

Penanggulangan Tindak Pidana Penyalahgunaan Data Pribadi Dalam Sistem Elektronik di Indonesia: Kajian Perbandingan Hukum Inggris dan Hukum Indonesia

Annisa Zahra Rahmadany¹, Erdiansyah², T. Arif Hidayat³

^{1,2,3} Fakultas Hukum Universitas Riau, Indonesia

E-mail: annisa.zahra1985@student.unri.ac.id¹, erdiansyah@lecturer.unri.ac.id²,
t.arifhidayat@lecturer.unri.ac.id³

Article History:

Received: 23 Agustus 2025

Revised: 10 Oktober 2025

Accepted: 16 November 2025

Keywords: *Criminal Acts,
Misuse of Personal Data,
Comparative Law, England,
Indonesia*

Abstract: *Criminal acts involving the misuse of personal data encompass a series of illegal actions, including the collection, processing, or use of personal information without the consent or authorization of the individual concerned. In today's digital context, where personal information is highly valuable, such actions can occur in various ways, including data theft through hacking, wiretapping, or social engineering techniques. This research is a normative legal study. A normative legal study is conducted by examining literature or secondary data consisting of primary, secondary, and tertiary legal materials. The findings of this study indicate that the regulation of criminal acts related to the misuse of personal data in Indonesia and the United Kingdom shares the same objective: to protect individuals' rights concerning personal data and to ensure public trust in data management. However, there are significant differences in terms of regulatory clarity, sanctions, supervision, and transparency.*

PENDAHULUAN

Perkembangan teknologi komputer berbasis internet telah mendorong lahirnya Revolusi Industri 4.0 yang mengubah tatanan sosial dan ekonomi menjadi berorientasi pada informasi. Arus informasi global yang cepat membawa manfaat, namun juga membuka peluang infiltrasi budaya dan ideologi yang dapat berdampak negatif pada nilai-nilai lokal. Salah satu dampak serius adalah meningkatnya kejahatan penyalahgunaan data pribadi dalam sistem elektronik. Data pribadi, seperti nama lengkap, jenis kelamin, agama, kewarganegaraan, dan informasi lain yang dapat mengidentifikasi seseorang, jika disalahgunakan, merupakan pelanggaran privasi yang dapat menimbulkan perbuatan melawan hukum.¹

Di Indonesia, kasus penyalahgunaan data pribadi semakin sering terjadi. Sebagai contoh, dugaan kebocoran data dua juta nasabah BRI Life yang diperjualbelikan secara ilegal, dengan sekitar 463.000 dokumen diduga berhasil diambil peretas. Penyalahgunaan data merupakan tindakan yang sengaja dilakukan untuk menembus sistem keamanan elektronik, sedangkan kebocoran data terjadi karena kelalaian atau lemahnya perlindungan sistem. Data yang bocor

¹ Christian Henry Ratulangi, et. al., "Tindak Pidana Cyber Crime Dalam Kegiatan Perbankan", Jurnal Lex Privatum, Fakultas Hukum Universitas Sam Ratulangi, Vol. IX, No. 5 April 2021, hlm. 179.

rentan dicuri dan dimanfaatkan untuk kepentingan merugikan. Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi telah mengatur hak dan kewajiban antara subjek data dengan pengendali data, tetapi penerapannya belum optimal. Kebocoran data membuka peluang bagi pihak ketiga untuk memanfaatkannya di luar kesepakatan yang sah, sehingga berpotensi merugikan pemilik data.²

Penanganan penyalahgunaan data pribadi di Indonesia umumnya merujuk pada Undang-Undang Nomor 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik. Namun, kasus besar seperti peretasan oleh hacker Bjorka, yang membocorkan data pejabat tinggi pemerintah, menunjukkan bahwa regulasi dan penegakan hukum nasional belum cukup kuat untuk mengantisipasi ancaman tersebut. Kondisi ini menegaskan perlunya pembaruan hukum agar dapat mengikuti dinamika perkembangan teknologi.³

Dalam konteks global, Inggris merupakan salah satu negara dengan sistem perlindungan data yang lebih maju. Berdasarkan Global Cybersecurity Index 2020, Inggris menempati peringkat kedua dunia dalam penanggulangan kejahatan siber. Keberhasilan ini tidak lepas dari penerapan Data Protection Act 2018 (DPA 2018) yang mengadopsi dan melengkapi General Data Protection Regulation (GDPR). Regulasi tersebut tidak hanya memberikan perlindungan hukum yang lebih jelas, tetapi juga mengatur sanksi tegas, pengawasan independen, transparansi, serta pembentukan lembaga khusus seperti National Cyber Crime Unit (NCCU) di bawah National Crime Agency (NCA). Pendekatan hukum Inggris yang berbasis common law memungkinkan penyesuaian cepat terhadap ancaman baru, berbeda dengan sistem hukum Indonesia yang cenderung tertinggal dari perkembangan teknologi.⁴

Selain itu, DPA 2018 dan GDPR dirancang untuk mengantisipasi kejahatan dalam masyarakat yang semakin bergantung pada teknologi. Perubahan dari Data Protection Act 1998 menjadi DPA 2018, yang merupakan bagian dari Serious Crime Act, memperkenalkan ketentuan yang mengkriminalisasi penyalahgunaan data pribadi yang berpotensi membahayakan keselamatan publik, ekonomi, lingkungan, atau keamanan nasional. Meskipun sudah diterapkan lebih dari tiga dekade, regulasi ini tetap relevan dan efektif dalam menangani pelanggaran siber.⁵

Perbandingan antara sistem hukum Inggris dan Indonesia menunjukkan bahwa hukum Indonesia sering kali bergerak lebih lambat dibandingkan perkembangan teknologi. Inggris, sebaliknya, mengantisipasi ancaman sejak dini dengan mengakomodasi kebiasaan sosial yang berkembang. Oleh karena itu, Indonesia perlu mengkaji model regulasi Inggris untuk memperkuat perlindungan hukum terhadap penyalahgunaan data pribadi, baik dalam konteks saat ini maupun masa depan.⁶

Sejalan dengan pandangan Muladi yang dikutip oleh Romli Atmasasmita, hukum nasional harus bersifat adaptif dan mampu mengikuti perkembangan teknologi. Studi perbandingan hukum menjadi sangat penting, tidak hanya untuk memperbaiki kelemahan hukum pidana positif, tetapi juga untuk merumuskan kebijakan baru yang dapat menjawab tantangan modern. Berdasarkan

² Endah Pertiwi, et. al., "Analisis Yuridis Terhadap Penyalahgunaan Data Pribadi Pengguna Media Sosial", Jurnal Rechten, Program Studi Ilmu Hukum Universitas Nusa Putra, Vol. 3, No. 3 Maret 2021, hlm. 10.

³ Deanne Destriani dan Muhammad Helmi, "Upaya Pencegahan Kebocoran Data Konsumen Melalui Pengesahan RUU Perlindungan Data Pribadi (Studi Kasus E-Commerce Bhinneka.com)", Jurnal Borneo Law Review, Fakultas Hukum Universitas Borneo Tarakan, Vol. 5, No. 1 Juni 2021, hlm. 48.

⁴ Ayumi Kartika Sari, "Aspek Hukum Perlindungan Data Pribadi Sebagai Hak Privasi Pengguna Media Sosial", Jurnal Rectum, Universitas Darma Agung, Vol. 5, No. 1 Januari 2023, hlm. 976.

⁵ Hanafi, "Urgensi Pengaturan Hukum Tentang Perlindungan Data Pribadi Pada Sistem Digital Dalam Pemenuhan Hak Privasi Di Indonesia", Jurnal Hukum dan Sosial, Yayasan Pendidikan Tanggui Baimbaian Kalimantan Selatan, Vol. 1, No. 1 Januari 2023, hlm. 20.

⁶ Fauzi Solihin, "Analisa Cakupan Hukum Pengelolaan Perlindungan Hukum Data Pribadi di Indonesia", JISPAR, FISIP Universitas Palangka Raya, Vol. 12, No. 1 Februari 2023, hlm. 105.

latar belakang tersebut, penelitian ini difokuskan pada topik “Penanggulangan Tindak Pidana Penyalahgunaan Data Pribadi dalam Sistem Elektronik di Indonesia: Kajian Perbandingan Hukum Inggris dan Indonesia”.

METODE PENELITIAN

Penelitian ini menggunakan metode hukum normatif dengan menelaah bahan pustaka berupa peraturan perundang-undangan dan regulasi terkait. Fokus kajian adalah penanggulangan tindak pidana penyalahgunaan data pribadi dalam sistem elektronik di Indonesia melalui perbandingan dengan hukum Inggris. Pendekatan yang digunakan adalah yuridis normatif dan yuridis komparatif, dengan tujuan mengidentifikasi persamaan serta perbedaan pengaturan penyalahgunaan data pribadi di kedua negara. Selain itu, penelitian ini juga bertujuan memberikan gambaran mengenai kemungkinan penerapan praktik hukum Inggris untuk memperkuat perlindungan data pribadi di Indonesia.⁷

LANDASAN TEORI

1. Teori Kebijakan Hukum Pidana

Menurut *Simons*, sebagaimana dikutip Erdianto menyatakan bahwa hukum pidana adalah semua tindakan keharusan dan larangan yang dibuat oleh negara atau penguasa yang diancamkan dengan derita khusus, yaitu pidana.⁸ Dalam hal hukum pidana yang dibuat oleh negara, maka negara wajib melindungi warga negaranya dari segala bentuk kejahatan.⁹ Berkenaan dengan perlindungan masyarakat dari kejahatan, dapat diketahui fungsi hukum pidana yaitu sebagai sarana penanggulangan kejahatan yang rasional.¹⁰ Fungsi ini merupakan bagian integral daripada kebijakan hukum pidana yang bertujuan untuk mencapai kesejahteraan masyarakat.¹¹

Usaha kebijakan untuk membuat peraturan hukum pidana yang baik, pada hakikatnya tidak dapat dilepaskan dari tujuan penanggulangan kejahatan. Dengan demikian, kebijakan hukum pidana juga merupakan bagian dari kebijakan kriminal atau politik kriminal. Dilihat dari sudut pandang kebijakan kriminal atau politik kriminal dapat dikatakan diperlukan usaha untuk mewujudkan peraturan-peraturan yang baik sesuai dengan keadaan dan situasi yang ada pada saat ini maupun yang akan datang. Kebijakan negara melalui badan yang berwenang merumuskan dan menetapkan peraturan-peraturan yang dapat digunakan untuk mengekspresikan apa yang terkandung dalam masyarakat guna mencapai apa yang dicita-citakan. Dengan kata lain, tujuan yang hendak dicapai dengan kebijakan hukum pidana adalah peraturan perundang-undangan pidana yang baik.¹²

2. Teori Perbandingan Hukum Pidana

Esin Orucu, seorang Profesor Perbandingan Hukum dari Universitas Glasgow mengatakan “Perbandingan hukum merupakan suatu disiplin ilmu hukum yang bertujuan menemukan persamaan dan perbedaan serta menemukan pula hubungan-hubungan erat antara berbagai sistem

⁷ Djoni Sumardi Gozali, *Pengantar Perbandingan Sistem Hukum (Civil Law, Common Law, dan Hukum Adat)*, Nusa Media, Bandung, 2018, hlm. 129.

⁸ Erdianto Effendi, *Hukum Pidana Indonesia – Suatu Pengantar*, Refika Aditama, Bandung, 2014, hlm. 6.

⁹ *Ibid.* hlm. 46.

¹⁰ *Ibid.* hlm. 36.

¹¹ H. John Kenedi, *Kebijakan Hukum Pidana (Penal Policy) Dalam Sistem Penegakan Hukum di Indonesia*, Pustaka Pelajar, Yogyakarta, 2017, hlm. 59.

¹² *Ibid.* hlm. 60.

hukum, melihat perbandingan lembaga-lembaga hukum dan konsep-konsep serta mencoba untuk menemukan suatu penyelesaian atas masalah-masalah tertentu dalam sistem hukum dimaksud, dengan tujuan seperti pembaruan hukum, atau unifikasi hukum”.¹³

Pengertian dari Orucu tersebut cukup untuk mengetengahkan istilah perbandingan hukum, dan bukan hukum perbandingan. Pengertian ini akan lebih lengkap apabila didukung oleh pengertian yang diketengahkan oleh *Guitens-Bourgis*: “Perbandingan hukum adalah metoda yang diperbandingkan pada ilmu hukum. Akan tetapi, perbandingan hukum bukanlah ilmu hukum, melainkan hanya sebagai suatu metoda studi untuk meneliti sesuatu, suatu cara kerja, yakni: perbandingan. Apabila hukum itu terdiri dari seperangkat peraturan, jelaslah hukum perbandingan itu tidak ada. Metode untuk membandingkan aturan hukum dari berbagai sistem hukum, tidak dapat mengakibatkan perumusan aturan yang berdiri sendiri, dengan kata lain tidak ada aturan hukum perbandingan.”

Perbandingan hukum sebagai suatu metode berarti bahwa suatu cara untuk lebih memahami suatu objek atau masalah yang akan diteliti. Oleh karena itu, sering digunakan sebagai metode perbandingan hukum. Jadi, pengertian di atas, telah menggambarkan bahwa perbandingan hukum itu dapat disebut sebagai metode atau juga bisa disebut sebagai ilmu.¹⁴

HASIL DAN PEMBAHASAN

1. Pengaturan Tindak Pidana Penyalahgunaan Data Pribadi dalam Hukum Pidana Indonesia dan Hukum Pidana Inggris

Penyalahgunaan data pribadi adalah tindakan ilegal yang melibatkan pengumpulan, pengolahan, atau penggunaan informasi pribadi tanpa izin, biasanya melalui peretasan, phishing, atau rekayasa sosial. Data yang dicuri dapat dimanfaatkan untuk penipuan identitas, pencurian finansial, atau pelanggaran privasi, menimbulkan kerugian finansial, psikologis, dan reputasi bagi korban maupun organisasi. Dalam era digital, di mana data pribadi menjadi aset penting, perlindungan keamanan informasi menjadi kebutuhan mendesak.¹⁵

Indonesia telah memiliki Undang-Undang Perlindungan Data Pribadi dan aturan pidana terkait, namun penerapannya belum sekuat Inggris yang memiliki kerangka hukum lebih matang melalui Data Protection Act 2018 dan GDPR, lengkap dengan lembaga pengawas yang berwenang menjatuhkan sanksi tegas. Kedua negara memiliki tujuan sama, yaitu melindungi hak individu dan menjaga keamanan data, tetapi Inggris lebih adaptif dan proaktif. Bagi Indonesia, memperkuat regulasi, meningkatkan pengawasan, serta membangun kesadaran publik menjadi langkah penting untuk menghadapi ancaman penyalahgunaan data pribadi di era teknologi.¹⁶

Sistem hukum Indonesia menganut tradisi Civil Law yang berasal dari Eropa Kontinental, khususnya Belanda pada masa penjajahan. Civil Law berakar pada kodifikasi hukum Romawi, menekankan hukum tertulis sebagai sumber utama. Undang-undang menjadi pedoman yang mengikat semua pihak, sedangkan putusan hakim hanya berlaku pada para pihak dalam perkara tersebut (doktrin Res Judicata) dan tidak memiliki kekuatan preseden. Hakim tidak menciptakan

¹³ Yesmil Anwar dan Adang, *Pembaruan Hukum Pidana: Reformasi Hukum Pidana*, Grasindo, Jakarta, 2008, hlm. 80.

¹⁴ *Ibid.* hlm. 81.

¹⁵ Trisandi, Desmon, and Ahmad Sofian. "Tindak Pidana Penyalahgunaan Data Pribadi Dalam Hukum Siber Indonesia." *Journal of Syntax Literate* 9.2 (2024).

¹⁶ Luthiya, Adik Nur, Benny Irawan, and Rena Yulia. "Kebijakan Hukum Pidana Terhadap Pengaturan Pencurian Data Pribadi Sebagai Penyalahgunaan Teknologi Komunikasi Dan Informasi." *Jurnal Hukum Pidana Dan Kriminologi* 2.2 (2021): hlm. 14

hukum baru, melainkan menerapkan undang-undang yang ada, sehingga tercipta kepastian, stabilitas, dan prediktabilitas hukum.¹⁷

Sistem hukum Inggris dikenal sebagai Common Law, berkembang melalui preseden (*stare decisis*) di mana putusan pengadilan yang lebih tinggi mengikat pengadilan yang lebih rendah. Sumber hukumnya meliputi:

- a. Legislasi (*Acts of Parliament*): hukum tertulis dengan kekuatan tertinggi.
- b. Yurisprudensi: keputusan pengadilan yang membentuk hukum hidup dan menyesuaikan dengan perkembangan masyarakat.
- c. Hukum kebiasaan (*customary law*): praktik tradisional yang diakui bila tidak ada aturan tertulis.

Struktur peradilan Inggris terdiri dari *Magistrates' Courts*, *County Courts*, *Crown Court*, *High Court*, *Court of Appeal*, dan *Supreme Court* sebagai pengadilan tertinggi. Sistem ini menekankan kemandirian hakim untuk menjamin keadilan bebas dari intervensi politik.¹⁸

Hukum Inggris menyeimbangkan common law (preseden) dan statutory law (legislasi). Undang-undang Parlemen dapat mengubah atau membatalkan preseden, tetapi selama tidak ada legislasi baru, preseden tetap mengikat. Kombinasi ini menciptakan sistem hukum yang fleksibel, adaptif, dan konsisten, memberikan kepastian hukum sekaligus kemampuan menyesuaikan diri dengan perkembangan sosial, ekonomi, dan teknologi.

Informasi pribadi di Indonesia rentan disalahgunakan baik secara online maupun offline. Banyak masyarakat tidak menyadari bahwa mereka memberi izin pemakaian data saat menyetujui "*Terms of Use*" di situs web, sehingga data dapat diakses pihak ketiga untuk pemasaran. Potensi pelanggaran juga muncul dalam program pemerintah seperti e-KTP dan e-health, yang tanpa regulasi ketat dapat dimanfaatkan industri lain untuk kepentingan ekonomi. Selain itu, pencurian identitas dan penggunaan data pelanggan oleh perusahaan menjadi ancaman nyata.¹⁹

Untuk mengatasi hal tersebut, Indonesia mengatur perlindungan data pribadi melalui beberapa undang-undang. UU No. 36 Tahun 1999 tentang Telekomunikasi melarang akses dan penyadapan tanpa izin, dengan sanksi penjara hingga 15 tahun. UU No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (ITE) mengatur sanksi pidana hingga 10 tahun penjara dan denda hingga Rp5 miliar bagi pelaku manipulasi, perusakan, atau penyebaran data elektronik tanpa hak. UU No. 27 Tahun 2022 tentang Perlindungan Data Pribadi (PDP) memperluas perlindungan hingga level transnasional, tetapi masih memiliki kelemahan, misalnya tidak tegas mencantumkan kewajiban persetujuan pemilik data untuk transfer internasional dan belum mengatur sanksi pidana bagi kegagalan melindungi data, hanya sanksi administratif.²⁰

Di Inggris, perlindungan data diatur melalui Data Protection Act 2018 yang mengadopsi prinsip GDPR. Regulasi ini menekankan persetujuan eksplisit pemilik data, hak untuk mengakses, memperbaiki, atau menghapus data, serta kewajiban organisasi menjaga keamanan informasi dengan ancaman denda besar dan pidana penjara. Selain itu, Computer Misuse Act 1990

¹⁷ Situmeang, Sahat Maruli Tua. "Penyalahgunaan data pribadi sebagai bentuk kejahatan sempurna dalam perspektif hukum siber." *Sasi* 27.1 (2021): hlm. 38

¹⁸ Jonimandala, G. W., Sondakh, D. K., & Sondakh, J. (2023). Peran Direktorat Tindak Pidana Siber (DITTIPIDSIBER) Bareskrim Polri Dalam Melakukan Penegakan Hukum Terhadap Kejahatan Pencurian dan Penyalahgunaan Data Pribadi. *Innovative: Journal Of Social Science Research*, 3(4), hlm. 680

¹⁹ Muhammad Fikri, Abdurrahman Alhakim, Urgensi Pengaturan Hukum Terhadap Pelaku Tindak Pidana Pencurian Data Pribadi di Indonesia, *Jurnal Hukum dan Hukum Islam*, Volume 9 Nomor 1 Juli 2022, Fakultas Hukum Universitas Internasional Batam, Indonesia, hlm. 234

²⁰ <https://www.legislation.gov.uk/ukpga/2018/12/part/6/crossheading/offences-relating-to-personal-data/> di terjemahkan menggunakan Google Translate diakses tanggal 24 September 2024, Jam 20.30 Wib

mengkriminalisasi akses tidak sah, peretasan, hingga penyebaran malware. Investigatory Powers Act 2016 memberi kewenangan negara melakukan pengawasan digital untuk keamanan nasional, namun tetap mensyaratkan izin pengadilan dan mekanisme pengawasan untuk mencegah penyalahgunaan.²¹

Tabel 1
Tabel Perbandingan Tindak Pidana Penyalahgunaan
Data Pribadi di Indonesia dan Inggris

No	Aspek	Indonesia	Inggris
1	Dasar Hukum	Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi	Data Protection Act 2018 dan GDPR
2	Jenis Pelanggaran	Penyalahgunaan data, pencurian identitas, dan pelanggaran privasi	Penyalahgunaan data, pencurian identitas, dan pelanggaran privasi
3	Sanksi	Sanksi administratif, denda, dan hukuman penjara	Denda besar, sanksi administratif, dan hukuman penjara
4	Pengawasan	Otoritas Perlindungan Data Pribadi	Information Commissioner's Office (ICO)
5	Persetujuan Pemilik Data	Diperlukan persetujuan pemilik untuk pemrosesan data	Diperlukan persetujuan untuk pengolahan data pribadi
6	Penerapan	Mencakup semua sektor yang mengolah data pribadi	Mencakup semua sektor dan penegakan hukum yang ketat
7	Perlindungan Data Internasional	Kelemahan dalam penegakan di luar negeri	Prosedur yang jelas untuk transfer data internasional
8	Fokus Perlindungan	Menjaga hak privasi individu	Menjaga hak privasi individu dan menjamin transparansi dalam pengolahan data

Sumber: Olah data Penulis 2024

Berdasarkan Tabel 1 di atas Perbandingan hukum pengaturan tindak pidana penyalahgunaan data pribadi di Indonesia dan Inggris dimulai dari dasar hukum. Di Indonesia, pengaturan utama terdapat dalam Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi, sementara Inggris mengandalkan *Data Protection Act* 2018 dan GDPR. Selanjutnya, dalam hal jenis pelanggaran, kedua negara mencakup penyalahgunaan data, pencurian identitas, dan pelanggaran privasi, menunjukkan kesamaan dalam mengidentifikasi masalah utama yang dihadapi.

Mengenai sanksi, Indonesia memberlakukan sanksi administratif, denda, dan hukuman penjara bagi pelanggar, namun mungkin kurang ketat dalam penegakan hukum, terutama di luar negeri. Sebaliknya, Inggris menerapkan denda besar dan hukuman penjara, mencerminkan pendekatan yang lebih tegas. Dalam hal pengawasan, Indonesia mengandalkan Otoritas Perlindungan Data Pribadi, sedangkan Inggris memiliki *Information Commissioner's Office* (ICO), yang lebih mapan dan memiliki kewenangan lebih besar.

²¹ <https://www.pinsentmasons.com/out-law/guides/misuse-of-private-information/> di terjemahkan menggunakan Google Translate diakses tanggal 24 September 2024, Jam 21.00 Wib

Ketika membahas persetujuan pemilik data, kedua negara mensyaratkan persetujuan dari pemilik data sebelum pemrosesan dilakukan. Namun, Inggris menunjukkan prosedur yang lebih jelas untuk transfer data internasional. Dalam hal penerapan, hukum di Indonesia mencakup semua sektor yang mengolah data pribadi, tetapi Inggris memiliki penegakan hukum yang lebih ketat. Mengenai perlindungan data internasional, Indonesia mengalami kelemahan dalam penegakan di luar negeri, sementara Inggris memiliki prosedur yang lebih jelas untuk transfer data antar negara.

Fokus perlindungan di kedua negara terletak pada menjaga hak privasi individu, tetapi Inggris lebih menekankan pada transparansi dalam pengolahan data. Dengan demikian, perbandingan ini menunjukkan perkembangan yang berbeda dalam konteks perlindungan data pribadi di Indonesia dan Inggris, serta tantangan yang harus dihadapi masing-masing negara.

Inggris memiliki regulasi perlindungan data yang lebih komprehensif melalui GDPR dan Data Protection Act 2018, dengan definisi jelas, hak individu yang kuat, kewajiban pengendali data yang tegas, serta sanksi berat berupa denda besar dan hukuman penjara. Pengawasan dilakukan oleh lembaga independen seperti ICO yang memastikan kepatuhan dan memberikan panduan kepada organisasi. Prosedur transfer data internasional di Inggris juga lebih terstruktur, mendukung keamanan data dalam konteks global. Transparansi pengolahan data menjadi fokus utama sehingga meningkatkan kepercayaan publik dan loyalitas pengguna.

Dari sudut teori perbandingan hukum, sistem Inggris lebih matang karena mampu menyesuaikan regulasi dengan perkembangan teknologi, memiliki mekanisme sanksi dan pengawasan yang jelas, serta memberikan efek jera yang tinggi. Sebaliknya, Indonesia meskipun telah memiliki UU No. 27 Tahun 2022, masih menghadapi kendala pada penerapan, penegakan, dan efektivitas pengawasan. Sanksi di Indonesia cenderung administratif, lembaga pengawas masih lemah, dan prosedur transfer data internasional belum seterstruktur Inggris. Agar lebih efektif melindungi data pribadi dan dapat bersaing di tingkat global, Indonesia perlu memperkuat regulasi, penegakan hukum, serta membangun sistem pengawasan yang lebih tegas.

Analisis perbandingan hukum menunjukkan bahwa Inggris memiliki regulasi perlindungan data pribadi yang lebih matang melalui GDPR dan Data Protection Act 2018, dengan sanksi tegas, pengawasan kuat, serta prosedur transfer data internasional yang jelas. Sistem ini efektif mencegah pelanggaran dan meningkatkan kepercayaan publik. Sebaliknya, Indonesia meski telah memiliki UU No. 27 Tahun 2022, masih lemah dalam penegakan, sanksi, dan pengawasan sehingga kurang memberikan efek jera. Untuk memperkuat perlindungan data pribadi dan bersaing secara global, Indonesia perlu memperbaiki regulasi, menegakkan hukum secara konsisten, serta memperkuat lembaga pengawas.

2. Penerapan Pengaturan Penanggulangan Penyalahgunaan Data Pribadi Di Inggris yang dapat Di Indonesia

Perkembangan teknologi dan perdagangan online meningkatkan risiko penyalahgunaan data pribadi di Indonesia, sering kali akibat kelalaian individu, seperti saat pendaftaran kartu perdana atau penggunaan aplikasi. Inggris telah lebih dulu merespons tantangan serupa dengan menerapkan regulasi ketat, dimulai dari Data Protection Act 1984 hingga Data Protection Act 2018 yang selaras dengan GDPR. Aturan ini memperkuat hak individu, menetapkan sanksi tegas, dan mengatur pengelolaan data pribadi untuk mencegah penyalahgunaan, termasuk dalam konteks big data, transfer lintas negara, serta keamanan nasional. Penerapan prinsip serupa di

Indonesia dapat memperkuat perlindungan privasi, meningkatkan kepercayaan publik, dan memudahkan integrasi dalam perdagangan global.²²

Penerapan kerangka hukum seperti di Inggris dapat membantu Indonesia menghadapi tantangan big data yang saat ini dimanfaatkan untuk analisis perilaku konsumen. Meski memiliki manfaat ekonomi, praktik ini juga membuka peluang penyalahgunaan data yang serius jika tidak diawasi secara ketat. Regulasi yang lebih tegas akan memberikan batasan jelas mengenai bagaimana data dikumpulkan, diproses, dan dibagikan, serta memastikan adanya persetujuan yang sah dari pemilik data. Hal ini penting agar inovasi digital tidak mengorbankan hak privasi masyarakat.²³

Selain itu, pengalaman Inggris menunjukkan bahwa keberadaan lembaga pengawas independen, seperti Information Commissioner's Office (ICO), sangat krusial dalam memastikan kepatuhan dan memberikan sanksi atas pelanggaran. Indonesia dapat mengadopsi konsep ini dengan memperkuat Otoritas Perlindungan Data Pribadi, baik dari sisi kewenangan, sumber daya, maupun mekanisme pengawasan. Tanpa pengawasan yang efektif, regulasi yang ada berpotensi menjadi normatif tanpa implementasi yang nyata di lapangan.²⁴

Sanksi yang berat di Inggris, seperti denda hingga 17,5 juta pound sterling atau 4% dari pendapatan global perusahaan, memberikan efek jera dan meningkatkan kepatuhan. Indonesia dapat mempertimbangkan penerapan sanksi yang lebih signifikan, bukan hanya administratif, untuk mendorong organisasi dan pelaku usaha lebih bertanggung jawab dalam mengelola data pribadi. Tanpa ancaman sanksi yang tegas, risiko kebocoran data dan penjualan informasi pribadi akan tetap tinggi.²⁵

Terakhir, Inggris menekankan pentingnya transparansi dalam setiap proses pengelolaan data. Setiap individu berhak mengetahui tujuan, cara penggunaan, serta pihak yang mengakses datanya. Prinsip ini jika diterapkan di Indonesia dapat meningkatkan kesadaran masyarakat tentang pentingnya melindungi data pribadi. Dengan begitu, perlindungan tidak hanya bergantung pada hukum, tetapi juga pada partisipasi aktif individu dalam menjaga privasinya sendiri.²⁶

Inggris memiliki regulasi perlindungan data pribadi yang lebih komprehensif melalui GDPR dan Data Protection Act 2018. Aturan ini mengatur hak subjek data, kewajiban pengendali, serta prosedur spesifik terkait penghapusan data dan hak untuk dilupakan. Sementara itu, UU No. 27 Tahun 2022 di Indonesia masih kurang rinci sehingga memerlukan penguatan terutama pada aspek kejelasan hak akses dan panduan teknis agar lebih efektif. Dari sisi sanksi, Inggris menerapkan denda yang signifikan hingga 17,5 juta pound sterling atau 4% dari omzet global, memberikan efek jera yang kuat. Sebaliknya, sanksi di Indonesia masih relatif ringan dan belum mampu meningkatkan kepatuhan secara optimal. Penerapan sanksi yang lebih berat dapat menjadi langkah strategis untuk memperbaiki tata kelola data di Indonesia.

Pengawasan di Inggris dilakukan oleh ICO, lembaga independen dengan kewenangan penuh untuk melakukan investigasi, memberikan panduan, dan menjatuhkan sanksi. Di Indonesia,

²² <https://diskominfomc.kalselprov.go.id/2020/10/01/perkembangan-teknologi-informasi-dalam-dunia-perdagangan/> diakses tanggal 24 September 2024, Jam 20.30 Wib.

²³ Andrean Antonius, et.al, Sosialisasi Perbandingan Hukuman Tindak Pidana Pembukaan Rahasia Data Pribadi Negara Indonesia dan Inggris, Jurnal Pengabdian West Science, Volume 03, Nomor 04, April 2024, Universitas Pelita Harapan, hlm. 383

²⁴ Sinta Dewi Rosadi, Perlindungan Privasi Dan Data Pribadi Dalam Era Ekonomi Digital Di Indonesia, Jurnal Vej, Fakultas Hukum, Universitas Padjadjaran, Volume 4 Nomor 1, hlm 88

²⁵ Namrysilia Buti Anjawai, Perbandingan Perlindungan Hukum Terkait Data Pribadi di Indonesia dan Jerman, Al-Manhaj: Jurnal Hukum dan Pranata Sosial Islam, Vol. 4, 2 (Desember, 2022), Universitas Internasional Batam hlm. 207

²⁶ Fanny Priscyllia, Perlindungan Privasi Data Pribadi Perspektif Perbandingan Hukum, Jurnal Jatiswara, Volume 34 Nomor 3 November 2019, hlm. 239.

lembaga pengawas perlindungan data masih dalam tahap penguatan, sehingga efektivitasnya dalam menegakkan aturan dan membangun kepercayaan publik belum maksimal. Prinsip transparansi dan akuntabilitas juga menjadi pilar penting di Inggris. Pengendali data wajib menjelaskan secara terbuka tujuan dan cara penggunaan data pribadi, yang meningkatkan kepercayaan publik. Indonesia perlu mengadopsi pendekatan serupa agar masyarakat lebih memahami haknya dan perusahaan lebih bertanggung jawab. Selain itu, Inggris memiliki prosedur ketat terkait transfer data internasional untuk memastikan perlindungan tetap terjaga, serta aktif meningkatkan kesadaran publik melalui edukasi dan kampanye. Indonesia dapat menerapkan langkah serupa agar lebih siap menghadapi tantangan globalisasi digital dan mengurangi risiko penyalahgunaan data pribadi.

KESIMPULAN DAN SARAN

1. Kesimpulan

- a. Pengaturan tindak pidana penyalahgunaan data pribadi dalam hukum pidana di Indonesia dan Inggris menunjukkan adanya kesamaan tujuan, yaitu melindungi hak-hak individu terkait data pribadi serta menjamin kepercayaan masyarakat terhadap pengelolaan data. Namun, terdapat perbedaan signifikan dalam hal kejelasan regulasi, sanksi, pengawasan, dan transparansi. Di Inggris, kebijakan yang diterapkan melalui GDPR dan Data Protection Act 2018 menawarkan kerangka hukum yang lebih jelas, sanksi yang tegas, dan lembaga pengawas yang independen seperti Information Commissioner's Office (ICO), yang berperan penting dalam penegakan hukum dan perlindungan data. Sementara itu, Indonesia masih perlu memperkuat regulasi dan penerapan kebijakan yang ada untuk memastikan perlindungan data pribadi yang lebih efektif, termasuk dalam hal penegakan hukum yang lebih tegas dan pengawasan yang berkelanjutan.
- b. Penerapan Pengaturan Penanggulangan Penyalahgunaan Data Pribadi Di Inggris yang dapat di Indonesia dapat menjadi contoh bagi Indonesia dalam penanggulangan penyalahgunaan data pribadi. Pengawasan independen yang kuat, transparansi dalam pengolahan data, serta pendidikan publik mengenai perlindungan data pribadi di Inggris menunjukkan bahwa aspek-aspek tersebut sangat penting untuk meningkatkan kepatuhan dan kesadaran masyarakat. Dengan mengadopsi pendekatan serupa, Indonesia dapat menciptakan lingkungan yang lebih aman dalam pengelolaan data pribadi.

2. Saran

- a. Menyarankan agar Pemerintah perlu memperbaharui dan memperjelas Undang-Undang Perlindungan Data Pribadi dengan memasukkan ketentuan-ketentuan yang lebih rinci mengenai hak-hak subjek data, termasuk hak untuk dilupakan dan akses yang lebih mudah terhadap data pribadi.
- b. Menyarankan agar menerapkan sanksi yang lebih berat bagi pelanggar perlindungan data untuk meningkatkan kepatuhan. Pendekatan ini dapat mendorong perusahaan dan individu untuk lebih berhati-hati dalam mengelola dan menggunakan data pribadi dan mengembangkan lembaga pengawas data yang independen dengan wewenang yang jelas dan sumber daya yang memadai untuk memastikan bahwa regulasi perlindungan data ditegakkan dengan baik.

DAFTAR REFERENSI

- Andrean Antonius, et.al, Sosialisasi Perbandingan Hukuman Tindak Pidana Pembukaan Rahasia Data Pribadi Negara Indonesia dan Inggris, Jurnal Pengabdian West Science, Volume 03, Nomor 04, April 2024, Universitas Pelita Harapan.
- Ayumi Kartika Sari, "Aspek Hukum Perlindungan Data Pribadi Sebagai Hak Privasi Pengguna Media Sosial", Jurnal Rectum, Universitas Darma Agung, Vol. 5, No. 1 Januari 2023.
- Christian Henry Ratulangi, et. al., "Tindak Pidana Cyber Crime Dalam Kegiatan Perbankan", Jurnal Lex Privatum, Fakultas Hukum Universitas Sam Ratulangi, Vol. IX, No. 5 April 2021.
- Deanne Destriani dan Muhammad Helmi, "Upaya Pencegahan Kebocoran Data Konsumen Melalui Pengesahan RUU Perlindungan Data Pribadi (Studi Kasus E-Commerce Bhinneka.com)", Jurnal Borneo Law Review, Fakultas Hukum Universitas Borneo Tarakan, Vol. 5, No. 1 Juni 2021.
- Djoni Sumardi Gozali, Pengantar Perbandingan Sistem Hukum (Civil Law, Common Law, dan Hukum Adat), Nusa Media, Bandung, 2018.
- Endah Pertiwi, et. al., "Analisis Yuridis Terhadap Penyalahgunaan Data Pribadi Pengguna Media Sosial", Jurnal Rechten, Program Studi Ilmu Hukum Universitas Nusa Putra, Vol. 3, No. 3 Maret 2021.
- Fanny Priscyllia, Perlindungan Privasi Data Pribadi Perspektif Perbandingan Hukum, Jurnal Jatiswara, Volume 34 Nomor 3 November 2019.
- Fauzi Solihin, "Analisa Cakupan Hukum Pengelolaan Perlindungan Hukum Data Pribadi di Indonesia", JISPAR, FISIP Universitas Palangka Raya, Vol. 12, No. 1 Februari 2023.
- Hanafi, "Urgensi Pengaturan Hukum Tentang Perlindungan Data Pribadi Pada Sistem Digital Dalam Pemenuhan Hak Privasi Di Indonesia", Jurnal Hukum dan Sosial, Yayasan Pendidikan Tanggui Baimbaian Kalimantan Selatan, Vol. 1, No. 1 Januari 2023.
- <https://diskominfo.mc.kalselprov.go.id/2020/10/01/perkembangan-teknologi-informasi-dalam-dunia-perdagangan/> diakses tanggal 24 September 2024, Jam 20.30 Wib.
- <https://www.legislation.gov.uk/ukpga/2018/12/part/6/crossheading/offences-relating-to-personal-data/> di terjemahkan menggunakan Google Translate diakses tanggal 24 September 2024, Jam 20.30 Wib
- <https://www.pinsentmasons.com/out-law/guides/misuse-of-private-information/> di terjemahkan menggunakan Google Translate diakses tanggal 24 September 2024, Jam 21.00 Wib
- Jonimandala, G. W., Sondakh, D. K., & Sondakh, J. (2023). Peran Direktorat Tindak Pidana Siber (DITTIPIDSIBER) Bareskrim Polri Dalam Melakukan Penegakan Hukum Terhadap Kejahatan Pencurian dan Penyalahgunaan Data Pribadi. *Innovative: Journal Of Social Science Research*, 3(4).
- Luthiya, Adik Nur, Benny Irawan, and Rena Yulia. "Kebijakan Hukum Pidana Terhadap Pengaturan Pencurian Data Pribadi Sebagai Penyalahgunaan Teknologi Komunikasi Dan Informasi." *Jurnal Hukum Pidana Dan Kriminologi* 2.2 (2021).
- Muhammad Fikri, Abdurrahman Alhakim, Urgensi Pengaturan Hukum Terhadap Pelaku Tindak Pidana Pencurian Data Pribadi di Indonesia, Jurnal Hukum dan Hukum Islam, Volume 9 Nomor 1 Juli 2022, Fakultas Hukum Universitas Internasional Batam, Indonesia.
- Namrysilia Buti Anjawai, Perbandingan Perlindungan Hukum Terkait Data Pribadi di Indonesia dan Jerman, Al-Manhaj: Jurnal Hukum dan Pranata Sosial Islam, Vol. 4, 2 (Desember, 2022), Universitas Internasional Batam.
- Sinta Dewi Rosadi, Perlindungan Privasi Dan Data Pribadi Dalam Era Ekonomi Digital Di

-
- Indonesia, Jurnal Vej, Fakultas Hukum, Universitas Padjadjaran, Volume 4 Nomor 1, hlm 88
- Situmeang, Sahat Maruli Tua. "Penyalahgunaan data pribadi sebagai bentuk kejahatan sempurna dalam perspektif hukum siber." Sasi 27.1 (2021).
- Trisandi, Desmon, and Ahmad Sofian. "Tindak Pidana Penyalahgunaan Data Pribadi Dalam Hukum Siber Indonesia." Journal of Syntax Literate 9.2 (2024).