CfDS
CENTER FOR DIGITAL SOCIETY

CASE STUDY SERIES #25

LEMAHNYA PERATURAN HUKUM PERLINDUNGAN DATA PRIBADI: STUDI KASUS EQUIFAX DI AMERIKA SERIKAT PADA 2017

Penulis
Ridho Bima Pamungkas

Editor
Dirgayuza Setiawan, M.Sc
Nabeel Khawarizmy Muna

Desain & Tata Letak
Galih Kartika Ade

LEMAHNYA PERATURAN HUKUM PERLINDUNGAN DATA PRIBADI: STUDI KASUS EQUIFAX DI AMERIKA SERIKAT PADA 2017

I. Pendahuluan

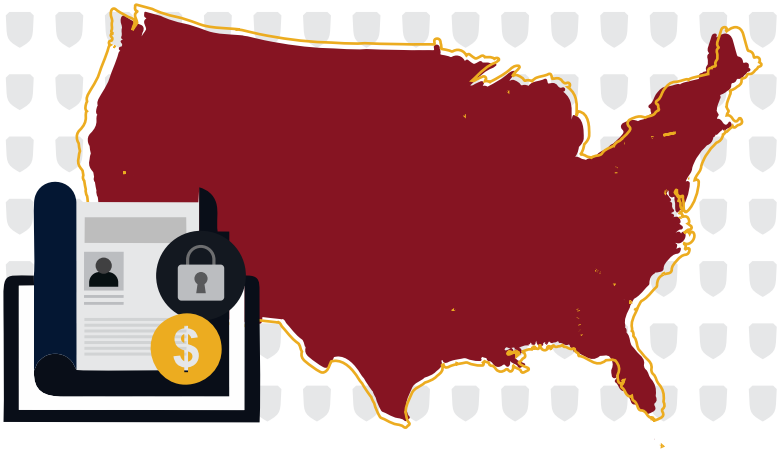
Sebagai perusahaan, pemerintah dan masyarakat diseluruh dunia terus memanfaatkan perkembangan digital yang sedang berlangsung saat ini, salah satu yang paling penting adalah keamanan dan perlindungan data pribadi. Beberapa tahun terakhir, khususnya, telah terjadi peningkatan terhadap kasus pelanggaran privasi para pengguna digital. Kasus seperti ini menyebabkan data pribadi para pengguna digital menjadi tersebar dan sangat beresiko karena data pribadi ini mungkin saja dapat disalahgunakan dalam kejahatan dunia maya seperti pencurian identitas. Pelanggaran data kerap kali terjadi di Amerika Serikat, dimana para peretas menanfaatkan celah dalam undang undang perlindungan data untuk melakukan aksi mereka. Celah tersebut seperti tidak adanya kerangka hukum yang menyeluruh mengenai perlindungan data serta tidak adanya undang-undang yang mengharuskan sebuah perusahaan untuk mengungkapkan pelanggaran yang terjadi sebelum waktu yang telah ditetapkan.

Sejarah mencatat pelanggaran data global terbesar dan terluas di Indonesia terjadi pada Agustus 2013 ketika tiga miliar akun Yahoo diretas. Pada awalnya, akun yang diretas hanya satu milar akun (dimana angka ini sudah sangat banyak), namun setelah penyelidikan dilakukan lebih lanjut, ditemukan pelanggaran berjumlah tiga kali yang telah diprediksi; mencakup semua akun Yahoo yang pernah dibuat.[i] Sebagai upaya untuk mencegah dan mengurangi peristiwa tersebut, pemerintah sudah memberlakukan berbagai peraturan yang membahas memgenai isu isu yang berkaitan dengan privasi dan perlindungan informasi pribadi. Berkenaan dengan hal ini, undang-undang tentang privasi data telah diberlakukan untuk mengatur pengumpulan, penggunaan, penyimpanan dan pengungkapan informasi individu seperti alamat email dan nomor telepon. Pemerintah juga menerapkan aturan khusus mengenai data pribadi yang bersifat lebih sensitif seperti nomor jaminan sosial, nomor kartu kredit dan debit, informasi akun

keuangan, dan kondisi medis. Menghadapi potensi ancaman pelanggaran data, undang-undang semacam itu dinilai penting dalam melindungi hak konsumen dan pengguna internet di Indonesia, dimana setidaknya sekitar 77% masyarakat merasa "sangat atau agak prihatin" atas terjadinya peretasan terhadap akun pribadi.[ii]

Meskipun demikian, penegakan hukum perlindungan data yang telah disebutkan di atas belum menunjukkan hasil yang memuaskan karena pelanggaran data masih terus terjadi dan konsumen tetap terus dirugikan. Pelanggaran terjadi di Amerika Serikat pada tahun 2017 yang mencapai 1.579 kasus pelanggaran, angka ini meningkat 45% dari tahun sebelumnya, meskipun jumlahnya hanya mencakup pelanggaran tetapi secara hukum diwajibkan untuk diserahkan kepada pihak berwenang.[iii] Yang paling penting dari kasus pelanggaran ini adalah yang dialami oleh Equifax, organisasi kredit keuangan di Amerika yang melaporkan bahwa pelanggaran ini mempengaruhi 143 juta individu atau setara dengan hampir setengah dari penduduk di negara itu. Meskipun jumlah ini jauh dari angka 3 miliyar yang terkena dampak pelanggaran data Yahoo empat tahun sebelumnya, tetapi pelanggaran Equifax memberikan dampak yang lebih signifikan karena nilai informasi pribadi yang dicuri.

Tulisan ini akan membahas mengenai sebuah peristiwa dengan menganalisis bagaimana ia berlaku secara signifikan dibanding dengan pelanggaran data sebelumnya yang terjadi di AS, yang kemudian diikuti dengan penjabaran dari dampaknya dan penanganan situasi dibawah hukum federal. Tetapi, sebelum membahas mengenai peristiwa ini, penulis akan memberikan gambaran terlebih dahulu mengenai situasi perlindungan data di AS, termasuk perkembangan sejarah privasi digital di AS serta celah yang dapat diindentifikasi dalam undang-undang perlindngan data pribadi. Dalam tulisan ini akan menyimpulkan beberapa rekomendasi tentang bagaimana celah celah dalam perlindungan data dapat ditutup dan dihindari



II. Perlindungan Data Pribadi di Amerika Serikat

Perlindungan Data Pribadi di Amerika Serikat

Undang-undang perlindungan data muncul pada tahun 1970an ketika database komputerisasi pertama kali digunakan. Penyimpanan informasi massal individu menimbulkan kekhawatiran mengenai potensi penyalahgunaannya oleh negara atau pihak lain yang tidak diinginkan, termasuk tindakan seperti pengawasan dan pengumpulan data yang dikumpulkan, yang akan menjamin pelanggaran terhadap privasi terhadap data individu. Untuk melindungi para pengguna dari potensi pelanggaran privasi, perwakilan legislatif mengusulkan pemerintah untuk menjunjung tinggi perlindungan data pribadi milik warga negara AS. Undang-undang AS pertama yang dibuat untuk mengatasi dampak penyimpanan data pribadi adalah *Fair Credit Reporting Act* (FCRA) pada tahun 1970 yang menjadi dasar penting dalam perlindungan data AS yang lebih komprehensif di masa depan. FCRA membuat beberapa terobosan dalam mengatur perlindungan data dengan mempromosikan "akurasi, keadilan dan privasi informasi" yang disimpan oleh agen pelaporan konsumen (*consumer reporting agencies*). Agensi seperti itu termasuk biro kredit (misalnya, Equifax) dan agen khusus lainnya yang memperjual-belikan data data/informasi pribadi seperti catatan medis dan memeriksa riwayat tulisan. FCRA juga mengatur kondisi dimana pengumpulan data diperbolehkan, serta pentingnya keterbukaan informasi kepada konsumen saat diminta dan pencegahan dari pencurian identitas dan kejahatan potensial lainnya yang berkaitan dengan perlindungan data.[v]

Selanjutnya, Departemen Kesehatan, Pendidikan dan Kesejahteraan AS menerbitkan laporan berjudul Rekaman, Komputer, dan Hak Warga pada tahun 1973. Laporan ini menguraikan secara jelas mengenai efek laten pencatatan dan mekanisme teknis berbasis computer yang diusulkan untuk memberi perlindungan privasi, dan juga menekankan pentingnya hak individu mengenai data pribadi yang mereka miliki.[vi] Selanjutnya, laporan tersebut merekomendasikan penerapan *Code of Fair Information Practices* (FIPs) tertentu yang harus dipahami oleh semua organisasi yang memanfaatkan penyimpanan data pribadi. Kode praktik ni melarang penanganan informasi pribadi yang bersifat "tidak adil" – seperti penggunaan data yang tidak konsisten untuk tujuan selain dari yang telah dikumpulkan diawal – dan menjadikan kasus tersebut tunduk kepada sanksi sah dari pemerintah. Laporan pada tahun 1973 memiliki pengaruh penting dan membuka ruang bagi evolusi instrument hukum di luar AS, yang semuanya berusaha melindungi individu dari kemungkinan pelanggaran data yang berbahaya. Hal ini termasuk pedoman privasi data yang ditegakkan oleh *Organization for Economic Cooperation and Development* (OECD) pada 1980, serta Konvensi Uni Eropa 1981 terhadap Perlindungan Individu berkaitan dengan Pengolahan Otomatis Data Pribadi (t*he European Union's 1981 Convention for the Protection of Individuals with Regard to the Automatic Processing of Personal Data*).

Sementara itu, di Amerika Serikat, *the Code of Fair Information Pratices* diusulkan dalam laporan 1973 yang kemudian diterapkan didalam negerinya didalam *Privacy Act* 1974- tetapi memiliki keterbatasan yang cukup berat. Sedangkan laporan awal mengusulkan sebuah hukum yang komprehensif yang mencakup semua bentuk sistem data pribadi bersifat otomatis, yang dirumuskan dalam Privacy Act yang mempersempit ruang lingkupnya dan hanya mengatur database federal yang dimiliki dan tidak termasuk sektor swasta serta sektor komersial sama sekali. Selanjutnya pengecualian ini terbukti fatal beberapa waktu kemudian dengan biro kredit komersial seperti Equifax gagal memastikan perlindungan sistem data mereka sendiri.

Setelah pemerintah federal membentuk *Privacy Act* 1974, undang-undang terpisah yang masing-masing mencakup tipe tipe tertentu dan beberapa sektor terus dikembangkan. Hal ini termasuk dalam *Family Educational Rights and Privacy* (FERPA) tahun 1974 yang ditujukan kepada pelindungan pendidikan dan *Right to Financial Privacy Act* (RFPA) tahun 1976 yang mengatur perlindungan terhadap informasi perbankan seseorang. Beberapa decade selanjutnya, pemerintah memperluas cakupan perlindungan data yang mencakup beberapa sektor seperti *Electronic Communications Privacy Act* 1986 (ECPA), the *Health Insurance Portability and Accountability* Act 1996 (HIPAA), *the Gramm-Leach-Billey Act of* 1999 (GLBA), dan *the Fair and Credit Transactions Act of* 2003 (FACTA) yang merupakan amandemen dari FCRA 1970.

1970
Fair Credit Reporting Act (FCRA)
Legislasi pertama AS mengatasi dampak yang tidak diingikan dari penyimpanan data pribadi.

1973
Records, Computers and the Right of Citizens
Diterbitkan oleh Departemen Kesehatan, Pendidikan dan Kesejahteraan AS, dan menetapkan kode penting dari praktik informasi yang adil (**Fair Information Practices)**

1974
Privacy Act
Hukum federal pertama yang menerapkan FIP, tetapi dengan batas yang sangat sempit

1974
Family Educational Rights and Privacy (FERPA)
Privasi informasi pendidikan dan catatan pendidikan.

1978
Right to Financial Privacy Act (RFPA)
menetapkan beberapa prosedur yang harus diikuti oleh otoritas pemerintah federal untuk mendapatkan informasi tentang catatan keuangan individu.

1986
Electronic Communications Privacy Act (ECPA)
ketentuan federal diperluas dan direvisi mengenai penyadapan komunikasi secara fisik dan penyadapan elektronik.

1996
Health Insurance Portability & Accountability Act (HIPAA)
mengatur privasi, pengumpulan, dan penyimpanan informasi kesehatan pribadi.

1999
Gramm-Leach-Billey Act (GLBA)
Lembaga keuangan diminta untuk menginformasikan pelanggan ketika informasi pribadi dibagi dengan cabang perusahaan atau afiliasinya, tapi pelanggan hanya bisa 'keluar' ketika data dibagi dengan pihak ketiga

2003
Fair and Accurate Credit Transactions Act (FACTA)
Mengubah FCPA 1970 dengan menambahkan ketentuan yang dirancang untuk meningkatkan akurasi catatan terkait kredit konsumen

Gambar 1 : sejarah hukum perlindungan data pribadi Amerika Serikat

Perbandingan Terhadap Perlindungan Data di Indonesia

Berdasarkan penjelasan sebelumnya, dapat disimpulkan bahwa Amerika Serikat telah melakukan perlindungan data melalui sebuah sarana yang lebih luas, dengan mengimplementasikan undang-undang yang berbeda pada setiap sektor. Walaupun pendekatan ini menawarkan sebuah analisis yang lebih dalam dan tindakan hukum yang lebih spesifik bagi masing masing sektor, ini juga mencegah AS dari kepemilikan hukum perlindungan data tunggal dan menyeluruh yang berlaku secara nasional. Hal ini cukup menyulitkan, dalam artian sebuah sistem *patchwork* hukum federal dan negara bagian yang saat ini digunakan akan mengarah pada kasus-kasus dimana terdapat undang-undang yang saling tumpang tindih atau bahkan bertentangan antara yang satu dengan yang lain.[vii] Beberapa bentuk pengumpulan data mungkin dilarang di California, misalnya yang dikenal dengan memiliki undang-undang paling ketat mengenai perlindungan data dibandingkan negara-negara lain-tetapi tindakan semacam itu mungkin tetap tidak diatur ditempat lain di AS yang akhirnya menyebabkan ketidak-konsistenan penegakan hukum. Selanjutnya, banyak mekanisme perlindungan data yang dikembangkan oleh lembaga pemerintah tidak memiliki kekuatan hukum, karena hanya merupakan bagian dari kerangka pengaturan diri tanpa substansial kekuatan hukum.

Selain itu, lemahnya undang-undang perlindungan data juga membawa beberapa masalah lainnya. Yang pertama adalah tidak adanya definisi hukum yang disepakati secara luas serta konsep 'identifikasi informasi pribadi,' karena dapat dilihat data yang berbeda tergantung pada peraturan yang digunakan.[viii] Hal ini tentu mengarah kepada *cross-sectional* ambiguitas ketika menegakkan hukum perlindungan data yang menyebabkan sulitnya menentukan tingkat pelangaran terhadap peraturan. Masalah kedua adalah bahwa AS tidak memiliki otoritas pemerintah tunggal yang didedikasi untuk mengawasi dan mengelola penegakan hukum terhadap undang-undang perlindungan data. Otoritas regulator yang bertanggung jawab dalam melaksanakan tugas tersebut tergantung pada peraturan khusus. Sebagai contoh, mengenai *Health Insurance Portability and Accountability Act* (HIPAA), penegakannya adalah tanggung jawab *Family Educational Rights and Privacy Act* (FERPA) diawasi oleh Departemen Pendidikan. Sementara memastikan bahwa perlindungan kerahasiaan dalam setiap sektor dikelola oleh pihak dan otoritas yang paling sesuai, pemisahan tanggang jawab menghasilkan kurangnya integrasi dan koordinasi antara lembaga pemerintah yang berbeda. Hal ini terbuka kemungkinan terjadi salah persepsi ketika berhadapan dengan pelanggaran yang bersifat multi-sektor data keamanan. Ketiadaan agen privasi data federal yang terpusat juga menempatkan kesulitan hukum terhadap setiap individu yang mencari akses data yang dilindungi karena alasan yang sah, seperti manajer keamanan di organisasi perawatan kesahatan yang akan melakukan penelitian investigative. Sifat perlindungan

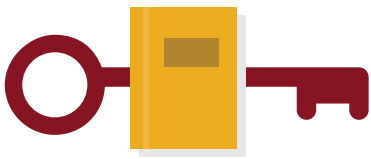
data yang multilayer dan lintas bagian hukum akan menghalangi akses hukum terhadap data yang dilindungi karena setiap individu tidak mempunyai pilihan tetapi harus mengikuti prosedur yang bersifat ekstensif dan berulang sebelum dapat ssdiberikan akses.

Selain itu, undang undang perlindungan data yang ada di AS juga menimbulkan kekhawatiran yang cukup mendasar yaitu tidak adanya hak individu. Misalnya, belum adanya hukum yang menawarkan hak individu untuk mengakses data pribadi yang disimpan oleh suatu organisasi. Akses tersebut hanya diberikan untuk jenis data tertentu, seperti catatan kesehatan di bawah HIPAA atau informasi anak bagi wali sah di bawah COPPA. Disisi lain, *California Shine the Light Law* menawarkan warganya sedikit hak yang berbeda: hukum memberlakukan organisasi pengumpulan data agar lebih transparan, seperti mereka berbagi informasi konsumen mereka dengan pihak ketiga, dimana sebuah individu dapat memilih untuk membatalkan berbagi informasi dengan beberapa pihak ketiga tertentu. Namun, peraturan ini tidak diterapkan di negara lain.

Dalam pendekatan yang lebih spesifik, *Privacy Act* 1974 –salah saatu undang undang yang paling terkenal di AS- membutuhkan revisi dan amandemen. Undang-undang ini mengatur proses data pribadi warga negara AS, khususnya pengumpulan, penggunaan, dan pengungkapan berbagai jenis informasi pribadi. Sedangkan hal lainnya, undang undang ini hanya mengatur data spesifik seperti catatan kesehatan atau informasi pendidikan, dimana *Privacy Act* mencakup jangkauan yang lebih luas- seperti transaksi keuangan, riwayat pekerjaan, riwayat medis, latar belakang pendidikan, dan jenis data lainnya. Namun, Undang-undang hanya berlaku secara hukum bagi database yang dimiliki oleh instansi pemerintah dan tidak termasuk database kepemilikan pribadi yang digunakan secara komersial. Hal ini membuka celah untuk penggunaan informasi pribadi para konsumen oleh organisasi yang berorientasi laba, seperti biro kredit, menjadi sangat rentan dan pelanggaran terhadap privasi data juga semakin rentan.

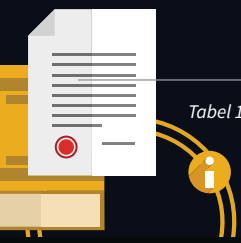
Celah (*loopholes*) yang dalam undang undang dapat diidentifikasi lebih lanjut ketika sistem hukum sektor per-sektor disandingkan dengan Uni Eropa. Berbeda dengan AS, Uni Eropa menerapkan perlindungan kesatuan hukum data serta menerapkan kerangka kerja yang sama di seluruh negara anggotanya, mencegah kemungkinan hukum yang bersifat tumpang tindih antar satu negara anggota dengan anggota negara lain. Di Uni Eropa, hukum seperti ini didasarkan pada konsepsi yang disetujui bahwa perlindungan data merupakan hak fundamental-sebuah pendekatan yang tidak digunakan oleh AS, meskipun undang-undang aturan yang komplek.[x]

Perbedaan yang lebih luas antara kedua sistem hukum dapat dilihat ketika memeriksa prinsip-prinsip perlindungan data pada Uni Eropa, yang mencakup aturan mengenai transfer data kepada pihak ketiga, pengawasan independen dan kekeliruan, persyaratan pemberitahuan setelah terjadinya pelanggaran data, akses dan koreksi hak, peninjauan kembali yang efektif, keamanan data dan perlindungan teknis, serta hal lain sebagainya.[xi] Beberapa prinsip ini, seperti pemberitahuan adanya pelanggaran atau peninjauan yudisial juga disebutkan dalam undang-undang di AS, tetapi sangat terbatas dan hanya berlaku dalam langkah tertentu dan spesifik. Prinsip-prinsip lain, seperti pengawasan independen, tidak terdapat dalam bidang hukum perlindungan data di AS. Sementara AS memang memberikan pengawasan terhadap perlindungan data, AS melakukannya dengan mekanisme pengawasan internal pengumpulan data dari organisasi itu sendiri – alih alih menggunakan badan independen seperti yang dilakukan oleh Uni Eropa.[xii] Selanjutnya, sementara hukum UE ketat mengatur mengenai pembagian data dengan lembga lain dengan mewajibkan untuk memiliki justifikasi yang spesifik, AS tampaknya tidak memiliki peraturan yang serupa dengan yang diterapkan UE.[xiii] Bahkan, data pribadi dianggap sebagai masalah ekonomi ketimbah hak mendasar mengenai pembagian data. Misalnya, FCRA melarang para kreditur untuk mengungkapkan informasi kredit pelanggaran terhadap pihak ketiga tetapi terdapat pengecualian ketika adanya transaksi keuangan antara kreditur dan pelanggan. Hal ini menyiratkan bahwa FCRA menempatkan signifikansi kegiatan ekonomi lebih tinggi daripada perlindungan terhadap privasi data.



Regulasi	Hukum Perlindungan Data UE	Hukum Perlindungan Data AS
Kerangka hukum kesatuan dan menyeluruh	Ya	Tidak, setiap negara memiliki hukum sendiri, diatas hukum federal pada spesifik tertentu
Perlindungan data sebagai hak fundamental	Ya	Tidak
Batas waktu maksimum untuk pemberitahuan pelanggaran	72 jam setelah pencurian data ditemukan (ditetapkan sejak 25 May 2018)	Bervariasi menurut negara. Batas waktu terpendek adalah 45 hari setelah pelanggaran ditemukan, sementara negara hanya membuat pemberitahuan “di waktu yang tepat” agar tidak terjadi ambiguitas.
Pengawasan eksternal perlindungan data	Ya	Tidak
Persyaratan pembenaran spesifik ketika mentransfer data pelanggan ke pihak ketiga	Ya	Tidak, pelanngan hanya diberitahu dan memiliki hak untuk memilih keluar ketika data di salurkan kepada pihak ketiga, tetapi hanya beberapa yang sadar dan menggunakan peran ini.

Tabel 1 : Perbandingan peraturan dan prinsip tentang keamanan data dalam hukum UE dan AS.



Comparison to Indonesian Data Protection Laws

Sementara AS masih tertinggal dari undang-undang Uni Eropa, Indonesia telah membuat kemajuan mengenai peningkatan perlindungan data bagi warga negaranya-meskipun sebelumnya menerapkan pendekatan patchwork yang sama dimana hukum mengatur masalah yang bervariasi. Pada tahun 2016, Menteri Komunikasi dan Informatika mengeluarkan peraturan No. 20 mengenai perlindungan data pribadi (berjudul Perlindungan Data Peraturan). Ini merupakan peraturan pelaksanaan dari Informasi Elektronika sebelumnya dan Hukum Transaksi (UU EIT) tahun 2008, dimana sekarang lebih melindungi pengunaan, penyimpanan, dan penyebaran data pribadi dalam sistem elektronik. Selain itu, peraturan tersebut juga menetapkan persyaratan pada persetujuan subjek data, yang memungkinkan untuk lebih banyak kontrol individu atas bagaimana data mereka diproses dan ditransfer.

Dalam beberapa aspek tertentu, peraturan baru mengenai undang-undang perlindungan yang ditetapkan oleh Indonesia lebih mendahului AS, misalnya dalam kasus pelanggaran data, sekarang hukum membutuhkan operator sistem elektronik untuk member tahu pengguna data yang terkena pelanggaran setelah 14 hari pelanggaran ditemukan. Transmisi, diseminasi, dan aksesiibilitas data pribadi juga secara eksklusif terbatas sejauh yang diungkapkan kepada dan yang diberikan persetujuan oleh pemilik data, yang berarti bahwa perusahaan tidak dapat dengan bebas berbagi data seperti yang terjadi di AS. Secara keseluruhan, Peraturan Perlindungan Data adalah tonggak penting dalam memastikan privasi dan perlindungan informasi warga negara di Indonesia, meskipun memang belum sekomprehensif regulasi di Uni Eropa.

III. Studi Kasus: Peretasan Equifax

Signifikansi Kasus Equifax

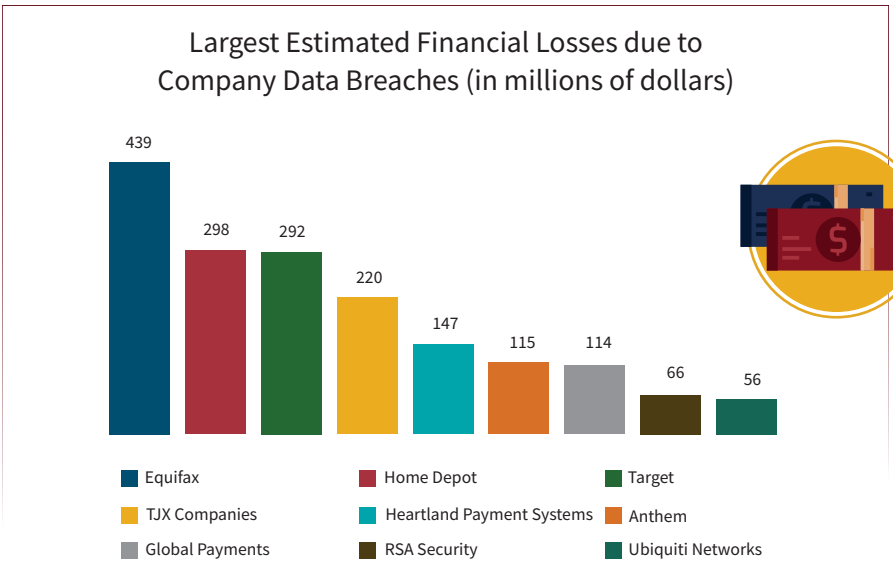
Pada September 2017, Equifax-Organisasi pelaporan kredit utama di AS- secara terbuka mengungkapkan pelanggaran data yang terjadi selama berbulan-bulan sebelumnya antara antara Mei dan Juli. Serangan ini diklaim telah mempengaruhi 145.5 juta orang dengan meretas secara illegal dengan mengakses nama, nomor jaminan sosial (*Social Security Number* – SSN), tanggal lahir, alamat dan 209.000 nomor kartu kredit, bersamaan dengan berbagai dokumen lain serta informasi pribadi konsumen.[xiv] Menurut Equifax, serangan ini mengeksploitasi kerangka web Apache Struts. Apache sudah dirilis untuk menyelesaikan masalah ini pada Maret 2017, tetapi Equifax gagal menerapkan pembaruan sebelum serangan terjadi pada pertengahan Mei.[xv]

Perusahaan	Pengungkapan kasus pencurian data	Jumlah yang terdampak	Data yang terdampak
Yahoo Inc	Desember 2016	3,000,000,000	Alamat email dan password
MySpace	Mei 2016	427,000,000	Akun username dan Password
LinkedIn Corp	Juni 2012	167,000,000	Alamat email dan password
Equifax Inc	September 2017	145,500,000	Alamat fisik, rekaman kredit, nomor kartu kredit
eBay Inc	Mei 2014	145,000,000	Nomor keamanan sosial
Heartland Payment	Januari 2009	130,000,000	Alamat fisik, alamat email, password, nomor telepon
Target Corp	Desember 2013	110,000,000	Nomor kartu kredit
Home Depot Inc	September 2014	108,000,000	Akun kredit dan debit, informasi kredit dan informasi akun kartu debit

Table 2 : Perbandingan dari pelanggaran data terbesar di AS berdasarkan jumlah catatan atau akun yang terpengaruh.[xvi]

Secara kuantitatif, kasus pelanggaran Equifax bukan yang terbesar di sepanjang sejarah AS. Meskipun sudah mempengaruhi hampir setengah dari total penduduk AS, jumlah ini masih jauh dari beberapa pelanggaran penting lainnya seperti Adobe (152 juta) yang terjadi pada tahun 2013.[xvii] Pelanggaran ini juga termasuk pelanggaran kecil didunia, pada tahun 2013 Yahoo, telah terjadi pelanggaran terhadap 3 miliar orang di seluruh dunia. Meskipun demikian, kualitas dan sensitivitas tinggi dari data yang dicuri menjadikan Equifax sebagai serangan yang paling merusak dan secara finansial merugikan dalam sejarah, dan ini merupakan pelanggaran terbesar yang melibatkan layanan jaminan sosial dan nomor kartu kredit. Sedangkan pelanggaran Yahoo hanya melanggar alamat email, kata sandi dan jawaban keamanan yang diretas, sedangkan pelanggaran Equifax memberikan informasi yang jauh lebih berharga bagi para peretas. Kredensial pribadi seperti SSN dan catatan kartu kredit memegang nilai yang cukup besar saat diperjualbelikan melalui web gelap karena dapat digunakan untuk kejahatan dunia maya seperti penipuan identitas dan serangan rekayasa sosial. Dengan jenis informasi ini, penjahat tidak akan mengalami kesulitan untuk mengklaim bahwasannya ia adalah konsumen bank, asuransi perusahaan atau bisnis keuangan lainnya, dan mereka dapat dengan mudah mengajukan pinjaman palsu serta membuka akun kartu kredit yang baru pula.

Untuk lebih menekankan pentingnya masalah ini, Equifax adalah salah satu lembaga pelaporan kredit terpercaya di AS, menjadi satu dari tiga agensi “tiga besar” bersamaan dengan TransUnion dan Experian. [xviii] Administrasi Jaminan Sosial AS, yang menangani pelepasan semua SSN, juga sebelumnya menggunakan layan Equfax untuk memverifikasi seseorang selama proses membuat akun jaminan sosial yang baru.[xix] Kegagalan Equifax dalam mengamankan databasenya tidak sejalan dengan reputasi dan tanggung jawabnya untuk melindungi data pribadi dan peringkat kredit dengan benar.



Gambar 2 : Perkiraan kerugian finansial dari pelanggaran Equifax dibandingkan dengan pelanggaran data sebelumnya di AS.

Selain itu, pelanggaran Equifax menyoroti permasalahan identitas diri di AS. Nomor jaminan sosial pada awalnya didirikan pada 1930'an untuk memantau kontribusi warga negara AS terhadap 'program jaminan sosial' yang berarti mereka tidak pernah dimaksudkan untuk bertindak sebagai identitas pribadi. Namun industri swasta, dan agen komersial telah memilih untuk menggunakan SSN sebagai pengidentifikasi individual yang menyebabkan penggunaan SSN secara luas yang sama sekali tidak terkait dengan fungsi yang diinginkan pada awalnya.[xxii] Implementasi SSN sebagai bentuk identitas formal bagi warga negara AS menimbulkan beberapa masalah. Pertama, menjaga SSN sebagai informasi pribadi merupakan tugas yang sulit di era digital, dengan bank dan institusi keuangan yang membagi informasi konsumen dengan agensi seperti biro kredit. Kedua, tidak seperti kredensial pribadi seperti nomor kartu kredit atau nomor PIN bank, SSN tidak dapat diubah dengan mudah dan membutuhkan proses yang panjang yang hanya dapat di 'kasus yang ektrim dari indentifikasi pencurian atau penyalahgunaan'.[xxiii] Merubah SSN juga tidak menjamin keamanan identitas pribadi; masih banyak organisasi dan institusi sudah memiliki nomor asli dari data-data yang masih dapat digunakan sebagai kejahatan, dan SSN baru yang diterima oleh konsumen setelah permintaan perubahan masih terikat dengan nomor lama mereka. Karena itu, dalam kasus pencurian data yang luas yang membahayakan jutaan SSN, konsekuensi penuh masih dapat

merusak dan masih akan dirasakan beberapa tahun kedepan. Pelanggaran Equifax juga disebabkan dari penggunaan SSN sebagai mekanisme identifikasi personal dan resiko jangkauan yang jauh implementasi yang baru, inovasi mekanisme indentifikasi yang akan memberikan perlindungan lebih baik bagi warga negaranya.

Respons dan Tindakan

Dalam kurang dari satu minggu sejak pemberitahuan publik terjadinya pelanggaran, lebih dari 30 gugatan hukum sudah diajukan untuk melawan Equifax dengan gugatan hukum terbesar bertujuan untuk mengklaim biaya hingga $70 juta.[xxiv] Equifax kemudian mencoba menenangkan konsumen dengan memberikan gratis biaya pemantauan selama satu tahun bagi setiap orang yang terdaftar dikategori tersebut. Namun, hal ini hanya memperburuk situasi karena ditemukan bahwa pendaftaran layanan secara otomatis mencegah individu untuk berpartisipasi dalam klaim hukum terhadap Equifax dimasa depan. Layanan pemantauan ini juga mengharuskan setiap individu untuk membayar secara penuh setelah periode gratis berakhir, yang pada akhirnya memberikan kesan kepada publik bahwa Equifax memanfaatkan gejolak ini untuk meningkatkan keuntungan ekonomi.

Agen pelaporan kredit juga menerima kritik yang sangat berat karena tidak dapat mengatasi pelanggaran dengan cepat dimana mereka mengumumkannya enam minggu setelah pelanggaran ditemukan oleh pihak agensi. Hal ini berarti konsumen dan data individu mungkin saja dalam keadaan berbahaya dan harus mengambil langkah pengamanan dengan segera. Secepatnya setelah pemberitahuan publik, konsumen menyarankan untuk melakukan pembekuan terhadap riwayat kredit mereka, tetapi masih ada kemungkinan bahwa peretas telah memperjualbelikan atau disalahgunakan seperti mencuri data untuk perbuatan kriminal sejak enam minggu yang lalu- hal ini kemudian menyulitkan korban yang ingin mengambil tindakan. Kritik juga ditujukan kepada beberapa pelaksana dan stakeholder yang diketahui menjual data mereka beberapa hari setelah pihak agensi mengetahui pencurian berskala besar.[xxv]

Serangan terhadap Equifax dan Celah pada Hukum terkait data pribadi di AS

Pelanggaran Equifax menggarisbawahi kelemahan terhadap hukum perlindungan data AS yang didirikan berdasarkan sektor persektor. Sementara legilasi kebanyakan mencakup peraturan mengenai perlindungan informasi keuangan dan kesehatan, AS masih belum memiliki undang-undang yang komprehensif yang bertujuan untuk mencegah pelanggaran data seperti angka kerahasiaan sosial – signifikansi yang telah diuraikan dalam paragraph sebelumnya. Faktanya, tidak ada hukum di AS yang mencegah perusahaan dan pembisnis dari pertanyaan nomor keamanan sosial; maksudnya adalah hal ini sudah berisiko disebarkan tanpa adanya pelanggaran data. AS juga memiliki ketimpangan hukum yang menjamin hak individu dari pelanggaran data, seperti regulasi mengenai jumlah uang total yang berhak di klaim oleh gugatam hukum.

Bahkan, Equifax menunda mengumumkan pelanggaran yang terjadi karena hukum patchwork di negara terhadap pemberitahuan. Sebagai perbandingan, Uni Eropa akan berlaku sebuah Peraturan Regulasi Umum pada Mei 2018 yang membutuhkan perusahaan untuk memberitahukan terhadap negara kurang dari 72 jam untuk menelusuri pelanggaran. Ini akan diterapkan kepada seluruh perusahaan berlaku bagi negara anggota Uni Eropa. Sebaliknya, tidak ada undang-undang di level federal yang memaksa perusahaan dan agensi untuk melaporkan pelanggaran data dengan cepat. Perbedaan hukum yang bervariasi dari setaip negara, ketika negara lain membutuhkan perusahaan untuk memberitahukan pelanggaran dalam 45 hari setelah ditemukan, ketika negara lain tetap ambigu bahkan tidak diatur. Dalam kasus Equifax, negara asli (Georgia) tidak memiliiki hukum yang spesifik yang memaksa perusahaan untuk membuka pencurian data dengan total waktu, dimana membiarkan agensi untuk menunda pembukaan data kepada publik hingga enam minggu. Juga, perbandingan selanjutnya dengan Uni Eropa menunjukkan tidak seperti negara negara Eropa, hukum AS tidak menggangap perlindungan data sebagai hak dasar bagi warga negaranya. Pada waktu lalu menyebabkan kurangnya urgensi bagi pembuat hukum untuk melakukan revisi celah-celah dalam regulasi yang telah ada.

Implikasi Hukum

Dampak positifnya, meluasnya pemberitaan atas pelanggaran Equifax mengembangkan kesadaran yang tinggi antara publik dan pemerintah terhadap resiko pencurian data. Terjadinya diskusi yang dipicu antara perwakilan legislative mengenai kemungkin amandemen terhadap hukum perlindungan data atau perumusahn dari undang-undang baru. Tiga bulan setelah Equifax membuka pelanggaran data, senator Demokrat dari Florida, *Connecticut* dan *Wisconsin* memulai usaha untuk melewati hukum yang membutuhkan perusahaan dan agensi untuk 'memberitahu kepada konsumen akan

bangkitnya pencurian data'.[xxvi] *Data Security and Breach Notification Act*, RUU akan berusaha untuk memberlakukan mekanisme pemberitahuan pelanggaran nasional di negara hukum *patchwork*.[xxvii] RUU juga memaksa sanksi legal melawan siapa saja dengan sengaja melakukan pencurian data, dengan ancaman lima tahun penjara. Demikian juga, senator mengusulkan *data breach prevention and compensation act*, membebankan denda wajib $100 bagi setiap individu yang memiliki bagian data personal sejak pencurian data.[xxviii] Tambahan denda $50 bagi setiap tambahan data baru yang terdampak dengan denda lebih lanjut jika perusahaan dengan sengaja melakukan penundaan dalam mengumumkan pelanggaran. Juga, setengah dari total hukum denda akan diberikan kembali bagi individu yang terkena dampaknya, dan menyediakan mekanisme kompensasi yang melakukan mitigasi kerugian finansial. Berlakunya peraturan ini akan memaksa Equifax untuk membayar hingga $1.5 milyar mengingat serangan baru yang mempengaruhi 143 orang. Namun, sampai saat ini, tak satu pun dari undang-undang itu lolos, dan diprediksikan warga negara AS akan tetap tidak terlindungi dan rentan terhadap pelanggaran data serupa di masa mendatang.

IV. Kesimpulan

Sistem *patchwork* dan implementasi mekanisme *sector-by-sector* dengan hukum proteksi data AS yang membuka kesempatan bagi pencurian data yang berbahaya mengakibatkan jutaan kerugian; tidak termasuk pelanggaran baru-baru ini yang dialami oleh Equifax, yang memanfaatkan undang-undang negara yang kontradiktif untuk mengungkapkan pelanggaran kepada publik dalam kurun waktu enam minggu. Meskipun demikian, upaya pemerintah untuk menetapkan undang-undang perlindungan data yang lebih baik sudah menunjukkan bahwa pemerintah mengakui kekurangan tersebut dan telah ada usaha untuk mendorong peningkatan kesadaran pemerintah. AS harus terus mengupayakan diberlakukannya kerangka kerja perlindungan data yang menyeluruh yang akan menyelesaaikan perbedaan yang ada di antara undang-undang federal dan negara bagian, yang akan menempatkan AS dalam tingkat perlindungan data yang sama dengan Uni Eropa. Setiap undang-undang perlindungan data di masa depan juga harus dapat diperbaiki dengan berbasis sektor sektor saaat ini yang memberlakukan data tertentu dengan mekanisme yang berbeda berdasarkan sektor asalnya. Selain itu, pemerintah juga harus mampu melakukan pencegahan terhadap pelanggaran tersebut melalui peningkatan keamanan bagi database yang dimiliki oleh komersial dan federal agar tidak hanya dengan cepat menangani pelanggaran data, tetapi juga mendorong pencegahan pelanggaran tersebut melalui peningkatan dan kemananan bagi keduanya.

References

[i]Yahoo 2013 data breach hit all three billion accounts.' BBC (online). Available at: http://www.bbc.com/news/business-41493494. 2017.

[ii]Global Commission on Internet Governance. Toward a Social Compact for Digital Privacy and Security. Centre for International

[iii]Governance Innovation. 2015.

[iv]Schwartz, M.J. 'U.S. Data Breaches Hit All-Time High'. Bank Info Security (online). Available at: https://www.bankinfosecurity.com/us-data-breaches-hit-all-time-high-a-10622. 2018.

[v]Fair Credit Reporting Act. US Federal Government. 1970.

[vi]Fair Credit Reporting Act, 1970.

[vii]Records, Computers and the Rights of Citizens. Report of the Secretary's Advisory Committee on Automated Personal Data Systems. 1973.

[viii]Jolly, I. 'Data protection in the United States: overview'. Thomson Reuters Practical Law (online). Available at: https://uk.practicallaw.thomsonreuters.com/6-502-0467?transitionType=Default&contextData=(sc.Default)&firstPage=true&bhcp=1.

[ix] Sotto, Lisa J. & Simpson, Aaron P. 'United States'. Data Protection & Privacy in 26 Jurisdictions Worldwide. Getting the Deal Through. 2013.

[x]Sotto & Simpson, 2013.

[xi]Boem, Franziska. A comparison between US and EU data protection legislation for law enforcement purposes. Directorate

[xii]General for Internal Policies, European Union. 2015.

[xiii]Boem, 2015.

[xiv]Boem, 2015.

[xv]Boem, 2015.

[xvi]Newcomb, A. 'Massive Equifax Data Breach Could Affect Half of the Population.' NBC News (online). Available at: https://www.nbcnews.com/tech/security/massive-equifax-data-breach-could-impact-half-u-s-population-n799686

[xvii]Pollack, D. 'Equifax Data Breach Highlights Consumer Privacy Risks'. ID Experts (online). Available at: https://www2.idexpertscorp.com/knowledge-center/single/equifax-data-breach-highlights-consumer-privacy-risks http://www.auditanalytics.com/blog/ranking-the-equifax-data-breach-updated/

[xviii]Global Commission on Internet Governance, 2015.

[xix]Making Sense of the Equifax Breach and What You Should Do Now. John G. Ullman & Associates, Inc. 2017.

[xx]Newman, L. H. 'The Equifax Breach Exposes America's Identity Crisis'. Wired (online). Available at: https://www.wired.com/story/the-equifax-breach-exposes-americas-identity-crisis/. 2017.

[xxi]https://www.reuters.com/article/us-equifax-cyber/equifax-breach-could-be-most-costly-in-corporate-history-idUSKCN1GE257

[xxii]Newman, 2017.

[xxiii]Newman, 2017.

[xxiv]Schwartz, M.J. 'Equifax Faces Mounting Anger, $70 Billion Lawsuit',. Data Breach Today (online). Available at: https://www.databreachtoday.com/equifax-faces-mounting-anger-70-billion-lawsuit-a-10282

[xxv]Schwartz, 'Equifax Faces Mounting Anger, $70 Billion Lawsuit'.

[xxvi]Cameron, D. 'New Senate Bill Includes Jail Time for Executives Who Conceal Data Breaches'. Gizmodo (online). Available at: https://gizmodo.com/new-senate-bill-includes-jail-time-for-executives-who-c-1820897003. 2017.

[xxvii]Cameron, 2017.

[xxviii]Muncaster, P. 'Equifax Would Have Paid $1.5bn Under New US Breach Laws.' Infosecurity (online). Available at: https://www.infosecurity-magazine.com/news/equifax-15bn-under-new-us-breach//

Center for Digital Society

Faculty of Social and Political Sciences
Universitas Gadjah Mada
Room BC 201-202, BC Building 2nd Floor,
Jalan Socio Yustisia 1
Bulaksumur, Yogyakarta, 55281, Indonesia

Phone : (0274) 563362, Ext. 116
Email : cfds.fisipol@ugm.ac.id
Website : cfds.fisipol.ugm.ac.id

facebook.com/cfdsugm
cfds.fisipol.ugm.ac.id
cfds_ugm
@cfds_ugm
@cfds_ugm
CfDS UGM