**Conceitos básicos sobre Dados Pessoais:**

**Dados pessoais:** informações que identifiquem directa ou indirectamente, ou possam ser usados para identificar, um indivíduo como o nome, apelido, número de identificação, endereço (de forma directa) ou de forma indirecta os dados que descrevem atributos físicos ou fisiológicos específicos, biométricos, ou características culturais ou sociais ou económicas.

**Dados sensíveis:** dados pessoais acerca da origem racial ou étnica; estado de saúde física ou mental; orientação sexual; opiniões/crenças políticas, religiosas ou filosóficas; registro criminal; dados biométricos.

**Dados biométricos:** características físicas, fisiológicas ou comportamentais exclusivas que podem ser autenticados digitalmente para identificar um indivíduo.

Por exemplo: fotos, íris scan, impressões digitais

**O que é violação de dados?**

As violações de dados, ou vazamento de dados, são definidas como incidentes que ferem o sigilo ou a integridade de informações sensíveis ou privadas. Geralmente, isso acontece quando os dados colectados, armazenados e tratados pela empresa são alvos de ataques cibernéticos ou acedidos por pessoas não autorizadas.

As informações vazadas podem estar relacionadas a dados pessoais, médicos, financeiros, entre outros que possam identificar e gerar transtornos para os seus titulares.

Nos casos de violação de dados pessoais, eles podem ser usados em diversas práticas criminosas, como roubo de identidade e fraudes, o que gera consequências e transtornos para os proprietários das informações e, consequentemente, punições para as empresas que deveriam ter zelado pela protecção dos dados.

**Quais os riscos e as consequências da exposição de dados pessoais na internet?**

Dados pessoais podem ser usados para fraudes de identidade, especialmente, mas também por agentes mal intencionados que estejam interessados em proteger alguém. Também podem ser usados para *perseguir/chantagear* uma pessoa, ou até para criar provas falsas contra alguém.

**Como evitar o vazamento de dados**

1. Usar firewall forte.
2. Usar senhas complexas.
3. Usar antivírus de qualidade.
4. Fazer backup regularmente.
5. Usar certificados digitais.
6. Manter softwares e programas actualizados;
7. Proteger dispositivos móveis.
8. Use protecções em sistemas de nuvem.

**Correspondência**

Departamento de Protecção de Dados
A/C: Délcia Nhantumbo
Rua José Mateus, No. 437
Cidade de Maputo