

Europol pede leis de dados mais fortes para combater o crime cibernético

Data: 2025-10-07 08:45:01

Autor: Inteligência Against Invaders

Os criminosos estão explorando criptografia, anonimização e novas tecnologias mais rapidamente do que os reguladores e as autoridades podem se adaptar, criando um desafio crítico no acesso a dados para investigações.

Este aviso foi proferido na 4ª Conferência Anual de Crimes Cibernéticos da Europol 2025, realizada na semana passada na sede da Europol em Haia.

O evento reuniu cerca de 500 participantes de todo o mundo para examinar um dos dilemas centrais na aplicação da lei moderna: como equilibrar o acesso legal aos dados com a proteção da privacidade e dos direitos digitais.

“Na Conferência de Crimes Cibernéticos deste ano, estamos enfrentando um dos dilemas definidores do nosso tempo: os dados como impulsionadores da inovação e a força vital da criminalidade moderna”, disse a diretora executiva da Europol, Catherine De Bolle.

“Quando as evidências digitais permanecem fora de alcance, as crianças não são identificadas, os planos terroristas avançam sem serem detectados e o crime organizado prospera nas sombras.”

Comissária da UE apela a uma cooperação reforçada

Magnus Brunner, comissário europeu para assuntos internos e migração, fez o discurso principal, enfatizando a urgência de uma resposta europeia coordenada.

“O crime cibernético não conhece fronteiras”, disse Brunner.

“Para proteger as pessoas e as empresas na UE, devemos integrar a segurança em todas as nossas políticas, fortalecer o mandato da Europol e garantir o acesso legal aos dados.”

Sob o tema “Dissecando os desafios de dados nas linhas de frente digitais”, o evento de dois dias explorou como o crescente volume de informações digitais está remodelando as investigações de crimes cibernéticos e os debates regulatórios.

[Leia mais sobre as iniciativas de crimes cibernéticos e estratégias de acesso a dados da Europol: Europol cria força-tarefa “Violência como serviço”](#)

Principais questões e operações destacadas

Os delegados examinaram cinco áreas críticas que moldam o cenário cibernético atual:

1.

Equilibrando acesso e privacidade na vida diária e estratégia global

2.

Melhorar a partilha de dados transfronteiras através de parcerias

3.

Atualizando as leis para corresponder à rápida mudança tecnológica

4.

Promoção da diplomacia cibernética entre governos e indústria

5.

Desenvolvimento de estratégias de prevenção baseadas em tecnologias emergentes

A conferência apresentou estudos de caso como a Operação Eastwood, que [interrompeu a atividade hacktivista pró-Rússia](#) visando a infraestrutura europeia e a Operação Ratatouille, que levou à prisão de um suposto administrador de uma importante plataforma de crimes cibernéticos de língua russa.

Fortalecimento da resiliência digital

A conferência seguiu um workshop com as Equipes Nacionais de Resposta a Incidentes de Segurança Informática (CSIRTs), co-organizado com a Agência da União Europeia para Segurança Cibernética (ENISA).

A sessão enfatizou a cooperação técnica e o compartilhamento de informações entre órgãos nacionais e europeus.

Agora em seu quarto ano, a Conferência de Crimes Cibernéticos da Europol tornou-se um espaço para formuladores de políticas, investigadores e representantes da indústria trocarem perspectivas sobre ameaças cibernéticas, estruturas legais e as implicações mais amplas do acesso a dados em um mundo interconectado.