

BAB I

PENDAHULUAN

1.1 Latar Belakang

Globalisasi dapat dirasakan salah satunya melalui perkembangan teknologi. Perkembangan tersebut dapat dinilai sebagai proses wajar yang tidak terhindar, perkembangan peradaban manusia di bidang ilmu pengetahuan dan teknologi, terutama pada teknologi komunikasi dan informasi telah memudahkan masyarakat dalam mendapatkan informasi. Perkembangan teknologi ini tidak pernah statis, melainkan semakin berkembang dan semakin canggih. Komunikasi yang dulunya memerlukan waktu yang lama dalam penyampaiannya, kini dengan teknologi segalanya menjadi sangat cepat dan seakan tanpa jarak. Salah satu bidang teknologi komunikasi yang kerap menjadi bagian keseharian masyarakat adalah *smartphone* dan internet, keberadaan tersebut membantu percepatan dalam segi komunikasi. Manusia dalam berinteraksi kini dipermudah dengan banyaknya macam media yang hadir. Seiring berjalannya waktu, perkembangan teknologi terkhususnya pada perkembangan internet sehingga menjadi kebutuhan bagi masyarakat. Perkembangan yang sangat signifikan adalah adanya media sosial. Media sosial merupakan media *online*, yaitu media yang diakses memanfaatkan internet dimana para penggunanya dapat menuangkan ide, mengekspresikan diri, maupun mendapatkan berbagai informasi. Kehadiran media sosial memberikan kemudahan bagi manusia untuk berkomunikasi, bersosialisasi, pertukaran informasi, dan lain-lain. Peran teknologi informasi, media,

komunikasi, dan sistem elektronik menjadi krusial dalam mempengaruhi bagaimana masyarakat berperilaku dan berinteraksi di tingkat global. Hal ini menegaskan bahwa perubahan perilaku dan keterhubungan globalitas kita sangat dipengaruhi oleh kemajuan teknologi, yang secara terus-menerus mengubah cara kita memandang dan menghadapi dunia di sekitar kita.¹

Pada konteks teknologi informatika dan sistem elektronik, keuntungan penggunaan internet tercermin dalam berbagai bidang antara lain kemudahan dan percepatan dalam melaksanakan pekerjaan, proses belajar, berkomunikasi dan masih banyak lagi, tetapi pada lain sisi juga telah timbul kasus baru yang perlu mendapat perhatian yaitu diperlukan aturan yang dapat menjamin perlindungan data pribadi dari para pengguna internet (*the protection of privacy rights*) agar dapat terhindar dari penyalahgunaan yang menyebabkan kerugian terhadap masyarakat sosial. Semakin bertambahnya pengguna *smartphone* dan internet pada satu dekade terakhir, maka disadari betapa pentingnya perlindungan data pribadi agar terhindar dari *cybercrime*. Kekhawatiran ini dapat dinyatakan sebagai konsekuensi dari internet dan percepatan teknologi informasi yang berpotensi menimbulkan dampak negatif. Terkadang terdapat situasi di mana kegagalan dan kesalahan seringkali muncul akibat kurangnya perhatian dalam melindungi data pribadi pelanggan yang telah mendaftarkan informasi pribadi mereka di dunia maya. Pada ekosistem digital, data baik berupa teks, gambar, atau video, tidak dapat dihapus secara

¹ Satrio, M. B., & Widiatno, M. W. "Pelindungan Hukum Terhadap Data Pribadi Dalam Media Elektronik (Analisis Kasus Kebocoran Data Pengguna Facebook di Indonesia)". JCA of Law, Vol.1 No.1, Juli 2020, hlm. 33–34

permanen, menciptakan jejak digital yang dapat dipelajari dan ditelusuri. Keberadaan rekam jejak ini menimbulkan risiko yang signifikan, khususnya jika tidak ada perlindungan yang memadai, karena informasi pribadi yang tidak dilindungi dapat bocor dan disalahgunakan oleh pihak yang tidak bertanggungjawab.

Kesadaran masyarakat terhadap kemajuan teknologi pada era globalisasi yang menuntut keefektifan maupun keefesienan menyebabkan bertambahnya pengguna internet, karena internet memudahkan keseharian dalam beraktivitas, maka tidak dapat dipungkiri internet juga menimbulkan bentuk modus kejahatan yang baru yang dikenal sebagai *cybercrime*. Kejahatan siber telah terjadi sejak semakin berkembangnya dunia maya, bahkan hasil data dari Norton Report pada tahun 2013 silam telah memperlihatkan indikasi dan akibat terhadap tindak kejahatan siber di Indonesia cukup serius dan adanya peningkatan sebagaimana dinyatakan pada laman Id-SIRTAII/CC (*Indonesia Security Incident Response Team on Internet Infrastructure/Cordination Center*).² Jika menengok beberapa tahun terakhir sebagaimana terjadi pada Januari 2022, DarkTracer melaporkan setidaknya lebih dari 40 ribu *internet user* (pengguna internet) di Indonesia terinfeksi *stealer* seperti *Redline*, *Raccoon*, *Vidar* dan lainnya. Diduga terdapat lebih dari 502 ribu data kredensial dengan akses domain “.id” (dot id) terbocorkan dan didistribusikan melalui situs gelap. Kebocoran data kredensial para pengguna yang mengakses

² Rosalinda Elsina Latumahina, “Aspek Hukum Perlindungan Data Pribadi di Dunia Maya”, Jurnal Gema Aktualita, Vol. 3, No. 2, Desember 2014, hlm. 15

sejumlah situs pemerintahan antara lain Kemdikbud, BKN, Ditjen Pajak, dan BPJS Ketenagakerjaan, hingga merambah ke data pengguna yang mengakses beberapa aplikasi *e-commerce* seperti *Shopee* dan *Lazada*.³ Direktorat Jenderal Pajak Indonesia (DJP) buka suara soal dugaan 40 ribu data pengguna bocor dan merupakan data kredensial pengguna untuk masuk dalam situs pemerintahan. Direktur Penyuluhan, Pelayanan, dan Hubungan Masyarakat Neilmaldrin Noor menyatakan “data yang dikelola DJP dalam kondisi aman dan dapat diakses sebagaimana mestinya.” Diduga kebocoran data berasal dari perangkat pengguna yang terinfeksi *malware*. Kemudian data diambil dan digunakan untuk masuk ke dalam situs pemerintahan. DJP menyarankan agar pengguna situs web pajak.go.id dan peserta Wajib Pajak segera mengganti kata sandi dengan kata sandi yang lebih kuat dan aman agar tak mudah diretas.⁴

Direktur Penyuluhan, Pelayanan dan Hubungan Masyarakat DJP Kemenkeu, Dwi Astuti menyatakan bahwa sistem DJP sering menjadi incaran para peretas. Kendati dinyatakan hingga saat ini (21/2/2024) sistem DJP memiliki sistem yang baik sehingga tidak pernah terjadi kebocoran data Wajib Pajak. Mengingat per 1 Juli 2024 Nomor Induk Kependudukan (NIK) telah disinkronisasi pada sistem perpajakan, dan digunakan juga sebagai Nomor Pokok Wajib Pajak (NPWP), DJP dapat menjamin kerahasiaan data Wajib

³ Mahmud, A. “Belajar Dari Kebocoran Data Kredensial: Data Yang Paling Berharga adalah Data Pribadi”. <https://www.djkn.kemenkeu.go.id/artikel/baca/14838/Belajar-Dari-Kebocoran-Data-Kredensial-Data-Yang-Paling-Berharga-adalah-Data-Pribadi.html>, Diakses 27 Agustus 2024

⁴ “Dirjen Pajak Buka Suara soal Dugaan Data Pengguna Bocor”, <https://www.cnnindonesia.com/ekonomi/20220303194435-78-766446/dirjen-pajak-buka-suara-soal-dugaan-data-pengguna-bocor>, Diakses 27 Agustus 2024

Pajak. Pada sisi lain, pegawai DJP memastikan data Wajib Pajak tetap dijaga dengan aman serta tidak dengan sengaja dipergunakan di luar kepentingan perpajakan. Direktur Penyuluhan, Pelayanan dan Hubungan Masyarakat DJP Kemenkeu, Dwi Astuti menyatakan apabila terjadi kebocoran data dengan sengaja untuk dipergunakan diluar kepentingan perpajakan maka ancaman atas tindakan tersebut adalah pidana.⁵

Bocornya data dapat bersumber dari berbagai hal antara lain serangan dari *hacker* (peretas), *human error*, atau kurangnya kepatuhan pada protokol keamanan. Perkembangan pertukaran informasi yang semakin cepat menimbulkan kekhawatiran terhadap privasi Wajib Pajak. Percepatan pertukaran informasi dapat disadari dengan keberadaan *Automatic Exchange of Information* (AEOI). Praktik *tax avoidance* yang dilakukan oleh wajib pajak tertentu demi mencari keuntungan merupakan misi atau tujuan utama sistem AEOI diadakan dengan harapan praktik tersebut dapat berkurang atau termitigasi. Indonesia telah menyepakati program pertukaran informasi otomatis yang selanjutnya dikenal sebagai *Automatic Exchange of Information* (disingkat AEOI) pada forum *Organization for Economic Cooperation and Development* (OECD). Hingga tahun 2024, OECD menyatakan dari 94 negara yang ada, sejumlah 55 negara telah sepakat berpartisipasi pada program AEOI. Indonesia turut melaksanakan program pertukaran informasi dimulai pada tahun 2018. AEOI merupakan pertukaran informasi yang melibatkan transmisi

⁵ “Hacker Serang Sistem Pajak, Ditjen Pajak Pastikan Data Wajib Pajak Aman”, <https://www.ssas.co.id/hacker-serang-sistem-pajak-ditjen-pajak-pastikan-data-wajib-pajak-aman/>, diakses 27 Agustus 2024

massal informasi wajib pajak secara internasional. Menelusuri kenaikan kekayaan atau penambahan *asset* setiap wajib pajak dapat dilakukan melalui AEOI, melalui pertukaran informasi saldo tabungan pada bank yang dimiliki setiap wajib pajak baik tabngan yang berada pada negara domisili maupun luar domisili.⁶

Dibangunnya perekonomian di Indonesia sehingga menjadi berkembang dengan kemajuan yang cepat⁷, salah satunya merupakan kontribusi lembaga perbankan. Perbankan dituntut untuk dapat bekerja secara profesional, dapat membaca dan menelaah, serta menganalisis semua kegiatan usaha serta perekonomian nasional. Oleh karena itu maka lembaga perbankan perlu dibina dan diawasi secara terus-menerus agar dapat berfungsi dengan efisien, sehat, wajar, mampu bersaing dan dapat melindungi dana yang disimpan oleh nasabah dengan baik.⁸ Kewajiban untuk merahasiakan rahasia bank dapat mejadi faktor yang meningkatkan rasa percaya masyarakat terhadap suatu bank, hal yang menjadi faktor bisa atau tidak suatu bank untuk mendapat kepercayaan dari nasabah untuk menyimpan dana dan/atau memanfaatkan berbagai macam jasa lain dari bank tersebut agar pengungkapan tidak dilakukan kepada pihak manapun mengenai posisi keuangan maupun riwayat transaksi nasabah yang bersangkutan terhadap lain pihak. Perlu

⁶ Muh. Afdal Yanuar. “*Optimalisasi Penerapan Automatic Exchange of Information (AEOI) dalam Mendorong Pendapatan Negara atas Pungutan Pajak Penghasilan*”. Scientax Jurnal Kajian Ilmiah Perpajakan Indonesia, Vol. 4, No. 2, April 2023, hlm. 219-232

⁷ Hasima, Rahman. “*Implikasi Hukum Terhadap Akad yang Memuat Klausula Penyelesaian Sengketa Perbankan Syariah Melalui Pengadilan Negeri Pasca Putusan Mahkamah Konstitusi Nomor 93/PUU-X/2012*”. SASI, Vol. 26 No. 3, September 2020, hlm. 287

⁸ Siti Sundari Arie, “*Laporan Kompendium Hukum Bidang Perbankan*”. Pusat Penelitian dan Pengembangan Sistem Hukum Nasional Badan Pembinaan Hukum Nasional Kementerian Hukum dan HAM RI, 2011, hlm. 2

diketahui seberapa pentingnya prinsip *bank secrecy*, mengingat faktor utama perkembangan dan pertumbuhan suatu bank berdasarkan rasa percaya dari masyarakat. Oleh karena itu, bagaimana cara-cara bank agar dapat menjaga kepercayaan masyarakat sekaligus yang menjadi nasabahnya yaitu melalui menjaga rahasia sehubungan dengan identitas dan segala sesuatu yang berhubungan dengan nasabahnya.⁹ Sejak dahulu kala prinsip atau asas pada bidang keuangan yaitu *bank secrecy* telah dikenal dalam sejarah keuangan dan finansial, dimulai pada zaman pertengahan, masalah rahasia bidang keuangan ini pengaturannya telah tertera dalam Kitab Undang-Undang Hukum Perdata Jerman dan di kota-kota Italia bagian Utara.¹⁰ Bank wajib menjaga data rekening nasabah karena menjadi bagian dari rahasia bank. Akan tetapi tidak menutup kemungkinan bahwa pihak berwenang seperti pemerintah perlu mengetahui data tersebut dalam rangka melakukannya penyelidikan karena terdapat dugaan adanya kejahatan atau tindakan kriminal seperti pencucian uang, atau penggelapan pajak, maka memungkinkan data nasabah tersebut wajib dibuka untuk selanjutnya dilakukan pemeriksaan.

Peraturan Undang – Undang Nomor 28 tahun 2007 tentang Perubahan Ketiga atas Undang-Undang Nomor 6 Tahun 1983 tentang Ketentuan Umum dan Tata Cara Perpajakan (UU KUP) Pasal 1 ayat 1 menjelaskan bahwa pajak merupakan sumbangan wajib kepada negara oleh orang atau badan.

⁹ Fitriah Faisal, “*Pengaruh Prinsip Kerahasiaan Bank Terhadap Tindak Pidana Pencucian Uang*”, Al-Amwal: Journal of Islamic Economic Law, Vol. 3, No.1, Agustus 2018, hlm. 36

¹⁰ Muhammad Djumhana, “*Hukum Perbankan di Indonesia*”, Citra Aditya Bakti, Bandung, 2006, hlm. 110

Keberadaan sistem AEoI ini membuat Wajib Pajak merasa dirugikan karena kewajiban yang timbul. Diperlukan kepastian perlindungan data pribadi di Indonesia atau adanya instrumen hukum yang responsif pada era global dengan percepatan pertukaran informasi yang menyebabkan peningkatan potensi pelanggaran kerahasiaan atau bahkan penyalahgunaan dalam penggunaan data yang diperoleh. Adanya pertukaran informasi pada segi perpajakan yang dikenal dengan AEoI maka privasi Wajib Pajak semakin terbuka, dan prinsip kerahasiaan bank menjadi tidak terlaksana, dan kebocoran data menjadi salah satu kekhawatiran yang perlu dipertimbangkan. Mengingat privasi atau perlindungan data pribadi merupakan hak asasi manusia, serta menimbang cepatnya pertukaran informasi, dan penyebaran data pada media sosial melalui internet, maka keberadaan instrumen hukum mengenai privasi atau perlindungan data wajib adanya. Apapun penyebab kebocoran data pribadi, akan berdampak merugikan individu dan masyarakat. Terdapat potensi ancaman langsung terhadap privasi, kebocoran ini juga merusak kepercayaan publik terhadap kemampuan pemerintah dalam melindungi data pribadi warganya. Beberapa poin dampak bocornya data antara lain dapat disimpulkan sebagai berikut;

- 1) Pencurian Identitas: Pelaku kejahatan dapat mencuri data pribadi atau identitas. Hal ini bisa berujung pada pembukaan rekening bank fiktif, aplikasi kredit palsu, dan bahkan kegiatan kriminal lainnya atas nama korban.

- 2) Publik Kehilangan Kepercayaan: Lembaga pemerintah yang mengalami kebocoran data dapat merusak kepercayaan masyarakat terhadap institusi pemerintah yang dinilai seharusnya menjadi pelindung. Hal tersebut berpotensi menyebabkan rakyat menjadi skeptis, atau kurang bahkan tidak berpartisipasi dalam program atau legitimasi pemerintahan.
- 3) Kerugian Ekonomi: Korban pencurian identitas biasanya mengalami kerugian finansial yang signifikan. Bagi perusahaan yang mengalami kebocoran data dapat diberi sanksi hukum dan kehilangan reputasi, yang berdampak pada penurunan nilai saham dan kepercayaan investor.

Negara berkewajiban memberikan rasa aman bagi masyarakat yang berpotensi mengalami berbagai bentuk penyalahgunaan atau kejahatan terhadap data pribadinya yang berasal dari dalam maupun luar negara. Negara melalui pemerintahnya memerlukan regulasi yang menggambarkan dan membatasi akses data pribadi pada keadaan tertentu sebagai bentuk perlindungan dan jaminan hukum atas pelanggaran yang dapat merugikan. Sehingga atas dikemukakan latar belakang tersebut, penulis menyimpulkan Rumusan Masalah serta Tujuan Penelitian sebagai berikut;

1.2 Rumusan Masalah

- 1) Bagaimana optimalisasi instrumen hukum menjamin perlindungan data Wajib Pajak Indonesia dengan diterapkannya sistem *Automatic Exchange of Information* pada perbankan?
- 2) Bagaimana pertanggungjawaban saat terjadi kebocoran data perbankan terhadap Wajib Pajak Indonesia?

1.3 Tujuan Penelitian

- 1) Untuk mengetahui optimalisasi instrumen hukum yang menjamin perlindungan data Wajib Pajak dengan diterapkannya sistem *Automatic Exchange of Information* pada perbankan.
- 2) Untuk mengetahui pihak yang bertanggung jawab apabila terdapat kebocoran data perbankan terhadap Wajib Pajak Indonesia.

1.4 Manfaat Penelitian

1.4.1 Manfaat Teoritis

Hasil penelitian ini diharapkan dapat memberikan manfaat secara teoritis dengan harapan dapat memberi kontribusi pengembangan ilmu hukum khususnya mengenai Pelindungan Data Pribadi di Indonesia.

1.4.2 Manfaat Praktis

Manfaat bagi peneliti hukum, dapat menambah wawasan terkait akibat terjadinya kebocoran data, prosedur penerapan Pelindungan Data Pribadi, dan pihak yang wajib bertanggungjawab apabila kebocoran data nasabah atau Wajib Pajak terjadi. Penelitian ini bertujuan agar dapat menambah wawasan para pembaca yaitu mengetahui lebih dalam terkait penerapan pertukaran informasi otomatis (AEOI) pada sistem perpajakan di Indonesia, dan risiko serta dampak sehubungan dengan data perbankan nasabah atau Wajib Pajak ditinjau pada sisi keamanan Pelindungan Data Pribadi.

1.5 Sistematika Penulisan

Sistematika Penulisan tesis ini terdiri dari 5 (lima) Bab, dimana masing-masing bab terdiri masing-masing dalam beberapa sub-bab yang bertujuan untuk memperjelas cakupan permasalahan yang diteliti di bab tersebut. Sistematika masing-masing bab dan cakupan pembahasannya sebagai berikut.

Bab I Pendahuluan. Bab ini merupakan awal penulisan dengan mengemukakan latar belakang tentang kemajuan teknologi yang membuat batas – batas dalam berkomunikasi terminimalisir, dan pertukaran informasi dapat dilakukan dengan cepat, yaitu salah satunya dengan penerapan sistem AEoI yang bertujuan optimalisasi pendapatan negara melalui pajak. Pertukaran informasi otomatis ini memberikan akses kepada aparat pajak mengenai data perbankan berupa tabungan atau simpanan nasabah. Penerapan AEoI menimbulkan pertanyaan mengenai optimalisasi kepastian hukum Pelindungan Data Pribadi Wajib Pajak. Apa tindakan hukum selanjutnya akan dibahas dalam tesis ini. Selanjutnya dikemukakan pula rumusan masalah, tujuan penelitian dan tipe penelitian yang digunakan yakni yuridis normatif.

Bab II Tinjauan Pustaka. Bab ini terbagi dalam 2 (dua) sub bab. Bab 2.1. Tinjauan Teori, pada sub bab ini terbagi dalam 3 (tiga) sub bab. Bab 2.1.1 Teori Perlindungan Hukum yang menjadi salah satu dasar teori penelitian ini. Bab 2.1.2 Pengertian dan Hakekat Wajib Pajak di Indonesia. Bab 2.1.3 Definisi dan Pengaturan *Automatic Exchange of Information* (AEoI) di

Indonesia yang telah diatur melalui Undang-Undang Nomor 9 Tahun 2017 tentang Penetapan Peraturan Pemerintah Pengganti Undang-Undang Nomor 1 Tahun 2017 Tentang Akses Informasi Keuangan Untuk Kepentingan Perpajakan Menjadi Undang-Undang (selanjutnya disingkat menjadi UU No 9 Tahun 2017). Bab 2.2 Tinjauan Konseptual yang terbagi menjadi 2 sub bab. Bab 2.2.1 Kepastian Hukum Pelindungan Data Perbankan Wajib Pajak Indonesia dengan memperhatikan berbagai aturan yang berlaku antara lain UU Perpajakan, UU Perbankan, Aturan OJK, Aturan Bank Indonesia, dan UU Pelindungan Data Pribadi. Bab 2.2.2 Akibat Hukum Bagi Penyebar Data, bab ini mengupas apa yang menjadi hak Wajib Pajak mengenai data pribadinya, selanjutnya mengenai kemungkinan terjadinya kebocoran data baik yang disebabkan oleh pihak-pihak tidak bertanggungjawab, maupun kesalahan sistem perbankan, atau sistem Direktorat Jenderal Pajak, dan menganalisa tindakan hukum yang dapat diterapkan pada para penyebar data pribadi menurut hukum positif yang berlaku yakni UU Perpajakan dan UU PDP.

Bab III Metode Penelitian, terbagi menjadi 5 (lima) sub bab. 3.1 Jenis Penelitian yuridis normatif yaitu penelitian hukum kepustakaan. Bab 3.2 Jenis Data yaitu bahan hukum primer yaitu peraturan yang berlaku, bahan hukum sekunder yaitu buku maupun jurnal dan bahan hukum tersier yaitu berita atau artikel dengan penelusuran pada internet. Bab 3.3 Cara Perolehan Data atau bahan hukum dilakukan melalui penelusuran studi pustaka, dan penelusuran internet, 3.4 Jenis Pendekatan dalam penelitian ini dilakukan adalah

pendekatan peraturan perundang-undangan atau *statute approach* dan *comparative approach* sebagai tambahan dalam melakukan analisa. Bab 3.5 Analisa Data menggunakan silogisme deduksi.

Bab IV Hasil Penelitian dan Analisis, pada bab ini terbagi menjadi 3 (tiga) sub bab. Bab 4.1 Hasil Penelitian tentang Penerapan AEOI Ditinjau dari Perspektif Pelindungan Data Pribadi, membahas mengenai penelitian terdahulu. Bab 4.2 Analisis Optimalisasi Instrumen Hukum Pelindungan Data Wajib Pajak dengan diterapkannya AEOI, dan Bab 4.3 Analisis Pertanggungjawaban atau Akibat Hukum Kebocoran Data Pribadi Wajib Pajak.

Bab V Penutup. Bab ini merupakan bab terakhir yang merupakan bagian penutup yang akan menyimpulkan hasil dari penelitian dan juga analisis pada bab - bab sebelumnya agar dapat mendapatkan kesimpulan atas permasalahan yang dikaji dalam penelitian ini. Selain kesimpulan, juga saran sebagai sarana bagi pihak-pihak terkait dalam bagi permasalahan tersebut.