

BAB I

PENDAHULUAN

I.1 Latar Belakang Masalah

Setelah peristiwa 9/11, banyak kebijakan keamanan dihadirkan dalam rangka menjaga keamanan warga negara, namun di satu sisi, kebijakan tersebut malah meningkatkan kekuatan dari agensi pemerintahan (Joseph Verble, 2014). Pola pikir yang terbentuk adalah bahwa rakyat harus mengorbankan sedikit kebebasan mereka untuk memperoleh keamanan dan apabila seseorang tidak bersalah dalam hal apapun itu, maka seharusnya tidak ada hal yang harus disembunyikan dari pemerintah (Joseph Verble, 2014). Oleh karena itu, setelah peristiwa 9/11, terjadi lah upaya keamanan yang dinilai tidak memudahkan maupun menyenangkan bagi individu maupun warga negara (Joseph Verble, 2014).

Tepatnya setelah serangan 9/11 2001, Presiden George W. Bush memperluas wewenang NSA yang memungkinkan untuk melakukan penyadapan terhadap kekuatan asing atau intelijen asing tanpa adanya surat perintah, dengan tujuan mencapai kecepatan dan kelincahan dalam aktivitas NSA (Susan Landau, 2013). Hal tersebut juga diatur dalam peraturan FISA 1978, yang mensyaratkan kemungkinan untuk melakukan penyadapan terhadap kemungkinan tersangka kejahatan yang merupakan agen kekuatan asing, namun dalam peraturan tersebut penyadapan merupakan upaya terakhir saat informasi tidak dapat diperoleh dengan cara lain (Susan Landau, 2013). Namun, ditemukan bahwa banyak kasus yang diduga sebagai plot terorisme besar ternyata tidak seserius yang dituduhkan (Susan Landau, 2013).

Pada tanggal 6 Juni 2013, *The Guardian* menertibkan tulisan yang menyatakan bahwa NSA (*National Security Agency*) memiliki kebijakan yang diperintahkan oleh FISC (*Foreign Intelligence Surveillance Court*) (Lyon, 2014). Dimana dalam kebijakan tersebut adanya keharusan untuk Verizon, sebuah perusahaan telekomunikasi besar, untuk menyerahkan metadata dari panggilan telepon jutaan warga negara AS kepada FBI dan NSA (Greenwald, 2014). Pada tanggal 7 Juni 2013, artikel di *Washington Post* dan *The Guardian* menjelaskan

mengenai program PRISM yang memberikan akses kepada NSA terhadap server dari beberapa perusahaan teknologi terbesar seperti Apple, Facebook, Google, Microsoft, Skype, Yahoo, dan YouTube (Greenwald, 2014). Selain itu diberitakan pula bahwa kebijakan tersebut menargetkan pula komunikasi internet dan data yang disimpan dari warga non-AS di luar AS dan orang-orang yang berkomunikasi dengan mereka. Dalam program Upstream, merupakan program Kerjasama antara GCHQ (General Communications Headquarters) UK yang berkejasama dengan NSA dalam *Five Eyes* (Greenwald, 2014). Dimana didalamnya terdapat program Tempora yang pada intinya memberikan akses yang sama kepada GCHQ dengan yang terjadi pada program PRISM di AS (Greenwald, 2014). Pada tanggal 9 Juni 2013, *The Guardian* menyatakan bahwa sumber dari tulisannya adalah berasal dari seseorang bernama Edward Snowden yang merupakan pegawai Booz Allen Hamilton yang disewa oleh NSA (Greenwald, 2014).

Data yang diperoleh dalam pengungkapan yang dilakukan oleh Snowden adalah berupa metadata yaitu data yang berisi informasi mengenai “data mengenai data” yaitu seperti alamat IP, identitas kontak, lokasi panggilan dan pesan, dan durasi kontak, data mengenai sistem pengenalan plat nomor otomatis, dan program pengolah kata (Lyon, 2014). Hampir 5 juta rekaman panggilan telepon dikumpulkan setiap hari nya oleh NSA yang dapat mengungkap data pribadi mengenai lokasi pengguna saat telepon aktif (Lyon, 2014). NSA kemudian dapat menganalisis pola perilaku untuk dapat menungkap lebih banyak mengenai informasi pribadi dan hubungan antara pengguna yang berbeda (Greenwald, 2014). Selain itu, proses pengumpulan data pribadi tidak didasarkan pada batasan, penspesifikan, atau tujuan tertentu. Seperti misalnya dilakukan untuk melaksanakan aktivitas intelijen terhadap beberapa orang saja yang bersangkutan atau dicurigai dalam konteks keamanan nasional (Lyon, 2014). Namun yang terjadi adalah aktivitas pengumpulan massal data pribadi dari berbagai sumber, tanpa sebelumnya ditentukan dulu penggunaannya.

Peristiwa Snowden telah membangun kesadaran publik mengenai program pengawasan massal. Kelegalan dari aktivitas pengawasan tersebut dipertanyakan oleh advokat privasi dan aktivis perlindungan data, dan apakah program-program tersebut melanggar hukum yang terkait dengan perlindungan kebebasan dan privasi warga negara (Lyon, 2014). Walaupun diberikan keyakinan oleh AS dan beberapa negara lain yang terlibat bahwa mereka tidak

menargetkan warga negara dalam sistem pengawasan tersebut, namun hal itu tidak membuat warga negara khususnya advokat privasi dan perlindungan data percaya begitu saja. Sehingga banyak pihak yang menuntut adanya tanggapan teknis dan hukum, akuntabilitas, penghapusan program, dan pemajuan etika bagi aktivitas tersebut. Masalah etika pun muncul dalam aktivitas tersebut yaitu dalam aspek privasi dan perlindungan data, di mana privasi dan perlindungan data dipahami sebagai suatu hak asasi manusia, dan juga berkaitan dengan kebebasan berekspresi dan demokrasi (Lyon, 2014).

Dalam sudut pandang seorang aktivis, hal-hal yang dibocorkan oleh Edward Snowden merupakan sesuatu yang sudah lama menjadi kecurigaan orang-orang, dengan kata lain bahwa pengawasan massal dipandang oleh para aktivis sebagai praktik oleh pemerintahan yang sudah berlangsung lama dan lumrah serta telah berkembang dari waktu ke waktu (Dencik & Cable, 2017). Aktivitas ini adalah sesuatu yang dikritik keras oleh aktivis karena negara dalam hal ini dianggap memiliki kekuatan yang berlebihan dan dapat mengganggu. Dimana dalam hal ini, para aktivis telah mengevaluasi dan menyesuaikan diri untuk hidup dalam iklim pengawasan negara dalam melaksanakan kegiatan dalam mengejar tujuan mereka (Dencik & Cable, 2017). Mereka menganggap bahwa terdapat rasa ketidakberdayaan terkait dengan kemampuan individu untuk menjaga ruang otonom atau pribadi yang sebenarnya (Dencik & Cable, 2017).

Para aktivis menganggap bahwa aktivitas pengawasan beralih dari proses yang ditujukan untuk menyediakan perlindungan dari ancaman yang nyata, menjadi sesuatu yang digunakan sebagai kekuasaan untuk mengontrol warga negara dan melindungi kepentingan oleh politisi maupun korporasi besar (Dencik & Cable, 2017). Para aktivis menganggap bahwa terhambatnya atau terganggunya aktivitas individu secara umum dan jurnalisme secara khusus dengan alasan kekhawatiran terhadap terorisme merupakan suatu bentuk pengawasan yang berlebihan, di mana batas antara privasi dan keamanan nasional menjadi tidak jelas. Para aktivis berpikir perlu untuk memperbaiki keseimbangan antara keduanya, dan yang mungkin untuk dilakukan adalah untuk meningkatkan tindakan individu untuk dapat menegaskan privasi mereka masing-masing.

Salah satu konflik yang terjadi berkaitan dengan pengungkapan yang dilakukan oleh Edward Snowden adalah Kasus Schrems II. Pada 2013, Max Schrems, seorang juru kampanye hak privasi Austria, menantang validitas perjanjian *EU-US Privacy Shield* dan khususnya

mengenai transfer data pribadinya (dan data pribadi anggota UE) oleh Facebook ke server yang berbasis di AS, di hadapan Komisi Perlindungan Data Irlandia. Komisi Eropa dan Departemen Perdagangan AS, berkumpul untuk menyusun kerangka kerja alternatif yang memberikan tingkat perlindungan data yang memadai untuk transfer data trans-Atlantik.. Pada tahun 2015, Schrems sekali lagi menantang penggunaan SCC oleh Facebook untuk mentransfer data warga negara UE ke AS dengan alasan bahwa hal itu tidak cukup melindungi hak subjek data yang berbasis di UE (Maximillian Schrems v Data Protection Commissioner, 2015). Komisi Perlindungan Data Irlandia merujuk kasus ini ke Pengadilan Tinggi Irlandia dan Pengadilan Tinggi, yang selanjutnya kasus tersebut akan dirujuk ke CJEU pada tahun 2018 (Maximilian Schrems v Facebook Ireland Limited, 2018).

Pada awalnya, CJEU mencatat bahwa untuk menemukan Perlindungan Privasi UE-AS yang memadai, harus dipastikan bahwa hukum domestik negara ketiga yang menjamin tingkat perlindungan hak-hak fundamental pada dasarnya setara dengan yang dijamin di bawah Hukum UE. CJEU menemukan bahwa batasan pada perlindungan data pribadi yang muncul dari undang-undang AS tidak memenuhi persyaratan kesetaraan yang esensial. Misalnya, diamati bahwa Pemerintah AS tidak memberikan subjek data hak yang dapat ditindaklanjuti di hadapan Pengadilan terhadap otoritas AS. Atas dasar ini, CJEU menemukan bahwa *Privacy Shield* UE-AS tidak memadai dan tidak valid (Data Protection Commissioner v Facebook Ireland Limited and Maximilian Schrems, 2020). Pengadilan mengklarifikasi bahwa kecuali Komisi Eropa telah membuat keputusan kecukupan sebelumnya, Komisi Perlindungan Data memiliki kewenangan dan diwajibkan untuk menengguhkan atau melarang transfer data pribadi ke negara ketiga jika mereka yakin bahwa negara ketiga tempat data sedang ditransfer tidak memberikan tingkat perlindungan data yang pada dasarnya setara jika dibandingkan dengan Undang-Undang UE.

Privacy Shield antara UE dan Amerika Serikat sendiri merupakan kerjasama yang memiliki tujuan untuk menyediakan berbagai institusi maupun perusahaan dari kedua belah pihak sebuah mekanisme untuk memenuhi persyaratan proteksi data saat memindahkan data pribadi dari UE ke Amerika Serikat dan juga sebaliknya. *Privacy Shield* sendiri sebenarnya telah banyak dikritik oleh para pakar dan aktivis yang menyuarakan hak mengenai privasi dan perlindungan data. Kritik-kritik tersebut dilatarbelakangi oleh karena tidak adanya

perlindungan konkret terhadap akses sewenang-wenang negara maupun institusi serta perusahaan terhadap data pribadi individu yang diakses dan diolah dengan tujuan keamanan nasional seperti yang dilakukan oleh Amerika Serikat melalui kebijakan pengawasan massal terhadap publik yang berada di luar batas wilayahnya dalam upayanya menghindarkan diri dari ancaman keamanan nasionalnya (Puccio, 2018).

Hasil dari CJEU yang menyatakan ketidakvalidan *Privacy Shield* dianggap sebagai sebuah ketegasan terhadap penegakan hak dasar warga negara UE dan penegakan piagam Hak Fundamental UE. Ian Manners dikenal sebagai seorang yang mendukung teori mengenai Kekuatan Normatif UE. Kekuatan Normatif menjelaskan mengenai kekuatan Eropa mengenai pemahaman tentang identitas UE melalui prinsip, keyakinan, dan norma bersama yang dipatuhi dan diabadikan dalam peraturan hukum UE (Manners, 2008). Diantara prinsip-prinsip yang ada, hak asasi manusia merupakan salah satu diantaranya. Pengembangan kesepakatan antara anggota UE mengenai prinsip-prinsip seperti kebebasan, demokrasi, dan hak asasi manusia ini, menyebabkan anggota UE memiliki komitmen yang mengikat secara hukum. Lebih jauh lagi UE dilihat sebagai aktor internasional yang jauh dari penyelesaian masalah secara militer, dimana Strategi Keamanan UE (ESS) didefinisikan sebagai *pre-emptive engagement* yang bertujuan untuk memastikan dunia yang menawarkan keadilan dan kesempatan bagi semua orang (Union, 2003). UE dianggap lebih *civilian* karena kebijakannya didasarkan pada pendekatan yang lebih kepada *soft policy* (Laidi, 2008).

Dengan itu, maka penulis berusaha untuk melakukan penelitian berkaitan dengan keputusan CJEU me-non valid kan *Privacy Shield* antara UE-AS jika dikaitkan dengan kepentingan UE dalam hal kekuatan normatif. Dalam hal ini adalah berkaitan dengan penegakan hukum UE dalam hal ini adalah GDPR, khususnya terhadap hak untuk mendapatkan perlindungan data yang diklasifikasikan oleh UE sebagai Hak Asasi Manusia. Dengan pemahaman bahwa berbagai aspek seperti deretan hak-hak, kebebasan, dan nilai yang harus diperhitungkan, maka dalam hal ini pendekatan dengan fokus terhadap hak dan nilai menjadi lebih utama serta konsekuensi dalam hal etika dan sosial dalam pengelolaan data.

I.2 Rumusan Masalah

Berkaitan dengan Teori Kekuatan Normatif yang dikemukakan oleh Ian Manners, banyak yang melihat bahwa keputusan CJEU mengenai ketidakvalidan *Privacy Shield* akibat ketidaksetaraan pengaturan perlindungan data yang ada di Amerika Serikat dengan UE didasarkan pada komitmen UE terhadap penegakan dan penghormatan terhadap hak asasi manusia dan GDPR yang dimilikinya. Di mana dalam hal ini UE menganggap bahwa hak untuk privasi dan perlindungan data merupakan bentuk dari hak asasi manusia. Sehingga dilatarbelakangi oleh hal tersebut penulis berusaha untuk menyimpulkan pertanyaan berupa, “Apakah Motif UE Menghapus Validitas *European Union-United States Privacy Shield* Dalam Mengatasi Kejahatan Siber Berdasarkan Konsep *European Normative Power*: Studi Kasus Schrems II?”

I.3 Tujuan Penelitian

Adapun tujuan dari penelitian ini adalah:

- a) Mengetahui General Data Protection Regulation (GDPR) UE.
- b) Memahami kasus Schrems II yang dibawa ke CJEU, dimulai dari kasus Schrems I.
- c) Menganalisa keputusan CJEU untuk menghapus kevalidan EU-US *Privacy Shield* sebagai suatu upaya proyeksi GDPR berdasarkan kaca mata Ilmu Hubungan Internasional melalui konsep Rezim Internasional yang diturunkan ke dalam konsep Kekuatan Normatif Eropa.

I.4 Manfaat Penelitian

Manfaat yang diperoleh oleh penulis dalam penelitian ini adalah:

- a) Secara akademis manfaat yang didapatkan dalam penelitian ini adalah untuk memberikan informasi, data, dan pengetahuan baru bagi keilmuan hubungan internasional terkait peraturan proteksi data di UE (GDPR), serta perjalanan kasus Schrems II berdasarkan konsep Kekuatan Normatif Eropa, yang merupakan turunan dari konsep Rezim Internasional.

- b) Secara praktis dapat membantu pemangku kepentingan dalam merumuskan kebijakan terkait hak perlindungan data pribadi, berpacu kepada peraturan proteksi data UE (GDPR).

I.5 Sistematika Penulisan

BAB I Pendahuluan

Pada Bab I, penulis akan membahas mengenai latar belakang masalah, rumusan masalah, tujuan penelitian, manfaat penelitian, dan sistematika penulisan

BAB II Tinjauan Pustaka

Pada Bab II, penulis akan membahas mengenai penelitian terdahulu, kerangka pemikiran yang berisi konsep-konsep yang digunakan, serta alur pemikiran dan hipotesis.

BAB III Metodologi Penelitian

Pada Bab III, penulis akan membahas mengenai jenis penelitian, pendekatan penelitian, teknik pengumpulan data, teknik analisa data, teknik keabsahan data, serta waktu dan lokasi penelitian.

BAB IV Sejarah Hukum Perlindungan Data UE dan Landasan Hukum Kasus Schrems sebagai Kekuatan Normatif UE

Pada bab ini penulis akan menjelaskan mengenai sejarah dari Konvensi 108, Directive 95/46/EC, GDPR yang di dalamnya mengandung prinsip-prinsip perlindungan data sebagai kekuatan normatif UE, serta dipakai sebagai landasan hukum dalam Kasus Schrems II.

BAB V Keputusan Scherms II sebagai Bukti Pelaksanaan GDPR dan Motifnya

Pada bab ini penulis akan menjelaskan mengenai Kebijakan Pengawasan Massal AS sebagai Faktor Keputusan CJEU, SCC, Motif Umum UE dalam Memproyeksikan GDPR secara Global, Motif Normatif dari Proyeksi GDPR Melalui Perusahaan Multinasional yang Berbasis di UE, Motif Normatif dari Proyeksi GDPR melalui Kelembagaan dan Regulasi UE.

BAB VII Kesimpulan dan Saran

Pada bab VII, penulis akan membahas kesimpulan dari penelitian yang berupa jawaban dari pertanyaan penelitian serta berisi saran dan masukan terkait dengan permasalahan yang diangkat oleh penulis.