

**KEAMANAN DATA PRIBADI E-COMMERCE LOGISTICS (Bagian 2)**

Oleh: Dr. Dhanang Widijawan, S.H., M.H.

Senior Consultant

Supply Chain Indonesia

**Ekosistem Perniagaan Elektronik**

Sehubungan hal tersebut, dalam lingkup nasional, keamanan siber merupakan salah satu dari tujuh isu utama dalam Paket Kebijakan Ekonomi XIV (PKE XIV 2016). PKE XIV 2016 memberikan posisi penting keamanan siber untuk mencapai kemajuan industri *e-commerce* Indonesia. Elemen keamanan siber diharapkan berperan dalam mempercepat realisasi peta jalan sistem perdagangan nasional berbasis elektronik. Sekaligus, membangun pranata dan efisiensi ekosistem perniagaan.

Efisiensi ekosistem perniagaan nasional yang bertumpu pada keamanan siber diharapkan menjadi stimulus bagi akselerasi pencapaian posisi Indonesia sebagai negara ekonomi digital terbesar di Asia Tenggara pada 2020. Secara simultan, dorongan pencapaian ini akan semakin didukung oleh kreasi, inovasi, dan invensi kegiatan ekonomi baru berbasis kepastian hukum. Hal ini didasarkan pada kenyataan, bahwa, di Indonesia terdapat 90-an juta pengguna internet dan 70-an juta pengguna *smartphone*.

Pada satu sisi, signifikansi pengguna internet dan *smartphone* merupakan potensi aset bagi terciptanya 1.000 *technopreneurs*. Kalkulasi asumsi ini didasarkan pada valuasi bisnis USD 10 miliar, yang, pada 2020, diprediksi akan mencapai nilai *e-commerce* USD 130 miliar (IDC, *En-Route to Digital Economy: What's Next for e-Commerce in Indonesia*, 21/11/2016).

Namun demikian, pada sisi lain, kecenderungan peningkatan jumlah *user* (internet dan *smartphone*), berbanding lurus pula dengan semakin meluasnya kekhawatiran terhadap keberadaan data pribadi karena tidak terkendalinya keamanan siber dalam transaksi elektronik akibat ketidakandalan penyelenggaraan sistem elektronik.

**Kendala Keamanan Siber**

Kemenkominfo dalam “Peta Jalan E-Commerce Indonesia, 2016”, menyebutkan tiga kendala terkait dengan keamanan siber, yaitu :

1. kurangnya kesadaran konsumen atas keamanan dan kejahatan siber
2. kurangnya partisipasi pedagang pada penerapan prinsip kehati-hatian, keamanan, integrasi sistem teknologi informasi, dan pengamanan kontrol atas kegiatan transaksi elektronik
3. kurangnya prosedur operasi standar yang memenuhi prinsip keamanan data pengguna dan transaksi elektronik

## ARTIKEL

Kesadaran konsumen dan kewajiban pelaku usaha terkait pemenuhan prosedur operasi standar dalam rangka keamanan siber, pada dasarnya merujuk pada syarat minimum penyelenggaraan sistem elektronik (UU ITE No. 11/2008 Pasal 16 Ayat (1)), yang mencakup:

1. dapat menampilkan kembali informasi/dokumen elektronik secara utuh sesuai dengan masa retensi yang ditetapkan peraturan perundang-undangan.
2. dapat melindungi ketersediaan, keutuhan, keotentikan, kerahasiaan, dan keteraksesan informasi elektronik.
3. dapat beroperasi sesuai dengan prosedur/petunjuk penyelenggaraan sistem elektronik.
4. dilengkapi dengan prosedur/petunjuk yang diumumkan dengan bahasa, informasi, atau simbol yang dapat dipahami.
5. memiliki mekanisme yang berkelanjutan untuk menjaga kebaruan, kejelasan, dan keberanggungjawaban prosedur/petunjuk

Kewajiban untuk memenuhi syarat minimum penyelenggaraan sistem elektronik bertujuan untuk mereduksi potensi risiko kerugian yang timbul. Sifat kerugian dapat bersifat material, immaterial, masif, dan meluas, seperti: kepentingan ekonomi dan politik, data strategis, harkat/martabat bangsa, pertahanan/keamanan negara, kedaulatan negara, warga negara, dan badan hukum (korporasi).

### **Penguatan Keamanan Siber**

Kepentingan nasional terhadap keamanan siber diatur dalam Perpres No. 53/2017 Tentang Badan Siber Dan Sandi Negara (BSSN). Penguatan keamanan siber bertujuan untuk mewujudkan peningkatan pertumbuhan ekonomi dan keamanan nasional. Penguatan dilakukan dengan cara memanfaatkan, mengembangkan, dan mengonsolidasikan seluruh *resource* internal dan eksternal BSSN.

Implementasi penguatan keamanan siber BSSN dijabarkan melalui empat aktivitas pokok, yaitu: (1) identifikasi dan deteksi, (2) proteksi, (3) penanggulangan dan pemulihan, dan (4) pemantauan dan pengendalian.

Keempat aktivitas pokok tersebut diselenggarakan melalui penyusunan, pelaksanaan, pemantauan, dan evaluasi, terkait dengan kebijakan teknis di bidang identifikasi, deteksi, proteksi, penanggulangan, pemulihan, pemantauan, evaluasi, pengendalian proteksi *e-commerce*, persandian, penapisan, diplomasi siber, pusat manajemen krisis siber, pusat kontak siber, sentra informasi, dukungan mitigasi, pemulihan penanggulangan kerentanan, insiden dan/atau serangan siber, dan kerjasama nasional, regional, dan internasional.

Dengan demikian, kebijakan penguatan keamanan siber di bidang *e-commerce logistics* yang disusun, dilaksanakan, dipantau, dan dievaluasi, berbasis BSSN, sudah saatnya dikendalikan dalam

## ARTIKEL

kerangka regulasi tata kelola sistem teknologi informasi dan komunikasi (TIK) nasional secara komprehensif dan implementatif.

### Kendali Regulasi TIK

Sejalan dengan tugas dan fungsi BSSN, secara nasional, kerangka regulasi tata kelola sistem TIK membutuhkan struktur dan mekanisme kendali (formal/non-formal) organisasi yang mengikat *stakeholder*, secara *sustain*, guna tercapainya efisiensi dan efektivitas tujuan bersama.

Menurut Jogiyanto dan Willy Abdillah (2011), terdapat empat kendali dan regulasi sistem tata kelola TI secara internasional, meliputi: (1) COBIT, (2) ITIL, (3) ISO 17799, dan (4) Sarbanes-Oxley (SOX).

COBIT (*Control Objectives for Information and related Technology*) memiliki 34 proses tingkat tinggi, mencakup 210 tujuan pengendalian dalam empat kategori: (1) perencanaan dan organisasi, akuisisi dan implementasi, *deliver* dan *support*, (4) dan monitoring dan evaluasi. Manfaat COBIT, bagi: (1) pengguna, adanya jaminan kendali, keamanan, dan proses tata kelola; (2) auditor, membantu identifikasi isu-isu kendali TI dalam infrastruktur perusahaan.

Sedangkan ISO 17799, digunakan khusus untuk keamanan informasi. ISO 17799 terbagi dalam 10 seksi dengan 36 *objectives* berikut masing-masing *sub-objective*. Sinergitas COBIT dan ISO menjadi model utama keunggulan keamanan TI secara rinci dan operasional.

Selanjutnya, ITIL (*Information Technology Infrastructure Library*) merupakan rincian deskriptif praktikal penting TI dan menyediakan daftar komprehensif tugas dan prosedur yang dapat disesuaikan. ITIL berbasis proses pengendalian dan pengelolaan operasi (siklus PDCA, *Plan-Do-Check-Act*). Dalam perkembangannya, dirilis ITIL v2 dan v3. ITIL v2 mengkonsolidasi 8 logis “set” yang menyelaraskan berbagai aspek berbeda manajemen IT, aplikasi, dan layanan. Sedangkan ITIL v3 mencakup *service-service* terkait dengan *strategy, design, transition, operation, dan continual improvement*.

Dan Sarbanes-Oxley (SOX) berisi 11 judul berikut beberapa bagian yang menggambarkan mandat spesifik dan persyaratan laporan keuangan. SOX mendorong peningkatan tanggung jawab CEO, CFO, anggota komite dan pengarah sistem tata kelola TI. Juga, meningkatkan mekanisme *internal checks & balances*, akuntabilitas korporat, menjaga struktur kendali internal, dan penilaian kinerja secara periodik.

### Sistem Perdagangan Elektronik

Pilihan tata kelola sistem kendali dan regulasi TIK nasional, seharusnya terintegrasi dengan regulasi-regulasi Sislognas, MP3EI, BSSN, dan terkait lainnya. Integrasi regulasi akan mendorong kemajuan industri *e-commerce logistics*, yang *resource*-nya terdapat di berbagai kementerian/ lembaga (perekonomian, BUMN, kominfo, perhubungan, perdagangan, keuangan, perindustrian, kemaritiman, bulog, dan terkait lainnya), baik pada tingkat pemerintah pusat maupun pemerintah

## ARTIKEL

daerah. Integrasi regulasi ini akan mendorong peningkatan daya saing logistik nasional dalam parameter LPI (*Logistics Performance Index*).

Integrasi kebijakan keamanan siber nasional terkait perlindungan data pribadi merupakan langkah konkrit mewujudkan pranata dan efisiensi ekosistem perniagaan. Langkah ini menjadi salah fokus dalam peta jalan sistem perdagangan elektronik nasional (*industri e-commerce logistics*) dalam Paket Kebijakan Ekonomi XIV 2016.

21 Agustus 2017

*\*Isi artikel merupakan pemikiran penulisan/atau sepenuhnya menjadi tanggung jawab penulis, serta tidak selalu mencerminkan pemikiran atau pandangan resmi Supply Chain Indonesia.*