Nama : Ferza Reyaldi
NIM : 09021281924060
Mata Kuliah : Etika Profesi

Undang-Undang/Regulasi yang Mengatur Ruang Siber di Berbagai Belahan Dunia

A. California - California Consumer Privacy Act (CCPA)

CPPA menciptakan beberapa persyaratan baru untuk perusahaan yang beroperasi di California, termasuk undang-undang IoT (internet of things) pertama yang disahkan di Amerika Serikat. Undang-undang IoT yang baru mengharuskan perusahaan untuk menyematkan "langkah-langkah keamanan siber yang wajar" di perangkat IoT mereka. Sementara undang-undang tersebut memberikan beberapa hal spesifik, para kritikus undang-undang tersebut mengatakan bahwa undang-undang tersebut tidak efektif karena deskripsinya yang tidak jelas dan kurangnya hukuman khusus untuk ketidakpatuhan.

B. New York - Stop Hacks And Improve Electronic Data Security (SHIELD) Act Of 2019

SHIELD Act di New York mengharuskan setiap perusahaan yang menjalankan bisnis di New York memiliki pengamanan administratif, teknis, dan fisik yang wajar untuk informasi pribadi yang dilacak oleh perusahaan. Undang-undang dengan jelas menjabarkan definisi dan persyaratan tentang apa yang merupakan informasi pribadi dan bagaimana perusahaan dapat mematuhi masing-masing dari ketiga bidang ini. Jaksa Agung New York dapat menuntut kasus ketidakpatuhan dengan hukuman hingga $5.000 untuk setiap pelanggaran. Undang-undang tersebut juga mencakup persyaratan bagi perusahaan untuk mengungkapkan pelanggaran keamanan siber kepada mereka yang informasinya diakses.

C. European Union - General Data Protection Regulation (GDPR)

GDPR dibuat untuk membantu melindungi informasi pribadi warga di Uni Eropa. Peraturan tersebut mengharuskan negara-negara anggota untuk memenuhi sertifikasi tertentu, menetapkan otoritas sertifikasi keamanan siber, dan menetapkan hukuman atas pelanggaran atau pelanggaran skema sertifikasi. Terlepas dari apakah perusahaan berlokasi di UE atau tidak, GDPR mengatur semua bisnis yang menggunakan, memproses, atau menyimpan data pribadi dari penduduk UE. Peraturan tersebut juga melampaui sebagian besar undang-undang di Amerika Serikat dalam hal apa yang diklasifikasikan sebagai informasi pribadi yang dilindungi. Ini termasuk data seperti lokasi, alamat IP, data cookie, dan tag RFID selain informasi lain seperti data biometrik, data ras atau etnis, opini politik, atau orientasi seksual. Situs web UE tentang GDPR berfungsi sebagai "Panduan lengkap untuk kepatuhan GDPR" dan telah memposting seluruh rangkaian peraturan bersama dengan daftar periksa dan panduan tentang cara menjadi patuh.

D. Nigeria - Cyber Crime Act 2015

Cyber Crime Act 2015 yang baru ditandatangani menjadi undang-undang pada 15 Mei 2015 menetapkan bahwa, setiap kejahatan atau cedera pada infrastruktur informasi nasional yang kritis, penjualan kartu SIM yang telah didaftarkan sebelumnya, akses yang tidak sah ke sistem komputer, terorisme dunia maya, antara lain akan dihukum berdasarkan undang-undang baru. Tujuan dari Undang-undang tersebut umumnya ditetapkan sebagai berikut:

i. Untuk menyediakan kerangka peraturan dan kelembagaan hukum yang efektif dan terpadu untuk larangan, pencegahan, deteksi, penuntutan, dan hukuman kejahatan dunia maya di Nigeria.

ii. Untuk memastikan perlindungan informasi nasional yang penting tentang infrastruktur.

iii. Mempromosikan keamanan siber dan perlindungan sistem dan jaringan komputer, data komunikasi elektronik dan program komputer, kekayaan intelektual dan hak privasi.

E. Japan - Act on the Protection of Personal Information (APPI)

Di Jepang, APPI menangani masalah perlindungan privasi data. APPI diubah secara drastis pada tahun 2016 dan telah berlaku penuh sejak 30 Mei 2017. Sebelum amandemen, APPI diterapkan hanya untuk pelaku bisnis yang telah menggunakan basis data informasi pribadi yang berisi rincian lebih dari 5.000 orang pada setiap hari di enam bulan terakhir tetapi persyaratan ini dihilangkan dengan amandemen. Berdasarkan amandemen APPI pada tahun 2017, Komisi *Personal Information Protection Commission* (PPC) didirikan sebagai lembaga independen yang tugasnya mencakup melindungi hak dan kepentingan individu sambil mempromosikan penggunaan informasi pribadi yang tepat dan efektif. Sejak amandemen APPI pada tahun 2017, kerangka hukum telah berubah secara drastis dan PPC memiliki tanggung jawab utama untuk kebijakan perlindungan informasi pribadi di Jepang. Sebelum amandemen, per Juli 2015, 39 pedoman untuk 27 sektor terkait perlindungan informasi pribadi telah diterbitkan oleh lembaga pemerintah, termasuk Kementerian Kesehatan, Tenaga Kerja dan Kesejahteraan, Badan Layanan Keuangan Jepang, dan Kementerian Ekonomi, Perdagangan, dan Industri.

F. South Korea - Personal Information Protection Act (PIPA)

PIPA bertindak sebagai undang-undang umum tentang pemrosesan dan perlindungan data pribadi. Singkatnya, “Informasi Pribadi” didefinisikan di bawah PIPA sebagai informasi yang berkaitan dengan seseorang di mana informasi tersebut dapat digunakan – baik dengan sendirinya atau digabungkan dengan informasi lain – untuk mengidentifikasi orang tersebut secara spesifik.

Untuk kategori khusus informasi pengenal pribadi (PII), PIPA juga memiliki definisi untuk (i) “Informasi Sensitif” yang didefinisikan sebagai informasi tentang ideologi, kepercayaan, penerimaan atau pengunduran diri dari serikat pekerja atau partai politik, opini politik , kesehatan, kehidupan seks, bio-data, catatan kriminal, dan informasi pribadi lainnya yang mungkin sangat mengancam privasi subjek data apa pun; dan (ii) “Informasi Unik yang Dapat Diidentifikasi” yang didefinisikan sebagai pengenal unik yang diberikan kepada setiap individu sebagaimana ditentukan oleh keputusan presiden PIPA, seperti

nomor registrasi penduduk, nomor SIM, nomor paspor, dan nomor registrasi orang asing.

Sumber:

1. https://www.ipohub.org/cybersecurity-laws-regulations/
2. https://core.ac.uk/download/pdf/322473244.pdf
3. https://thelawreviews.co.uk/title/the-privacy-data-protection-and-cybersecurity-law-review/japan
4. https://www.legal500.com/guides/chapter/south-korea-data-protection-cyber-security/