BAB V
PENUTUP

5.1 Kesimpulan

Penelitian ini telah berhasil membuktikan efektivitas metode *Open Source Intelligence (OSINT)* Hibrida, yang mengombinasikan teknik *Google Dorking* dan *Social Media Intelligence (SOCMINT)*, sebagai pendekatan investigasi yang sahih dan dapat direplikasi dalam konteks analisis kebocoran data sensitif perseorangan. Melalui tahapan sistematis mulai dari *Information Gathering*, *Processing*, hingga *Correlation*, penelitian ini menunjukkan bahwa OSINT mampu mengungkap data pribadi yang terekspos secara pasif maupun aktif di ruang publik digital.

Jenis data yang paling sering ditemukan dalam kebocoran meliputi tanggal lahir, alamat rumah, nomor telepon, serta riwayat pendidikan. Data ini sebagian besar berasal dari dokumen lama yang terindeks mesin pencari tanpa perlindungan privasi, serta unggahan media sosial yang tidak dikonfigurasi dengan baik. Temuan ini menegaskan bahwa jejak digital pasif merupakan sumber kebocoran utama, karena individu sering kali tidak menyadari bahwa informasi yang pernah mereka unggah tetap dapat diakses publik dalam jangka panjang.

Korelasi data yang dilakukan membuktikan bahwa meskipun hanya berawal dari informasi sederhana, pihak yang tidak bertanggung jawab dapat menyusun profil digital yang lengkap dan meyakinkan. Profil ini berpotensi digunakan untuk serangan *doxing*, *identity theft*, maupun penipuan berbasis rekayasa sosial (*social engineering*). Dengan demikian, penelitian ini menyimpulkan bahwa perlindungan data pribadi masih menjadi tantangan yang serius, baik dari sisi regulasi maupun kesadaran masyarakat. Mekanisme perlindungan yang ada belum sepenuhnya mampu mengantisipasi ancaman OSINT, sehingga diperlukan peningkatan literasi digital dan penguatan regulasi agar risiko kebocoran data dapat diminimalkan.

5.2 Saran

Berdasarkan hasil penelitian dan simulasi kebocoran data, rekomendasi yang diajukan dibagi menjadi dua kategori utama: aplikasi praktis dan arah akademik.

A. Aplikasi Praktis

1. Individu perlu melakukan audit jejak digital (*self-dorking)* secara berkala dengan memanfaatkan teknik sederhana seperti *Google Dorking*, untuk memastikan tidak ada file sensitif yang terindeks publik.
2. Pemerintah dan lembaga terkait harus memperkuat kampanye literasi digital, menekankan bahaya pengunggahan dokumen identitas ke platform daring tanpa pengaturan privasi. Edukasi ini harus menyasar masyarakat umum, pelajar, hingga pegawai instansi agar kesadaran kolektif meningkat.
3. Organisasi dan perusahaan disarankan untuk menerapkan prosedur audit internal terhadap data yang disimpan di layanan cloud, serta memastikan kebijakan privasi dan keamanan sesuai dengan standar internasional seperti ISO/IEC 27001.

B. Arah Akademik

1. Penelitian selanjutnya dapat membandingkan efektivitas metode OSINT Hibrida manual dengan framework OSINT otomatis seperti *Maltego* atau *theHarvester*, guna mengukur tingkat akurasi, kecepatan, dan skalabilitas proses korelasi data.
2. Perluasan penelitian dapat diarahkan pada integrasi OSINT dengan *machine learning* dan *big data analytics*, sehingga deteksi kebocoran data dapat dilakukan secara lebih adaptif dan *real-time*.
3. Studi lanjutan juga dapat menguji penerapan OSINT dalam konteks lingkungan korporasi, misalnya untuk mendeteksi kebocoran data internal atau mengukur risiko keamanan informasi perusahaan.

Dengan demikian, saran yang diberikan tidak hanya relevan bagi masyarakat dan regulator, tetapi juga membuka ruang pengembangan akademik yang lebih luas. Penelitian ini diharapkan dapat menjadi pijakan awal bagi kajian-kajian berikutnya yang berfokus pada perlindungan data pribadi, keamanan digital, dan mitigasi ancaman berbasis OSINT.