoleh/diproses tidak atas persetujuan pemilik, diperoleh dengan cara melawan hukum serta ditampilkan oleh penyelenggara sistem elektronik yang mengakibatkan kerugian bagi pemilik data pribadi. Disini dapat dikaitkan dengan kasus yang sedang terjadi bahwa diperoleh dengan melawan hukum tersebut adalah pihak ketiga mencuri data pribadi seseorang.

Bilamana terjadi pelanggaran terhadap data pribadi, maka Undang-Undang ITE menyebutkan beberapa bentuk penegakan hukum yaitu sanksi pidana, gugatan keperdataan serta Altefnatif Penyelesaian Sengketa. Adapun beberapa ketentuan sanksi dijelaskan sebagai berikut: (Hertianto)

- a) Sanksi pidana terhadap akses secara tanpa hak atau melawan hukum terhadap komputer atau sistem elektronik untuk mendapatkan informasi elektornik;
- b) Sanksi pidana terhadap perbuatan tanpa hak atau melawan hukum mengubah, merusak, menghilangkan, memindahkan, membuka atau menyembunyikan Informasi Eketronik dan/atau Dokumen Elektronik;
- c) Gugatan perdata terhadap pihak yang menimbulkan kerugian atau melanggar hak;
- d) Mekanisme alternatif penyelesaian sengketa yang dapat dilakukan selain mengajukan gugatan perdata.

Pencurian data pribadi ini berkaitan dengan aturan penegakan hukum dalam Undang-Undang ITE mengenai perbuatan yang dilarang yaitu pada Pasal 30 Ayat (2) UU ITE yang menyebutkan bahwa setiap orang dengan sengaja tanpa hak atau melawan hukum mengakses sistem elektronik dengan cara apapun dengan tujuan memperoleh informasi/dokumen elektronik. Melihat pasal ini maka pelaku pencurian data pribadi telah memenuhi unsur Pasal 30 Ayat (2) UU ITE. Kalimat "dengan cara apapun" dapat dimaksud menggunakan sistem elektronik baik dengan menggunakan software tertentu atau tidak yang tujuannya adalah mencuri data atau informasi seseorang. Hal ini sesuai dengan ketentuan Pasal 46 Ayat (2) bahwa pelaku dapat dikenakan sanksi pidana penjara paling lama 7 (tujuh) tahun dan/atau denda paling banyak Rp. 700.000.000,00 (tujuh ratus juta rupiah). Pelaku tindak pidana pencurian data melalui *cyber* ini seharusnya wajib untuk memberikan restitusi dan kompensasi pada korban sebagai bentuk pertanggungjawabannya. (Putra, R. Caesalino W & Widiatja)

### 3.2 Penerapan fitur Pengamanan Instagram sebagai Upaya Perlindungan Data Pribadi

Data pribadi merupakan data penting yang dimiliki oleh setiap orang. Mengacu pada Peraturan Menteri Komunikasi dan Informatika Nomor 20 Tahun 2016 tentang Perlindungan Data Pribadi Dalam Sistem Elektronik, menyebutkan bahwa data pribadi merupakan data perseorangan yang wajib dijaga serta dilindungi kerahasiaannya. Di dalam data pribadi mencakup fakta-fakta, komunikasi atau pendapat yang berkaitan dengan individu yang merupakan informasi yang sifatnya rahasia, pribadi atau sensitif sehingga pribadi yang bersangkutan ingin menyimpan atau membatasi orang lain untuk mengoleksi, menggunakan atau menyebarkannya kepada pihak lain. (Sautunnida)

Jika melihat pada kasus yang terdapat pada pendahuluan, terdapat adanya penyalahgunaan data pribadi dari korban. Bermula, dari adanya fitur baru dari sebuah platform sosial media yaitu *Instagram* yang menyediakan fitur bernama "Add Yours". Pada dasarnya cara kerja dari fitur ini adalah memberikan *challenge* pada para pengguna *Instagram*. *Challenge* ini pada mulanya dibuat sendiri oleh para pengguna dan juga bentuknya bervariasi. Salah satunya adalah seperti meminta alamat, variasi nama panggilan, foto tanda tangan hingga ada juga yang memberikan *challenge* untuk mengunggah foto KTP atau Kartu Tanda Penduduk dari pengguna. Sangat disayangkan, karena pada kenyataannya masih banyak orang yang mengikuti *challenge* tersebut. Para pengguna seperti kurang waspada akan data pribadi yang mereka bagikan pada akun mereka. Terlebih lagi, pada fitur ini, tidak hanya pengikut mereka saja yang dapat mengakses unggahan mereka, namun juga semua orang yang ikut berpartisipasi dalam *challenge* tersebut. Sehingga hal ini memungkinkan adanya penyalahgunaan data pribadi oleh orang-orang yang tidak bertanggung jawab.

Seperti halnya yang terjadi pada korban dalam kasus ini. Korban menceritakan pada temannya bahwa ia telah ditipu oleh seseorang setelah mengikuti *challenge* tersebut. Korban mengaku bahwa ia mengunggah *challenge* tentang variasi nama panggilannya. Hal ini ternyata dimanfaatkan oleh orang-orang diluar sana untuk melakukan tindak kejahatan. Korban mengaku bahwa ia dihubungi oleh seseorang yang memanggilnya dengan nama kecilnya. Pelaku meminta korban untuk mentransfer sejumlah uang. Pada saat itu, korban mengira itu adalah seseorang yang dikenalnya karena pelaku memanggilnya dengan menggunakan nama kecilnya. Melihat dari kejadian tersebut, maka tidak menutup kemungkinan bahwa kejahatan dapat terjadi ketika kesempatan tersebut ada. Sebagai pengguna media sosial, masyarakat diharapkan dapat bijak dalam menggunakan segala fitur yang ada di dalam platform media sosial. Namun, disisi lain, hal ini juga menjadi hak kebebasan bagi para pengguna media sosial untuk berkekespresi. Dengan adanya Perlindungan data menjadi pendorong kuat bagi terwujudnya kebebasan politik, spiritual, keagamaan bahkan kegiatan seksual. Juga, diperlukan adanya hak privasi sebagai perlindungan data bagi kebebasan setiap individu. Konsep hak privasi dapat dilihat dari perspektif antropologi dan sosiologi yaitu hak privasi sebagai permintaan dari seseorang atau kelompok untuk memutuskan sendiri bagaimana, apa, dan kapan informasi mengenai data pribadi seseorang atau kelompok dipublikasikan kepada publik. (Tejomurti et al.)

Mengenai fitur dalam sistem elektronik, dalam Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik, disebutkan pada Pasal 30 bahwa Penyelenggara Sistem Elektronik harus menyediakan fitur yang sesuai dengan karakteristik sistem elektronik yang digunakan. Dalam hal ini tidak disebutkan secara komprehensif karakteristik yang seperti apa. Kemudian pada Pasal 30 ayat (2) menyebutkan bahwa fitur tersebut paling sedikit berupa fasilitas untuk, a. melakukan koreksi; b. membatalkan perintah; c. memberikan konfirmasi atau rekonfirmasi; d. memilih meneruskan atau berhenti melaksanakan aktivitas berikutnya; e. melihat informasi yang disampaikan berupa tawaran Kontrak Elektronik atau iklan; f. mengecek status berhasil atau gagalnya Transaksi Elektronik; dan g. membaca perjanjian sebelum melakukan Transaksi Elektronik. Dapat dilihat, bahwa fitur tersebut tidak cocok jika diterapkan pada media sosial seperti *Instagram*. Diperlukan adanya pengamanan khusus pada fitur-fitur yang ada pada platform *Instagram*, seperti misalnya adalah adanya fitur anti-screenshot atau akses terbatas untuk melihat unggahan pada *Instagram*. Fitur anti-screenshot banyak diterapkan seperti pada aplikasi komik dan

aplikasi edit gambar. Pada Instagram sendiri, fitur ini telah diterapkan untuk gambar yang dikirim melalui pesan langsung (direct message) sehingga akun lawan bicara tidak dapat mengambil gambar yang telah dikirim. Hal ini dapat diterapkan juga untuk gambar-gambar yang dipublikasi melalui fitur "add yours" agar orang lain tidak dapat mengambil gambar secara sembarangan. Fitur tersebut penting untuk mencegah adanya kebocoran data yang nantinya dapat disalahgunakan. Dengan adanya fitur pengamanan yang kuat, akan memberikan kebebasan pada seseorang untuk beraktivitas di media sosial. Tetapi di samping itu, juga diperlukan adanya kesadaran akan pentingnya menjaga privasi data pribadi dari setiap masing-masing individu. Aktivitas di dunia *cyber* sifatnya sangat cepat dan mudah untuk diakses, sehingga masyarakat juga harus waspada dengan apa yang diunggahnya untuk publik. Privasi adalah hak penuh seseorang dan pemenuhannya tidak didasarkan pada hak orang lain, tetapi hak tersebut dapat hilang apabila dikehendaki oleh pemiliknya untuk mempublikasikan informasi yang bersifat pribadi kepada publik dan seseorang berhak untuk tidak membagikan semua informasi mengenai pribadinya dalam kehidupan sosial. (Priscyllia)

#### 4. Kesimpulan

Kasus pencurian data dan penyalahgunaan data pada Instagram memerlukan perlindungan yaitu melalui adanya peraturan perundang-undangan yang berlaku. Perlindungan data pribadi telah diisyaratkan oleh berbagai peraturan perundang-undangan baik dari Undang-Undang Dasar NRI 1945, Undang-Undang Informasi dan Teknologi Elektronik hingga peraturan-peraturan pelaksanaannya yaitu Peraturan Pemerintah mengenai Penyelenggaraan Sistem dan Transaksi Elektronik dan Peraturan Menteri Komunikasi dan Informatika tentang Perlindungan Data Pribadi. Adanya upaya pencegahan terjadinya pelanggaran dengan menerapkan mekanisme manajemen resiko dan edukasi kepada masyarakat. Adapula penanggulangan bila pelanggaran telah terjadi dan merugikan korban maka pihak penyelenggara sistem elektronik wajib untuk menghapus data-data yang tidak relevan tersebut. Tak hanya kewajiban penyelenggara sistem elektronik, namun juga ada pertanggungjawaban pelaku yang telah melakukan pelanggaran. Hal ini disebutkan dalam Undang-Undang ITE bahwa pertanggungjawaban tersebut dapat berupa sanksi pidana, gugatan keperdataan serta Alternatif Penyelesaian Sengketa.

Adanya fitur pengamanan pada platform media sosial seperti Instagram adalah menjadi penting, karena dengan adanya hal tersebut dapat menjamin kebebasan seseorang untuk berekspresi di dalam kehidupan sosialnya. Namun, disamping itu juga diperlukan adanya kesadaran masyarakat untuk tidak memberikan akses pada publik untuk dapat melihat segala informasi tentang data pribadinya. Sehingga dengan begitu, upaya perlindungan terhadap data pribadi juga dapat terwujud dari dua sisi, yaitu dari penyelenggara sistem elektronik dan juga pengguna sistem elektronik.

#### Ucapan Terima Kasih

Peneliti mengucapkan terima kasih atas pendanaan kepada Fakultas Hukum Universitas 17 Agustus 1945 Surabaya dan Lembaga Penelitian dan Pengabdian kepada Masyarakat (LPPM) Universitas 17 Agustus 1945 Surabaya.

#### DAFTAR PUSTAKA

- [1] Hertianto, M. Rafifnafia. "Sistem Penegakan Hukum Terhadap Kegagalan Dalam Perlindungan Data Pribadi Di Indonesia." *Kertha Patrika*, vol. 43, no. 1, 2021, doi:10.24843/kp.2021.v43.i01.p07.
- [2] Kusnadi, Sekaring Ayumeida, and Andy Usmina Wijaya. "Perlindungan Hukum Data Pribadi Sebagai Hak Privasi." *AL WASATH Jurnal Ilmu Hukum*, vol. 2, no. 1, 2021, pp. 9–16, doi:10.47776/alwasath.v2i1.127.
- [3] Marzuki, Peter Mahmud. *Penelitian Hukum Edisi Revisi*. 13th ed., Kencana, 2017.
- [4] 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)*, vol. 6, no. 1, 2020, pp. 1–14, doi:10.35814/selisik.v6i1.1699.
- [5] Priscyllia, Fanny. "Perlindungan Privasi Data Pribadi Dalam Perspektif Perbandingan Hukum." *Jatiswara*, vol. 34, no. 3, 2019, doi:10.29303/jatiswara.v34i3.218.
- [6] Putra, R.Caesalino W & Widiatja, IGN. Parikesit. Perlindungan Hukum Bagi Korban Pencurian Informasi Pribadi Melalui Dunia Cyber Ditinjau dari Undang-Undang No. 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik (Uu Ite). no. 11, 2008, pp. 1–5.
- [7] Sautunnida, Lia. "Urgensi Undang-Undang Perlindungan Data Pribadi Di Indonesia: Studi Perbandingan Hukum Inggris Dan Malaysia." *Kanun Jurnal Ilmu Hukum*, vol. 20, no. 2, 2018, doi:10.24815/kanun.v20i2.11159.
- [8] Situmeang, Sahat Maruli Tua. "Penyalahgunaan Data Pribadi Sebagai Bentuk Kejahatan Sempurna Dalam Perspektif Hukum Siber." *Sasi*, vol. 27, no. 1, 2021, p. 38, doi:10.47268/sasi.v27i1.394.

- [9] Tejomurti, Kukuh, et al. "Legal Protection for Urban Online-Transportation-Users' Personal Data Disclosure in the Age of Digital Technology." *PADJADJARAN Jurnal Ilmu Hukum (Journal of Law)*, vol. 5, no. 3, 2019, doi:10.22304/pjih.v5n3.a5.