

BAB I

PENDAHULUAN

A. Latar Belakang

Setiap orang memiliki hak konstitusional, yaitu hak dasar yang dijamin oleh Undang-Undang Dasar 1945. Negara memiliki kewajiban melindungi seluruh kepentingan dari warga Negara. Kewajiban konstitusional yang dimaksud tertuang dalam Alinea Ke 4 pembukaan Undang-Undang Dasar Negara Republik Indonesia Tahun 1945, yang menyatakan bahwa Negara wajib melindungi segenap bangsa Indonesia dalam meningkatkan kesejahteraan umum, mencerdaskan kehidupan bangsa, dan melaksanakan ketertiban dunia berdasar kemerdekaan, perdamaian dunia serta keadilan sosial (UUD 1945).¹ Maka sebagai dasar legal formal Undang-undang Dasar menjadi tumpuan bagi keamanan hidup bernegara, di mana warga Negara baik secara sosial dan politik maupun ekonomi, dilindungi secara utuh hak mereka.

Manusia dan HAM merupakan dua kesatuan yang tidak dapat dipisahkan. Sejak manusia lahir ke muka bumi, manusia telah memiliki Hak Asasi Manusia yang menjadi kodrat bagi mereka dan tidak dapat diambil oleh manusia lain. Dalam artikel “Transpuan Kian Terpinggirkan” disebutkan bahwa HAM itu sebenarnya hanya membutuhkan manusia. HAM tidak memandang latar belakang, transpuan, pemain bulutangkis, maupun presiden sekalipun, selama ia seorang manusia dia dipastikan mempunyai Hak Asasi dan tidak boleh diciderai atau dilanggar dengan

¹ Undang-Undang Dasar Negara Republik Indonesia Tahun 1945

alasan apapun. Baik itu dengan pilihan politik, orientasi seksual, gender, identitas, maupun kewarganegaraan. Selama ia seorang manusia maka ia berhak memiliki hak yang sama untuk dapat hidup layaknya manusia lainnya di dunia ini.² Terdapat 2 (dua) teori mengenai perolehan hak, yaitu teori McCloskey dan teori Joel Feinberg. Menurut teori McCloskey, dikatakan bahwa pemberian hak itu merupakan sesuatu yang harus dilakukan, dimiliki, atau telah dilakukan. Sedangkan dalam teori Joel Feinberg diasumsikan bahwa pemberian hak secara penuh merupakan satu kesatuan tuntutan hukum (manfaat yang diperoleh dari pelaksanaan hak yang menyertai pelaksanaan kewajiban³

Hak konstitusional yang diatur dalam UUD 1945, salah satunya adalah hak atas perlindungan diri pribadi. Hak tersebut, ditegaskan oleh Pasal 28 G Ayat (1) bahwa warga Negara berhak atas perlindungan diri pribadi, keluarga, kehormatan, martabat dan harta benda di bawah kekuasaannya serta berhak atas rasa aman dan perlindungan dari ancaman ketakutan untuk berbuat atau tidak berbuat sesuatu yang merupakan hak asasi (UUD 1945)⁴. Pada pasal tersebut, mengasumsikan hak pribadi sebagai hak yang melekat pada diri, salah satunya hak milik. Tetapi, dengan berkembangnya teknologi informasi dan komunikasi harusnya hak pribadi tidak hanya diartikan sebagai hak milik. Hak pribadi seharusnya

² National Geographic Indonesia, "*Transpuan Kian Terpinggirkan*", Kompas Gramedia, September, 2020, 15.

³ Tim ICCE UIN Jakarta, *Demokrasi, Hak Asasi Manusia dan Masyarakat Madani* (Jakarta: Prenada Media, 2003), 199.

⁴ Undang-Undang Dasar Negara Republik Indonesia Tahun 1945, Pasal 28G Ayat (1).

juga sebagai hak atas privasi. Hak privasi bersifat lebih sensitif yang dapat mewakili hak pribadi tersebut. Hak pribadi merupakan hak yang sensitif yang berkaitan dengan data pribadi atau identitas seseorang. Identitas, menurut interpretasi akan termasuk di antaranya: Kartu Tanda Penduduk (KTP); Surat Ijin Mengemudi (SIM); Paspor, Kartu Keluarga (KK); Nomor Pokok Wajib Pajak (NPWP); Nomor Rekening, Sidik jari, e-mail, Nomor Telepon, ciri khas seseorang serta data pribadi media sosial dan sebagainya.⁵

Pada era kemajuan teknologi informasi dan komunikasi sekarang, bukan hanya perkembangan industri manufaktur saja yang sudah berkembang dengan pesat. Fasilitas atau layanan perbankan juga telah berkembang jauh. Fasilitas yang perubahannya paling membawa dampak yang signifikan terhadap jalannya aktifitas perbankan di Indonesia salah satunya adalah layanan perbankan elektronik. Layanan perbankan elektronik adalah suatu layanan kegiatan yang bisa digunakan oleh nasabah bank untuk bertransaksi dan pembayaran melewati website atau internet dengan berbagai macam fitur yang disediakan dan difasilitasi sistem keamanan online oleh pihak Bank. Fasilitas layanan perbankan elektronik ini memberikan kemudahan bagi masyarakat dalam bertransaksi atau pembayaran tanpa harus pergi ke Bank secara langsung. Walaupun begitu, terlepas diterimanya kelebihan dan dampak positif perkembangan ini oleh para nasabah, dalam menggunakan layanan perbankan elektronik

⁵ Kusnadi. *Perlindungan Hukum Terhadap Data Pribadi dalam Era Digital*, Jakarta 2023: Pustaka Keadilan

harus didasarkan pada prinsip kehati-hatian dalam bertransaksi.⁶ Bank adalah lembaga keuangan yang berperan penting dalam menyediakan berbagai layanan keuangan kepada masyarakat. Dalam era digital yang berkembang, banyak Bank telah mengadopsi layanan perbankan elektronik untuk memberikan kemudahan akses dan transaksi kepada nasabah mereka. Namun, dalam beberapa kasus, Bank dapat mengalami gangguan pelayanan elektronik yang disebabkan oleh serangan Hacker.⁷

Secara teoritik, perlindungan data pribadi berakar pada teori hak privasi (*right to privacy*) yang pertama kali diperkenalkan oleh Samuel D. Warren dan Louis D. Brandeis dalam artikel mereka berjudul *The Right to Privacy*. Sebuah hak yang melekat pada diri pribadi, perdebatan mengenai pentingnya perlindungan terhadap hak atas privasi seseorang, semula dikemukakan dalam putusan-putusan pengadilan di Inggris dan kemudian di Amerika Serikat. Hingga kemudian menuliskan konsepsi hukum hak atas privasi dalam “*The Right to Privacy*”, yang pertama kali mengonseptualisasikan hak atas privasi sebagai sebuah hak hukum.⁸

Secara sederhana, gagasan ini diadopsi dari teks yang ditulis berjudul “*Treatise on the Law of Torts*” yang memperkenalkan istilah “*the right to*

⁶ Ade Borami Ju, R. Nurhayati, & A. A. R. D. Taufik, *Perlindungan Hukum terhadap Nasabah dalam Transaksi Perbankan Elektronik di Indonesia*. Jurnal Hukum & Pembangunan, 51(2) 2021, 123–134.

⁷ Marcelliana, R., Putri, S. M., & Yuliana, D, *Analisis Serangan Siber terhadap Sistem Perbankan Elektronik di Indonesia*. Jurnal Teknologi dan Keamanan Siber, 5(1) 2023, 45–58

⁸ Warren, S. D., & Brandeis, L. D. *The Right to Privacy*. Harvard Law Review, 4(5) 1890, 193–220.

be let alone” atau “hak untuk dibiarkan sendiri”.⁹ Definisi atau hak untuk dibiarkan sendiri didasarkan atas dua hal: (i) kehormatan pribadi, dan; (ii) nilai-nilai seperti martabat individu, otonomi dan kemandirian pribadi. Ini kemudian mendapat justifikasi dan pengakuan dengan adanya beberapa gugatan hukum kemudian yang memberikan pembenaran tentang betapa perlunya perlindungan hak atas privasi, terutama dengan sandaran alasan moralitas. Dalam konteks ini juga menegaskan bahwa perlindungan data pribadi, terutama kaitannya dengan transaksi pinjaman online, menjadi sangat urgen.¹⁰

Konsep tersebut mencoba mendetailkan cakupan ruang lingkup dari hak privasi seseorang, dengan merujuk setidaknya pada empat bentuk gangguan terhadap diri pribadi seseorang, yakni:

1. Gangguan terhadap tindakan seseorang mengasingkan diri atau menyendiri atau gangguan terhadap relasi pribadinya.
2. Pengungkapan fakta-fakta pribadi yang dilakukan secara publik.
3. Publisitas yang menempatkan seseorang secara keliru dihadapan publik.

⁹ Cooley, T. M. *A Treatise on the Law of Torts or the Wrongs Which Arise Independent of Contract*. Chicago, 1879. Callaghan & Company.

¹⁰ Priliyasi, R. A. *Perlindungan Data Pribadi Konsumen dalam Transaksi Pinjaman Online di Indonesia*. Jurnal Hukum dan Teknologi, 3(2) 2019, 112–126

4. Penguasaan tanpa ijin atas kemiripan seseorang untuk keuntungan orang lain.¹¹

Indonesia sebagai Negara berasaskan hukum maka Negara harus menjamin perlindungan atas Hak Asasi Manusia, termasuk kerahasiaan data pribadi warga Negeranya. Maraknya kasus pelanggaran hukum terhadap penyalahgunaan data pribadi dipicu semakin meningkatnya penggunaan teknologi informasi dan komunikasi dalam aktivitas masyarakat yang menggunakan platform digital dalam mengakses data.¹²

Data pribadi yang dimiliki oleh nasabah menjadi suatu kerahasiaan yang harus dilindungi oleh bank. Adanya kelalaian maupun lemahnya sistem perlindungan, mengakibatkan Bank belum mampu memberikan perlindungan secara maksimal dalam menjaga data pribadi para nasabahnya, hal ini akan menimbulkan penyalahgunaan data pribadi nasabah oleh orang yang tidak memiliki wewenang terhadap data tersebut, kemudian digunakan untuk keperluan komersil pribadi maupun kepentingan lain yang dapat merugikan nasabah. Banyaknya penyalahgunaan data pribadi ini dilihat dari banyaknya pesan singkat atau short message service (SMS) maupun panggilan telepon dalam menawarkan produk-produk di bidang jasa keuangan seperti produk

¹¹ Prosser, W. L. *Privacy*. California Law Review, 48(3) 1960, 383–423.

¹² Evelyn, Y., & Emmy, F. S. *Perlindungan Hukum Terhadap Penyalahgunaan Data Pribadi di Era Digital*. Jurnal Hukum dan Teknologi, 4(1) 2020, 55–68

asuransi, fasilitas kredit, penawaran voucher liburan ataupun jenis penyalahgunaan lainnya.¹³

Beberapa regulasi yang mengatur tentang perlindungan data pribadi konsumen dan nasabah yang berlaku di Indonesia:

1. Undang-Undang Nomor 7 Tahun 1992 Tentang Perbankan dengan perubahan Undang-Undang Nomor 10 Tahun 1998, yang menentukan bahwa Bank sebagai pihak yang menawarkan jasanya sebagai penyimpanan keuangan dan kegiatan keuangan lainnya harus merahasiakan keterangan terkait nasabahnya, penyimpanannya dan simpanannya;
2. Undang-Undang Nomor 43 Tahun 2009 tentang Kearsipan, yang mengatur mengenai arsip data-data nasabah dan pelanggan yang merupakan warga negara Indonesia yang memiliki hak untuk dilindungi;
3. Undang-Undang Nomor 8 Tahun 1997 tentang Dokumen Perusahaan, yang mengatur mengenai dokumen berkaitan dengan data pribadi para pengguna;
4. Undang-Undang Nomor 36 Tahun 2009 tentang Kesehatan, yang dalam perannya memiliki kedudukan hukum atas keamanan data pribadi pasien;

¹³ Violiana, E., & Zahrani, A. *Tinjauan Yuridis Terhadap Penyalahgunaan Data Pribadi oleh Pihak Ketiga dalam Penawaran Produk Jasa Keuangan*. Jurnal Hukum dan Etika, 2020, 101–115.

5. Undang-Undang Nomor 36 Tahun 1999 tentang Telekomunikasi (UU Telekomunikasi), yang mengatur berbagai macam tindakan yang kemungkinan berpeluang membahayakan penggunaan data pribadi pelanggan dan nasabah di sistem elektronik;
6. Undang-Undang Nomor 24 Tahun 2013 tentang Perubahan Atas Undang-Undang Nomor 23 Tahun 2006 tentang Administrasi Kependudukan (UUAdminduk)
7. Undang-Undang Nomor 19 Tahun 2016 Tentang perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.
8. Peraturan Pemerintah Nomor 82 Tahun 2012 Tentang Penyelenggaraan Sistem dan Transaksi Elektronik.
9. Peraturan Menteri Komunikasi dan Informasi Nomor 20 Tahun 2016 tentang Perlindungan Data Pribadi Dalam Sistem Elektronik
10. Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik.

Dengan adanya peraturan-peraturan tersebut maka secara otomatis pengolahan data dan informasi harus dikelola secara baik, jelas dan terarah. Apabila tidak dikelola dengan tepat, maka akibatnya bisa fatal dan berbahaya karena berujung dengan penyalahgunaan dan

penyerangan kejahatan *cybercrime*. Maka dari hal tersebut diperlukan analisis manajemen risiko guna menghadapi serangan *cybercrime*.¹⁴ Karena *cybercrime* memiliki potensi terhadap hilangnya sistem informasi dan kendali data pribadi dan hal tersebut sulit untuk diatasi. Kejahatan pencurian data yang dilakukan oleh *hacker* yang tidak bertanggung jawab tentu menimbulkan kerugian bagi korbannya. Begitupun dengan korban atas tindakan *phising* yang membuat data-data pribadi korban dengan bebas diperjual belikan dengan risiko yang harus ditanggung korban sangat besar. Maka penindakan kejahatan siber harus dikenakan hukuman yang berat.

Terjadinya kasus kebocoran data pribadi, maka dapat terlihat adanya kelemahan sistem, kurangnya pengawasan, sehingga data pribadi dapat disalahgunakan dan mengakibatkan kerugian bagi pemilik data tersebut. Penyalahgunaan, pencurian, penjualan data pribadi merupakan suatu pelanggaran hukum dalam bidang teknologi informasi dan juga dapat dikategorikan sebagai pelanggaran atas hak asasi manusia, karena data pribadi merupakan bagian dari hak asasi manusia yang harus dilindungi.¹⁵ Banyak kejahatan yang memanfaatkan data pribadi di era digital ini, sehingga harus dilindungi. Namun, banyak orang tidak menyadari bahwa informasi pribadi mungkin disalahgunakan oleh pihak

¹⁴ Ineu Rahmawati, "Analisis Manajemen Risiko Ancaman Kejahatan Siber (Cyber Crime) Dalam Peningkatan Cyber Defense," Jurnal Pertahanan & Bela Negara7, No. 2 (October 3, 2017), hal 53.

¹⁵ Situmeang, F. *Perlindungan Data Pribadi dalam Era Digital: Tinjauan Hukum dan Hak Asasi Manusia*. Jurnal Teknologi dan Hukum, 2021, 45–59.

ketiga yang tidak bertanggungjawab. Pelindungan data yang buruk telah mengakibatkan peretasan dan kebocoran data yang meluas. Peristiwa hukum seperti ini merupakan suatu bentuk kejahatan di dunia maya (*cyber crime*) seperti peretasan (*hacking*) media sosial dan *cracking* (pembajakan), sehingga mengarah pada pelanggaran data pribadi, pemerasan, intimidasi, pencemaran nama baik, hingga terjadinya penipuan online. Perlu diketahui bahwa, transaksi timbul akibat adanya suatu hubungan hukum yang dilindungi disengaja maupun tidak disengaja.¹⁶

Contoh kasus kebocoran data yang terjadi pada Bank BSI, Kebocoran data pribadi yang terjadi pada Bank Syariah Indonesia (BSI) pada Mei 2023 menjadi preseden serius dalam dunia perbankan nasional. Insiden ini tidak hanya mengganggu operasional layanan perbankan, tetapi juga mengancam hak-hak dasar nasabah atas pelindungan data pribadi yang dijamin oleh Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi (UU PDP). Gangguan pada sistem layanan BSI mulai terjadi pada tanggal 8 Mei 2023, yang menyebabkan nasabah tidak dapat mengakses layanan digital seperti BSI Mobile, ATM, maupun teller. Pada awalnya, gangguan ini disebut sebagai pemeliharaan sistem rutin. Namun, publik dikejutkan dengan klaim dari kelompok peretas LockBit, yang menyatakan telah meretas sistem BSI dan mencuri sekitar 1,5 *terabyte* data, termasuk data pribadi dan keuangan milik lebih dari 15 juta

¹⁶ Siahaan, M. *Cyber Crime dan Perlindungan Data Pribadi dalam Hukum Indonesia*. Jurnal Hukum dan Teknologi Informasi, 2022, 78–90

nasabah dan karyawan BSI. Insiden ini menimbulkan kekhawatiran serius mengenai ketidakpatuhan institusi perbankan terhadap standar perlindungan data yang telah ditetapkan dalam UU PDP. Berdasarkan ketentuan dalam pasal 35 sampai 39 UU PDP, setiap pengendali data pribadi, termasuk institusi keuangan, wajib melindungi data yang dikelolanya dari akses ilegal, kebocoran, dan penyalahgunaan. Kegagalan BSI dalam mencegah serangan ini menunjukkan lemahnya ketahanan siber lembaga keuangan nasional, serta kurangnya sistem mitigasi dan respons insiden siber yang memadai.¹⁷

Kejadian ini menjadi ujian nyata bagi efektivitas Undang-Undang Nomor. 27 Tahun 2022, apakah regulasi tersebut cukup kuat dalam memaksa lembaga keuangan memprioritaskan perlindungan data nasabah secara menyeluruh. Peristiwa ini menegaskan perlunya kolaborasi antara pemerintah, regulator seperti Otoritas Jasa Keuangan (OJK) dan Kementerian Komunikasi dan Informatika (Kominfo), serta institusi perbankan untuk memperkuat infrastruktur keamanan nasional. Selain itu, insiden BSI menjadi momentum penting bagi lembaga keuangan lain untuk melakukan audit keamanan data secara berkala, memperbarui protokol keamanan siber, dan meningkatkan investasi pada teknologi proteksi data. Edukasi dan sosialisasi kepada masyarakat dan nasabah juga menjadi hal yang tidak kalah penting, agar mereka memahami risiko serta

¹⁷ Maulana, R. A., & Fitriana, N. D. (2023). *Dampak Kebocoran Data terhadap Kepercayaan dan Loyalitas Nasabah di Bank Syariah Indonesia*. Jurnal RAIS: Research and Innovation in Islamic Studies.

langkah mitigasi yang dapat dilakukan dalam penggunaan layanan perbankan elektronik.

Kasus kebocoran data pada Bank Syariah Indonesia merupakan peringatan serius tentang pentingnya implementasi perlindungan data pribadi yang komprehensif dan berkelanjutan dalam layanan perbankan elektronik. Kegagalan dalam aspek teknis, manajerial, dan kepatuhan hukum dapat berdampak luas, tidak hanya bagi nasabah yang terdampak, tetapi juga bagi stabilitas sistem keuangan nasional dan kepercayaan publik terhadap layanan digital perbankan. Oleh karena itu, penguatan regulasi, pengawasan, serta penerapan teknologi dan budaya keamanan siber yang holistik harus menjadi prioritas utama semua pemangku kepentingan.

Alasan hak privasi harus dilindungi adalah, Pertama, dalam membina hubungan dengan orang lain, seseorang harus menutupi sebagian kehidupan pribadinya sehingga dia dapat mempertahankan posisinya pada tingkat tertentu. Kedua, seseorang di dalam kehidupannya memerlukan waktu untuk menyendiri sehingga privasi sangat dibutuhkan oleh seseorang, Ketiga, privasi adalah hak yang berdiri sendiri dan tidak bergantung kepada hak lain akan tetapi hak ini akan hilang apabila orang tersebut mempublikasikan hal-hal yang bersifat pribadi kepada umum. Keempat, privasi juga termasuk hak seseorang untuk melakukan hubungan domestik termasuk bagaimana seseorang membina perkawinan, membina keluarganya dan orang lain tidak boleh mengetahui hubungan pribadi

tersebut sehingga kemudian menyebutnya sebagai *the right against the word*. Kelima, alasan lain mengapa privasi patut mendapat perlindungan hukum karena kerugian yang diderita sulit untuk dinilai. Kerugiannya dirasakan jauh lebih besar dibandingkan dengan kerugian materil, karena telah mengganggu kehidupan pribadinya, sehingga bila ada kerugian yang diderita maka pihak korban wajib mendapatkan ganti rugi.¹⁸

Fenomena ini mendorong pemerintah untuk merespons kebutuhan regulatif dalam perlindungan data pribadi melalui pengesahan Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi (UU PDP). Undang-undang ini merupakan instrumen hukum pertama di Indonesia yang secara khusus mengatur hak dan kewajiban subjek data, tanggung jawab pengendali data, serta mekanisme perlindungan hukum bagi korban pelanggaran data. Undang-Undang Perlindungan Data Pribadi juga menandai transisi penting dalam sistem hukum nasional menuju perlindungan hak digital warga negara, sejalan dengan tren global yang mengedepankan prinsip privasi sebagai hak asasi manusia. Namun demikian, meskipun secara yuridis formal Indonesia telah memiliki payung hukum yang progresif, implementasi Undang-Undang Perlindungan Data Pribadi masih menghadapi berbagai tantangan struktural dan kultural, terutama dalam sektor keuangan dan perbankan. Perbankan merupakan salah satu sektor yang sangat sensitif terhadap isu perlindungan data karena keterkaitannya dengan rahasia nasabah dan

¹⁸ Kusnadi, B. *Perlindungan Hukum terhadap Hak Privasi dalam Era Digital*. Jurnal Hukum dan Hak Asasi Manusia, 2021, 134–146.

stabilitas sistem keuangan. Belum meratanya literasi digital di kalangan nasabah, lemahnya tata kelola data di sebagian lembaga keuangan, dan kurangnya mekanisme pengawasan yang efektif menjadi tantangan besar dalam penerapan ketentuan UU PDP.

Dalam konteks Indonesia sebagai negara dengan mayoritas penduduk Muslim, kajian terhadap perlindungan data pribadi tidak hanya penting dari aspek legal-formal, namun juga relevan untuk dikaji dari sudut pandang normatif Islam, khususnya dalam kerangka *Sadd Az-Dzariah*. *Sadd Az-Dzariah*, yaitu prinsip penutupan segala jalan yang dapat menjerumuskan pada kerusakan (*mafsadat*), meskipun pada awalnya perbuatan tersebut secara hukum asal bersifat mubah atau netral. Konsep ini berangkat dari kehati-hatian syariat dalam mencegah *kemudharatan* dan menyelamatkan *maslahat* umat. Sebagaimana dikemukakan oleh Imam al-Qarafi, “*Sadd Az-Dzari’ah* adalah menutup sarana yang secara lahiriah mubah tetapi membawa kepada perbuatan yang haram.”¹⁹

Secara terminologis, *Sadd Az-Dzari’ah* berarti menutup jalan atau sarana menuju kerusakan (*mafsadah*). Dalam kerangka *ushul fiqh*, konsep ini digunakan untuk mencegah hal-hal yang pada dasarnya mubah namun berpotensi besar menimbulkan kemudharatan atau pelanggaran syariat apabila dibiarkan. Imam Malik merupakan ulama yang konsisten menggunakan konsep ini dalam banyak fatwanya. Ia berpendapat bahwa mencegah kerusakan lebih diutamakan daripada menarik kemaslahatan,

¹⁹ Al-Qarafi, *Al-Furūq*, Jilid 2, Beirut: *Dār al-Ma’rifah*, 2001, h. 33.

terutama jika risiko kerusakan lebih dominan.²⁰ Perlindungan data pribadi dalam sistem perbankan elektronik, *Sadd Az-Dzari'ah* dapat diaplikasikan sebagai kerangka etik dan hukum yang mencegah segala bentuk tindakan, prosedur, atau sistem yang berpotensi membuka celah pelanggaran data. Misalnya, praktik pengumpulan data tanpa persetujuan eksplisit, penggunaan data nasabah untuk kepentingan komersial, atau lemahnya sistem keamanan informasi dalam bank digital merupakan *dzari'ah* yang harus ditutup karena mengarah pada potensi pelanggaran terhadap kehormatan dan harta nasabah. Kebocoran data, dalam konteks ini, dapat menyebabkan pencurian identitas, kerugian finansial, hingga pelanggaran privasi yang merupakan hak dasar manusia.²¹

Perlindungan terhadap *al-māl* (harta) dan *al-'ird* (kehormatan) adalah bagian dari lima tujuan pokok syariat. Ketika data pribadi nasabah digunakan secara tidak sah, hal ini dapat merusak dua aspek penting tersebut. Dengan pendekatan *Sadd az-Dzari'ah*, tindakan-tindakan preventif dapat diambil sebelum pelanggaran terjadi, seperti pembatasan akses data, peningkatan enkripsi digital, edukasi terhadap pegawai bank mengenai etika pengelolaan informasi, serta implementasi prinsip *data minimization*, yaitu hanya mengumpulkan data yang benar-benar diperlukan.²²

²⁰ Yusuf al-Qaradawi, *Kaedah-Kaedah Fiqhiyyah* (Kairo, Maktabah Wahbah, 1994), hl.

²¹ Yusuf al-Qaradawi, *Kaedah-Kaedah Fiqhiyyah*, hl 92–95.

²² Zuhaili, *Ushul al-Fiqh al-Islami*, Jilid 2 (Damaskus: Dar al-Fikr, 1986), hl. 838–840.

Dalam konteks perlindungan data pribadi, akses bebas terhadap data nasabah tanpa pengamanan yang kuat merupakan bentuk *dzari'ah* (sarana) yang secara potensial mengarah pada pelanggaran hak, penipuan, peretasan, dan pencemaran reputasi digital seseorang. Maka, dari sudut pandang *fiqh siyasah*, sistem keamanan digital harus dirancang tidak hanya sebagai alat reaktif terhadap pelanggaran yang sudah terjadi, tetapi menjadi instrumen *preventif* untuk mencegah terjadinya potensi kejahatan digital, sebagai penerapan nyata prinsip *Sadd az-Dzari'ah* dalam konteks hukum perbankan elektronik modern. Prinsip ini selaras dengan nilai-nilai dalam Al-Qur'an yang secara tegas melarang segala bentuk pelanggaran privasi. Seperti firman Allah SWT dalam Al-Qur'an berbunyi:

يَا أَيُّهَا الَّذِينَ آمَنُوا اجْتَنِبُوا كَثِيرًا مِّنَ الظَّنِّ إِنَّ بَعْضَ الظَّنِّ إِثْمٌ وَلَا تَجَسَّسُوا وَلَا يَغْتَبَ بَعْضُكُم بَعْضًا
أَيُّحِبُّ أَحَدُكُمْ أَنْ يَأْكُلَ لَحْمَ أَخِيهِ مَيْتًا فَكَرِهْتُمُوهُ وَاتَّقُوا اللَّهَ إِنَّ اللَّهَ تَوَّابٌ رَّحِيمٌ

Artinya: “Wahai orang-orang yang beriman, jauhilah banyak prasangka! Sesungguhnya sebagian prasangka itu dosa. Janganlah mencari-cari kesalahan orang lain dan janganlah ada di antara kamu yang menggunjing sebagian yang lain. Apakah ada di antara kamu yang suka memakan daging saudaranya yang sudah mati? Tentu kamu merasa jijik. Bertakwalah kepada Allah! Sesungguhnya Allah Maha Penerima Tobat lagi Maha Penyayang” (Q.S. Al- Hujurat Ayat 12)

Ayat ini secara eksplisit melarang *tajassus* (memata-matai), yang dalam konteks modern sangat relevan dengan kegiatan seperti penyadapan, peretasan, atau pengumpulan data tanpa izin. Maka praktik penyalahgunaan data pribadi merupakan pelanggaran serius terhadap nilai-nilai syariah.

Dalam hadist riwayat bukhari muslim nomor 2442 dijelaskan

فَرَّجَ وَمَنْ حَاجَتْهُ، فِي اللَّهِ كَانَ أَخِيهِ حَاجَةً فِي كَانَ وَمَنْ يُسْلِمُهُ، وَلَا يَظْلِمُهُ لَا الْمُسْلِمَ أَخُو الْمُسْلِمِ
الْقِيَامَةِ يَوْمَ اللَّهُ سَتَرَهُ مُسْلِمًا سَتَرَ وَمَنْ الْقِيَامَةِ، يَوْمَ كُرْبَاتٍ مِنْ كُرْبَةٍ عَنْهُ اللَّهُ فَرَّجَ كُرْبَةَ مُسْلِمٍ عَنْ

“Seorang muslim adalah saudara muslim lainnya. Ia tidak menzalimi dan tidak berbuat aniaya kepadanya. Barang siapa yang memenuhi (membantu) kebutuhan saudaranya, Allah akan memenuhi kebutuhannya. Dan barang siapa yang menutupi aib seorang muslim, Allah akan menutupi aibnya pada hari kiamat kelak.” (HR. *al-Bukhari*, no. 2442).

Dalam kerangka ini, undang-undang perlindungan data pribadi di indonesia khususnya Undang-Undanag Nomor 27 Tahun 2022, dapat dipaandang sebagai manifestasi modern yang mengatur bagaimana negara harus mengelola dan menjaga keamanan data warga negara. Negara memiliki peran sebagai regulator dan pengawas yang wajib memastikan bahwa hak privasi dan keamanan data dijaga demi kemaslahatan bersama. Dengan mengintegrasikan prinsip *Sadd az-Dzari'ah* dalam perlindungan data pribadi, maka pelanggaran terhadap data nasabah tidak hanya berdampak secara hukum positif dan sosial, tetapi juga termasuk pelanggaran terhadap prinsip-prinsip moral Islam yang melindungi kehormatan (*karāmah*), hak milik (*mālikiyyah*), dan keselamatan jiwa (*hifz al-nafs*) individu.

Berdasarkan berbagai problematika yang telah dipaparkan sebelumnya pada bagian latar belakang masalah, maka penulis tertarik untuk membahas **Analisis Yuridis Pelindungan Data Pribadi Nasabah Perbankan Elektronik Perspektif Sadd Az-Dzariah**

B. Identifikasi Masalah

1. Implementasi perlindungan data pribadi di sektor perbankan elektronik masih menghadapi berbagai tantangan
2. Belum efektifnya Undang-Undang Nomor 27 Tahun 2022 dalam melindungi data pribadi nasabah layanan perbankan elektronik di tengah lemahnya pengawasan dan literasi digital
3. Bahwa dalam banyak kasus, kelemahan dalam perlindungan data pribadi tidak hanya mengancam privasi individu, tetapi juga berisiko merusak integritas sistem keuangan secara keseluruhan
4. Tidak Sinkronya antara regulasi yang ada dengan realitas teknologis dan praktik di lapangan, khususnya dalam hal kepatuhan sektor perbankan terhadap standar pengamanan data pribadi
5. Pelaksanaan Undang-Undang Perlindungan Data Pribadi di sektor perbankan masih menghadapi tantangan berupa kesiapan keamanan siber
6. Negara sebagai pengelola urusan publik dapat diharapkan untuk melaksanakan amanah perlindungan data pribadi dengan cara yang adil (*al-'adl*) dan tidak menzalimi (*lā tazlīmū*)

C. Rumusan Masalah

Berdasarkan latar belakang di atas, maka rumusan masalah dalam penelitian ini sebagai berikut:

1. Bagaimana bentuk perlindungan data pribadi nasabah pengguna layanan perbankan elektronik?
2. Bagaimana implementasi perlindungan data pribadi nasabah dalam layanan perbankan elektronik di Indonesia?
3. Bagaimana perspektif *Sadd Az-Dzariah* dalam kaitannya dengan perlindungan data pribadi nasabah di layanan perbankan elektronik?

D. Tujuan Penelitian

1. Untuk Mengetahui bentuk perlindungan data pribadi nasabah pengguna layanan perbankan elektronik berdasarkan Undang-Undang Nomor 27 Tahun 2022
2. Untuk menganalisis hukum perlindungan data pribadi nasabah layanan perbankan elektronik berdasarkan Undang-Undang No. 27 Tahun 2022
3. Untuk mengevaluasi kesesuaian prinsip-prinsip *Sadd Az-Dzariah* dengan perlindungan data pribadi dalam perbankan elektronik

E. Manfaat Penelitian

1. Memberikan pemahaman tentang implementasi Undang-Undang Pelindungan Data Pribadi dalam perbankan elektronik.
2. Memberikan wawasan dalam memperbaiki sistem perlindungan data pribadi di layanan perbankan elektronik.
3. Memberikan kontribusi dalam evaluasi kebijakan terkait perlindungan data pribadi dalam perbankan elektronik

F. Penelitian Terdahulu

Sejauh hasil telaah penulis terhadap buku, literatur yang ada, Tinjauan Yuridis Terhadap Pelindungan Data Pribadi Nasabah Layanan Perbankan Elektronik Berdasarkan Undang-Undang Nomor 27 Tahun 2022 Perspektif *Sadd Az-Dzariah*. Telah banyak yang dibahas oleh para peneliti sebelumnya, antara lain:

1. Tesis Karya Rahman, T.M. yang berjudul “*Fiqh Siyasah dan Regulasi Perlindungan Data Pribadi: Studi Komparatif antara UU PDP dan Prinsip Syariah*”, Penelitian ini membandingkan prinsip-prinsip dalam Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi dengan nilai-nilai yang terkandung dalam *fiqh siyasah*. Penelitian ini menunjukkan bahwa *fiqh siyasah* memiliki landasan kuat dalam hal pelindungan privasi individu, dengan mengedepankan prinsip-prinsip seperti amanah, keadilan, dan tanggung jawab negara dalam menjaga informasi warga. Peneliti juga menggarisbawahi bahwa prinsip *maqāṣid al-syarī'ah*, seperti penjagaan harta (*ḥifẓ al-māl*) dan kehormatan (*ḥifẓ al-'ird*), memiliki korelasi langsung dengan norma hukum positif dalam UU PDP. Tesis ini memberikan kontribusi signifikan terhadap pendekatan integratif antara hukum positif dan *fiqh siyasah*, yang sangat relevan untuk mengkaji pelindungan data pribadi nasabah

dari dua perspektif hukum yang menjadi fokus utama dalam tema tesis ini.²³

2. Tesis karya Bagus Satrio Ramadha, S.H, dengan judul “Kemampuan Hukum Pidana Terhadap Kejahatan Siber Terkait Perlindungan Data Pribadi Di Indonesia” Penelitian ini membahas sejauh mana efektivitas hukum pidana di Indonesia dalam menangani kejahatan siber yang berkaitan dengan pelanggaran data pribadi. Fokus kajian diarahkan pada analisis normatif terhadap ketentuan pidana dalam Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi (UU PDP) dan Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE), serta relevansinya dalam menjerat pelaku kejahatan siber. Tesis ini menyoroti berbagai bentuk kejahatan digital seperti phishing, hacking, dan illegal data trading, yang makin marak terjadi seiring dengan meningkatnya digitalisasi layanan publik dan keuangan. Ramadha juga mengkaji hambatan dalam penegakan hukum, seperti keterbatasan aparat penegak hukum dalam mendeteksi dan membuktikan tindak pidana siber, serta kurangnya koordinasi antar lembaga penegak hukum siber.²⁴

²³ Rahman, T.M., *Fiqh Siyasah dan Regulasi Perlindungan Data Pribadi Studi Komparatif antara UU PDP dan Prinsip Syariah* (Tesis Magister, Universitas Islam Negeri Syarif Hidayatullah Jakarta, 2023)

²⁴ Bagus Satrio Ramadha, *Kemampuan Hukum Pidana Terhadap Kejahatan Siber Terkait Perlindungan Data Pribadi di Indonesia* (Tesis Magister, Universitas Islam Indonesia, 2021)

3. Jurnal karya Marcelliana, D., dkk. Dengan judul “Tanggung Jawab Perbankan Terhadap Kebocoran Data Nasabah Akibat Serangan Siber Jurnal Keamanan Siber dan Hukum”. Penelitian ini menilai tanggung jawab hukum dan teknis bank dalam menghadapi serangan siber yang mengakibatkan kebocoran data pribadi nasabah. Artikel ini mengungkapkan bahwa meskipun banyak bank telah mengimplementasikan sistem keamanan data, serangan siber masih dapat mengekspos data sensitif nasabah. Peneliti mengusulkan perlunya peningkatan regulasi dan pengawasan yang lebih ketat, serta teknologi keamanan yang lebih canggih untuk melindungi data nasabah. Temuan ini penting untuk memperbaiki kebijakan perlindungan data di sektor perbankan di Indonesia.²⁵
4. Jurnal karya Pangestika, W., Kamilataakhir, S.A., & Ul Hosnah, A, yang berjudul “Pertanggung Jawaban Bank terhadap Pencurian Data Personal Nasabah dengan Menggunakan Teknik Phishing Penelitian ini mengkaji secara mendalam tanggung jawab lembaga perbankan terkait pencurian data pribadi nasabah yang terjadi melalui teknik phishing. Fokus utama dari Jurnal ini adalah mengidentifikasi faktor-faktor yang memperbesar kemungkinan terjadinya pencurian data, termasuk rendahnya literasi digital nasabah dan adanya kelemahan dalam sistem perlindungan yang diterapkan

²⁵ Marcelliana, D., dkk., “Tanggung Jawab Perbankan Terhadap Kebocoran Data Nasabah Akibat Serangan Siber,” Jurnal Keamanan Siber dan Hukum 12, no. 2 (2023): 114-115.

oleh bank. Peneliti menyimpulkan bahwa meskipun bank telah mengimplementasikan berbagai sistem keamanan, celah di sektor edukasi nasabah mengenai potensi bahaya phishing membuat data pribadi nasabah tetap rentan terhadap serangan. Oleh karena itu, penelitian ini merekomendasikan dua hal penting: pertama, penguatan sistem proteksi internal bank untuk menghindari kebocoran data, dan kedua, program edukasi yang lebih intensif untuk nasabah mengenai pentingnya menjaga informasi pribadi serta cara menghindari serangan *phishing*. Penelitian ini juga membahas kebijakan dan kewajiban hukum yang harus dijalankan oleh bank berdasarkan peraturan perundang-undangan yang ada, termasuk Undang-Undang Perlindungan Data Pribadi (UU PDP) yang baru disahkan. Selain itu, artikel ini menyoroti pentingnya kolaborasi antara lembaga perbankan dan regulator untuk menciptakan kebijakan yang dapat mengatasi ancaman siber yang terus berkembang.²⁶

5. Jurnal karya Bhoki, A., Aloysius, S., & Dju Bire, C.M. Berjudul “Perlindungan Hukum Terhadap Kebocoran Data Nasabah Ditinjau dari Undang-Undang Nomor 10 Tahun 1998 tentang Perbankan”. Penelitian ini mengkaji secara mendalam tanggung jawab lembaga perbankan terkait pencurian data pribadi nasabah yang terjadi melalui teknik phishing. Fokus utama dari jurnal ini adalah

²⁶ Pangestika, W., Kamilataahir, S.A., & Ul Hosnah, A., “Pertanggung Jawaban Bank terhadap Pencurian Data Personal Nasabah dengan Menggunakan Teknik Phishing,” Jurnal Keamanan Siber dan Hukum 13, no. 1 (2024): 88-89.

mengidentifikasi faktor-faktor yang memperbesar kemungkinan terjadinya pencurian data, termasuk rendahnya literasi digital nasabah dan adanya kelemahan dalam sistem perlindungan yang diterapkan oleh bank. Penulis menyimpulkan bahwa meskipun bank telah mengimplementasikan berbagai sistem keamanan, celah di sektor edukasi nasabah mengenai potensi bahaya *phishing* membuat data pribadi nasabah tetap rentan terhadap serangan. Oleh karena itu, penelitian ini merekomendasikan dua hal penting: pertama, penguatan sistem proteksi internal bank untuk menghindari kebocoran data, dan kedua, program edukasi yang lebih intensif untuk nasabah mengenai pentingnya menjaga informasi pribadi serta cara menghindari serangan *phishing*. Penelitian ini juga membahas kebijakan dan kewajiban hukum yang harus dijalankan oleh bank berdasarkan peraturan perundang-undangan yang ada, termasuk Undang-Undang Perlindungan Data Pribadi (UU PDP) yang baru disahkan. Selain itu, jurnal ini menyoroti pentingnya kolaborasi antara lembaga perbankan dan regulator untuk menciptakan kebijakan yang dapat mengatasi ancaman siber yang terus berkembang.²⁷

6. Jurnal karya Fitriani, N., & Sihombing, R. Dengan judul “Perlindungan Hukum Nasabah dalam Kasus Pencurian Data Pribadi melalui Serangan Phishing: Analisis UU PDP dan UU

²⁷ Bhoki, A., Aloysius, S., & Dju Bire, C.M., “*Perlindungan Hukum Terhadap Kebocoran Data Nasabah Ditinjau dari Undang-Undang Nomor 10 Tahun 1998 tentang Perbankan*,” Jurnal Keamanan Siber dan Hukum 14, no. 3 (2024): 122-123.

ITE”. Penelitian ini mengkaji perlindungan hukum bagi nasabah dalam kasus pencurian data pribadi yang terjadi melalui teknik phishing, sebuah metode penipuan di dunia maya yang sering disalahgunakan oleh pihak ketiga untuk memperoleh akses tidak sah terhadap data pribadi nasabah. Penulis membahas relevansi penerapan Undang-Undang Perlindungan Data Pribadi (UU PDP) dan Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) dalam menangani dan melindungi data pribadi nasabah yang dicuri atau disalahgunakan oleh pihak yang tidak berwenang. Penting untuk dicatat bahwa dalam hukum Indonesia, bank sebagai pengendali data pribadi nasabah memegang peranan penting dalam menjaga kerahasiaan dan keamanan data yang mereka kelola. Penelitian ini memfokuskan pada kewajiban bank untuk mengambil langkah-langkah preventif dalam melindungi data nasabah agar terhindar dari potensi pelanggaran data, seperti serangan phishing. Langkah-langkah preventif tersebut mencakup penggunaan teknologi yang tepat, pelatihan keamanan bagi pegawai bank, serta edukasi kepada nasabah mengenai cara-cara menjaga keamanan data pribadi mereka saat bertransaksi secara online.²⁸

7. Jurnal karya Lilis Ekayani, Hardianto Djanggih & Moh. Akli Suong dengan judul “Perlindungan Hukum Nasabah Terhadap

²⁸ Fitriani, N., & Sihombing, R., “Perlindungan Hukum Nasabah dalam Kasus Pencurian Data Pribadi melalui Serangan Phishing: Analisis UU PDP dan UU ITE,” Jurnal Hukum dan Teknologi Informasi 15, no. 2 (2024): 101-102.

Kejahatan Pencurian Data Pribadi (*Phising*) Di Lingkungan Perbankan”. Membahas perlindungan hukum bagi nasabah perbankan yang menjadi korban kejahatan pencurian data pribadi melalui teknik phishing. Penelitian ini menyoroti lemahnya sistem keamanan data perbankan dan terbatasnya kesadaran hukum nasabah sebagai faktor yang berkontribusi terhadap meningkatnya kasus phishing di sektor keuangan. Metode yang digunakan adalah pendekatan yuridis normatif dengan analisis terhadap UU Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi, serta keterkaitannya dengan UU Nomor 10 Tahun 1998 tentang Perbankan dan UU ITE. Peneliti mengkaji sejauh mana tanggung jawab hukum bank sebagai pengendali data, termasuk kewajiban memberikan ganti rugi kepada nasabah yang dirugikan akibat kelalaian sistem perlindungan data. Selain itu, artikel ini juga membahas perlunya literasi digital dan perlindungan hukum preventif yang berbasis teknologi dalam sistem perbankan. Penelitian ini menyimpulkan bahwa perlindungan hukum terhadap nasabah belum sepenuhnya efektif, baik dari sisi regulasi maupun implementasi di lapangan. Diperlukan upaya peningkatan pengawasan oleh otoritas keuangan serta reformasi sistem keamanan data di lingkungan perbankan.²⁹

²⁹ Lilis Ekayani, Hardianto Djanggih, & Moh. Akli Suong, “*Perlindungan Hukum Nasabah Terhadap Kejahatan Pencurian Data Pribadi (Phishing) di Lingkungan Perbankan*,” Jurnal Keamanan dan Hukum Perbankan 16, no. 1 (2024): 80-81.

8. Jurnal karya Maramis, A.V., Doodoh, M., & Lambonan, M.L. Dengan judul “Tinjauan Yuridis terhadap Perlindungan Data Pribadi dalam Mengatasi Cybercrime pada Kasus *Phishing*”. Membahas secara mendalam pengaturan hukum terkait perlindungan data pribadi dalam konteks tindak pidana dunia maya, khususnya kejahatan *phishing*. Fokus utama kajian diarahkan pada efektivitas implementasi Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi (UU PDP) sebagai instrumen hukum nasional dalam merespons kejahatan siber yang semakin meningkat, khususnya yang menasar lembaga keuangan dan data nasabah perbankan. Penelitian ini menyoroti bahwa *phishing* sebagai bentuk serangan rekayasa sosial tidak hanya merugikan individu, tetapi juga menimbulkan tantangan hukum dalam pembuktian dan pertanggungjawaban. Oleh karena itu, jurnal ini mengulas peran negara dan lembaga penegak hukum dalam penanggulangan *cybercrime* dan urgensi harmonisasi antara UU PDP dengan UU ITE dan peraturan sektor keuangan seperti regulasi dari OJK dan Bank Indonesia. Jurnal ini juga menyoroti tanggung jawab lembaga perbankan sebagai pengendali data, dengan menekankan pentingnya kepatuhan terhadap prinsip-prinsip perlindungan data, seperti minimalisasi data, akuntabilitas, dan keamanan informasi. Ketidakpatuhan terhadap prinsip-prinsip

ini dianggap sebagai bentuk kelalaian yang dapat dimintakan pertanggungjawaban hukum.³⁰

9. Jurnal karya, Ema Irmawati, John Pieries, Wiwik Sri Widiarty dengan judul “Perlindungan Hukum Atas Data Pribadi Nasabah Bank Pengguna Mobile Banking dalam Perspektif Undang-Undang No 27 Tahun 2022 tentang Kebocoran Data” membahas untuk menganalisis pengaturan hukum mengenai perlindungan data pribadi nasabah yang menggunakan layanan mobile banking. Pendekatan yang digunakan adalah kombinasi antara studi yuridis normatif dan empiris. Pendekatan yuridis normatif dilakukan dengan mengkaji peraturan perundang-undangan yang berlaku, terutama Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi, sementara pendekatan empiris diperoleh melalui pengamatan dan pengumpulan data lapangan guna melihat penerapan regulasi tersebut dalam praktik perbankan elektronik. Hasil penelitian menunjukkan bahwa meskipun secara normatif perlindungan hukum terhadap data pribadi nasabah telah diatur melalui undang-undang tersebut, implementasinya di lapangan masih menghadapi berbagai tantangan. Salah satu kendala utama adalah rendahnya tingkat pemahaman masyarakat terhadap hak-hak mereka sebagai pemilik data pribadi. Selain itu, mekanisme penegakan hukum atas pelanggaran data pribadi masih belum

³⁰ Maramis, A.V., Doodoh, M., & Lambonan, M.L., “*Tinjauan Yuridis terhadap Perlindungan Data Pribadi dalam Mengatasi Cybercrime pada Kasus Phishing*,” Jurnal Hukum dan Keamanan Siber 17, no. 2 (2024): 99-100.

optimal, termasuk lemahnya penerapan sanksi terhadap pelaku pelanggaran. Berdasarkan temuan tersebut, penelitian ini merekomendasikan perlunya peningkatan sosialisasi Undang-Undang Nomor 27 Tahun 2022 kepada masyarakat luas, khususnya kepada pengguna layanan perbankan digital. Selain itu, penting pula dilakukan penguatan terhadap sistem pengawasan dan regulasi teknis yang mengatur kinerja penyelenggara layanan mobile banking, agar perlindungan terhadap data pribadi nasabah dapat dijamin secara lebih efektif.³¹

10. Tesis karya, Fawzia Apriandini dengan judul “ Analisis Pelindungan Hukum Data Pribadi Nasabah Pada Pelaksanaan Bank Digital Di Indonesia Berdasarkan Undang-Undang Nomor 27 Tahun 2022 Tentang Pelindungan Data Pribadi”. Tesis ini membahas bahwa dalam implementasi layanan bank digital, bank wajib mematuhi ketentuan yang ada dalam Undang-Undang Perbankan, yang juga mencakup aturan terkait pelindungan data pribadi nasabah. Selain itu, bank digital diharuskan untuk melakukan mitigasi risiko terkait dengan pelaksanaan kegiatan usaha mereka, terutama yang berhubungan dengan pengelolaan dan penggunaan data pribadi nasabah.

Penting untuk dicatat bahwa dalam menjalankan aktivitasnya, bank digital harus menjaga transparansi terkait

³¹ Ema Irmawati, John Pieries, dan Wiwik Sri Widiarty, "Perindungan Hukum Atas Data Pribadi Nasabah Bank Pengguna Mobile Banking dalam Perspektif UU No 27 Tahun 2022 tentang Kebocoran Data" Jurnal Syntax Admiration, vol. 5, no. 1 (2024): 12–27

dengan pengelolaan data nasabah. Hal ini berarti bahwa bank digital harus memberikan informasi yang jelas dan terbuka kepada nasabah mengenai bagaimana data mereka dikumpulkan, diproses, dan disimpan. Bank juga diwajibkan untuk menginformasikan nasabah mengenai jangka waktu penyimpanan data pribadi mereka, serta jenis data yang dikumpulkan dan tujuan pengumpulannya. Hal ini bertujuan agar nasabah dapat memahami dan menyetujui proses yang dijalankan terkait pengolahan data pribadi mereka. Penelitian ini menekankan bahwa penerapan ketentuan Undang-Undang Nomor 27 Tahun 2022 dalam bank digital harus dilakukan secara menyeluruh, dengan mempertimbangkan perlindungan hak-hak nasabah terhadap data pribadi mereka. Oleh karena itu, bank digital tidak hanya diwajibkan untuk mematuhi regulasi yang berlaku, tetapi juga untuk memperkuat sistem pengelolaan data pribadi guna mencegah kebocoran atau penyalahgunaan data yang dapat merugikan nasabah. Dengan demikian, penelitian ini menyimpulkan bahwa perlindungan data pribadi dalam industri bank digital di Indonesia harus dipandang sebagai sebuah kewajiban hukum yang bersifat mendasar, dan perlu adanya peningkatan pengawasan serta transparansi yang lebih besar dalam pengelolaan data pribadi nasabah.³²

³² Fawzia Apriandini dan Antari Innaka Turingsih, *Analisis Pelindungan Hukum Data Pribadi Nasabah Pada Pelaksanaan Bank Digital Di Indonesia Berdasarkan Undang-Undang*