END-TO-END ENCRYPTION: APAKAH INI SEBUAH ANCAMAN?
END-TO-END ENCRYPTION: IS IT A THREAT?

Messa Prima Kaldera

Badan Siber dan Sandi Negara

Meme Indriana Putri

Badan Siber dan Sandi Negara

ABSTRAK

Policy brief ini menganalisis dampak kebijakan *end-to-end encryption* yang diterapkan oleh Facebook pada *platform* komunikasi seperti WhatsApp, Facebook Messenger, dan Instagram, yang menimbulkan kekhawatiran di beberapa negara, termasuk Indonesia, terkait dengan hambatan dalam akses informasi oleh pihak berwenang untuk investigasi dan penegakan hukum terhadap kejahatan online seperti pelecehan anak dan terorisme. Dengan menggunakan metode *grid analysis*, *policy brief* ini mengevaluasi opsi kebijakan nasional yang dapat diambil oleh pemerintah Indonesia. Hasil analisis menunjukkan bahwa kebijakan yang paling tepat adalah meminta hak akses bagi pemerintah terhadap data terenkripsi, yang sejalan dengan peraturan perundang-undangan yang ada dan disertai sanksi bagi penyelenggara sistem elektronik yang tidak mematuhi, termasuk teguran, penghentian sementara, pemutusan akses, dan pencabutan izin.

Kata Kunci: *End-to-end encryption*, Kebijakan, Indonesia.

ABSTRACT

This policy brief analyzes the impact of the end-to-end encryption policy implemented by Facebook on communication platforms such as WhatsApp, Facebook Messenger, and Instagram, which has raised concerns in several countries, including Indonesia, related to barriers in access to information by authorities for investigations and law enforcement against online crimes such as child abuse and terrorism. Using a grid analysis method, this policy brief evaluates national policy options that can be taken by the Indonesian government. The results of the analysis show that the most appropriate policy is to require access rights for the government to encrypted data, which is in line with existing laws and regulations and is accompanied by sanctions for non-compliant electronic system providers, including warnings, temporary suspension, termination of access, and revocation of licenses.

Keywords: *End-to-end encryption, Policy, Indonesia.*

A. Latar Belakang

Beberapa waktu terakhir, Facebook menerapkan kebijakan *end-to-end encryption* (E2EE) pada aplikasi WhatsApp, Facebook Messenger, dan Instagram, yang merupakan teknologi untuk melindungi komunikasi pengguna sehingga tidak dapat diakses oleh siapa pun, termasuk penyedia layanan. Kebijakan ini diharapkan dapat melindungi data pribadi dari penyalahgunaan, terutama setelah munculnya kasus peretasan oleh hacker Bjorka yang berhasil membobol data pribadi di Indonesia, termasuk data pelanggan Indihome dan 1,3 miliar data registrasi SIM Card milik Kemenkominfo. Namun, di sisi lain, penerapan enkripsi ini juga menimbulkan kekhawatiran, karena mempersulit penegak hukum dalam mengakses informasi yang dibutuhkan untuk investigasi dan penegakan hukum, khususnya dalam kasus kejahatan online seperti pelecehan seksual pada anak dan penyebaran konten terorisme.

Seperti diketahui bersama bahwa Indonesia berkomitmen dalam penanganan masalah terorisme dan pelecehan seksual pada anak, termasuk dalam menghadapi penyebaran kontennya secara *online*. Hal tersebut dapat terlihat dari beberapa kebijakan yang dikeluarkan yaitu :

a. Undang-Undang Nomor 35 Tahun 2014 tentang Perubahan Atas Undang-Undang Nomor 23 Tahun 2002 tentang Perlindungan Anak;
b. Undang-Undang Nomor 15 tahun 2003 tentang Penetapan Peraturan Pemerintah Pengganti Undang-Undang Nomor 1 Tahun 2002 Tentang Pemberantasan Tindak Pidana Terorisme;
c. Undang-Undang Nomor 9 Tahun 2013 tentang Pencegahan dan Pemberantasan Tindak Pidana Pendanaan Terorisme;
d. Peraturan Presiden Nomor 46 Tahun 2010 tentang Badan Nasional Penanggulangan Terorisme;
e. Peraturan Menteri Komunikasi dan Informatika Republik Indonesia Nomor 19 Tahun 2014 tentang Penanganan Situs Internet Bermuatan Negatif.

Selain berkomitmen terhadap permasalahan terorisme dan pelecehan seksual, pemerintah Indonesia juga memiliki perhatian khusus terkait pelindungan data pribadi melalui:

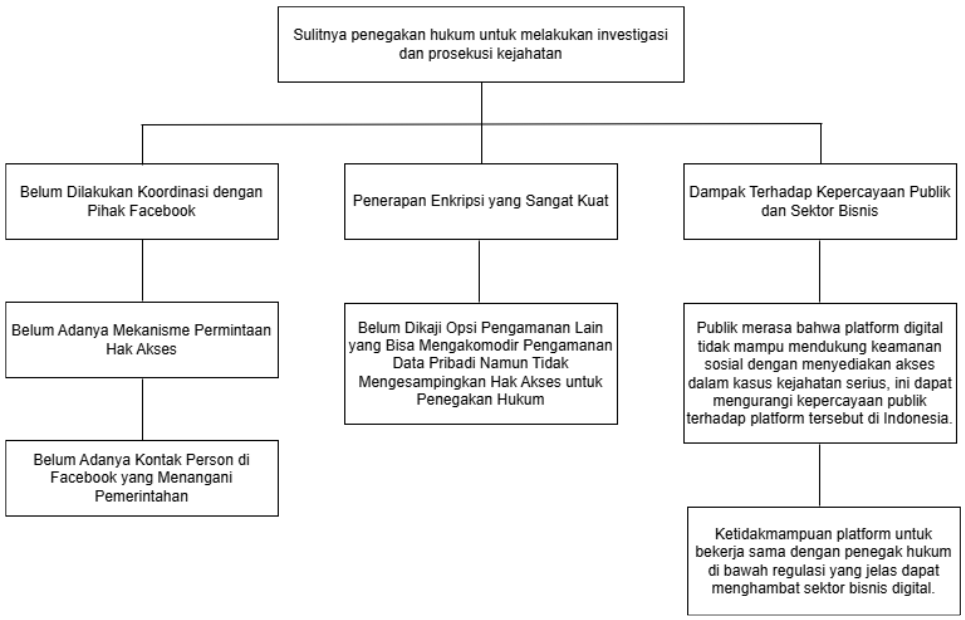
a. Undang-Undang Dasar 1945 Pasal 28G yaitu Setiap orang berhak atas perlindungan diri pribadi, keluarga, kehormatan, martabat, dan harta benda yang di bawah kekuasaannya, serta berhak atas rasa aman dan perlindungan dari ancaman ketakutan untuk berbuat atau tidak berbuat sesuatu yang merupakan hak asasi.
b. Undang-Undang Nomor 36 Tahun 1999 tentang Telekomunikasi
c. Undang-Undang Nomor 39 Tahun 1999 tentang Hak Asasi Manusia
d. Undang-Undang Nomor 19 Tahun 2016 tentang perubahan Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik
e. Undang-undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi.
f. Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik

B. Fokus Permasalahan

Pasca penerapan Kebijakan E2EE, beberapa negara mempermasalahkan Kebijakan E2EE yang diberlakukan oleh Facebook pada aplikasi Whatsapp, Facebook Messenger dan Instagram. Dampak penerapan kebijakan E2EE pada hak privasi individu sangat signifikan dan terkait erat dengan hak asasi manusia, terutama dalam konteks hak atas privasi. Kebijakan E2EE memberikan perlindungan data sensitif dari ancaman peretasan, pengawasan illegal, atau pencurian data. Dengan E2EE, hanya pengirim dan penerima yang memiliki kunci yang dapat mengakses konten pesan, sehingga data pengguna lebih aman dan rahasia.

Namun, kebijakan ini juga menimbulkan tantangan bagi penegak hukum dalam menangani kejahatan di ranah siber. Di satu sisi, privasi adalah hak asasi yang diakui secara internasional dan dijamin oleh berbagai instrumen hukum, seperti *Universal Declaration of Human Rights*/Deklarasi Universal Hak Asasi Manusia (Pasal 12). Di sisi lain, enkripsi yang tidak dapat diakses oleh penegak hukum bisa menghambat penyelidikan kasus kejahatan serius, seperti eksploitasi anak, terorisme, dan penyebaran kebencian.

Dilema ini mencerminkan tantangan bagi negara-negara, termasuk Indonesia. Untuk mencari keseimbangan antara kebutuhan keamanan nasional dan penegakan hukum dengan perlindungan hak privasi individu. Kebijakan E2EE berpotensi menjadi ”dua sisi mata uang”, di mana satu sisi melindungi individu dari ancaman yang membahayakan data pribadi, di sisi lain beresiko mengurangi efektivitas penegakan hukum.



Gambar 1. Pohon Masalah

C. Alternatif Kebijakan

Terdapat tiga alternatif kebijakan terkait kondisi penerapan *end-to-end encryption* dengan mempertimbankan perlindunga data pribadi serta proses penegakan hukum yakni:

1. Tidak menerapkan enkripsi sama sekali
2. Menerapkan algoritma yang lemah
3. Meminta hak akses untuk pemerintah

Untuk mengetahui alternatif kebijakan yang paling tepat dalam mengatasi permasalahan tersebut dilakukan analisis menggunakan teknik *grid analysis* dengan kriteria efektivitas, efisiensi, dan keberterimaan.

Tabel 1. *Grid Analysis*

No.	Alternatif Kebijakan	Efek-tifitas 40%	Efi-siensi 40%	Accept-ability 20%	Total
1	Tidak menerapkan enkripsi sama sekali	1 (0,4)	1 (0,4)	1 (0,2)	1
2	Menerapkan algoritma yang lemah	2 (0,8)	3 (1,2)	2 (0,4)	2,4
3	Meminta hak akses untuk pemerintah	4 (1,6)	3 (1,2)	4 (0,8)	3,6
Ket: Skor 1-5					

Setelah dilakukan pembobotan dan skoring diperoleh urutan alternatif kebijakan sebagai berikut:

a. Tidak menerapkan enkripsi sama sekali dengan total skor 1

   Alternatif kebijakan ini diusulkan karena terdapat beberapa negara yang tidak mendukung penerapan E2EE salah satunya Inggris. Inggris berpendapat bahwa dengan pengaplikasian E2EE dapat membani penegak hukum dalam melaksanakan tugasnya khususnya terkait pemberantasan teroris dan melindungi anak-anak dari pelecehan di berbagai platform. Alternatif kebijakan ini tidak direkomendasikan untuk diterapkan karena dari sisi bisnis, kebijakan ini dapat menyebabkan kerugian karena fitur keamanan merupakan salah satu nilai jual dari Penyelenggara Sistem Elektronik. Selain itu, dari segi kebijakan yang berlaku pun menyalahi aturan UU No.36 Tahun 1999 tentang Telekomunikasi pada Pasal 42 ayat (1), UU No. 27 Tahun 2022 tentang Pelindungan Data Pribadi dan Peraturan Menteri Komunikasi dan Informatika Nomor 20 Tahun 2016 tentang Perlindungan Data Pribadi Dalam Sistem Elektronik pada Pasal 15 ayat (2). Selain dari segi tidak taatnya pada peraturan perundang-undangan pilihan ini pun dapat mengakibatkan ketidak sesuaian dengan kebijakan di luar Indonesia seperti GDPR dan dapat mengakibatkan kerentanan terhadap serangan siber.

b. Menerapkan algoritma yang lemah dengan total skor 2,4

   Pilihan kebijakan ini tidak direkomendasikan karena bertentangan dengan peraturan perundang-undangan yang berlaku salah satunya yaitu UU No.36 Tahun 1999 tentang Telekomunikasi pada Pasal 42 ayat (1), UU No. 27 Tahun 2022 tentang Pelindungan Data Pribadi , PP No. 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik pada Pasal 3 ayat (1) dan Peraturan Menteri Komunikasi dan Informatika Nomor 20 Tahun 2016 tentang Perlindungan Data Pribadi Dalam Sistem Elektronik pada Pasal 15 ayat (2). Selain dari segi tidak taatnya pada peraturan perundang-undangan pilihan ini pun dapat mengakibatkan ketidak sesuaian dengan kebijakan di luar Indonesia seperti GDPR dan standar internasional yang ada seperti PCI-DSS dan dapat mengakibatkan kerentanan terhadap serangan siber.

c. Memiliki hak akses untuk pemerintah dengan total skor 3,6

   Kebijakan ini dapat menjadi pilihan jika dikaitkan dengan proses penegakan hukum karena tercantum pula dalam peraturan perundang-undangan yakni:

   - UU No. 36 Tahun 1999 tentang Telekomunikai pada Pasal 42 ayat (2)
   - UU No. 39 Tahun 1999 tentang Hak Asasi Manusia pada Pasal 32
   - PP No. 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik
   - Peraturan Menteri Komunikasi dan Informatika Nomor 20 Tahun 2016 tentang Perlindungan Data Pribadi Dalam Sistem Elektronik pada Pasal 23 ayat (1)
   - Peraturan Menteri Komunikasi dan Informatika Nomor 5 Tahun 2020 tentang Penyelenggaraan Sistem Elektronik Lingkup Privat pada Pasal 21 ayat (1), Pasal 21 ayat (2), Pasal 32 ayat (1), Pasal 33 ayat (1), Pasal 35.

D. Rekomendasi Kebijakan

Berdasarkan total skor masing-masing alternatif kebijakan, maka rekomendasi kebijakan yang paling tepat dilakukan untuk mengatasi masalah penerapan kebijakan end to end encryption pada beberapa platform adalah "Meminta hak akses untuk pemerintah khususnya terkait penegakan hukum untuk kepentingan penyidikan, penuntutan, persidangan". Agar rekomendasi kebijakan dapat terlaksana dengan optimal diperlukan strategi pelaksanaan rekomendasi kebijakan dan mekanisme pengawasan serta akuntabilitas sebagai berikut:

1. Penerapan Protokol *Multiple Escrow Agent*

Pemberian hak akses juga memenuhi beberapa aspek yang dijabarkan pada Peraturan Menteri Komunikasi dan Informatika Nomor 5 Tahun 2020 tentang Penyelenggara Sistem Elektronik Lingkup Privat Pasal 30 ayat (3). Teknik kriptografi yang dapat mengakomodir hal tersebut yakni dengan menerapkan Kunci *Escrow* menggunakan Protokol *Multiple Escrow Agents*. *Agents escrow* yang dipilih merupakan pihak-pihak yang memiliki kewenangan berdasarkan peraturan perundang-undangan.

Tabel 2. *Agents Escrow* Terpilih

No.	Nama Instansi	Keterangan
1.	Jaksa Agung	Merujuk Undang-Undang Nomor 36 Tahun 1999 tentang Telekomunikasi Pasal 42 ayat (2) dalam rangka proses penegakan hukum
2.	Kepala Kepolisian Republik Indonesia	Merujuk Undang-Undang Nomor 36 Tahun 1999 tentang Telekomunikasi Pasal 42 ayat (2) dalam rangka proses penegakan hukum
3.	Kementerian atau Lembaga dalam rangka pengawasan sesuai dengan peraturan perundang-undangan	Merujuk peraturan Menteri Komunikasi dan Informatika Nomor 5 Tahun 2020 tentang Penyelenggara Sistem Elektronik Lingkup Privat dalam rangka pengawasan sesuai dengan peraturan perundang-undangan.
4.	Aparat Penegak Hukum Lain	Merujuk peraturan Menteri Komunikasi dan Informatika Nomor 5 Tahun 2020 tentang Penyelenggara Sistem Elektronik Lingkup Privat dalam rangka kepentingan penyidikan, penuntutan, atau persidangan tindak pidana dalam wilayah hukum Negara Kesatuan Republik Indonesia.

Mekanisme pengawasan dalam penerapan protokol ini dilakukan dengan membentuk badan pengawas yang terdiri dari pihak-pihak berwenang, lembaga independen, dan perwakilan masyarakat sipil yang akan menjadi pengambil keputusan dalam hal permintaan akses data untuk keperluan hukum. Setiap permintaan harus melalui proses validasi yang transparan, dengan persyaratan ketat terkait jenis kejahatan dan bukti permulaan yang cukup. Setiap akses ke data harus dicatat dalam sistem audit yang dapat diawasi oleh lembaga independen atau Ombudsman.

2. Menyusun prosedur perizinan berlapis
   Setiap permintaan akses data harus melalui proses yang jelas serta pembatasan akses yang ketat dan pemberlakuan sanksi atas penyalahgunaannya. Terkait hal tersebut dapat diatur oleh lembaga yang menangani pelindungan data pribadi seperti yang diamanatkan pada UU 27 Tahun 2022 tentang Pelindungan Data Pribadi.

3. Menempatkan Pusat data (*data center*) dan pusat pemulihan bencana (*disaster recovery center*) untuk pelayanan publik yang digunakan untuk proses perlindungan Data Pribadi ditempatkan dalam wilayah negara Republik Indonesia
   Menempatkan Pusat data (*data center*) dan pusat pemulihan bencana (*disaster recovery center*) untuk pelayanan publik yang digunakan untuk proses perlindungan Data Pribadi ditempatkan dalam wilayah negara Republik Indonesia merujuk pada Peraturan Menteri Komunikasi dan Informatika Nomor 20 Tahun 2016 tentang Perlindungan Data Pribadi Dalam Sistem Elektronik Pasal 17 ayat (1).
   Mekanisme pengawasannya dapat dilakukan dengan membentuk badan pengawas untuk mengawasi kepatuhan terhadap prosedur akses data pribadi,

dengan kewajiban melaporkan setiap akses atau pemulihan data yang dilakukan.

4. Menunjuk Narahubung yang berdomisili di Wilayah Indonesia yang bertugas untuk memfasilitasi permintaan akses
   Menunjuk Narahubung yang berdomisili di wilayah Indonesia yang bertugas untuk memfasilitasi permintaan akses terhadap Sistem Elektronik dan/atau Data Elektronik yang disampaikan oleh Kementerian atau Lembaga merujuk pada Peraturan Menteri Komunikasi dan Informatika Nomor 5 Tahun 2020 tentang Penyelenggara Sistem Elektronik Lingkup Privat. Pemerintah Indonesia dapat berkoordinasi dengan pihak Facebook terkait pembahasan:
   - Prosedur untuk penapisan konten negatif
   - *Government Channel* agar komunikasi dengan pemerintah lebih cepat dan efisien
   - Otoritas sebagai *Trusted Flagger* terhadap akun atau kanal dalam layanan Telegram. Melalui Fitur ini laporan dari pemerintah pemerintah harus ditangani sebagai prioritas.
   - Pembuatan *software* internal Telegram untuk memfilter konten, khususnya mengenai terorisme dan radikalisme.

   Mekanisme pengawasannya diatur dengan protokol transparan, di mana narahubung hanya akan memproses permintaan yang telah disetujui oleh badan pengawas. Narahubung juga harus melaporkan aktivitas mereka secara berkala untuk memastikan akuntabilitas.
5. Melaksankan dialog dengan pihak terkait
   Mengingat perusahaan teknologi sering menjadi penyedia layanan yang mengenkripsi data, dialog yang konstruktif antara pemerintah dan perusahaan menjadi langkah penting untuk mencari solusi yang saling menguntungkan dengan mempertimbangkat hak pelindungan data pribadi.

DAFTAR PUSTAKA

Buku

Raj, A. (2022). Analysing the Interplay between End-to-End Encryption & Privacy: Symbiotic Association or a Mere Facilitation?. *RGNUL Fin. & Mercantile L. Rev.*, 99.

Watney, M. (2020, July). Law enforcement access to end-to-end encrypted social media communications. In *Proceedings of the 7th European Conference on Social Media* (pp. 322-329). Reading, UK: AC

Peraturan Perundang-Undangan

Undang-Undang Dasar 1945.

Undang-Undang Nomor 36 Tahun 1999 tentang Telekomunikasi.

Undang-Undang Nomor 39 Tahun 1999 tentang Hak Asasi Manusia

Undang-Undang Nomor 15 tahun 2003 tentang Penetapan Peraturan Pemerintah Pengganti Undang-Undang Nomor 1 Tahun 2002 Tentang Pemberantasan Tindak Pidana Terorisme.

Undang-Undang Nomor 9 Tahun 2013 tentang Pencegahan dan Pemberantasan Tindak Pidana Pendanaan Terorisme.

Undang-Undang Nomor 35 Tahun 2014 tentang Perubahan Atas Undang-

Undang Nomor 23 Tahun 2002 tentang Perlindungan Anak.

Undang-Undang Nomor 19 Tahun 2016 tentang perubahan Undang-Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.

Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik

Peraturan Presiden Nomor 46 Tahun 2010 tentang Badan Nasional Penanggulangan Terorisme.

Peraturan Menteri Komunikasi dan Informatika Republik Indonesia Nomor 19 Tahun 2014 tentang Penanganan Situs Internet Bermuatan Negatif.

Peraturan Menteri Komunikasi dan Informatika Nomor 20 Tahun 2016 tentang Perlindungan Data Pribadi Dalam Sistem Elektronik

Peraturan Menteri Komunikasi dan Informatika Nomor 5 Tahun 2020 tentang Penyelenggara Sistem Elektronik Lingkup Privat.