Bankers Update

BULETIN
IKATAN
BANKIR
INDONESIA
Vol. 21/2018

TRANSFORMASI DIGITAL: RISIKO DAN MITIGASINYA

DITERBITKAN OLEH:
IBI
Ikatan Bankir Indonesia

TRANSFORMASI DIGITAL: RISIKO DAN MITIGASINYA

Lion Air JT160 dan Malaysian Airlines MH370, Jamal Khassogi dan Lady Diana, apa hal penting yang membedakannya? Data. *Blackbox* pesawat Lion Air JT160 ditemukan dalam waktu 3 hari, sedangkan Malaysian Airlines MH370 sudah lebih dari 4 tahun tidak jelas di mana, hal tersebut karena data posisi terakhir JT160 jelas namun posisi terakhir MH370 tidak jelas. Jamal Khassogi diketahui dibunuh dalam tempo 1 hari dan penyebab kematian Lady Diana sampai sekarang masih misteri. Pembunuhan Khassogi di Turki diketahui segera karena didapatkan data dari CCTV, sedangkan dalam kasus Lady Diana tidak jelas apa yang menyebabkan mobilnya kecelakaan begitu fatal di terowongan di Paris 21 tahun yang lalu. Ternyata konsekuensi dari adanya data atau tidak, bisa membuat dua hal yang mirip mempunyai konsekuensi yang berbeda jauh.

DATA SEBAGAI JIWA DARI TRANSFORMASI DIGITAL

Data inilah yang menjadi jiwa dari Transformasi *Digital* yang membedakannya dengan masa sebelum transformasi *digital*. Data dulu disimpan sebagai tulisan di buku, atau *print out* di kertas, yang memerlukan orang untuk membacanya, mengolahnya menjadi informasi, mengkomunikasikannya dengan orang lain, dan kemudian mengambil kesimpulan, misalkan apakah saldo orang tersebut cukup untuk uang kontan yang akan ditariknya. Dengan transformasi *digital*, data dapat dikumpulkan, diolah, dikomunikasikan, kemudian kesimpulan atau keputusan dapat diambil, tanpa perlu intervensi manusia. Di samping proses yang bertransformasi, dua dimensi di mana proses itu terjadi yaitu ruang dan waktu juga mengalami perbedaan yang besar dalam transformasi *digital*. Data yang dulu cakupannya lokal kini menjadi *global*, transmisi data yang dulu lambat kini terjadi dalam waktu yang cepat hitungan milidetik. Dulu transfer internasional memerlukan waktu kliring minimal 3 hari, kini bisa terjadi *instant*.

Karena data merupakan jiwa dari transformasi *digital*, maka perbedaan risiko dan mitigasinya dalam transformasi digital adalah berpusat pada data ini. Tidak heran maka peraturan otoritas keuangan mewajibkan data center (DC) maupun *data recovery center (DRC)* data nasabah bank di Indonesia harus berada di teritori Indonesia, sebagai bagian dari manajemen risiko.

TRANSFORMASI *DIGITAL* BAGAIKAN *BLACK HOLE* BAGI *DATA*

Industri bank merupakan industri yang highly regulated karena dianggap aspek finansial merupakan aspek yang sangat vital dalam bermasyarakat, oleh karenanya ada berbagai macam peraturan mengenai penggunaan data nasabah oleh institusi *(bank).* Namun ternyata transformasi *digital* menghadirkan hal yang tidak pernah dipikirkan sebelumnya oleh regulator, yaitu aspek pengumpulan data nasabah yang merupakan sisi i*nput* sebelum menjadi sisi *output* yaitu penggunaan data nasabah. Hal itu terjadi karena sebelum transformasi *digital*, data merupakan hal yang diberikan oleh nasabah secara sadar dan rela, biasanya data identitas diri, yang kemudian disimpan oleh institusi *(bank).* Namun dengan transformasi *digital*, banyak data yang bisa diambil oleh institusi tanpa kesadaran dan kerelaan dari pemilik *data*, yang bisa diolah menjadi informasi yang bisa menjadi *output* yang tak terhingga kemungkinannya. Misalkan data nasabah berbelanja di mana, dalam jumlah berapa, di jam menit detik berapa, jenis barang yang dibeli, jumlahnya, mereknya, warna barangnya, ukurannya, dan jenis data tak terhingga lainnya. Dan bukan hanya ketika sang nasabah bertransaksi maka datanya diambil, ketika tidak bertransaksi pun nasabah terdeteksi pergerakannya ke mana saja, berapa lama, tidur di mana dan sebagainya. Hal ini dimungkinkan ketika sang nasabah menggunakan aplikasi digital banking dengan *data location on*. Transformasi digital mampu menarik semua data tanpa ampun bagaikan *Blackhole* dalam sistem tatasurya.

RISIKO PENYALAHGUNAAN *DATA*

Lalu apa risiko terkumpulnya data tersebut? Bayangkan betapa menghebohkan kasus *Cambridge Analytica* di Amerika Serikat (kita di sini kurang merasakan kehebohannya karena penggunaan data tersebut untuk kepentingan politis *internal* Amerika Serikat). Itu pun hasil dari pengumpulan data yang sangat terbatas dari penggunaan media sosial *Facebook*. Namun kemampuan institusi *bank* dalam pengumpulan data perseorangan dalam transformasi *digital* jauh melampaui yang dilakukan oleh *Cambridge Analytica*. Besaran *data* yang terkumpul berbanding lurus dengan makin pentingnya aset *data* tersebut sehingga tentunya juga berbanding lurus dengan besarnya risiko intrinsik. *Data* yang sedemikian detail dan lengkap apabila dikuasai oleh satu pihak dapat digunakan untuk menguasai atau menghancurkan reputasi lawan politiknya, lawan bisnisnya, atau lawan pribadinya.

STAKEHOLDERS RISIKO TRANSFORMASI *DIGITAL*

Kita dapat melihat risiko transformasi digital dari berbagai sudut pandang *stakeholders*:

1. **INDIVIDU**. Dari sisi individu risiko terbesar adalah hilangnya privasi. Dengan terjadinya transformasi *digital*, semua barang terkoneksi *internet* (*Internet of Things*), maka apapun yang kita lakukan bisa di*data*. Anda mungkin berpikir bahwa dengan mematikan *handphone* maka tidak akan ada yang tahun ketika Anda masuk ke *toilet*. Namun dengan transformasi *digital* lampu di *toilet* Anda akan menyala otomatis ketika Anda masuk dan mengirim *data* melalui *internet* bahwa Anda ada di dalam *toilet*, berapa lama, bahkan berapa banyak buangan yang Anda hasilkan serta analisisnya, karena *toilet* Anda pun terkoneksi dengan *internet*. Demikian pula privasi kita dalam menggunakan uang kita maupun dari mana sumbernya, tidak ada yang bisa disembunyikan lagi jika kita memilih menjadi warganegara yang baik (tentunya akan selalu ada perlawanan untuk mereka yang ingin bersembunyi, misalkan dengan menggunakan *cryptocurrency*). Di satu sisi individu merupakan pihak yang banyak diuntungkan melalui peningkatan kualitas hidup karena transformasi *digital*, namun di sisi lain individu adalah pihak yang paling rentan terhadap risikonya.

2. **PEMERINTAH**. Pada dasarnya tugas utama pemerintah adalah memperjuangkan kepentingan penduduknya. Oleh karena itulah pemerintah sebagai pemegang kekuasaan rakyat harus bisa menjadi pelindung risiko penduduknya. Apabila pemerintah tidak cukup kuat melindungi privasi data penduduk, maka bisa terjadi reaksi penduduk yang tidak dikehendaki. Misalkan kebijakan pemerintah untuk dapat mengakses rekening nasabah *bank* saja telah menimbulkan keresahan, yang pada sebagian masyarakat yang melek *digital* dapat mendorong penggunaan *cryptocurrency* sebagai *asset*, ataupun sebagai *media* transaksi atau *media* memindahkan *asset* ke luar negeri. Pemerintah pula yang punya kewajiban melindungi penduduknya dari risiko privasi *data* oleh institusi dan korporasi. Suatu terobosan baru mengenai ini adalah yang dilakukan oleh *regulator European Union* dengan meluncurkan *General Data Protection Rules (GDPR)* yang merupakan undang-undang perlindungan pengumpulan dan penggunaan data. Perlu dicatat, bukan hanya penggunaan, tapi juga aspek pengumpulannya diatur, dengan ancaman hukuman yang jelas. *GDPR* ini diberlakukan sejak 25 Mei 2018, yang membuat semua perusahaan legal yang beroperasi global harus mematuhinya.

   Di samping berperan sebagai 'orang tua' bagi penduduknya, Pemerintah sendiri sesungguhnya merupakan individu dari masyarakat pemerintah dunia. *Data* yang diperoleh dari pemerintah suatu negara dapat menjadi senjata bagi pemerintah

negara lain untuk mengambil keuntungan bersaing. Oleh karena itu Pemerintah harus juga dengan jeli melindungi data negaranya. Salah satunya adalah apa yang dilakukan oleh pemerintah China dengan melarang penggunaan *Google, Facebook, Whatsapp* oleh penduduknya, untuk mencegah pengumpulan data melalui *media-media* tersebut, yang pasti merupakan risiko bagi negaranya.

3. **INSTITUSI/KORPORASI**. *Stakeholder* inilah yang merupakan *driver* dari transformasi *digital*. Berawal dari dorongan untuk mempengaruhi individu, baik secara bisnis maupun sosial, institusi/korporasi menghimpun kemampuan kolektif untuk berinovasi yang menghasilkan transformasi *digital* yang berlangsung saat ini. Dari semua *stakeholders*, institusi/korporasi merupakan *stakeholder* utama.

   Sebagai *stakeholders* utama, institusi/korporasi menghadapi risiko dari berbagai sisi, yaitu:

   a. Risiko pasar yang terdiri dari para individu yang mempunyai hubungan dengannya. Kesalahan langkah dalam pengelolaan risiko bisa menyebabkan individu menghindar untuk berhubungan dengannya. *Cambridge Analytica* menutup operasinya di Amerika Serikat dan Inggris, dua bulan sesudah skandalnya terungkap, dan kemudian bangkrut. *Bank* yang rekeningnya sering mengalami kebobolan, tentunya membuat nasabah takut, namun di sisi lain dorongan transformasi *digital* membuat sistem bank harus terus menerus terkoneksi dengan internet yang merupakan jalan masuk bagi *hackers*.

   b. Risiko peraturan yang merupakan usaha pemerintah untuk melindungi individu. *Facebook* didenda pemerintah Inggris sebesar 500.000 *poundsterling* atas kasus *Cambridge Analytica*. Pada tanggal 1 Oktober 2018 *Tesco Bank* didenda pemerintah Inggris sebesar 16,4 juta *poundsterling* karena kejadian pada tanggal 5 November 2016 9.000 rekening nasabahnya dibobol *hacker*.

   c. Risiko kompetisi yang justru merupakan pendorong bagi institusi/korporasi untuk mengambil risiko pasar dan risiko peraturan yang lebih tinggi, karena jika institusi/korporasi tidak bisa mengatasi risiko kompetisi, maka eksistensinya bisa dipastikan lenyap. Jadi walaupun transformasi digital menambah risiko bagi institusi/korporasi, hal tersebut merupakan sesuatu yang tidak bisa ditolak atau dihindarkan, jika masih ingin hidup. Kasus bank yang jelas bankrut karena menghindari transformasi *digital* mungkin tidak terlalu nyata terlihat, karena biasanya *bank* yang tertinggal tersebut diakuisisi oleh bank yang lebih besar. Namun penggerusan bisnis perbankan oleh transformasi *digital* sudah terlihat di seluruh dunia.

MITIGASI RISIKO

Fokus mitigasi risiko yang di sini adalah mitigasi yang perlu dilakukan oleh *stakeholder* Institusi/Korporasi sebagai *driver* dari transformasi *digital*.

Mitigasi yang pertama tentunya adalah mitigasi risiko kompetisi, karena ini risiko yang paling fatal apabila tidak dimitigasi dengan baik. Untuk memitigasinya berarti institusi/korporasi harus:

a. Mempunyai *mindset digital. Mindset digital* berarti berpola pikir pilihan pertama adalah *digital*, jika belum bisa *digital* baru dilakukan dengan cara *non-digital*.

b. Membangun kompetensi *digital*. Kompetensi *digital* bukan berarti kompetensi teknis *IT* saja, namun justru yang lebih penting adalah kompetensi bisnis dan kepemimpinan *digital*, antara lain kompetensi strategi dan model bisnis *digital*. Sebaliknya anggota tim di bidang bisnis pun sekarang harus mengerti perkembangan teknis *IT* secara konseptual.

c. Bergerak cepat. Lupakan cara bergerak lama yang bekerja hanya pada jam kantor dan birokrasi otorisasi. Saat ini semua harus cepat dan oleh karenanya birokrasi menjadi halangan. Cara kerja *Agile* saat ini bukan hanya diterapkan pada tim pengembangan *software*, namun harus menjadi standar cara kerja di semua departemen. Dengan demikian SOP lama yang mengatur prosedur antar individu atau antar tim perlu berubah, dan kultur pun harus berubah.

Mitigasi yang kedua adalah mitigasi risiko operasi yang ditujukan untuk mengelola risiko pasar dan risiko peraturan, dan menyangkut manajemen risiko teknis. Untuk memitigasinya berarti institusi/korporasi harus melakukan:

a. Pencegahan risiko: Institusi/Korporasi harus menguasai peraturan otoritas yang berlaku, bukan hanya di tempat ia beroperasi, namun juga apa regulasi yang mengatur pelanggannya (misalkan *GDPR* melindungi warganegara EU di mana pun ia berada). Ketika membuat rancangan *data collection*, Institusi/Korporasi pun perlu memikirkan rancangan di mana risiko kebocoran data sebagai paket dicegah dengan misalnya memisahkan beberapa jenis data sensitif ke beberapa tempat. Manajemen perancangan dan pengelolaan API (*Application Protocol Interface*) dengan pihak mitra pun harus dilakukan dengan hati-hati. Selain itu infrastruktur data pun perlu diperhatikan karena faktor bencana alam misalkan gempa bumi dapat menghancurkan data center secara fisik sehingga perlu dipikirkan letak *back-up data center* dengan profil risiko bencana yang berbeda. Kita masih ingat kejadian bulan Agustus tahun lalu, bagaimana Telkom terganggu operasinya sampai dua minggu karena Satelit Telkom 1 yang menyimpan data hilang dan *data recovery*-nya harus dilakukan secara manual. Bayangkan jika ini terjadi pada *bank*.

b. Pengamanan proses: Dengan makin terbukanya saluran komunikasi baik lewat kabel maupun *wi-fi*, maka jalur komunikasi perlu dijaga dengan *anti virus* dan *firewall* yang selalu *up-to-date* dan berlapis. Regulasi perbankan mensyaratkan tingkat keamanan sistem *level* tertentu, namun setiap saat selalu terjadi peningkatan kemampuan *hackers* maupun teknologi baru. Oleh karenanya kasus pembobolan rekening nasabah masih cukup sering terjadi. Di samping itu *software* yang digunakan pun harus yang bereputasi, karena perusahaan yang bereputasi tidak akan menggunakan *back-door* untuk mencuri data kliennya, selain selalu memperbaiki bugs. Jangan lupa bahwa seringkali pembobolan dilakukan oleh orang dalam, oleh karena itu sistem keamanan terhadap orang dalam pun harus terus diperkuat dan dievaluasi.

c. Protokol kejadian kebobolan. Seberapa kecil pun risikonya, masih ada kemungkinan terjadi kebobolan. Sama seperti kita mengantisipasi kebakaran pada gedung, kita harus siapkan protokol apabila terjadi kebobolan. Tim 'pemadam kebakaran' sudah harus dibentuk dan disiapkan, dan dijaga agar setiap saat dapat dihubungi. Prosedur dan otorisasinya pun harus sudah jelas, tidak mungkin dalam situasi genting misalkan tim 'pemadam kebakaran' harus minta ijin kepada sang Presiden Direktur yang mungkin dalam pesawat *long-haul*. Arsitektur *program* yang modular memudahkan mengisolasi bagian yang terinfeksi baik oleh *virus* maupun *hacker*, sehingga meminimisasi gangguan operasi secara keseluruhan. Selain itu secara berkala perlu dilakukan simulasi, agar dapat diidentifikasi faktor-faktor yang bisa menghalangi proses 'pemadaman kebakaran' apabila benar-benar terjadi.

Sebagai penutup, perlu kita sadari bahwa segala sesuatu mengandung risiko. Perubahan karena transformasi *digital* tentunya mengandung risiko yang baru, namun tidak berubah pun mengandung risiko yang jelas lebih fatal.

PROFIL PENULIS

Dr. Bayu Prawira Hie
Executive Director Intellectual Business Community,
anggota tim riset Ikatan Bankir Indonesia

DAFTAR BUKU IKATAN BANKIR INDONESIA

Pemesanan buku melalui Sekretariat IBI dengan:
Sdri. Dewi: 021-75901547 atau email: katri.dewi@ikatanbankir.or.id

TELAH TERBIT

PROFIL IBI

Ikatan Bankir Indonesia (IBI) berdiri pada 12 Desember 2005 sebagai hasil merger antara Institut Bankir Indonesia dengan Bankers Club Indonesia. Pendirian tersebut disaksikan oleh Gubernur Bank Indonesia dan Menteri Keuangan RI. Visi IBI adalah menjadi asosiasi profesi bankir di Indonesia yang memberikan manfaat bagi anggotanya dalam bidang pengembangan profesi, praktik perbankan yang sehat, dan penerapan tata kelola yang baik untuk membantu pemerintah mengembangkan ekonomi nasional yang kuat melalui 6 kegiatan utama: (i) Menyatukan bankir dari seluruh bank yang beroperasi di Indonesia; (ii) Meningkatkan profesionalisme dan integritas bankir; (iii) Membantu para anggota; (iv) Menyediakan sertifikasi kompetensi profesi bagi para anggota; (v) Menjadi mitra profesional bagi otoritas perbankan dan pemerintah untuk mewujudkan sistem perbankan yang sehat; dan (vi) Mewujudkan anggota yang disiplin melalui Kode Etik Bankir Indonesia.

PROFIL LSPP

Lembaga Sertifikasi Profesi Perbankan (LSPP) didirikan oleh IBI, Perbanas, Himbara, Asbisindo, Asbanda, dan Perbarindo pada tahun 2006 di bawah lisensi Badan Nasional Sertifikasi Profesi (BNSP). LSPP menyediakan sertifikasi untuk 9 unit kompetensi yaitu Manajemen Risiko, Audit Internal, *General Banking*, *Treasury Dealer*, *Compliance*, *Funding and Services*, *Operations*, *Credit and Wealth Management*. Sertifikasi kompetensi yang dikelola oleh LSPP meliputi 3 aspek yang ditentukan oleh BNSP yaitu Pengetahuan, Keahlian, dan Perilaku, untuk menghadapi tantangan industri modern perbankan. Sejak 2008 sampai dengan 2017, LSPP telah mensertifikasi tidak kurang dari 144.000 bankir dari seluruh bank di Indonesia.

IKATAN BANKIR INDONESIA
Menara IBI Lantai 2
Jl. Fatmawati No. 2-4 Jakarta 12430,
Cilandak - Jakarta Selatan
Phone : (+62) 21 75901547 ext.: 203
Email : sekretariat@ikatanbankir.or.id
www.ikatanbankir.or.id

Bankers Update BULETIN IKATAN BANKIR INDONESIA

Bankers Update merupakan buletin yang diterbitkan secara periodik oleh Bidang Riset, Pengkajian, dan Publikasi dan Bidang komunikasi Ikatan Bankir Indonesia.