Pemateri : Deska Agriana Permatasari, S.H., M.Kn. & Sandi Kurniawan, S.H.

Peserta : Hakim, Panitera, Panmud Perkara, Panmud Hukum, dan Pranata Komputer PTUN Kupang

Jalannya Kegiatan :

Kegiatan dibuka oleh Pemateri, kemudian dilanjutkan dengan pemaparan materi sebagai berikut :

A. Pembukaan Kegiatan:

1. Acara sosialisasi dibuka secara resmi, dilanjutkan dengan penyampaian pengantar oleh narasumber;
2. Sosialisasi ini merupakan kewajiban pasca keikutsertaan Bimbingan Teknis (Bimtek) yang diselenggarakan pada hari Rabu hingga Jumat;
3. Disampaikan bahwa peralihan sistem peradilan dari metode konvensional ke persidangan elektronik (*e-Court* dan *e-Litigation*) menuntut adanya pemahaman mendalam terkait keamanan siber dan hukum siber (*cyber law*) untuk melindungi data elektronik instansi maupun masyarakat;

B. Pemaparan Materi Pertama : Persidangan Elektronik (e-Court):

1. Diperlukan harmonisasi aturan pelaksanaan *e-Court* agar sejalan dengan pedoman Hukum Acara Peradilan Tata Usaha Negara;
2. Majelis Hakim agar menyampaikan kepada pihak yang berperkara bahwa di PTUN tidak dilakukan verifikasi terhadap bukti surat yang diunggah para pihak di e-Court. Hal ini untuk mencegah pihak lawan mengakses bukti tersebut sebelum waktunya, mengingat fitur *disclaimer box* pada sistem dirasa kurang cukup untuk mencegah penyalahgunaan data;
3. Sering ditemukan kendala teknis berupa kesalahan atau pengunggahan berulang oleh pihak berperkara. Oleh karena itu, muncul usulan pengadaan fitur edit atau hapus bukti di dalam sistem *e-Court*;

4. Terdapat perbedaan penafsiran terkait pemeteraian kemudian (*nazegelen*) untuk alat bukti elektronik berupa video atau rekaman dalam media penyimpanan (CD/Flashdisk). Mengacu pada UU Bea Meterai, bukti berupa rekaman tersebut dimungkinkan untuk tidak memerlukan pemeteraian kemudian;
5. Disoroti perlunya penambahan fitur notifikasi catatan persidangan di *e-Court* serta keseragaman praktik antar Majelis Hakim terkait keharusan penyerahan dokumen fisik asli di luar *e-Court*;

C. Pemaparan Materi Kedua : Keamanan Siber (*Cyber Security*):

1. Pengamanan data harus berpegang teguh pada tiga prinsip: Kerahasiaan (*Confidentiality*), Integritas (*Integrity*), dan Ketersediaan (*Availability*);
2. Seluruh aparatur diimbau menjalankan kebiasaan pengamanan dasar: menggunakan *password* yang kuat, mengaktifkan otentikasi dua faktor (MFA), mengunci layar perangkat, dan tidak membagikan kredensial kepada pihak mana pun;
3. Anonimitas identitas para pihak, saksi, dan ahli yang memuat data pribadi sensitif wajib diterapkan secara ketat dalam unggahan putusan pengadilan;
4. Penggunaan Tanda Tangan Elektronik (TTE) merupakan tanggung jawab mutlak pemiliknya. Penyerahan sandi maupun OTP kepada orang lain atau staf adalah tindakan pelanggaran keamanan siber yang tidak dibenarkan;
5. Mahkamah Agung didorong untuk menyediakan *cloud services* yang independen dan mengatur mekanisme pelacakan jejak digital (*audit trail*) di *e-Court* maupun SIPP demi akuntabilitas penanganan data;

D. Pemaparan Materi Ketiga : Hukum Siber (*Cyber Law*):

1. Dokumen elektronik sah sebagai alat bukti sesuai UU ITE, namun harus dipastikan lolos dari empat uji utama: Autentisitas, Integritas, Relevansi, dan Legalitas;