



MINISTÉRIO PÚBLICO
PORTUGAL

PROCURADORIA-GERAL DA REPÚBLICA
PROCURADOR-GERAL

Conferência Cibersegurança e Transparência – Fraudes Digitais

Sessão de abertura

É com muito gosto que participo na abertura desta conferência dedicada à “Cibersegurança e Transparência – Fraudes Digitais”, um tema particularmente atual e relevante, que exige uma reflexão séria, informada e necessariamente multidisciplinar.

Permitam-me começar com uma breve nota sobre o local onde hoje nos encontramos. O facto de esta conferência se realizar em Bragança, no interior do país, tem um significado especial. A reflexão sobre os grandes desafios da justiça, da tecnologia e da segurança digital não deve ficar confinada aos grandes centros urbanos. Pelo contrário, é importante que este debate aconteça em todo o território, aproximando instituições e conhecimento das diferentes regiões do país. A transformação digital tem de envolver e convocar todos os cidadãos, independentemente do local onde vivem; também por isso é particularmente simbólico que este encontro tenha lugar aqui.

A progressiva digitalização da economia, dos serviços públicos, do trabalho e até da forma como nos relacionamos trouxe benefícios inegáveis. A tecnologia permitiu ganhos significativos em termos de eficiência, rapidez e acessibilidade. Aproximou pessoas e instituições e tornou possível realizar, à distância e em poucos instantes, operações que há poucos anos exigiam tempo, deslocações e múltiplos intermediários.

Vivemos hoje num mundo profundamente digitalizado, em que grande parte das atividades da vida quotidiana passa, direta ou indiretamente, por alguma forma de intermediação tecnológica.



Mas esta evolução trouxe também novas vulnerabilidades e abriu espaço a formas de criminalidade cada vez mais sofisticadas. A mesma infraestrutura tecnológica que permite inovação e conectividade global pode ser utilizada por redes criminosas organizadas para desenvolver esquemas de fraude em larga escala, atingir simultaneamente milhares de potenciais vítimas e explorar fragilidades técnicas, institucionais ou humanas.

Uma dessas fragilidades prende-se com a dificuldade que a generalidade dos cidadãos ainda tem em distinguir conteúdos digitais legítimos de conteúdos fraudulentos. A isto acresce, em vários segmentos da população, um nível ainda insuficiente de literacia digital. Este conjunto de fatores cria um contexto particularmente favorável ao surgimento de novas modalidades de criminalidade, muitas vezes dirigidas precisamente às pessoas mais vulneráveis.

Estas novas formas de criminalidade proporcionam novas dimensões de exploração das vítimas: económicas, psicológicas e sociais. Esta exploração cresceu exponencialmente nos últimos anos.

Para muitas pessoas, estas situações representam não apenas perdas patrimoniais significativas, mas também sentimentos de insegurança, de exposição e, por vezes, de vergonha ou isolamento.

É por isso particularmente importante que, neste debate, a vítima permaneça no centro da nossa atenção. O trabalho desenvolvido por organizações da sociedade civil que prestam apoio às vítimas de crime, designadamente associações especializadas neste domínio, desempenha um papel essencial no acolhimento, no acompanhamento e na orientação das pessoas que se encontram em situações de grande vulnerabilidade. A articulação entre estas estruturas, as autoridades de investigação e as restantes instituições públicas constitui um elemento fundamental para garantir uma resposta mais completa e mais humana a estes fenómenos.



A resposta a estes fenómenos não pode ser pensada apenas a partir do sistema de justiça. A prevenção eficaz das fraudes digitais exige a participação ativa de outros atores institucionais e económicos.

Neste domínio, os reguladores desempenham um papel particularmente relevante. As entidades responsáveis pela supervisão de setores como as comunicações, o sistema financeiro ou o mercado digital dispõem de instrumentos que lhes permitem atuar a montante do problema, através da definição de padrões de segurança, da monitorização de práticas de mercado e da promoção de mecanismos de cooperação institucional.

Ao mesmo tempo, os operadores privados — nomeadamente nos setores das telecomunicações, da banca e das plataformas digitais — encontram-se muitas vezes na primeira linha da deteção destas fraudes. São estas entidades que lidam, diretamente, com os fluxos de comunicação e com as transações financeiras, onde muitas destas atividades ilícitas se manifestam. A sua capacidade para desenvolver sistemas de monitorização, mecanismos de alerta precoce e soluções tecnológicas de prevenção é, por isso, absolutamente decisiva.

A cooperação entre autoridades judiciais, reguladores e operadores privados assume, assim, uma importância crescente. A partilha de informação, a articulação institucional e o desenvolvimento de estratégias conjuntas de prevenção podem fazer uma diferença muito significativa na capacidade de resposta das instituições.

A lei é, em última análise, o principal instrumento de que o Estado dispõe para responder aos riscos associados à digitalização da sociedade e ao crescimento de fenómenos criminais praticados por grupos cada vez mais organizados, que recorrem a infraestruturas tecnológicas complexas e que operam frequentemente em contextos transnacionais.

Importa, por isso, refletir sobre a adequação dos instrumentos legais de que dispomos. Diplomas fundamentais – como o Código Penal, o Código de Processo Penal, a Lei do



Cibercrime ou os regimes de recuperação de ativos – foram concebidos em contextos muito diferentes do atual, ainda que tenham sido objeto de sucessivas adaptações. A questão que se coloca é saber se estas adaptações têm sido suficientes para acompanhar a evolução dos fenómenos criminais que hoje enfrentamos.

O Ministério Público tem procurado assumir um papel proativo na identificação de regimes jurídicos que carecem de atualização ou aperfeiçoamento. Foram apresentados contributos no âmbito das propostas de reforma do processo penal, designadamente no que respeita à recolha e preservação de prova digital, uma matéria cada vez mais relevante nas investigações relacionadas com criminalidade informática e económica. Foram também formuladas observações relativamente a algumas soluções constantes do projeto legislativo, destinado a transpor a recente diretiva da União Europeia sobre confisco. Tais propostas poderão, no nosso ponto de vista, contribuir para assegurar uma maior eficácia dos mecanismos de recuperação de ativos.

Perante estes desafios, o papel da justiça e das autoridades de investigação criminal é fundamental. Cabe-lhes investigar, responsabilizar os autores e assegurar que o direito continua a cumprir a sua função essencial: proteger os cidadãos e garantir a segurança jurídica num contexto social em rápida transformação.

A conferência que hoje iniciamos insere-se, precisamente, num esforço coletivo de reflexão e de resposta. Ao reunir magistrados, órgãos de polícia criminal, académicos, reguladores, especialistas tecnológicos, representantes do setor financeiro e das comunicações, bem como organizações de apoio às vítimas, pretendemos criar um espaço particularmente importante de diálogo e cooperação entre diferentes áreas de conhecimento e diferentes responsabilidades institucionais.

Estou certo de que o debate que aqui terá lugar contribuirá para aprofundar o nosso entendimento destes fenómenos e para identificar caminhos que reforcem a capacidade das instituições em prevenir, investigar e responder às fraudes digitais que hoje desafiam as nossas sociedades.



MINISTÉRIO PÚBLICO
PORTUGAL

PROCURADORIA-GERAL DA REPÚBLICA
PROCURADOR-GERAL

Porque a segurança no espaço digital não é apenas uma questão tecnológica. É, antes de mais, uma questão de confiança pública e de proteção dos cidadãos.

E proteger essa confiança — no mundo digital como no mundo físico — continua a ser uma responsabilidade essencial do Estado de direito.

Desejo a todos, por isso, uma excelente conferência e um debate profícuo.

Bragança, 12 de março de 2026

O Procurador-Geral da República
Amadeu Guerra