

## BAB III

# Diskursus Tata Kelola Informasi: Jalan Tengah Nilai Tambah dan Risiko

Muhammad Usman Noor

---

### A. Sampai Mana Diskursus Tata Kelola Informasi Kini?

Istilah *information is the new oil* (informasi adalah minyak baru) adalah terminologi yang perlu diluruskan. Terminologi ini muncul karena banyak pihak yang merasa bahwa informasi memiliki nilai ekonomi yang tinggi, salah satunya seperti yang dikemukakan oleh Wang et al. (1998). Informasi diproposisikan sebagai salah satu bentuk produk dan memiliki nilai ekonomi. Pemahaman tersebut kemudian berkembang sebagai dasar argumen bahwa informasi dalam berbagai media dan bentuk dapat dianggap sebagai aset (Hagmann, 2013; Horne, 1995). Namun, perlu diingat bahwa informasi tidak serta-merta menjadi “minyak”. Seperti halnya minyak mentah yang perlu diolah

---

M. U. Noor

Universitas Indonesia, e-mail: usmannoor@ui.ac.id

© 2024 Editor & Penulis

Noor, M. U. (2024). Diskursus tata kelola informasi: Jalan tengah nilai tambah dan risiko. Dalam Laksmi (Ed.), *Tren dan Dinamika Kajian Ilmu Perpustakaan dan Informasi* (49–68). Penerbit BRIN. DOI: 10.55981/brin.1079.c1184. E-ISBN: 978-602-6303-45-5.

untuk bisa bernilai guna dan siap pakai, informasi pun demikian. Informasi dalam bentuk yang “mentah” dapat dikatakan kurang bernilai karena tidak bisa langsung digunakan. Agar suatu data dan informasi dapat bernilai, harus ada proses yang dilakukan terlebih dahulu, yaitu proses pertambahan nilai (*value-added processing*). Selain itu, data yang banyak sekalipun—misalnya dalam bentuk *big data*—tidak serta-merta menjadikannya langsung memiliki nilai tambah jika hanya sekadar disimpan saja (Foster et al., 2018a). Perlu strategi untuk mengubah informasi mentah tersebut menjadi sesuatu yang memiliki nilai tambah, antara lain mengorganisasi, menganalisis, menilai, serta menggunakan informasi tersebut dalam konteks yang tepat atau sesuai (Taylor, 1986).

Faktor lain yang tidak kalah penting untuk diperhatikan dalam proses pertambahan nilai dari informasi adalah pertimbangan faktor risiko yang menyertainya. Sebagaimana kita pahami, dengan bertambahnya jumlah data secara eksponensial maka diperlukan biaya tambahan untuk menyimpan dan mengelola informasi tersebut. Sekalipun informasi atau data tersebut dalam bentuk digital, tidak serta-merta membuat proses simpan dan perawatannya menjadi lebih murah. Pada beberapa kasus, penyimpanan dalam bentuk digital justru lebih mahal daripada menyimpan informasi dalam bentuk dokumen atau arsip konvensional (Tallon et al., 2013).

Faktor risikonya pun tidak berhenti sampai di biaya saja. Dengan suatu organisasi atau lembaga menyimpan informasi dalam jumlah besar, membuat risiko keamanan akan informasi tersebut meningkat tajam. Organisasi perlu menerapkan strategi khusus untuk mengamankan isi informasi yang mereka simpan, termasuk ancaman dari luar, seperti *hacker*, *malware*, *phishing*, dan sebagainya.

Merujuk data dari Verizon (2022), dikatakan bahwa 80% serangan kebocoran informasi disebabkan dari pihak eksternal, tetapi terdapat 20% kebocoran informasi yang berawal dari kelalaian atau kesalahan di faktor internal. Adapun beberapa ancaman internal yang perlu diperhatikan adalah kebocoran informasi yang diakibatkan oleh rekayasa sosial (*social engineering*) yang dilakukan oleh orang luar yang ingin mengambil informasi di organisasi tersebut,

kebocoran informasi yang diakibatkan faktor murni ketidaksengajaan ketika sedang mengelola informasinya (*inadvertent disclosure*), serta kebocoran informasi yang diakibatkan adanya intensi dari seseorang di dalam organisasi untuk membocorkan informasi keluar demi keuntungan pribadi (Tran et al., 2016; Coffey, 2017). Meskipun secara rasio tidak sebanyak risiko serangan dari pihak luar, tetapi bukan berarti ancaman dari internal menjadi sesuatu yang dianggap enteng. Perspektif ini adalah sesuatu yang harus dipertimbangkan bagi tiap organisasi ketika ingin mengambil manfaat dan nilai dari informasi yang mereka hasilkan, miliki, dan simpan.

Proses menjadikan informasi bernilai untuk organisasi dapat dicapai dengan melakukan tata kelola yang tepat—dalam hal ini, hal yang dikelola adalah informasi yang dihasilkan dan dimiliki oleh suatu organisasi. Tata kelola informasi berkaitan erat dengan hierarki tata kelola yang umum dikenal di organisasi, antara lain tata kelola organisasi dan tata kelola teknologi informasi yang lebih dahulu berkembang (Smallwood, 2014). Pada perkembangannya, penggunaan komputer yang mulai muncul di pertengahan abad ke-20 mengakibatkan tata kelola teknologi informasi lebih dahulu berkembang. Komputer yang lebih terlihat dan *tangible* objeknya menjadikannya lebih mudah ditatakelolakan ketimbang informasi yang lebih bersifat *intangible*. Hal ini mengakibatkan tata kelola informasi boleh dikatakan lebih lambat berkembang. Organisasi lebih mudah menata informasi dengan melihat kontainernya, seperti perangkat keras dan perangkat lunaknya, tetapi justru belum menata kelola konten informasi yang ada pada perangkat-perangkat tersebut (Tallon et al., 2013).

Perkembangan tata kelola informasi sendiri baru mulai banyak dibahas oleh peneliti luar pada tahun 2010-an. Sebelumnya, terminologi yang digunakan adalah tata kelola data (*data governance*), seperti yang dibahas dalam penelitian Weber et al. (2009), Khatri dan Brown (2010); serta Otto (2011). Kemudian, terminologi ‘tata kelola data’ berkembang menjadi ‘tata kelola informasi’ pada tahun 2010-an hingga sekarang melalui beberapa tulisan yang menonjol, antara lain karya Lomas (2011), Haggmann (2013), Tallon et al. (2013), dan Smallwood (2014).

Kemudian, yang menjadi pertanyaan, apa dan sudah sampai mana kondisi diskursus tata kelola informasi di Indonesia? Penggunaan terminologi tata kelola informasi di Indonesia masih sangat terbatas. Ranah akademis dan praktis di Indonesia masih lebih mengenal dan membahas istilah ‘tata kelola informasi teknologi’ (*IT governance*). Argumen ini berawal dari hasil penelusuran terhadap artikel dengan topik tata kelola informasi di lingkup peneliti Indonesia. Dari *database* artikel Garuda (Garba Rujukan Digital) yang dikelola oleh pemerintah Indonesia, ditemukan dalam kurun waktu 11 tahun terakhir hanya ada empat artikel yang mengandung kata “tata kelola informasi” atau “*information governance*” pada judulnya. Adapun di periode yang sama, ada lebih dari 120 artikel yang membahas mengenai tata kelola IT (*IT governance*). Disparitas yang lebar ini menunjukkan diskursus informasi masih lebih banyak berkuat pada artefak komputer ketimbang fokus pada konten informasi atau nilai yang terdapat dalam informasi.

Lebih lanjut, dari hasil penelitian mengenai tata kelola informasi yang telah dilakukan Janah dan Mayesti (2020) di stasiun televisi nasional dan Apriyanto (2022) serta Susanawati et al. (2021) di lembaga pemerintahan, masih menunjukkan tingkat penerapan tata kelola yang rendah. Berdasarkan penelitian tersebut, menunjukkan rendahnya penerapan tata kelola informasi di Indonesia berawal dari lemahnya kebijakan dan tata kelola di lembaga-lembaga tersebut. Hal ini yang mendorong penulis memberikan tambahan warna pada diskursus tata kelola informasi di ranah *stakeholder* dan peneliti di Indonesia melalui tulisan ini.

Pada tulisan ini, penulis mencoba mengajak pembaca untuk berdialog dan melakukan diskursus mengenai apa itu tata kelola informasi, lebih khusus membahas mengenai nilai tambah yang dapat diperoleh dari kegiatan tata kelola informasi dengan tidak lupa membahas faktor risiko yang dapat muncul dari kegiatan proses pertambahan nilai tersebut.

## B. Nilai Tambah Informasi

Informasi agar dapat bernilai perlu melalui serangkaian proses. Salah satu model yang dapat digunakan untuk menarik nilai dari informasi adalah model pertambahan nilai (*value-added model*) dari pemikiran Robert S. Taylor. Meskipun model ini pertama kali dipublikasikan tahun 1986, jauh sebelum komputer mendominasi sebagaimana kondisi hari ini, tetapi masih tetap relevan dan dapat digunakan. Salah satunya adalah untuk menjelaskan seperti apa sistem yang bisa diandalkan dan seperti apa atribut sistem yang bisa memberikan manfaat atau tidak (Eisenberg & Dirks, 2008).

Model pertambahan nilai bertujuan untuk menjelaskan apa yang pengguna inginkan, mengapa mereka (pengguna) menginginkan itu, dan bagaimana suatu sistem dapat (atau tidak dapat) memenuhi kebutuhan tersebut. Merujuk pada teori pertambahan nilai dari Taylor (1986), dijelaskan bahwa terdapat tujuh model pertambahan nilai (*value-added model*), yaitu kemudahan penggunaan (*easy of use*); pengurangan gangguan (*noise reduction*); kualitas (*quality*); adaptabilitas (*adaptability*); penghematan waktu (*time savings*); dan terakhir, pengurangan biaya (*cost savings*). Dalam prosesnya diperlukan tiga komponen utama (Eisenberg & Dirks, 2008). Ketiga komponen tersebut adalah sebagai berikut.

- 1) Manusia. Fokus utama komponen ini ada pada pengguna, sebuah sistem hadir untuk memenuhi kebutuhan informasi penggunanya.
- 2) Informasi. Terdapat hierarki pada spektrum informasi. Jika nilai dari suatu informasi sudah ditarik, informasi bergerak dari spektrum data menuju pengetahuan yang bisa digunakan.
- 3) Sistem. Tujuan dari suatu sistem informasi adalah untuk menambah nilai dari informasi yang dapat membantu pengguna. Proses kerja sistem dapat bervariasi disesuaikan dengan tujuan pengguna.

Dari proses pertambahan nilai ini, informasi berkembang menjadi tata kelola data dan tata kelola teknologi informasi. Kemudian, perkembangan menjadi makin komprehensif sehingga melahirkan konsep tata kelola informasi.

## C. Tata Kelola Informasi

Tata kelola informasi memainkan peranan penting untuk memaksimalkan nilai dari suatu informasi dengan meminimalkan risiko dan biaya (IGI, 2014). Lebih lanjut, tata kelola informasi didefinisikan sebagai kumpulan kemampuan dan praktik pada proses penciptaan, penangkapan, penilaian, penyimpanan, penggunaan, kendali, akses, pengarsipan, dan pemusnahan dari suatu informasi dan sumber daya terkait selama proses daur hidup informasi tersebut (Mikalef et al., 2020; Tallon et al., 2013). Tata kelola informasi sendiri adalah konsep yang memayungi berbagai konsep kunci dalam pengelolaan informasi, antara lain manajemen rekod (*record*), keamanan informasi, *e-discovery*, kesiapan litigasi, manajemen konten, tata kelola IT dan data, privasi data, manajemen risiko, dan kepatuhan terhadap aturan. Lebarnya rentang bahasan dan tema dari tata kelola informasi membuat sulit menentukan satu definisi yang pasti dan dapat diterima secara universal. Terlebih dalam praktiknya, tata kelola informasi melibatkan berbagai disiplin dan saling tumpang tindih (Smallwood, 2014). Namun, Soares (2012) dan Ballard et al. (2014) mengatakan bahwa inti dari tata kelola informasi adalah struktur, manajemen metadata, keamanan dan privasi, kualitas data, integrasi bisnis proses, integrasi master data, dan manajemen siklus informasi.

Hal umum yang dapat diterima adalah bahwa semangat tata kelola informasi adalah bagaimana upaya organisasi meningkatkan nilai informasi dengan tetap meminimalkan risiko dan biaya yang timbul dari proses tersebut. Dalam tata kelola informasi, penting untuk memastikan bahwa informasi yang dikelola sesuai dengan tempatnya, hal ini dapat tercapai dengan penataan yang terorganisasi dengan baik dan dijalankan secara konsisten, terstruktur, dan terstandarisasi (Smallwood, 2014).

Sifat tata kelola informasi yang menaruh perhatian terhadap pengurangan biaya membuat tata kelola informasi berfokus pada informasi yang memiliki nilai guna tinggi dalam prosesnya. Menurut Smallwood (2014), dari seluruh arsip atau dokumen yang dimiliki oleh perusahaan, hanya sekitar 25% data tersimpan di organisasi yang memiliki nilai bisnis. Kemudian, 5% di antaranya punya masa

retensi yang panjang karena dianggap sebagai rekod (*record*) bisnis dan 1% yang harus disimpan permanen karena memiliki nilai guna hukum. Sementara itu, 69% sisanya umumnya adalah arsip yang kurang bernilai guna atau arsip yang bersifat pengurangan.

Tata kelola menjadi hal yang dibutuhkan di era sekarang. Ketika data dan informasi bertumbuh secara eksponensial, data kasar menunjukkan bahwa 90% data yang dihasilkan sekarang hanya diciptakan dalam kurun waktu dua tahun terakhir. Hal ini sebagaimana yang dikatakan oleh Smallwood bahwa dalam dua hari lebih banyak informasi yang diciptakan daripada sebelum tahun 2003. Ini sejalan dengan apa yang telah dikatakan di awal bahwa banyaknya informasi tidak serta-merta menjadikan informasi tersebut bernilai, justru yang ada malah menambah berat faktor risiko yang mungkin muncul.

Walaupun diskursus tata kelola informasi sudah banyak dibahas sejak satu dekade silam, secara umum diskursus tata kelola informasi belum banyak berkembang dan jumlah artikel maupun peneliti yang membahas tema tata kelola informasi masih terbatas. Hal ini berbeda dengan tata kelola IT yang sudah lebih dahulu dikenal dan telah banyak dibahas. Padahal, jika dilihat dari cakupannya, tata kelola informasi berusaha melihat pengelolaan informasi dari sudut pandang yang lebih utuh dan komprehensif, tidak melulu fokus pada nilai manfaat, tetapi juga faktor risiko yang menyertai.

#### **D. Literatur Utama Konsep Tata Kelola Informasi**

Penulisan ini menggunakan pendekatan studi literatur untuk menjawab sejauh mana diskursus mengenai tata kelola informasi dibahas. Studi literatur dapat digunakan untuk menjawab tujuan dari penulisan ini karena metodenya dianggap paling relevan untuk mengetahui sejauh mana riset dan *state of the art* dari suatu tema (Snyder, 2019). Pada penelitian ini, digunakan beberapa sumber literatur utama sebagai acuan dalam menyajikan pembahasan sejauh mana diskursus mengenai tata kelola informasi. Literatur yang dipilih ditentukan setelah melalui proses penelusuran pada artikel yang membahas mengenai tata kelola informasi dalam tiga tahun ke belakang. Kemudian, dari artikel tersebut, penulis menelusuri daftar

sitasinya dan mengambil beberapa artikel yang rutin digunakan sebagai acuan mengenai penulisan dalam tema tata kelola informasi. Adapun sumber literatur utama yang digunakan dalam penulisan ini dapat dilihat pada Tabel 3.1.

**Tabel 3.1** Sumber Literatur Utama

No.	Judul	Penulis	Tahun
1.	<i>Value Added Process</i>	Robert S. Taylor	1986
2.	<i>Designing Data Governance</i>	Vijay Khatri & Carol Brown	2010
3.	Organizing Data Governance: Findings from the telecommunication industry and consequences for large service providers	Boris Otto	2011
3.	<i>Information governance: Beyond Buzz</i>	Juerg Hagemann	2013
4.	<i>The Information artifact in IT Governance: Toward a theory of information governance</i>	Paul Tallon, Ronald Ramirez, & James Short	2014
5.	<i>Data work in context: Value, risks, and governance</i>	Jonathan Foster, Julie McLeod, Jan Nolin, & Elke Greifeneder	2018
6.	<i>Data governance: A conceptual framework, structured review and research agenda</i>	Rene Abraham, Johannes Schneider, & Jan vom Brocke	2019
7.	<i>The role of information governance in big data analytics driven innovation</i>	Patrick Mikalef, Maria Boura, George Lekakos, & John Krogstie	2020

Dalam prosesnya, studi literatur ini dapat membantu dalam menemukan celah pada suatu tema, menemukan bahasan pada tema, dan juga dapat membantu dalam membangun teori (Torraco,

2016). Analisis yang digunakan pada penulisan ini adalah tinjauan sistematis. Tinjauan sistematis adalah metode tinjauan literatur yang mengombinasikan dan membandingkan hasil dari beberapa penelitian dengan tujuan menentukan pola yang muncul, perdebatan yang terjadi, dan hubungan antara beberapa hasil penelitian dalam satu topik tertentu (Davis et al., 2014). Pada penulisan ini, penulis menggunakan istilah informasi dan data secara bergantian, meskipun pada dasarnya terdapat perbedaan antara definisi data dan informasi. Namun, dalam konteks penulisan ini, penulis memilih menggunakan dua istilah ini secara bergantian sesuai dengan konteks pembahasan.

## **E. Menelusur Perkembangan Tata Kelola Informasi**

Ketika organisasi sudah lazim menggunakan komputer dan teknologi informasi untuk mendukung proses kerjanya, kemudian berkembang pandangan bahwa sistem teknologi informasi adalah salah satu aset organisasi. Oleh karena itu, sistem teknologi informasi ini kemudian perlu ditata kelola di organisasi dan melahirkan tata kelola teknologi informasi yang di antaranya fokus mengelola dan mengatur penggunaan IT, termasuk di dalamnya adalah akuntabilitas dan pengaturan keputusan yang menggunakan informasi dan IT (Weill & Ross, 2004). Namun, kemudian anggapan ini berkembang, tata kelola IT lebih fokus pada pengelolaan sistem informasinya, atau dengan kata lain, fokus pada komputer dan jaringannya. Sementara itu, informasi yang dikandung di dalamnya bisa ditransmisikan dalam berbagai bentuk dan jaringan. Hal ini justru adalah roh dari apa yang nantinya mempunyai nilai sehingga kemudian berkembang bahwa yang perlu ditata kelola adalah informasinya juga, tidak hanya sekadar menata kelola sistem informasinya. Perubahan ini menumbuhkan terminologi tata kelola informasi di kalangan peneliti dan *stakeholder* di bidang pengelolaan informasi di dunia Barat di era 2000-an akhir.

Salah satu perbedaan mendasar antara tata kelola IT dengan tata kelola informasi adalah titik fokus tata kelola IT yang lebih berat pada IT sebagai artefak, sedangkan tata kelola informasi lebih melihat

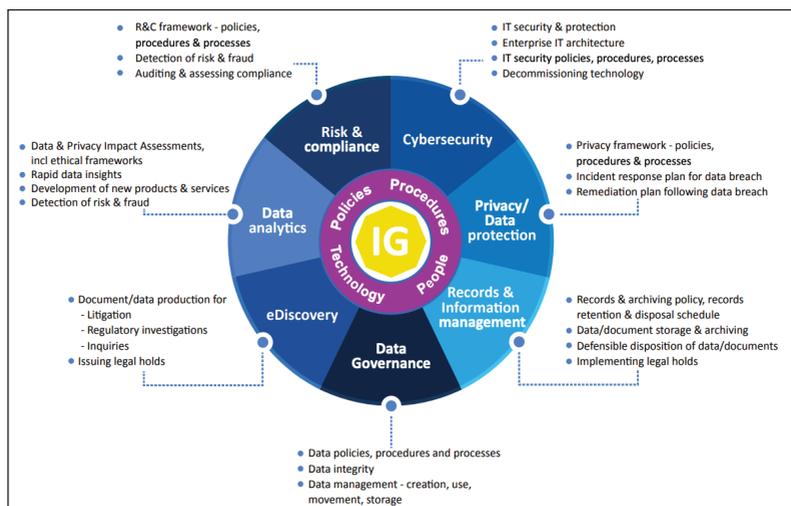
informasi sebagai kontennya (Tallon et al., 2013). Sebagaimana sudah disebutkan di awal bahwa kini informasi telah dianggap sebagai aset oleh banyak organisasi, termasuk di antaranya data. Data atau informasi yang memiliki nilai umumnya diberi batasan sehingga tidak serta-merta semua informasi atau data disebut sebagai aset. Umumnya, informasi yang memiliki nilai atau nilai potensial yang didokumentasikan adalah apa yang dapat disebut sebagai aset (Khatri & Brown, 2010). Kemudian, agar informasi memiliki nilai guna, perlu upaya untuk menarik nilai dari informasi tersebut sehingga perlu adanya investasi dalam bentuk sistem dan teknologi bagi pemilik informasi, dalam konteks ini adalah organisasi (Chang, 2018).

Pada pelaksanaannya, tata kelola informasi dapat dilihat dari tiga mekanisme atau praktik, yaitu struktural, prosedural, dan relasional. Tiga mekanisme ini diajukan oleh Tallon et al. (2013) yang kemudian diperkuat oleh argumen dari Borgman et al. (2016) dan Abraham et al. (2019). Secara umum, mekanisme struktural menjelaskan bahwa dalam tata kelola informasi diperlukan komite, kelompok, atau grup yang bertanggung jawab dalam menentukan kebijakan tata kelola informasi di suatu organisasi. Kelompok ini bertugas menentukan peran dan tanggung jawab dalam hal pengelolaan informasi di suatu organisasi (Abraham et al., 2019).

Mekanisme berikutnya adalah prosedural. Mekanisme ini mengatur bagaimana data atau informasi secara akurat direkam, disimpan dengan aman, digunakan secara efektif, dan dibagikan dengan cara yang benar. Mekanisme prosedural juga turut mengatur tentang bagaimana informasi dikelola dalam siklus hidupnya, mulai dari penilaian informasi, pengaksesan, retensi, pengarsipan, hingga pemusnahan. Mekanisme ini juga mengatur bagaimana biaya yang timbul dari proses pengelolaan informasi (Borgman et al., 2016).

Mekanisme yang ketiga adalah mekanisme relasional yang lebih fokus pada memfasilitasi komunikasi antar-*stakeholder* yang berkaitan dengan informasi tersebut. Praktik pada mekanisme relasional meliputi pelatihan, pendidikan, berbagi pengetahuan, resolusi konflik, dan koordinasi antarpengelola (Tallon et al., 2013).

Kemudian, ketiga mekanisme tersebut oleh Bennet (2017) dibagi ke beberapa aspek-aspek dalam praktik tata kelola informasi, meliputi aspek prosedur, kebijakan, manusia, dan teknologi. Selanjutnya, aspek ini melebar ke bagaimana mengatur praktik manajemen rekod (*record*) dan informasi, tata kelola data, *e-discovery*, analisis data, risiko dan kepatuhan, keamanan siber, serta perlindungan privasi dan data. Penjelasan lebih lengkap ditunjukkan pada Gambar 3.1.



Sumber: Bennett (2017)

**Gambar 3.1** Tata Kelola Informasi

Dari Gambar 3.1, terlihat lingkup tata kelola informasi tidak hanya fokus pada upaya menarik nilai dari informasi, tetapi juga mengelola risiko dan upaya mengikuti aturan (*compliance*) dengan regulasi atau aturan yang berjalan di negara organisasi tersebut.

Proses menambahkan nilai pada informasi dan data yang dimiliki oleh organisasi melalui proses ekstraksi, analisis, dan penggunaan data untuk mendukung tujuan organisasi adalah hal yang dikerjakan oleh mereka yang bertugas mengelola data di organisasi. Proses ini disebut oleh Carter dan Sholler (2015) sebagai

proses “*data science work*” dan “*data analysis work*”. Kemudian, oleh Foster (2016) istilah tersebut diringkaskan menjadi “*data work*”. Istilah ini belum memiliki padanan dalam bahasa Indonesia. Jika pun digunakan istilah bahasa Indonesia, penulis berpendapat istilah “mengaryakan data” sebagai padanan dalam bahasa Indonesia yang dapat digunakan. Pada praktiknya, mengaryakan data ini adalah upaya menambahkan nilai dari informasi dengan cara menganalisis, mengorganisasi, melakukan penilaian, dan membuat keputusan pada sebuah data (Foster et al., 2018b).

Selain itu, ada hal yang perlu dipertimbangkan dalam proses meningkatkan nilai informasi berdasarkan informasi hasil pengumpulan dari pihak ketiga atau pelanggan, yaitu nilai akurasi. Informasi yang tidak lengkap atau tidak diisi sesuai dengan kenyataannya akan mengakibatkan hasil analisis yang keliru dan pengambilan keputusan yang salah (Otto, 2011). Oleh karena itu, perlu standarisasi kualitas informasi yang kelak akan dilakukan proses pengaryaan data untuk menghasilkan nilai informasi yang bermanfaat dan dapat membantu dalam menyelesaikan masalah atau tujuan.

## **F. Tata Kelola Informasi sebagai Mitigasi Risiko**

Pada praktiknya, sering kali upaya organisasi atau lembaga meningkatkan nilai informasi tidak maksimal. Misalnya, nilai dari informasi yang diperoleh tidak terlalu banyak atau signifikan. Sebaliknya, risiko yang ditimbulkan malah dapat mengakibatkan kerugian yang lebih banyak. Sebagai contoh, dalam konteks penanganan pandemi Covid-19, organisasi kesehatan saling berlomba mengumpulkan data-data pasien atau data pergerakan orang (*tracing*) dengan tujuan untuk mengendalikan pandemi, tetapi tanpa adanya perlindungan data pribadi yang kuat di satu sisi, justru mengakibatkan rentan terjadi kebocoran data pribadi milik banyak orang. Salah satu hal yang sering terlewatkan—walaupun sebenarnya penting—pada tata kelola informasi merupakan salah satu tujuan utama dari tata kelola informasi, yaitu tidak hanya berusaha menarik manfaat dari informasi yang dimiliki, tetapi juga mengelola informasi yang sifatnya rahasia atau sensitif (Chang, 2018). Pada sisi inilah yang masih banyak

organisasi luput untuk memanfaatkan tata kelola informasi sebagai jalan untuk memenuhi kepatuhan terhadap regulasi pengelolaan data sensitif.

Proses pengumpulan informasi dengan tujuan untuk menyelesaikan masalah atau mendukung pencapaian target tertentu juga menimbulkan pertanyaan dalam bidang privasi, persetujuan, dan keamanan dari data tersebut. Sejauh mana pemrosesan data yang dihimpun oleh suatu organisasi atau lembaga masih belum banyak dibahas atau direncanakan dengan baik. Hal ini termasuk data atau rekod (*record*) dalam bentuk digital yang dapat diolah dan diproses secara otomatis dengan menggunakan algoritma, tetapi malah membawa masalah baru, yaitu memberikan konsekuensi—misalnya, kesalahan kategorisasi dan pemfilan yang tidak akurat—sehingga informasi hasil olahannya malah tidak lagi objektif (Dormehl, 2015).

Tata kelola informasi berusaha mengambil manfaat sebanyak-banyaknya dari informasi yang dimiliki dengan tetap menekan biaya dan risiko yang timbul dari proses tersebut. Faktor risiko yang sering kali terlewatkan adalah masih kerap terjadi kebocoran informasi yang disebabkan belum ajeknya praktik perlindungan data pada tiap organisasi yang mengelola data pribadi sebagai informasi yang mereka gunakan dalam proses bisnisnya.

Kondisi belum siapnya perlindungan data pribadi menjadi sandungan. Salah satu permasalahan yang dihadapi oleh pemerintah dan organisasi di Indonesia terkait masalah perlindungan data adalah belum adanya payung hukum yang menjadi dasar perlindungan data pribadi di tingkat nasional. Dengan kata lain, Indonesia masih belum memiliki undang-undang perlindungan data pribadi. Kabar baiknya, rancangan undang-undang perlindungan data pribadi telah dibahas oleh DPR sejak 2019. Kabar buruknya, hingga 2022, RUU ini masih dalam tahap pembahasan dan belum selesai disahkan. Hal ini sangat disayangkan karena dengan demikian, Indonesia menjadi salah satu negara di ASEAN yang belum memiliki aturan perlindungan data pribadi yang komprehensif, setidaknya hingga tahun 2021 (Khumon, 2021).

Absennya payung hukum di level nasional tidak menyurutkan upaya level sektoral untuk bergerak. Demi kelancaran proses bisnis di suatu industri atau sektor, telah banyak kementerian yang mengeluarkan peraturan menteri yang mengatur bagaimana melindungi data pribadi di lingkup kerja mereka. Beberapa peraturan yang telah dikeluarkan dalam upaya melindungi data pribadi, antara lain Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik dan Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik yang mencabut Peraturan Pemerintah Nomor 82 Tahun 2012 tentang hal yang sama. Namun, konsekuensi yang muncul dari belum adanya tameng legislatif dalam hal perlindungan data pribadi ini adalah terjadinya tumpang tindih aturan mengenai perlindungan data pribadi di level sektoral atau industri (Djafar, 2019; Sargunraj, 2020).

Konsekuensi dari belum adanya perlindungan data pribadi yang komprehensif di level nasional membuat belum terbangunnya kesadaran untuk menjaga data pribadi, baik itu miliknya sendiri maupun milik orang lain. Foster et al. (2018b) berargumen dalam tulisannya mengenai pengayaan data bahwa kondisi pengelolaan informasi yang terjadi di level makro akan memengaruhi dan memberi konsekuensi pengelolaan informasi di level mikro. Namun, tidak hanya itu. Kondisi di level mikro juga bisa memengaruhi kondisi pengelolaan di level yang lebih tinggi, seperti di level sektoral atau industri hingga di level nasional atau makro. Hal ini berujung pada praktik tata kelola informasi secara umum. Masih terjadi kelalaian yang dilakukan oleh pelaku pengelola informasi ketika menangani atau memproses informasi yang memuat data pribadi di dalamnya. Belum terbangun kesadaran sehingga masih sering terjadi bocornya data rahasia atau data sensitif, baik itu karena faktor internal secara tidak sengaja ataupun serangan dari pihak luar.

Bicara mengenai serangan dari pihak luar, faktor risiko dapat diredam dengan menggunakan jaring pengaman yang canggih. Namun, manusia adalah titik yang paling lemah dalam jejaring keamanan informasi. Faktor manusia inilah yang sering terlewatkan, padahal sebenarnya ini adalah faktor yang paling mudah untuk

menjadi titik akses bocornya informasi. Kebocoran ini kemudian membawa dampak kerugian lebih besar bagi organisasi, baik kerugian yang bersifat materiel maupun imateriel, seperti hilangnya kepercayaan publik atau rusaknya citra organisasi tersebut di mata umum.

## G. Jalan Tengah Tata Kelola Informasi

Keseimbangan antara nilai tambah dan faktor biaya serta risiko adalah hal yang ingin dicapai dengan adanya implementasi tata kelola informasi. Tata kelola informasi berusaha memberikan aturan pengelolaan dan penanganan dokumen yang dimiliki oleh organisasi. Meskipun demikian, tidak ada satu rumus pasti pada implementasi tata kelola informasi. Tiap organisasi memiliki fungsi substantif dan fungsi fasilitatif yang khas sesuai dengan *core business*-nya masing-masing sehingga tidak ada satu pun regulasi tata kelola informasi yang bisa cocok diterapkan di segala tempat (Weber et al., 2009). Akan tetapi, ada beberapa hal yang dapat dilakukan oleh organisasi untuk menginisiasi penerapan tata kelola informasi di lingkungannya, yaitu pertama, mendeskripsikan organisasi dengan sejelas-jelasnya, mulai dari situasi terkini, model bisnis, dan implikasi yang diharapkan; dan kedua, melihat karakteristik organisasi dan sejauh mana budaya organisasi dapat memengaruhi desain tata kelola data atau informasinya (Weber et al., 2009).

Selain itu, penerapan tata kelola informasi di organisasi dapat diinisiasi dengan dua pendekatan, sebagaimana yang dikemukakan oleh Otto (2011), yaitu berbasis proyek atau bersifat dari bawah ke atas (*bottom-up*) dan bisa juga dimulai dengan cara yang lebih struktural dan konstitutif, yaitu pendekatan dari manajemen atas ke tingkat yang berada di subordinat atau bawahnya (*top-down*). Hal ini memberikan gambaran bahwa praktik tata kelola informasi dapat menyesuaikan dengan kondisi dan kebutuhan yang ada pada tiap organisasi sehingga yang paling dapat menentukan seperti apa pendekatan tata kelola informasi yang tepat untuk organisasinya adalah organisasi itu sendiri dengan melihat kaidah dan praktik tata kelola informasi.

Tidak bisa disangkal bahwa informasi memiliki nilai ekonomi, dengan catatan jika informasi tersebut digunakan secara tepat dan membantu tercapainya suatu tujuan. Namun, masih ada anggapan bahwa jika suatu organisasi sudah menghimpun dan menyimpan informasi, berarti organisasi tersebut sudah dianggap memiliki aset dalam bentuk informasi. Padahal pada praktiknya, diperlukan kerangka kerja yang dapat mengubah informasi menjadi sesuatu yang bernilai. Pemahaman ini berkembang dari proses pertambahan nilai melalui sistem informasi yang tepat. Sejalan dengan berkembangnya *microchip* dan komputer, muncul konsep tata kelola teknologi informasi yang kemudian berkembang pesat dalam menata dan mengelola teknologi informasi sebagai kontainer dari informasi. Dengan menyadari bahwa informasi yang menjadi roh dari proses tersebut, maka muncul diskursus tata kelola data hingga terus berkembang ke arah yang lebih komprehensif, yaitu tata kelola informasi. Praktik tata kelola informasi dapat memberikan jalan tengah antara manfaat yang bisa diambil dari pengelolaan informasi dengan tetap mempertimbangkan dan memitigasi faktor risiko dan biaya yang dapat muncul dari proses pengelolaan tersebut. Penulis berharap akan makin banyak diskusi mengenai praktik dan pelaksanaan tata kelola informasi di berbagai organisasi dan memunculkan studi-studi empiris mengenai hubungan tata kelola informasi dengan berbagai macam keluaran yang diharapkan oleh organisasi.

## Referensi

- Abraham, R., Schneider, J., & vom Brocke, J. (2019). Data governance: A conceptual framework, structured review, and research agenda. *International Journal of Information Management*, 49(7), 424–438. <https://doi.org/10.1016/j.ijinfomgt.2019.07.008>.
- Apriyanto, H. (2022). Analysis of information governance principal implementation in the management information system of Indonesian botanical gardens' plant collections data (Makoyana). *Jurnal Teknologi Komputer dan Sistem Informasi*, 5.

- Ballard, C., Compert, C., Jesionowski, T., Milman, I., Plants, B., Rosen, B., & Smith, H. (2014). Information governance principles and practices for a big data landscape. *IBM Information Management Software*, 280.
- Bennett, S. (2017). What is information governance and how does it differ from data governance? *Governance Directions*, September, 462–467.
- Borgman, H., Heier, H., Bahli, B., & Boekamp, T. (2016). Dotting the I and crossing (out) the T in IT governance: New challenges for information governance. Dalam T. X. Bui, & R. H. Sprague Jr. (Eds.), *Proceedings of the 49th Hawaii International Conference on System Sciences (HICSS) 2016* (4901–4909). IEEE Computer Society. <https://doi.org/10.1109/HICSS.2016.608>.
- Carter, D., & Sholler, D. (2015). Data science on the ground: Hype, criticism, and everyday work. *Journal of the American Society for Information Science and Technology*, 67(10), 2309–2319. <https://doi.org/10.1002/asi>.
- Chang, H. (2018). *An overview of data governance, information governance, and IT governance data, information, and IT as assets to be governed*. [https://informationscience.unt.edu/sites/default/files/overview\\_of\\_data\\_information\\_and\\_it\\_governance\\_chang.pdf](https://informationscience.unt.edu/sites/default/files/overview_of_data_information_and_it_governance_chang.pdf).
- Coffey, J. W. (2017). An analysis of inadvertent data disclosure incidents, 2005–2017. *International Journal of Cyber Security and Digital Forensics*, 6(2), 84–91. <https://doi.org/10.17781/p002272>.
- Davis, J., Mengersen, K., Bennett, S., & Mazerolle, L. (2014). Viewing systematic reviews and meta-analysis in social research through different lenses. *SpringerPlus*, 3(1), 1–9. <https://doi.org/10.1186/2193-1801-3-511>.
- Djafar, W. (2019). Perlindungan data pribadi di Indonesia: Lanskap, urgensi, dan kebutuhan pembaruan. *Jurnal Becoss*, 1(1), 147–154.
- Dormehl, L. (2015). *The formula: How algorithms solve all our problems... and create more*. Ebury Publishing.
- Eisenberg, M., & Dirks, L. (2008). Taylor's value-added model: Still relevant after all these years. *IConference, UCLA*, 4, 1–13.
- Foster, J. (2016). Towards an understanding of data work in context: Emerging issues of economy, governance, and ethics. *Library Hi Tech*, 34(2), 182–196. <https://doi.org/10.1108/LHT-12-2015-0121>.

- Foster, J., Clough, P., Court, R., & Street, P. (2018a). Embedded, added, cocreated: Revisiting the value of information in an age of data. *Journal of the Association for Information Science and Technology*, 69(5), 744–748. <https://doi.org/10.1002/asi.23987>.
- Foster, J., Mcleod, J., Nolin, J., & Greifeneder, E. (2018b). Data work in context: Value, risks, and governance. *Journal of the Association for Information Science and Technology*, 69(12), 1414–1427. <https://doi.org/10.1002/asi.24105>.
- Hagmann, J. (2013). Information governance: Beyond the buzz. *Records Management Journal*, 23(3), 228–240. <https://doi.org/10.1108/RMJ-04-2013-0008>.
- Horne, N. W. (1995). Information as an asset: The board agenda. *Computer Audit Update*, 1995(9), 5–11.
- IGI. (2014). *Information governance initiative annual report 2014: Information goes to work*. <https://iginitiative.com/wp-content/uploads/2014-IGI-Annual-Report.pdf>
- Janah, N., & Mayesti, N. (2020). Maturity model matrix of information governance in the Republic of Indonesia public television broadcasting institution: A technical note. *Australasian Accounting, Business and Finance Journal*, 14(1 special issue), 97–104. <https://doi.org/10.14453/aabfj.v14i1.10>.
- Khatri, V., & Brown, C. V. (2010). Designing data governance. *Communications of the ACM*, 53(1), 148–152. <https://doi.org/10.1145/1629175.1629210>.
- Khumon, P. (2021, 3–5 Maret 2021). *Overview of data and privacy protection in the ASEAN region* [Presentasi makalah]. US-Thailand Cybersecurity and Data Protection Standards Workshop (Acara virtual). <https://share.ansi.org/Shared%20Documents/U.S.-Thailand%20Cybersecurity%20and%20Data%20Protection%20Standards%20Workshop/Overview%20of%20Data%20and%20Privacy%20Protection%20in%20ASEAN,%20Office%20of%20Personal%20Data%20Protection%20Committee.pdf>
- Lomas, E. (2011). Information governance: Information security and access within a UK context. *Records Management Journal*, 20(2), 182–198. <https://doi.org/10.1108/09565691011064322>.

- Mikalef, P., Boura, M., Lekakos, G., & Krogstie, J. (2020). The role of information governance in big data analytics driven innovation. *Information and Management*, 57(7), 103361. <https://doi.org/10.1016/j.im.2020.103361>.
- Otto, B. (2011). Organizing data governance: Findings from the telecommunications industry and consequences for large service providers. *Communications of the Association for Information Systems*, 29(1), 45–66. <https://doi.org/10.17705/1cais.02903>.
- Sargunraj, N. (2020). Personal data protection in ASEAN. *Ethics*, 47, 4–9.
- Smallwood, R. F. (2014). *Information governance: Concepts, strategies and best practices*. John Wiley & Sons.
- Snyder, H. (2019). Literature review as a research methodology: An overview and guidelines. *Journal of Business Research*, 104(3), 333–339. <https://doi.org/10.1016/j.jbusres.2019.07.039>.
- Soares, S. (2012). *Big data governance: An emerging imperative*. MC Press.
- Susanawati, N., Astuti, R. S., Priyadi, B. P., & Afrizal, T. (2021). Tata kelola informasi peta zona nilai tanah pada kantor pertanahan Kota Semarang. *Perspektif*, 10(2), 345–351. <https://doi.org/10.31289/perspektif.v10i2.4463>.
- Tallon, P. P., Ramirez, R. V., & Short, J. E. (2013). The information artifact in IT governance: Toward a theory of information governance. *Journal of Management Information Systems*, 30(3), 141–178. <https://doi.org/10.2753/MIS0742-1222300306>.
- Taylor, R. S. (1986). *Value-added processes in information systems*. Ablex Publishing Corporation. <https://books.google.co.uk/books?id=y-bgAAAAMAAJ>.
- Torraco, R. J. (2016). Writing integrative literature reviews: Using the past and present to explore the future. *Human Resource Development Review*, 15(4), 404–428. <https://doi.org/10.1177/1534484316671606>.
- Tran, T. T. H., Childerhouse, P., & Deakins, E. (2016). Supply chain information sharing: Challenges and risk mitigation strategies. *Journal of Manufacturing Technology Management*, 27(8), 1102–1126. <https://doi.org/10.1108/JMTM-03-2016-0033>.
- Verizon. (2022). *Data breach investigations report 2022*. <https://www.verizon.com/business/resources/reports/2022/dbir/2022-data-breach-investigations-report-dbir.pdf>

- Wang, R. Y., Lee, Y. W., Pipino, L. L., & Strong, D. M. (1998). Manage your information as a product. *Sloan Management Review*, 39(4), 95–105. <http://libezproxy.open.ac.uk/login?url=http://search.ebscohost.com.libezproxy.open.ac.uk/login.aspx?direct=true&db=bth&AN=887820&scope=site>.
- Weber, K., Otto, B., & Österle, H. (2009). One size does not fit all: A contingency approach to data governance. *Journal of Data and Information Quality*, 1(1). <https://doi.org/10.1145/1515693.1515696>.
- Weill, P., & Ross, J. W. (2004). *IT governance: How top performers manage IT decision rights for superior results*. Harvard Business Review Press. <https://books.google.com.ec/books?id=0Gfraz7FyrYC>.