| NIHIL INSTRUMEN PENDUKUNG |

CELAH TERBUKA KEBOCORAN DATA

Lambatnya gerak pemangku kebijakan dalam menyusun instrumen teknis serta lembaga pengawas dinilai kian membuka celah kebocoran data yang sejatinya cukup menganga dalam beberapa tahun terakhir.

Aziz Rahardyan & Maria Elena
redaksi@bisnis.com

BISNIS Fokus

Persoalannya, meski tak memungkiri adanya risiko tersebut, pemerintah seolah minim aksi dalam merespons perangkat teknis pendukung UU No. 27/2022 tentang Pelindungan Data Pribadi atau PDP yang diterapkan 17 Oktober 2024.

Hal ini kemudian dinilai mereduksi efektivitas UU PDP sebagai instrumen penutup celah kebocoran data di Tanah Air.

Singkat kata, sepanjang lembaga khusus belum terbentuk dan aturan teknis belum dirilis, maka implementasi UU itu pun masih setengah hati.

Ruang terbukanya celah kebocoran data kian menganga, lantaran Kementerian Komunikasi dan Digital belum memberikan kepastian soal petunjuk teknis.

Jikalau regulasi teknis disusun dan Lembaga Penyelenggaraan Pelindungan Data Pribadi (LPPDP) dibentuk, implementasi dan operasional dari perangkat pendukung itu pun membutuhkan waktu yang tidak singkat.

Dengan kata lain, risiko bocornya data masyarakat masih cukup besar setidaknya hingga awal warsa mendatang.

Terlebih, Kepala Badan Siber dan Sandi Negara (BSSN) Hinsa Siburian, mengatakan bahwa penerapan UU PDP secara penuh membutuhkan kesiapan dari berbagai pemangku kepentingan.

Sejalan dengan itu, BSSN pun akan fokus meningkatkan pengamanan siber yang salah satunya mencegah kebocoran data masyarakat.

"Kami bersiap memperkuat sisi pengamanan ruang siber secara umum, termasuk infrastruktur dan data strategis. Selama ini, kami pun melengkapi yang diperlukan di sisi kami, baik berkaitan dengan kelengkapan peraturan, maupun pemenuhan standar-standar yang diperlukan," ujarnya kepada *Bisnis*.

Kesiapan implementasi UU PDP menjadi salah satu sorotan BSSN, mengingat laporan tahunan Lanskap Keamanan Siber Indonesia membuktikan tren respons atas pengiriman notifikasi dari Tim Pusat Kontak Siber BSSN masih jauh dari kata ideal.

Sepanjang 2023, BSSN mengirimkan 1.762 notifikasi indikasi insiden siber ke berbagai sektor. Namun, tercatat baru 755 notifikasi yang direspons pihak terkait, alias hanya 43%, tidak sampai separuhnya.

Berdasarkan jenis insiden, indikasi terbanyak berasal dari trafik anomali sebanyak 858 insiden, disusul data *breach* sebanyak 268 insiden, web *defacement* sebanyak 172 insiden, *sensitive data exposure* 113 insiden, dan *malicious software* 104 insiden.

Adapun, berdasarkan sektor yang mendapat notifikasi, tiga terbesar adalah administrasi pemerintahan sebanyak 980 notifikasi, teknologi informasi dan komunikasi (TIK) sebanyak 244 notifikasi, dan keuangan 146 notifikasi.

Terkhusus kasus dugaan kebocoran data, sepanjang 2023 BSSN mendeteksi 103 insiden.

Berdasarkan sektornya, administrasi pemerintahan menjadi tang terbanyak dengan 71 kasus, disusul keuangan dan lainnya yang masing-masing 12 kasus, dan sektor energi dan sumber daya mineral dengan 3 kasus.

Data Jumlah Akun yang Alami Kebocoran Data di Indonesia 5 Tahun Terakhir hingga Kuartal III/2024

Dari seluruh kasus indikasi kebocoran data tersebut, terdapat 60 *stakeholder* yang merespons notifikasi, serta 3 *stakeholder* yang melakukan tidak lanjut dan asistensi bersama BSSN.

Secara umum, tren sepanjang tahun lalu itu memang lebih baik dibandingkan dengan periode 2022. Kala itu, BSSN telah mengirimkan 1.433 notifikasi, tetapi hanya 126 notifikasi yang direspons.

Terbanyak adalah *web defacement* sebanyak 933 insiden, disusul data *breach* sebanyak 138 insiden. Terkhusus data *breach*, sepanjang 2022 BSSN mendeteksi 311 dugaan insiden data *breach* terhadap 248 *stakeholder*.

Namun, hanya terdapat 85 *stakeholder* yang merespons notifikasi, dan 35 *stakeholder* yang melakukan tidak lanjut dan asistensi bersama BSSN.

Selain data tersebut, sejatinya pemerintah juga bisa belajar dari pengalaman beberapa waktu lalu tatkala terjadi serangan siber terhadap Pusat Data Nasional Sementara (PDNS).

Hinsa menjelaskan, ketika aturan turunan dari UU PDP telah terbit dan lembaga terkhusus terbentuk, maka pemerintah memiliki landasan hukum kuat dalam rangka pengawasan dan penanganan kasus pelanggaran keamanan data, sampai penegakan hukum serta pemberian sanksi-sanksi kepada pelanggar.

> **Kami bersiap memperkuat sisi pengamanan ruang siber secara umum, termasuk infrastruktur dan data strategis.**

"Bagaimana aturan turunan, termasuk kaitannya dengan otoritas khusus dalam rangka pengawasan, tergantung kementerian terkait yang akan memimpin. Terpenting, kami bersiap, seluruh *stakeholder* juga harus siap," ujarnya.

EFEKTIVITAS TERBATAS

Sementara itu, Ketua Asosiasi Cloud Computing Indonesia (ACCI) Alex Budiyanto, menilai bahwa efektivitas dari implementasi UU No. 27/2022 masih terbatas dalam menangkal kebocoran data lantaran beberapa faktor.

Salah satunya, belum adanya LPPDP yang berperan sebagai pengawas dan penegak aturan, serta aturan turunan yang belum lengkap.

"Sanksi administratif dan teknis belum diatur secara detail, sehingga pelaku pelanggaran belum mendapatkan konsekuensi tegas," katanya.

Selain itu, menurutnya banyak perusahaan di Indonesia belum sepenuhnya siap menerapkan sistem keamanan data yang memadai karena pemahaman dan investasi pada teknologi pelindungan data yang minim.

Alex mengatakan, untuk memastikan UU PDP berjalan maksimal, lembaga pengawas atau otoritas pelindungan data harus dibentuk dan diberikan kewenangan yang jelas dalam mengawasi implementasi, menangani pelanggaran, serta memberikan sanksi.

Peraturan pelaksanaan terkait dengan sanksi administratif dan standar teknis juga harus segera dirilis agar regulasi dapat diterapkan dengan jelas dan konsisten.

Alex menambahkan, pemerintah juga harus menyediakan pelatihan dan edukasi kepada pelaku industri dan masyarakat, sehingga semua pihak paham atas kewajiban dan haknya.

"Implementasi yang efektif pun membutuhkan sinergi antara kementerian, regulator, dan sektor swasta untuk menghindari duplikasi regulasi dan konflik kepentingan," jelasnya.

Di sisi lain, Presiden Direktur Microsoft Indonesia Dharma Simorangkir, menyampaikan perusahaan berkomitmen mendukung implementasi UU PDP dan membantu pelaku bisnis untuk mempercepat upaya memenuhi kepatuhan dengan Microsoft Cloud.

Dharma mengatakan, Microsoft telah memperkenalkan Premium Assessment Template untuk UU PDP Indonesia di Microsoft Purview Compliance Manager.

"Panduan ini menguraikan ketentuan spesifik UU PDP dan memetakannya ke perangkat dan kontrol Microsoft, sehingga membantu organisasi untuk memenuhi kepatuhan dengan lebih cepat dan mudah," katanya.

Selain itu, bersama dengan EY Indonesia, Microsoft telah menerbitkan *white paper* yang memberikan gambaran umum komprehensif mengenai UU PDP dan ketentuan-ketentuan utamanya, serta rekomendasi mengenai cara mempraktikkan perlindungan data pribadi yang sejalan dengan UU PDP.

Dia menuturkan, di Indonesia, kepatuhan terhadap UU PDP bukan hanya sekadar kewajiban hukum, melainkan merupakan komitmen bagi seluruh pihak terkait untuk menjunjung tinggi privasi dan kepercayaan masyarakat. B