

## BAB I

### PENDAHULUAN

#### A. Latar Belakang Masalah

Pesatnya perkembangan teknologi dan informasi telah banyak manfaat bagi kehidupan manusia saat ini. Perkembangan teknologi dalam kehidupan sehari-hari dapat dirasakan dalam berbagai aktivitas seperti bidang transportasi, pariwisata, perdagangan, industri keuangan, dan pemerintahan. Peningkatan kualitas masyarakat Indonesia secara berkelanjutan dengan memanfaatkan teknologi informasi serta ilmu pengetahuan merupakan salah satu tujuan pembangunan nasional. Peningkatan kualitas tersebut sekaligus menjadi suatu tantangan global.<sup>1</sup> Penggunaan teknologi dan informasi dapat dirasakan manfaatnya pada bidang pendidikan, perekonomian dan hal-hal yang berkaitan dengan perkembangan ilmu pengetahuan, sains dan lain sebagainya. Melalui perkembangan teknologi dan informasi, segala sesuatu dapat dengan mudah diakses secara cepat.

Pada lain sisi, perkembangan teknologi dan informasi saat ini menjadi semacam pedang bermata dua, karena selain memberikan banyak kontribusi dalam peningkatan kesejahteraan, kemajuan dan peradaban manusia, bisa juga

---

<sup>1</sup> Sudaryanti, K. D., Darmawan, N. K. S., & Purwanti, N. P. *Perlindungan Hukum Terhadap Invenstor Dalam Perdagangan Obligasi Secara Elektronik*. KerthaWicara, 2(1), 1-5. 2013, hlm; 1.

menjadi sarana perbuatan melawan hukum. Salah satu contohnya, kejahatan dunia maya atau lebih dikenal dengan istilah *cybercrime*.<sup>2</sup> Pada tahun 2003, mulai



---

<sup>2</sup> A. Aco Agus dan Riskawati, Penanganan KasusCybercrime Di Kota Makassar (Studi Pada Kantor Kepolisian Resort Kota Besar Makassar), Jurnal Supremasi, Vol. 10, N 2016, hlm; 56.

banyak terjadi kejahatan di dunia maya (*cyber crime*) yang bermunculan dengan memanfaatkan kemajuan dari teknologi informasi, seperti kejahatan *carding (credit card fraud)*, *ATM/EDC skimming*, *hacking*, *cracking*, *phishing (internet banking fraud)*, *malware (virus/worm/trojan/bots)*, *cybersquatting*, pornografi, perjudian online, trans nasional *crime* (perdagangan narkoba, mafia, terorisme, *money laundering*, *human trafficking*, *underground economy*).<sup>3</sup> Melalui kemudahan yang diberikan oleh kemajuan teknologi dan informasi ini, kejahatan-kejahatan tersebut semakin meluas ke berbagai bidang kehidupan manusia. Dalam tulisan jurnal yang berjudul “*Cyber-Bullying, Kejahatan Dunia Maya Yang Terlupakan, Wacana Kritis Cyber Crime Di Negara Berkembang*”, Al Sentot Sudarwanto menjelaskan, kriminalitas di internet atau *cyber crime* pada dasarnya adalah suatu tindak pidana yang berkaitan dengan *cyber space* (ruang atau dunia maya), baik yang menyerang fasilitas umum dalam *cyber space* maupun menyerang atau meretas kepemilikan akun pribadi (Al Sentot Sudarwanto, 2009 : 4).

Salah satu bentuk kejahatan dalam dunia maya yang sangat memprihatinkan saat ini adalah mengenai kebocoran data pribadi, baik yang tersimpan pada akun pribadi media sosial, *platform online* seperti tokopedia, maupun data pribadi yang tersimpan pada badan layanan negara seperti Badan Penyelenggara Jaminan Sosial (BPJS). Oleh karena perintah peraturan perundang-undangan di dalam Pasal 6 Perpres No. 82 Tahun 2018 Tentang Jaminan Kesehatan, bahwa “Setiap penduduk

---

<sup>3</sup> Maulia Jayantina Islami, “Tantangan Dalam Implementasi Strategi Keamanan Siber Nasional Indonesia Ditinjau Dari Penilaian Global Cybersecurity Index,” Jurnal Masyarakat Telematika Dan Informasi, Vol. 8 No. (2017), hlm ; 137.

Indonesia wajib ikut serta dalam program Jaminan Kesehatan. Ikut serta dalam program Jaminan Kesehatan sebagaimana dimaksud pada ayat (1) dilaksanakan dengan cara mendaftar atau didaftarkan pada BPJS Kesehatan”, maka masyarakat mempercayakan data pribadi mereka untuk disimpan dan dikelola secara digital oleh suatu lembaga resmi untuk kepentingan umum yang juga berkaitan langsung dengan pemilik data pribadi. Namun data pribadi tersebut diretas atau diambil secara ilegal oleh oknum yang tidak bertanggungjawab kemudian memperdagangkan data tersebut ke pasar gelap (forum perdagangan dunia maya yang ilegal), fakta seperti inilah yang kemudian memunculkan istilah kebocoran data pribadi.<sup>4</sup> Berdasarkan hal itu maka pemerintah menerbitkan sejumlah instrumen hukum seperti Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE), dan Undang-Undang Nomor 27 Tahun 2022 Tentang Pelindungan Data Pribadi. Penelitian dalam tesis ini hanya akan mengkaji Undang-Undang Nomor 27 Tahun 2022 Tentang Perlindungan Data Pribadi (selanjutnya dalam tesis ini disingkat UUPDP).

Dalam Pasal 67 ayat (1), (2), (3), UU. PDP secara jelas mengatakan:

(1) Setiap Orang yang dengan sengaja dan melawan hukum memperoleh atau mengumpulkan Data Pribadi yang bukan miliknya dengan maksud untuk menguntungkan diri sendiri atau orang lain yang dapat mengakibatkan kerugian Subjek Data Pribadi sebagaimana dimaksud dalam Pasal 65 ayat (1) dipidana dengan pidana penjara paling lama 5 (lima) tahun dan/atau pidana denda paling banyak Rp. 5.000.000.000,00 (lima miliar rupiah). (2) Setiap Orang yang dengan

---

<sup>4</sup> Akbari Amarul Zaman, dkk. Pertanggung Jawaban Pidana Kebocoran Data BPJS Dalam Perspektif UU ITE. Jurnal Juncto Delicti, Volume 1 Nomor 2 Tahun 2021. Hlm ; 147-148.

sengaja dan melawan hukum mengungkapkan Data Pribadi yang bukan miliknya sebagaimana dimaksud dalam Pasal 65 ayat (2) dipidana dengan pidana penjara paling lama 4 (empat) tahun dan/atau pidana denda paling banyak Rp. 4.000.000.000,00 (empat miliar rupiah). (3) Setiap Orang yang dengan sengaja dan melawan hukum menggunakan Data Pribadi yang bukan miliknya sebagaimana dimaksud dalam Pasal 65 ayat (3) dipidana dengan pidana penjara paling lama 5 (lima) tahun dan/atau pidana denda paling banyak Rp. 5.000.000.000,00 (lima miliar rupiah).

Jadi, jika terjadi kebocoran data pribadi maka dipastikan perbuatan tersebut merupakan perbuatan melawan hukum atau bisa juga disebut sebagai perbuatan pidana.<sup>5</sup> Indah Sari dalam tulisan jurnalnya yang berjudul “Perbuatan Melawan Hukum (PMH) Dalam Hukum Pidana Dan Hukum Perdata”, menerangkan, perbuatan melawan hukum merupakan perbuatan yang terbukti melanggar undang-undang, perbuatan yang bertentangan dengan hak-hak orang lain, ataupun perbuatan yang bertentangan dengan nilai kesusilaan dan kesopanan dalam masyarakat. (Indah Sari. 2020 : 53). Berdasarkan pengertian ini maka dapat diketahui bahwa perbuatan melawan hukum itu mencakup ranah pidana ataupun perdata. Sementara terkait bunyi Pasal 67 ayat (1), (2), (3), UU. PDP sangat ditekankan pada ranah pidana, mengingat perbuatan pembocoran data pribadi telah sangat meresahkan publik Indonesia, terutama peserta BPJS.

Pada bulan Mei 2021, BPJS mengalami kebocoran data, dalam peristiwa itu diduga terdapat 279 juta data penduduk Indonesia yang merupakan peserta BPJS

---

<sup>5</sup> Hezekiel Bram Setiawan, *Perlindungan Data Pribadi Warga Negara Indonesia Terkait Dengan Kebocoran Data*. Jurnal Kewarganegaraan. Universitas Sebelas Maret. Volume 6 Nomor 1 2022. Hlm. 977.

Kesehatan bocor lalu kemudian dijual ke “pasar gelap”. Menurut sumber CNN Indonesia, jutaan data penduduk itu bukan saja masyarakat sipil tetapi juga TNI dan Polri. Data-data tersebut terdiri dari nama lengkap, data KTP, nomor telepon, NID, email serta alamat tempat tinggal.<sup>6</sup> Mirisnya, pada bulan Maret tahun 2023 ini dugaan kebocoran data pribadi peserta BPJS kembali bocor, tanpa ada satu pihak yang merasa bertanggungjawab terhadap kebocoran dimaksud.<sup>7</sup>

Pada tahun 2022 Pemerintah telah menerbitkan Undang-Undang No. 27 Tahun 2022 Tentang Pelindungan Data Pribadi (dalam proposal ini peneliti menyebut UUPDP). Dalam UU. PDP ini mengatur tentang hak-hak dari subjek data pribadi, hak subjek data, ketentuan-ketentuan pemrosesan data, proses transfer data, juga mengatur mengenai kewajiban para pihak yang mengumpulkan serta mengelola data pribadi milik orang lain. Tentu saja diatur juga sanksi bagi penyelenggara sistem elektronik (PSE) atas tata kelola data pribadi yang diproses dalam masing-masing sistem penyelenggara dimaksud. Harapan pemerintah dan juga publik, melalui UUPDP ini data pribadi dapat diproteksi secara maksimal.

Berdasarkan fakta kebocoran data peserta BPJS sebagaimana disebutkan di atas, peneliti melihat belum ada bentuk pertanggungjawaban hukum atas peristiwa tersebut, maksudnya tidak ada satu pihak pun yang merasa bertanggungjawab atau dimintai pertanggungjawaban hukum. Fakta kebocoran data peserta BPJS dalam tesis ini sebagai salah satu contoh kasus tentang kebocoran data pribadi yang disimpan dan dikelola oleh suatu badan hukum, karena sesungguhnya ada pula

---

<sup>6</sup> (<https://www.cnnindonesia.com/teknologi/20210903142047-185-689370/rentetan-kasus-dugaan-kebocoran-data-kesehatan-pemerintah>. Diakses pada 20/03/2023).

<sup>7</sup> <https://www.kompas.id/baca/polhuk/2023/03/14/bpjs-ketenagakerjaan-investigasi-klaim-bjorka>. Diakses 20/03/2023).

kasus-kasus lainnya yang serupa. Misalnya, pada Oktober 2021 data nasabah milik Bank Jawa Timur diduga bocor dan dijual pada situs *Raidforums* (situs jual beli data ilegal online). Sumber berita CNN Indonesia menjelaskan bahwa 259 data base yang terdiri dari data sensitif nasabah dan data keuangan pribadi yang rentan disalahgunakan. Padahal sebelum kebocoran data nasabah Bank Jatim, pada bulan Maret 2020, Tokopedia (*platform* online) juga mengalami kebocoran data pelanggannya, kemudian pada Mei 2020, BPJS juga mengalami kebocoran data peserta BPJS.<sup>8</sup>

Pada kasus kebocoran data nasabah Bank Jatim, Tokopedia, maupun BPJS tahun 2020 di atas, tidak ada satu pihak pun yang mengakui bersalah atau bertanggungjawab secara hukum. Padahal peristiwa kebocoran data itu benar-benar terjadi serta diperdagangkan secara ilegal pada *website-website* ilegal pula. Pada saat itu, instrumen hukum yang dipakai pada berbagai perbuatan pidana berbasis elektronik adalah UU. No. 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik (UUITE), namun tidak cukup mempan untuk mengatasi permasalahan kebocoran data. UUITE lebih fokus mengatur tentang informasi dan transaksi elektronik (BAB I Ketentuan Umum), serta agen elektronik (BAB V Tentang Transaksi Elektronik). Tujuan UUITE sendiri mencerdaskan kehidupan bangsa; mengembangkan perdagangan dan perekonomian nasional dalam rangka meningkatkan kesejahteraan masyarakat; meningkatkan efektivitas dan efisiensi pelayanan publik; membuka kesempatan untuk memajukan pemikiran dan kemampuan di bidang penggunaan dan pemanfaatan Teknologi Informasi dan memberikan rasa aman,

---

<sup>8</sup> (<https://www.cnnindonesia.com/teknologi/20211022110011-185-710874/jenis-data-nasabah-bank-jatim-diduga-bocor>. Diakses 24/04/2023).

keadilan, dan kepastian hukum bagi pengguna dan penyelenggara Teknologi Informasi. Sama sekali tidak ada Pasal yang mengatur tentang perlindungan data pribadi dan bentuk pertanggungjawaban hukum jika terjadi kebocoran data pribadi.

Berdasarkan fakta itulah kemudian Pemerintah menerbitkan UUPDP pada tahun 2022, dengan harapan mampu mengatasi permasalahan kebocoran data. Meskipun demikian, UUPDP juga belum cukup memadai untuk menjamin perlindungan data pribadi secara maksimal. Saat peneliti menelusuri rumusan Pasal 15 ayat (1) huruf c UUPDP:

”hak-hak subjek data pribadi sebagaimana dimaksud dalam Pasal 8, Pasal 9, Pasal 10 ayat (1), Pasal 11, dan Pasal 13 ayat (1) dan ayat (2) dikecualikan untuk: a). kepentingan pertahanan dan keamanan nasional; b). kepentingan proses penegakan hukum; c). kepentingan umum dalam rangka penyelenggaraan negara; d). kepentingan pengawasan sektor jasa keuangan, moneter, sistem pembayaran, dan stabilitas sistem keuangan yang dilakukan dalam rangka penyelenggaraan negara; atau e). kepentingan statistik dan penelitian ilmiah.”

Tentunya norma hukum (undang-undang) tersebut di atas bersifat umum (tidak menyebut secara khusus BPJS) namun demikian, dapat ditafsirkan bahwa PT. BPJS merupakan salah satu badan publik (milik negara) yang diberikan hak untuk memroses atau menghapus data pribadi (Pasal 8 dan 9), mengajukan keberatan atas tindakan pengambilan keputusan yang hanya didasarkan pada pemrosesan secara otomatis, termasuk pemfilan, yang menimbulkan akibat hukum (Pasal 10), berhak menunda atau membatasi pemrosesan Data Pribadi (Pasal 11) berhak menggunakan dan mengirimkan Data Pribadi tentang dirinya ke Pengendali Data Pribadi lainnya, sepanjang sistem yang digunakan dapat saling



berkomunikasi secara aman sesuai dengan prinsip Pelindungan Data Pribadi berdasarkan Undang-Undang ini (Pasal 13). Tentu tidak semua hak tersebut dilakukan oleh BPJS, namun sebagai badan publik yang menjalankan kepentingan umum dalam rangka penyelenggaraan negara maka BPJS oleh UU. PDP ini diberikan kewenangan.

Sehubungan dan kebocoran data peserta BPJS, maka bagaimana pertanggungjawaban hukum selaku badan publik yang menjalankan kepentingan umum penyelenggaraan negara ? Pada UUPDP sama sekali tidak ada Pasal yang menerangkan bahwa jika terjadi kebocoran data yang dikelola badan publik adalah merupakan tanggungjawab badan publik itu sendiri. Pada BAB VIII tentang Sanksi Administratif, Pasal 57 ayat (1) pun tidak menyebut Pasal 15 sebagai Pasal yang jika dilanggar akan dikenakan Sanksi Administratif. Pemerintah tentu memiliki maksud baik dalam menerbitkan UUPDP. Bagaimanapun juga ada manfaat atau rumusan Pasal yang menunjukkan kebaruan (sesuatu yang tidak ada sebelumnya) yang jika dibandingkan dengan UITE (tahun 2008) tentunya UUPDP lebih *up to date* dan aktual menjawab persoalan kebocoran data pribadi. Namun demikian, masih saja terdapat kekurangan, yakni belum ada Pasal yang menerangkan tentang pertanggungjawaban badan publik atas kebocoran data pribadi yang dikelolanya.

Fakta yuridis tentang kebocoran data seperti yang terjadi pada BPJS (dan juga badan publik lainnya) dan tidak ada pertanggungjawaban hukum badan publik tersebut menunjukkan tidak adanya kepastian hukum. Rakyat sudah mempercayakan data pribadi mereka dikelola oleh negara (melalui badan publik seperti BPJS) namun saat terjadi kebocoran data tersebut, badan publik tidak bisa dimintai pertanggungjawaban hukum, karena memang tidak tertulis di dalam UUPDP tentang pertanggungjawaban dimaksud. Padahal asas dalam UUPDP ini

diantaranya asas kepastian hukum dan asas pertanggungjawaban, namun dalam kasus kebocoran data pada BPJS, sama sekali tidak ada kepastian hukum dan tidak ada pertanggungjawaban hukum. Selalu yang disalahkan adalah para peretas<sup>9</sup> atau saling lempar tanggungjawab antara Kementerian Kominfo dengan Badan Siber dan Sandi Negara (BSSN)<sup>10</sup>

Dalam salah satu diskusi publik pada channel youtube Kompas TV tertanggal 25 Mei 2023, Ketua Lembaga Riset Keamanan Siber CissReC, Pratama Persadha menilai bahwa pemerintah melalui BPJS dan Kementerian Kominfo lalai dalam memproteksi data masyarakat yang mereka kelola. Persadha bahkan menuding pihak pemerintah (selaku penyelenggara sistem elektronik) yang melemparkan tanggungjawab atau menyalahkan peretas (hacker) adalah bentuk *playing victim*, karena sesungguhnya penyelenggara sistem elektronik (BPJS) mengerti tentang memproteksi data secara ketat sehingga tidak mudah bocor. Persadha mencontohkan, dalam dunia penguncian data digital ada metode enkripsi yang dapat digunakan untuk memproteksi data digital, namun sayangnya, menurut Persadha, BPJS tidak menggunakan penguncian enkripsi atau memang gunakan sistem penguncian enkripsi namun diduga ada pihak internal yang sengaja membuka penguncian tersebut untuk mengambil data peserta BPJS.

Ketiadaan Pasal tentang tuntutan pertanggungjawaban hukum oleh badan publik atas kebocoran data pribadi yang disimpan dan dikelolanya, menunjukkan bahwa UUPDP belum cukup maksimal dalam memproteksi data pribadi. UUPDP

---

<sup>9</sup> (<https://www.jawapos.com/nasional/01407116/pemerintah-diminta-tak-lempar-tanggung-jawab-soal-kebocoran-data>. Diakses 08/05/2023),

<sup>10</sup> (<https://inet.detik.com/security/d-6368474/curhat-bssn-selalu-disalahkan-tiap-ada-kebocoran-data>. Diakses 08/05/2023).

masih perlu dilakukan perubahan untuk perbaikan kedepannya. Oleh karena itulah, proposal tesis ini hendak mengkaji bentuk pertanggungjawaban hukum badan publik atas kebocoran data pribadi yang disimpan dan dikelolanya. Kajian ini memfokuskan pada pentingnya rumusan Pasal pertanggungjawaban hukum badan publik, tidak sekedar dalam bentuk sanksi administratif, melainkan juga sanksi pidana penjara.

Hezkiel Bram Setiawan dan Fatma Ulfatun Najicha dalam tulisan jurnal mereka yang berjudul “Perlindungan Data Pribadi Warga Negara Indonesia Terkait Dengan Kebocoran Data”, menjelaskan, data digital masyarakat Indonesia (64% dari populasi dunia nyata) sering diakses oleh pihak ilegal (hacker) karena sistem digital Indonesia memiliki potensi kebocoran data yang sangat besar. Lebih lanjut, jurnal ini menyebut bahwa berdasarkan data Yayasan Lembaga Konsumen Indonesia (YLKI), pencurian data pribadi pada tahun 2019 paling banyak terjadi pada badan publik sektor perbankan, yaitu sebanyak 106 kasus, disusul dibawahnya terjadi pada sektor pinjaman online (96 kasus), perumahan (81 kasus), belanja online (54 kasus), leasing (32 kasus). Catatan ini mengindikasikan bahwa kebocoran data pribadi di Indonesia sudah sangat memprihatinkan, sehingga dibutuhkan instrumen hukum yang efektif dan efisien untuk mencegah sekaligus memberikan efek jera bagi pelaku pencurian data pribadi dalam bentuk sanksi pidana, terutama bagi badan publik.<sup>11</sup>

Berdasarkan fakta bahwa sistem digital Indonesia memiliki potensi kebocoran data yang sangat besar, maka terkait dengan perlindungan data pribadi,

---

<sup>11</sup> Hezkiel Bram Setiawan, *Perlindungan Data Pribadi Warga Negara Indonesia Terkait Dengan Kebocoran Data*. Jurnal Kewarganegaraan. Universitas Sebelas Maret. Volume 6 Nomor 1 2022, hlm. 977.

peneliti ingin menganalisis bentuk pertanggungjawaban hukum badan publik yang menyimpan dan mengelola data tersebut. Hal ini penting dilakukan karena sebagaimana disebutkan di atas bahwa instrumen hukum di dalam UUPDP belum cukup memadai karena tidak ada Pasal yang menjelaskan tentang pertanggungjawaban hukum oleh badan publik, jika data pribadi yang mereka simpan dan kelola, bocor. Analisis ini juga penting supaya tidak terjadi saling lempar tanggungjawab antara sesama badan publik atau lembaga negara (Kemenkominfo dan BSSN). Berbicara mengenai pertanggungjawaban hukum maka tentu akan ada Pasal yang menjelaskan tentang sanksi, baik itu sanksi pidana maupun sanksi perdata<sup>12</sup>.

Oleh karena itu, peneliti hendak mengangkat judul “Pertanggungjawaban Hukum Atas Kebocoran Data Pribadi Peserta BPJS Berdasarkan Kepastian Hukum”. Ketiadaan pertanggungjawaban hukum badan publik di dalam UUPDP itulah yang memunculkan tidak adanya kepastian hukum bagi subjek data pribadi (masyarakat) yang mempercayakan data mereka untuk disimpan dan dikelola oleh Badan Publik.

Kepastian hukum merupakan ajaran yuridis dogmatik yang berangkat dari pemikiran positivistik hukum, bahwa hukum merupakan sesuatu yang otonom dan di dalamnya berisi sistem aturan yang jelas dan tegas untuk mengatur perilaku manusia. Melihat pada awal perkembangannya, sesungguhnya ajaran tentang kepastian hukum ini pertama kali digagas oleh Filsuf Hukum, Gustav Radbruch, tujuan hukum ada 3 (tiga) yaitu keadilan, kepastian dan kemanfaatan sosial. Dalam

---

<sup>12</sup> TommyJ.Bassang, *Pertanggungjawaban Pelaku Tindak Pidana Deelneming*. Jurnal Lex Crimen Vol. IV/No. 5/Juli/2015. Hlm. 122.

bukunya *Rechtsphilosophie* (terbit tahun 1932) Radbruch menulis, keadilan merupakan nilai utama dari hukum. Meskipun keadilan merupakan konsep yang abstrak namun dapat dipahami dalam bentuk yang aplikatif seperti kesamarataan (equality) yang terdistribusi bagi semua orang. Kepastian yang dimaksud adalah berkaitan dengan kepastian hukum. Melalui kepastian hukum itu maka akan terwujud kejelasan hukum, ketentraman (*peace*) dan ketertiban (*social order*). Sementara itu, kemanfaatan sosial maksudnya adalah bahwa hukum harus memberikan manfaat nyata bagi kehidupan sosial. Tanpa kemanfaatan sosial, hukum hanya akan menjadi alat pemerintahan yang tiran. (Bdk. Heather Leawoods. 2000. 492-493).

Terinspirasi dari gagasan Gustav Radbruch mengenai kepastian hukum, ahli hukum UAJY Hyronimus Rhiti dalam bukunya “Kepastian Hukum, Pengantar Teoretis Dan Filosofis” mempertegas bahwa kepastian hukum itu berkaitan erat dengan peraturan perundang-undangan (hukum positif), yang mana melalui peraturan perundang-undangan tersebut maka akan tercipta keadilan. Rhiti menulis:

“... bahwa yang utama tentang kepastian hukum adalah keberadaan hukum positif sebagai landasan kepastian hukum. Namun, seperti ditulis Radbruch, hukum positif mengungguli keadilan, kecuali kalau hukum positif itu melahirkan ketidakadilan, dapat disebut hukum yang tidak adil. Jika kita menganggap hukum positif selalu baik, benar dan adil, hukum ini tetap lebih unggul daripada keadilan (Radbruch). Ini dapat berarti bahwa kepastian hukum berbasiskan hanya pada peraturan perundang-undangan yang tidak menghancurkan keadilan. Meskipun demikian, kepastian hukum-menurut Radbruch- tidak berdasar pada keadilan itu

sendiri. Tetapi tetap pada hukum positif. Hukum positif adalah sumber utama kepastian hukum, menurut Radbruch”.<sup>13</sup>

Berdasarkan kutipan di atas, maka dapat diketahui bahwa kepastian hukum itu erat kaitannya dengan peraturan perundang-undangan. Ketiadaan ataupun ketidakjelasan rumusan peraturan perundang-undangan dapat berpengaruh pada ketiadaan maupun ketidakjelasan hukum, sehingga memunculkan ketidakpastian hukum. Adanya kepastian hukum, akan menghasilkan keadilan, sebaliknya, ketidakpastian hukum pasti memunculkan ketidakadilan. sehubungan dengan topik dalam tesis ini, ketiadaan sanksi yang jelas dan tegas dalam rumusan UUPDP bagi BPJS (badan publik) ketika terjadi kebocoran data pribadi pesertanya maka tidak ada pula kepastian hukum bagi masyarakat yang data pribadinya dibocorkan, karena tidak ada pihak yang mau atau dapat dimintai pertanggungjawaban hukum.

## **B. Rumusan Masalah**

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

1. Bagaimana pertanggungjawaban hukum badan publik dalam UU. No. 27 Tahun 2022 Tentang Perlindungan Data Pribadi demi mencegah kejahatan dunia maya (*cyber crime*) ?
2. Bagaimana Kepastian Hukum Hak Subjek Data Pribadi pada kasus kebocoran data pribadi peserta BPJS ditinjau dari teori kepastian hukum Gustav Radbruch ?

---

<sup>13</sup> Hyronimus Rhiti, 2023, *Kepastian Hukum, Pengantar Teoretis Dan Filosofis*. Yogyakarta. Kanisius. Hlm. 170-171.

### **C. Tujuan Penelitian**

1. Untuk mengetahui pentingnya UU. No. 27 Tahun 2022 Tentang Perlindungan Data Pribadi dalam mencegah kejahatan dunia maya (cyber crime).
2. Untuk mengetahui Kepastian Hukum Hak Subjek Data Pribadi Pada kasus kebocoran data pribadi peserta BPJS ditinjau dari teori kepastian hukum Gustav Radbruch.

### **D. Manfaat Penelitian**

1. Manfaat Teoritis
  - a. Penelitian ini dapat mengembangkan Ilmu Hukum terutama dalam bidang Perlindungan Data Pribadi
  - b. Penelitian ini dapat bermanfaat bagi penelitian lanjutan terutama dalam penyusunan bahan Perlindungan Data Pribadi
2. Manfaat Praktis
  - a. Penelitian ini dapat bermanfaat bagi masyarakat umum yang menggunakan data pribadi
  - b. Penelitian ini dapat bermanfaat bagi pemerintah selaku pelaksana perlindungan data pribadi

### **E. Keaslian Penelitian**

Penulisan tesis ini merupakan hasil pemikiran penulis dan tidak sama dengan tulisan/hasil karya ilmiah/penelitian yang dilakukan orang lain

sebelumnya. Oleh karena itu peneliti menyertakan penelitian perbandingan antara lain :

1. Bagus Satryo Ramadha, S.H., Tesis, *Kemampuan Hukum Pidana Terhadap Kejahatan Siber Terkait Perlindungan Data Pribadi di Indonesia*, 2021, dengan rumusan masalah Bagaimana kemampuan pidana pada Undang-Undang Informasi dan Transaksi Elektronik dalam menanggulangi kejahatan siber terkait perlindungan data pribadi?

Kesimpulan penelitian tersebut adalah Kemampuan Hukum Pidana terhadap kejahatan siber terkait data pribadi dalam Undang-Undang Informasi dan Transaksi Elektronik dapat diterapkan mengenai Pasal tentang akses ilegal, sebab data pribadi yang bersifat elektronik termasuk bagian dari informasi elektronik yang juga berupa sekumpulan data elektronik yang tidak terbatas pada tulisan, suara, gambar yang dilindungi atas kerahasiaannya dalam sistem elektronik. Pasal 30 Undang-Undang Informasi dan transaksi elektronik mengatur mengenai akses ilegal yang terdapat adanya pembatasan terhadap akses dalam sistem elektronik, yang mana ciri dari pembatasan akan akses adanya suatu pengamanan baik dari kode akses atau password tertentu atau dengan menggunakan bahasa pemrograman untuk masuk dengan membobol sistem keamanan, disamping itu untuk mengetahui bahwa data elektronik tersebut merupakan akses publik atau tidak dengan melihat adanya suatu sistem keamanan. Keterbatasan pada Undang-Undang ITE tidak dapat menjangkau akan modus yang dilakukan tanpa merusak sistem keamanan dan perubahan data yang dilakukan (data interference) baik itu menghilangkan atau memusnahkan data tersebut sehingga tidak lagi dapat dikenali oleh sistem komputer.



Persamaan antara penelitian yang akan dilakukan penulis dengan penelitian tersebut diatas adalah objek penelitian yakni perlindungan terhadap data pribadi, adapun perbedaannya adalah penelitian terdahulu menggunakan pertanyaan seputar hukum pidana yang berpengaruh terhadap penegakan perlindungan data pribadi, sedangkan penulis berencana meneliti perlindungan data pribadi dari sudut pandang penggunaan negara.

2. Nur Utami Hadi Putra Rezkia, Tesis, *Perlindungan Hukum terhadap Data Pribadi Konsumen dalam Registrasi SIM Card*, 2020, dengan rumusan permasalahan berupa Apakah pengaturan mengenai perlindungan hukum data pribadi konsumen dalam registrasi SIM card sudah sesuai dengan peraturan yang berlaku?

Adapun kesimpulan dari penelitian tersebut adalah pengaturan perlindungan data pribadi yang diberikan dalam proses registrasi SIM card mengacu pada Peraturan Menteri Komunikasi dan Informatika Nomor 20 Tahun 2016 tentang Perlindungan Data Pribadi dalam Sistem Elektronik. Penyelenggara jasa telekomunikasi dalam melaksanakan proses registrasi SIM card memiliki aturan internal dan telah menerapkan International Organization for Standardization (ISO) dan bekerjasama dengan International Electrotechnical Commission (IEC) Pelanggan jasa telekomunikasi dapat mengajukan pengaduan melalui Menteri atas penyalahgunaan data pribadi yang diberikan pada saat registrasi SIM card. Pada Peraturan Menteri Komunikasi dan Informatika Nomor 20 Tahun 2016 tentang Perlindungan Data Pribadi dalam Sistem Elektronik, sanksi yang diatur apabila terjadi kegagalan perlindungan data pribadi adalah berupa sanksi administratif.

Persamaan antara penelitian terdahulu dengan penelitian yang akan dilakukan oleh penulis terletak pada objek penelitian yakni perlindungan data pribadi dari sudut pandang konsumen/warga negara. adapun perbedaannya adalah penelitian terdahulu menggunakan sudut pandang warganegara sebagai konsumen SIM Card, sedangkan penulis berencana meneliti perlindungan data pribadi dari sudut pandang penggunaan negara.

3. Moh Hamzah Hizbuloh, “*Urgensi Rancangan Perlindungan Data Pribadi*”, Jurnal Hukum, Universitas Islam Sultan Agung, Volume 39 Nomor 1, Tahun 2023. Rumusan masalahnya adalah bagaimana Urgensi Pengesahan RUU PDP melihat banyaknya kasus yang bermunculan terkait kebocoran data pribadi baik di instansi swasta maupun instansi pemerintahan.

Adapun kesimpulan dari penelitian tersebut adalah Permasalahan kebocoran data pribadi menjadi hal yang sangat serius dalam penangannya, karena mengingat kurangnya regulasi pengaturan dan aturan hukum yang dapat menjerat pelanggar perlindungan data pribadi, oleh karena itu pengesahan RUU PDP menjadi UU menjadi hal yang sangat diperlukan, sehingga ada regulasi aturan khusus yang dapat melindungi hak privasi warga masyarakat, tanpa takut akan terjadi kebocoran data yang dimiliki dan setiap instansi swasta maupun pemerintah juga lebih berhati-hati dan meningkatkan sistem keamanan mereka dalam melindungi data pribadi masyarakat dan/atau customer. Sehingga tidak lagi ada kasus kebocoran data yang dikarena adanya pembobolan sistem oleh cyber. Dengan ini maka kasus-kasus pencurian data Pribadi di Indonesia dapat di berantas secara mendalam, karen

adanya regulasi yang jelas dan aturan hukum yang mengikat bagi pelanggar/pencuri data pribadi.

Persamaan antara penelitian yang akan dilakukan penulis dengan penelitian tersebut diatas adalah objek penelitian yakni perlindungan terhadap data pribadi, adapun perbedaannya adalah penelitian terdahulu merupakan penelitian pra pengundangan undang-undang perlindungan data pribadi tentang penegakan perlindungan data pribadi, sedangkan penulis berencana meneliti perlindungan data pribadi dari sudut pandang undang-undang yang baru.

