

Journal of International Relations Diponegoro

Volume 11 Issue 1 Year 2025 Page 97-106

**SCHREMS II DAN HAK KITA ATAS DATA:
PERTARUNGAN ANTARA KEAMANAN DAN KEPENTINGAN
GLOBAL**

Received: 24th March 2025; Revised: 28th April 2025

Accepted: 26th June 2025

Dhaifan Salhan Darari Ardiantoro, Ika Riswanti Putranti

**Departemen Hubungan Internasional, Fakultas Ilmu Sosial dan Ilmu Politik,
Universitas Diponegoro**

Jalan Prof. H. Soedarto, SH., Tembalang, Semarang, Jawa Tengah

dhaifansalhan14@gmail.com

Abstrak

Kasus Schrems II menjadi tonggak penting dalam penegakan hak asasi manusia (HAM) di era digital, terutama hak privasi. Keputusan Mahkamah Eropa (CJEU) pada tahun 2020 membatalkan Privacy Shield, mekanisme transfer data antara Uni Eropa (UE) dan Amerika Serikat (AS), yang menimbulkan tantangan signifikan dalam perlindungan hak privasi. Keputusan ini menegaskan bahwa perlindungan hak privasi harus diprioritaskan, bahkan dalam konteks hubungan ekonomi dan perdagangan internasional. Penelitian ini bertujuan untuk menganalisis putusan CJEU dalam kasus Schrems II dan implikasinya terhadap keamanan data sebagai bentuk pemenuhan HAM. Dengan menggunakan metode kualitatif dan pendekatan deskriptif analitis, penelitian ini mengumpulkan data dari sumber primer seperti putusan CJEU dan GDPR EU, serta sumber sekunder berupa buku, artikel jurnal, dan laporan penelitian terkait. Penelitian ini juga menggunakan teori Liberalisme dan Human security untuk menganalisis putusan Schrems II. Hasil penelitian menunjukkan bahwa putusan Schrems II memperkuat perlindungan data pribadi warga UE dengan membatasi transfer data ke negara-negara yang tidak memiliki standar perlindungan data yang memadai. Penelitian ini juga mengungkap adanya ketegangan antara keamanan data dan kepentingan ekonomi serta implikasi putusan Schrems II terhadap kebijakan perlindungan data di berbagai negara. Studi ini memberikan kontribusi penting dalam memahami perlindungan hak privasi di era digital serta dampaknya terhadap hubungan internasional.

Kata kunci : Schrems II, CJEU, Privacy Shield, GDPR, keamanan data, hak asasi manusia, privasi.

Abstract

The Schrems II case marks a significant milestone in the enforcement of human rights in the digital age, particularly the right to privacy. The decision by the Court of Justice of the European Union (CJEU) in 2020 invalidated the Privacy Shield, a data transfer mechanism between the European Union (EU) and the United States (US), posing significant challenges in protecting the right to

privacy. This decision affirms that the protection of the right to privacy must be prioritized, even in the context of international economic and trade relations. This study aims to analyze the CJEU's decision in the Schrems II case and its implications for data security as a form of human rights fulfillment. Employing a qualitative method with a descriptive-analytical approach, this research gathers data from primary sources such as CJEU decisions and the EU GDPR, along with secondary sources including books, journal articles, and relevant research reports. This research also employs Liberalism and Human Security theories to analyze the Schrems II ruling. The findings indicate that the Schrems II decision strengthens the protection of EU citizens' personal data by restricting data transfers to countries lacking adequate data protection standards. This study also reveals tensions between data security and economic interests, as well as the implications of the Schrems II decision for data protection policies in various countries. This research provides a crucial contribution to understanding privacy rights protection in the digital era and its implications for international relations.

Keywords: Schrems II, CJEU, Privacy Shield, GDPR, data security, human rights, privacy.

PENGANTAR

Keputusan *Schrems II* yang dijatuhkan oleh *Court of Justice of the European Union* (CJEU) pada tahun 2020 membantalkan kerangka kerja *EU-US Privacy Shield*, yang sebelumnya digunakan sebagai dasar hukum untuk transfer data pribadi dari Uni Eropa ke Amerika Serikat. Putusan ini menjadi tonggak penting dalam penguatan perlindungan hak asasi manusia, khususnya hak atas privasi di era digital. CJEU menilai bahwa perlindungan hukum terhadap data pribadi yang diberikan oleh pemerintah AS tidak sepadan dengan standar yang ditetapkan dalam hukum Uni Eropa, terutama karena ketidakhadiran mekanisme yang memungkinkan individu UE untuk menggugat pemrosesan data oleh otoritas AS di pengadilan. Dengan demikian, transfer data lintas batas hanya dapat dilakukan apabila negara tujuan memiliki perlindungan yang setara dengan yang dijamin oleh GDPR dan Piagam Hak Asasi Uni Eropa.

Dalam konteks global, *cross-border data flow* (CBDF) menjadi elemen esensial dalam mendukung pertumbuhan ekonomi digital dan perdagangan internasional. Perkembangan teknologi seperti komputasi awan, analisis data besar, dan layanan digital lintas negara menjadikan data sebagai sumber daya strategis. Namun, aliran data lintas negara juga menghadirkan tantangan signifikan, seperti risiko terhadap keamanan nasional, gangguan terhadap kedaulatan data, dan potensi pelanggaran hak privasi individu. Negara-negara kini menghadapi dilema antara memfasilitasi perdagangan digital dan menjaga kepentingan nasional serta hak-hak individu. Beberapa pemerintah menerapkan kebijakan pembatasan aliran data, seperti kewajiban *data localization*, untuk mengontrol data strategis dan menghindari akses tidak sah oleh pihak asing.

Kasus *Schrems II* juga berakar pada peristiwa pengungkapan oleh Edward Snowden mengenai praktik pengawasan massal oleh lembaga intelijen AS. Hal ini memunculkan kekhawatiran mengenai penyalahgunaan data pribadi oleh otoritas negara maupun korporasi besar. Max Schrems, aktivis privasi asal Austria, menantang legalitas kerangka transfer data yang digunakan Facebook, dengan alasan bahwa mekanisme tersebut tidak memberikan perlindungan hukum yang memadai. Setelah sebelumnya sukses menggugat *Safe Harbor* pada 2015, gugatan kedua Schrems terhadap penggunaan *Standard Contractual Clauses* (SCC) oleh Facebook berujung pada pembatalan *Privacy Shield* oleh CJEU. Pengadilan juga menegaskan bahwa otoritas perlindungan data nasional memiliki kewajiban untuk menghentikan transfer data jika perlindungan yang diberikan tidak setara dengan standar Eropa.

Dengan demikian, kasus *Schrems II* menegaskan bahwa perlindungan data pribadi merupakan hak fundamental yang tidak boleh dikompromikan dalam hubungan ekonomi internasional. Putusan ini menuntut perusahaan dan negara di luar UE untuk menyelaraskan praktik dan regulasi perlindungan data mereka agar sesuai dengan standar Uni Eropa. Dampaknya bersifat global, mendorong reformasi hukum perlindungan data dan menempatkan hak individu atas kontrol data sebagai prioritas utama dalam arsitektur hukum digital. Penegakan HAM dalam era digital memerlukan keseimbangan antara inovasi teknologi, kepentingan ekonomi, dan jaminan perlindungan hak privasi yang kuat.

TINJAUAN PUSTAKA

kompleksitas regulasi perlindungan data antara Uni Eropa (UE) dan Amerika Serikat (AS), dengan fokus utama pada kasus *Schrems I* dan *II* serta implikasinya terhadap kebijakan privasi global. Sejumlah penelitian menyoroti perbedaan mendasar antara pendekatan UE. Pembatalan *Safe Harbor* dalam kasus *Schrems I* dan kemudian *Privacy Shield* dalam kasus *Schrems II* menunjukkan ketidakseimbangan dalam standar perlindungan data yang diakui oleh Pengadilan Uni Eropa (CJEU), yang menekankan perlunya kepatuhan terhadap prinsip GDPR untuk memastikan keamanan data lintas batas. Beberapa penelitian mengkaji bagaimana perjanjian-perjanjian ini tidak hanya mempengaruhi hubungan transatlantik tetapi juga mencerminkan kekuatan normatif UE dalam menetapkan standar global, yang dalam konteks European Normative Power (ENP).

Dalam jangka panjang, ketidakpastian hukum akibat pembatalan mekanisme perlindungan data ini mendorong perdebatan mengenai perlunya reformasi kebijakan privasi di AS agar lebih selaras dengan standar UE serta pentingnya kerja sama internasional dalam mengembangkan regulasi perlindungan data yang lebih harmonis dan efektif. Maka dari itu untuk penelitian ini berfokus pada dampak hasil putusan Kasus *Schrems II* ini dari sisi interaksi

METODE RISET

Penelitian ini menggunakan metode penelitian secara kualitatif di mana metode penelitian digunakan untuk menjelaskan suatu fenomena secara komprehensif. Untuk memahami dan menjelaskan fenomena secara komprehensif maka tentunya diperlukan untuk mengumpulkan, menganalisis serta interpretasi data yang berupa kata-kata maupun gambar yang akan dianalisis secara induktif dan interpretatif (Merriam, 2009). Maka dengan ini penelitian ini nantinya akan memberikan penyajian pemahaman dan memberikan analisis secara objektif berdasarkan data-data dan fakta yang ada mengenai analisis penyelesaian kasus *Schrems II* dalam menangani hak keamanan data terhadap penegakan Hak Asasi Manusia.

PEMBAHASAN

MOTIF YANG MENDASARI KEPUTUSAN SCHREMS II DALAM MENJAMIN KEAMANAN DATA

Keputusan *Schrems II* yang dikeluarkan oleh *Court of Justice of the European Union* (CJEU) pada Juli 2020 merupakan tonggak penting dalam penguatan kerangka hukum perlindungan data internasional. Putusan ini tidak hanya membatalkan mekanisme

EU-US Privacy Shield, tetapi juga mempertegas bahwa perlindungan data pribadi merupakan hak fundamental yang harus dijamin bahkan dalam konteks hubungan perdagangan internasional. Secara normatif, keputusan ini menggarisbawahi peran penting Uni Eropa (UE) dalam membentuk tata kelola data global berbasis hak asasi manusia (HAM), serta menyoroti ketegangan antara kepentingan ekonomi, keamanan nasional, dan privasi individu dalam aliran data lintas batas (*cross-border data flow*).

Asal muasal kasus *Schrems II* tidak dapat dilepaskan dari *Schrems I*, yang berakar pada kekhawatiran Max Schrems terhadap praktik transfer data oleh Facebook dari UE ke Amerika Serikat (AS). Kekhawatiran ini semakin kuat setelah terungkapnya program pengawasan PRISM oleh NSA melalui pembocoran dokumen oleh Edward Snowden pada 2013. Schrems menggugat keabsahan mekanisme *Safe Harbor*, yang dinilai tidak memberikan perlindungan setara dengan yang dijamin oleh hukum UE. Pada 2015, CJEU membatalkan *Safe Harbor*, menyatakan bahwa warga negara UE tidak memiliki perlindungan hukum yang memadai terhadap pengawasan pemerintah AS, dan membuka jalan bagi pengantinya, yaitu *Privacy Shield*.

Namun, *Privacy Shield* pun tidak bertahan lama. Melalui *Schrems II*, CJEU membatalkannya karena menilai bahwa hukum pengawasan AS, khususnya berdasarkan *Foreign Intelligence Surveillance Act* (FISA) dan *Executive Order 12333*, masih membuka celah pengawasan luas terhadap data pribadi tanpa jalur hukum yang dapat diakses oleh warga negara UE. Meski CJEU tetap mengakui keberlakuan *Standard Contractual Clauses* (SCCs) sebagai mekanisme alternatif, keputusan ini memperketat prasyarat penggunaannya, mengharuskan perusahaan melakukan evaluasi menyeluruh atas perlindungan data di negara tujuan dan mengambil langkah teknis tambahan jika diperlukan.

Dari perspektif UE, keputusan *Schrems II* mempertegas peran Uni Eropa sebagai kekuatan normatif global. GDPR, sebagai kerangka hukum utama UE dalam perlindungan data, mengatur bahwa data pribadi warga UE hanya dapat ditransfer ke negara ketiga yang menyediakan tingkat perlindungan yang “esensial setara” dengan standar yang berlaku di Eropa. Ketentuan ini didasarkan pada Pasal 7 dan 8 Piagam Hak Asasi Fundamental UE serta Pasal 44–50 GDPR. Putusan tersebut mengukuhkan bahwa kepentingan komersial atau kerja sama ekonomi tidak dapat mengesampingkan hak privasi individu, dan transfer data harus tunduk pada prinsip proporsionalitas serta legalitas.

Sementara itu, dari sisi AS, pemerintah menekankan bahwa program pengawasan seperti PRISM dan UPSTREAM bertujuan melindungi keamanan nasional dan merespons ancaman seperti terorisme atau penyebaran senjata pemusnah massal. Namun, pendekatan ini dinilai tidak sejalan dengan standar UE karena bersifat diskriminatif terhadap warga non-AS yang tidak memiliki perlindungan hukum di pengadilan AS. Keputusan *Schrems II* memunculkan tekanan terhadap pemerintah AS untuk mereformasi pendekatan kebijakan privasi nasionalnya guna menjamin kesetaraan perlindungan data dalam konteks global.

Dampak dari keputusan ini cukup luas, khususnya dalam hal praktik bisnis dan pengelolaan data internasional. Banyak perusahaan yang sebelumnya mengandalkan *Privacy Shield* terpaksa beralih ke SCCs, yang kini harus dilengkapi dengan *Data Transfer Impact Assessment* (DTIA) dan langkah teknis seperti enkripsi dan pseudonimitas. Hal ini menimbulkan tantangan baru bagi perusahaan dalam hal biaya, kepatuhan, dan keberlanjutan operasional lintas batas. Selain itu, ketidakpastian hukum memaksa banyak perusahaan untuk mengevaluasi kembali kebijakan privasi mereka.

Secara sosial, putusan *Schrems II* meningkatkan kesadaran publik terhadap pentingnya perlindungan data pribadi dan mendorong transparansi dalam pengelolaan data oleh penyedia layanan digital. Meskipun ada risiko pengguna kehilangan akses ke beberapa layanan global yang tidak memenuhi standar GDPR, keputusan ini secara keseluruhan memperkuat jaminan atas privasi dan hak digital masyarakat UE. Lebih jauh, keputusan ini memberikan dorongan bagi AS dan UE untuk merundingkan kerangka perlindungan data baru yang lebih komprehensif dan dapat diterima oleh kedua belah pihak.

Secara hukum, keputusan CJEU didasarkan pada analisis terhadap kesesuaian hukum pengawasan AS dengan prinsip-prinsip HAM di bawah GDPR. Pengadilan menekankan bahwa negara ketiga yang menerima data harus menjamin hak akses hukum yang setara, transparansi dalam proses pengawasan, dan perlindungan efektif terhadap pelanggaran data. Dalam konteks ini, keputusan *Schrems II* menandai pentingnya *due diligence* dan *accountability* dalam setiap aktivitas transfer data internasional.

Secara normatif, keputusan ini juga mencerminkan konsep *European Normative Power*, yakni upaya UE membentuk norma global melalui standar internalnya. Dengan menegaskan bahwa perlindungan data tidak hanya berlaku di wilayahnya, tetapi juga dalam interaksi global, UE mengukuhkan posisi GDPR sebagai model tata kelola data yang semakin diakui secara internasional. Standar ini tidak hanya berdampak terhadap AS, tetapi juga terhadap negara-negara lain yang ingin menjalin kerja sama data dengan UE, mendorong harmonisasi hukum perlindungan data di tingkat global.

Kerangka hukum GDPR, khususnya Pasal 44–50, menjadi dasar legal utama dalam keputusan ini. Ketentuan ini menetapkan bahwa transfer data hanya diperbolehkan jika ada keputusan kecukupan, SCCs yang sah, atau mekanisme lain yang menjamin kesetaraan perlindungan. SCCs tetap valid pasca-*Schrems II*, tetapi penggunaannya diwajibkan untuk disertai analisis konkret terhadap hukum lokal di negara penerima data dan penyesuaian teknis dan kontraktual yang memadai.

Sebagai penutup, konseptualisasi kerangka hukum dalam *Schrems II* mencerminkan supremasi hak asasi manusia dalam kebijakan digital UE. Putusan ini tidak hanya memperkuat perlindungan data sebagai hak fundamental, tetapi juga menetapkan tolok ukur internasional untuk transfer data yang aman dan adil. Dengan pendekatan yang menyeimbangkan antara kedaulatan digital, keamanan, dan privasi, *Schrems II* menjadi preseden penting dalam evolusi hukum data internasional serta refleksi dari kebutuhan akan tatanan digital global yang lebih bertanggung jawab dan berbasis hak.

KEPUTUSAN SCHREMS II SERTA DAMPAKNYA PADA HUMAN SECURITY

Putusan *Schrems II* yang dikeluarkan oleh *Court of Justice of the European Union* (CJEU) merupakan keputusan yudisial penting yang tidak hanya berdampak pada aspek hukum dan ekonomi, tetapi juga menyentuh inti dari konsep *human security*, khususnya dalam konteks perlindungan data pribadi dan keamanan individu di era digital. Dengan membatalkan mekanisme *EU-US Privacy Shield*, putusan ini menandai titik balik dalam pengaturan transfer data internasional, yang menuntut standar perlindungan data pribadi setara dengan General Data Protection Regulation (GDPR) Uni Eropa. Putusan ini memperkuat posisi Uni Eropa dalam menjadikan privasi sebagai bagian tak terpisahkan dari hak asasi manusia.

Dampak *Schrems II* terasa kuat di berbagai negara, terutama negara-negara di luar Uni Eropa yang menjalin hubungan dagang dan pertukaran data dengan kawasan tersebut. Misalnya, Inggris pasca-Brexit, dan negara-negara dengan regulasi perlindungan data yang belum memenuhi standar GDPR, kini harus melakukan evaluasi individual terhadap transfer data. Selain mempengaruhi sektor bisnis, putusan ini mengharuskan negara-negara untuk memperkuat perlindungan data pribadi, membentuk lembaga pengawas independen, serta meningkatkan transparansi dalam kegiatan pengawasan. Di sektor kesehatan dan penerbangan, hambatan regulasi atas pertukaran data lintas batas menyebabkan tantangan baru dalam riset internasional dan layanan publik yang bergantung pada data digital.

Kasus serangan siber yang dilakukan kelompok peretas seperti Mirror Face terhadap Jepang menunjukkan bagaimana isu keamanan data semakin beriris dengan ancaman terhadap keamanan nasional. Di tengah lanskap ancaman digital global, negara seperti Jepang meningkatkan anggaran untuk intelijen siber dan memperkuat legislasi perlindungan data. Kasus ini menggambarkan bahwa keamanan data bukan hanya persoalan privasi, tetapi juga menyangkut kedaulatan dan ketahanan nasional.

Dalam kerangka *human security*, pendekatan keamanan yang berfokus pada individu menggantikan paradigma lama yang berpusat pada negara. Berdasarkan laporan *United Nations Development Programme* (UNDP) tahun 1994, *human security* mencakup tujuh dimensi: ekonomi, pangan, kesehatan, lingkungan, pribadi, komunitas, dan politik. Konsep ini menekankan pentingnya perlindungan multidimensi terhadap ancaman yang mengganggu hak dan martabat manusia.

Dimensi ekonomi *human security* berfokus pada jaminan pendapatan dasar dan stabilitas ekonomi. Dalam konteks *Schrems II*, pembatalan *Privacy Shield* menciptakan ketidakpastian hukum bagi pelaku usaha yang melakukan transfer data ke AS. Perusahaan menghadapi ancaman denda besar jika tidak mematuhi GDPR, sehingga berdampak langsung pada kelangsungan usaha kecil dan menengah. Meskipun Standard Contractual Clauses (SCCs) masih diperbolehkan, penggunaannya membutuhkan evaluasi risiko yang kompleks. Dalam jangka panjang, keputusan ini dapat memperkuat fondasi ekonomi digital global melalui standar tata kelola data yang lebih transparan.

Sementara itu, dimensi keamanan pribadi menyoroti ancaman terhadap individu dari negara atau entitas yang menyalahgunakan kekuasaan, seperti pengawasan massal tanpa dasar hukum yang memadai. Keputusan CJEU dalam *Schrems II* memperjelas bahwa pengawasan oleh lembaga intelijen AS seperti NSA tidak memberikan perlindungan hukum yang sepadan bagi warga UE, karena tidak tersedia mekanisme peradilan yang setara. Dalam konteks ini, UE menetapkan batasan tegas terhadap negara mitra dalam hal akses terhadap data warga Eropa. Dengan demikian, *Schrems II* memperkuat hak privasi sebagai komponen utama dalam menjaga keamanan pribadi individu.

Dimensi keamanan komunitas juga terpengaruh, mengingat komunitas digital saat ini bergantung pada transfer data internasional yang aman. *Schrems II* memastikan bahwa hak komunitas tidak dapat dikompromikan oleh kepentingan ekonomi negara atau perusahaan. Perusahaan global yang tidak dapat menjamin perlindungan setara terhadap data pribadi harus menghentikan transfer data, menciptakan ekosistem digital yang lebih terlindungi. Dalam perspektif politik, keputusan ini memperkuat posisi normatif UE sebagai pemimpin global dalam penegakan perlindungan data. Penolakan terhadap praktik pengawasan massal menandai pergeseran ke arah tata kelola digital yang demokratis, inklusif, dan berbasis HAM.

Peran GDPR dalam mendukung dimensi-dimensi *human security* sangat signifikan. Regulasi ini memberikan hak kepada individu atas akses, koreksi, penghapusan, portabilitas data, serta penolakan terhadap pengambilan keputusan otomatis. GDPR juga memaksa organisasi untuk meningkatkan transparansi dan akuntabilitas dalam pengelolaan data. Hal ini tidak hanya memberikan perlindungan hukum, tetapi juga memperkuat kepercayaan publik terhadap sistem digital.

Dalam dimensi ekonomi, walaupun perusahaan menghadapi beban administratif dan biaya kepatuhan yang tinggi, kebijakan ini mendorong konsistensi hukum dan perlindungan yang lebih merata di pasar digital. *Binding Corporate Rules* dan SCCs masih dapat digunakan, tetapi hanya jika diiringi dengan penilaian risiko dan penerapan langkah-langkah teknis tambahan seperti enkripsi dan pseudonimitas. Negara-negara mitra seperti AS pun dituntut untuk melakukan reformasi hukum yang menjamin hak atas privasi warga asing.

Dimensi politik dalam *human security* menjadi sangat relevan dalam kasus ini. *Schrems II* menolak logika bahwa keamanan nasional dapat dijadikan dalih untuk pengumpulan data tanpa batas. Dengan menegaskan bahwa perlindungan data pribadi adalah hak asasi manusia, CJEU memperkuat prinsip-prinsip demokrasi dan supremasi hukum dalam ranah digital. Negara-negara yang ingin menjalin kerja sama data dengan UE harus tunduk pada standar HAM yang ditetapkan, menjadikan perlindungan data sebagai instrumen diplomasi digital dan alat pembentuk tata kelola global berbasis norma.

Tantangan besar yang dihadapi adalah harmonisasi regulasi perlindungan data lintas negara. Perbedaan struktural antara regulasi AS dan GDPR menimbulkan hambatan serius dalam membangun sistem transfer data yang sah. Beberapa solusi yang diusulkan mencakup perjanjian internasional yang mengikat, peningkatan pengawasan oleh otoritas perlindungan data, serta reformasi internal di negara-negara mitra. Tanpa harmonisasi ini, stabilitas hukum dalam aliran data global akan terus terganggu, berpotensi menghambat pertumbuhan ekonomi digital.

Tantangan lainnya adalah menciptakan keseimbangan antara keamanan nasional dan perlindungan HAM. Negara sering menggunakan dalih keamanan untuk membenarkan pengumpulan data secara besar-besaran. Namun, tanpa batasan yang jelas, hal ini rentan menjadi penyalahgunaan kekuasaan. *Schrems II* memberikan batasan tegas bahwa pengumpulan data harus sesuai dengan prinsip legalitas, proporsionalitas, dan adanya mekanisme pemulihan hukum bagi subjek data.

Sebagai kesimpulan, *Schrems II* tidak hanya menjadi putusan hukum, tetapi juga simbol pergeseran paradigma dalam tata kelola data global. Keputusan ini menegaskan bahwa di era digital, keamanan individu dan komunitas harus dijaga dengan serius. Dengan mengintegrasikan prinsip-prinsip *human security* ke dalam kebijakan perlindungan data, Uni Eropa menunjukkan bahwa privasi adalah hak universal yang tidak bisa dikompromikan oleh tekanan ekonomi, politik, atau teknologi. Tantangan dalam implementasinya masih besar, tetapi dengan pendekatan kolaboratif dan berbasis HAM, sistem perlindungan data yang lebih adil dan efektif dapat diwujudkan dalam skala global.

KESIMPULAN

Penelitian ini menyoroti dampak dan implikasi hukum dari putusan *Schrems II* dalam konteks pemenuhan hak asasi manusia, khususnya hak atas privasi dan perlindungan data pribadi. Keputusan yang dikeluarkan oleh *Court of Justice of the European Union* (CJEU) pada tahun 2020 yang membantalkan kerangka *EU-US Privacy*

Shield memiliki pengaruh yang luas terhadap tata kelola transfer data lintas batas. Putusan ini menegaskan bahwa transfer data internasional hanya dapat dilakukan apabila negara tujuan memiliki standar perlindungan data yang secara esensial setara dengan standar Uni Eropa yang diatur dalam General Data Protection Regulation (GDPR). Dalam konteks tersebut, perlindungan data tidak lagi hanya menjadi isu hukum dan ekonomi, tetapi juga menyangkut hak fundamental individu dalam kerangka *human rights* dan *human security*.

Dibandingkan dengan penelitian sebelumnya yang lebih menitikberatkan pada aspek perbandingan regulasi atau konsekuensi bisnis dari pembatalan *Privacy Shield*, penelitian ini menawarkan pendekatan yang lebih holistik. Fokus utama diletakkan pada hubungan antara perlindungan data pribadi dan pemenuhan hak asasi manusia. Penelitian ini mengangkat pentingnya memahami keputusan *Schrems II* tidak semata-mata sebagai isu legal formal, melainkan sebagai instrumen perlindungan terhadap individu dari potensi pelanggaran HAM, khususnya dalam mencegah praktik pengawasan massal oleh negara atau pihak ketiga.

Lebih lanjut, analisis dalam penelitian ini menunjukkan bahwa meskipun keputusan *Schrems II* memperkuat standar internasional perlindungan data melalui penguatan mekanisme *Standard Contractual Clauses* (SCCs), keputusan ini juga memunculkan tantangan praktis, terutama bagi perusahaan global. Mereka dituntut untuk menyesuaikan kebijakan dan infrastruktur data mereka agar sesuai dengan ketentuan GDPR. Ketentuan ini tidak hanya menambah beban administratif, tetapi juga mengharuskan adanya evaluasi risiko dan penyesuaian teknis yang signifikan. Di sisi lain, keputusan ini menuntut pemerintah negara ketiga untuk melakukan reformasi hukum yang dapat menjamin kesetaraan perlindungan data sebagai prasyarat kerja sama digital dengan UE.

Dari perspektif *human security*, *Schrems II* menjadi tonggak penting dalam memastikan bahwa perlindungan terhadap data pribadi merupakan bagian dari keamanan individu yang komprehensif. Keputusan ini membantu memperkuat hak individu atas kendali terhadap informasi pribadinya serta membatasi ruang lingkup intervensi negara dalam kehidupan digital masyarakat. Namun, tantangan utama yang tersisa adalah bagaimana menyeimbangkan perlindungan data dengan kepentingan ekonomi dan kebutuhan keamanan nasional.

Sebagai implikasi praktis, penelitian ini menekankan pentingnya pendekatan lintas sektor dalam merespons dinamika regulasi perlindungan data global. Pemerintah, sektor swasta, dan masyarakat sipil perlu membangun kerja sama yang berkelanjutan untuk menciptakan sistem perlindungan data yang tidak hanya sesuai dengan standar hukum internasional, tetapi juga menjamin penghormatan terhadap hak-hak dasar manusia dalam tatanan digital yang terus berkembang.

UCAPAN TERIMA KASIH

Artikel jurnal ini dihasilkan atas bantuan dan dukungan dari para dosen yang telah memberikan masukan, arahan, dan evaluasi kritis sehingga tulisan ini dapat diselesaikan dengan baik. Apresiasi dan rasa terima kasih juga penulis ucapkan kepada keluarga dan teman-teman yang telah memberikan dukungan moril di setiap proses yang penulis jalani. Terima kasih banyak, Bapak dan Ibu dan teman-teman.

REFERENSI

(Buku)

- Chandler, D. (1999). *Brother number one: A political biography of Pol Pot*.
- Donnelly, J. (2003). *Universal human rights in theory & practice*. New York: Cornell University Press.
- Donnelly, J. (2007). *International human rights*. Colorado: Westview Press.
- Maxwell, J. A. (2013). *Qualitative research design: An interactive approach*. Sage Publications.
- Merriam, S. B. (2009). *Qualitative research: A guide to design and implementation*. Jossey-Bass.
- Smith, R. K. (2010). *Textbook on international human rights*. New York: Oxford University Press.
- Wagner, B., Kettemann, M. C., & Vieth, K. (2019). *Research handbook on human rights and digital technology: Global politics, law and international relations*. Edward Elgar Publishing.

(Jurnal Artikel / Artikel Website)

- Caamíña Domínguez, C. M. (2019). La noción de “consumidor” en internet: El asunto C-498/16, Maximilian Schrems y facebook Ireland Limited = Internet consumer: Case C-498/16, Maximilian Schrems v. Facebook Ireland Limited. *CUADERNOS de DERECHO TRANSNACIONAL*, 11(1), 711. <https://doi.org/10.20318/cdt.2019.4642>
- Chin, Y.-C., & Zhao, J. (2022). Governing Cross-Border Data Flows: International Trade Agreements and Their Limits. *Laws*, 11(4), 63. <https://doi.org/10.3390/laws11040063>
- Churches, G., & Zalnieriute, M. (2020). “Contracting out” human rights in international law: Schrems II and the fundamental flaws of U.S. surveillance laws. *SSRN Electronic Journal*.
- Dencik, L., Hintz, A., & Cable, J. (2016). Towards data justice? The ambiguity of anti-surveillance resistance in political activism. *Big Data & Society*, 3(2), 205395171667967. <https://doi.org/10.1177/2053951716679678>
- Dimas, W. (2018). Failed herd immunity: American business compliance and the United States cyber-security policy's clash with the European Union's General Data Protection Act. *Loyola University Chicago International Law Review*, 15(2).
- Du, X., & Liu, A. (2023). Security and openness: China's cross-border data flow scheme. *Pacific International Journal*, 138–141.
- Fantin, S. (2020). Data Protection Commissioner v Facebook Ireland Limited, Maximillian Schrems: AG Discusses the Validity of Standard Contractual Clauses and Raises Concerns Over Privacy Shield (C-311/18 Schrems II, Opinion of AG Saugmandsgaard Øe). *European Data Protection Law Review*, 6(2), 325–331. <https://doi.org/10.21552/edpl/2020/2/21>
- Hallinan, D., & Bernier, A. (2021). International transfers of personal data for health research following Schrems II: A problem in need of a solution. *European Journal of Human Genetics*.
- Lam, C. (2017). Unsafe harbor: The European Union's demand for heightened data privacy standards in Schrems v. Irish Data Protection Commissioner. *Boston College International and Comparative Law Review*, 40(3), E. Supp. 1.

- Morschbach, F. (2023). Third Country PNR Mechanisms After the CJEU's Schrems II Judgment. *Air and Space Law*, 48(Issue 1), 91–112. <https://doi.org/10.54648/aila2023012>
- Rotenberg, M. (n.d.). Schrems II, from Snowden to China: Toward a new alignment on transatlantic data protection. *European Law Journal*, 26(1-2). <https://doi.org/0.1111/eulj.12370>
- Tracol, X. (2020). "Schrems II": The return of the Privacy Shield. *Computer Law & Security Review*, 39, 105484. <https://doi.org/10.1016/j.clsr.2020.105484>
- Ziyi, X. (2022). International Law Protection of Cross-Border Transmission of Personal Information Based on Cloud Computing and Big Data. *Mobile Information Systems*, 2022, 1–9. <https://doi.org/10.1155/2022/9672693>

(Working Paper / Laporan Penelitian / Skripsi / Tesis)

Ananda, S. A. S., Putranti, I. R., & Basith, A. A. (2021). *Pengaruh The Cybersecurity Act terhadap Digital Single Market Uni Eropa* (Skripsi Sarjana, Fakultas Ilmu Sosial dan Ilmu Politik, Universitas Diponegoro).

Domínguez, C. M. (2019). *Internet consumer: Case C-498/16, Maximilian Schrems v. Facebook Ireland Limited*. Universidad Carlos III de Madrid.

Puvalova, N. (2017). *Transatlantic data flow under the EU-U.S. Privacy Shield: An adequate protection of the fundamental right to protection of personal data?* (Master's thesis, Faculty of Law, University of Oslo).

(Konferensi, Internet, Reports, and Others)

Casalini, F., & Gonzalez, J. L. (2019). *Trade and cross-border data flows*. OECD.

Union, C. o. (2020, July 16). The Court of Justice invalidates Decision 2016/1250 on the adequacy of the protection provided by the EU-US Data Protection Shield. Retrieved from THE COURT OF JUSTICE OF THE EUROPEAN UNION.