VIII Congresso Internacional

Direitos Fundamentais e Processo Penal na Era Digital

Painel 2 | Inteligência Artificial, Dataveillance e Justiça Criminal

Vinícius Gonçalves (Núcleo de Direito, Internet e Sociedade)

O avanço da tecnologia e o uso de sistemas de Inteligência Artificial (IA) no âmbito da justiça criminal trouxeram novas questões éticas, jurídicas e técnicas que desafiam os operadores do Direito e os formuladores de políticas públicas. No Painel 2 do evento, intitulado “Inteligência Artificial, Dataveillance e Justiça Criminal”, as especialistas Jamilla Sarkis (PUC/MG), Keity Saboya (UFRN/TJRN) e Thallita Lima (CESeC) discutiram os impactos dessas ferramentas no campo da vigilância e da investigação criminal, destacando a urgência de regulamentação e governança adequadas.

Abrindo os trabalhos, Keity Saboya, juíza de direito e professora da UFRN, trouxe à tona a relevância dos metadados no contexto contemporâneo da vigilância. Enfatizou que tratar apenas de terminologias como surveillance, dataveillance, vigilância, sinóptico e panóptico esvazia o debate, porque a leitura contextualizada de dados sensíveis deve prevalecer. Enquanto o controle estatal clássico focava na interceptação de conteúdo, como telefonemas e mensagens, o cenário atual evidencia a importância das informações periféricas, como quem se comunica com quem, quando e onde. Saboya explicou que essas informações aparentemente inofensivas podem revelar detalhes íntimos sobre a vida das pessoas, sendo tão sensíveis quanto o conteúdo protegido. Adiante, fez uma analogia simples e poderosa: “o conteúdo da carta está protegido, mas o envelope, que contém informações como remetente e destinatário, também deveria ser”. Citando experimentos da década de 1990, como o projeto ‘Metaphone’, Saboya demonstrou como padrões simples de dados podem revelar informações sensíveis, como doenças e decisões pessoais, ressaltando a urgência de estender as proteções legais para os metadados.

Jamilla Sarkis, doutora em Direito pela PUC/MG, levantou uma questão crucial: o que acontece com os dados apreendidos em investigações criminais após

o término dos processos? Descrevendo esse estado como um “limbo jurídico”, Sarkis destacou a ausência de normas claras no Brasil para o tratamento e descarte de dados digitais, em contraste com a regulamentação de vestígios físicos, como armas ou documentos.

Segundo a especialista, os dados digitais têm características únicas — são maleáveis, voláteis e não perecíveis —, o que exige diretrizes específicas para evitar abusos. Ela citou padrões internacionais, como os definidos pelo NIST (EUA), que incluem métodos como a limpeza (remoção de dados por software), a purgação (armazenamento temporário) e a destruição definitiva. Além disso, Sarkis enfatizou a necessidade de uma governança estruturada para garantir segurança, fiscalização e documentação adequada em todas as etapas da cadeia de custódia.

Thallita Lima, coordenadora de pesquisa no Centro de Estudos de Segurança e Cidadania (CESeC), abordou as implicações éticas e sociais da expansão de sistemas de reconhecimento facial no Brasil. Dados apresentados por ela indicam que 79 milhões de cidadãos estão sob potencial vigilância, com 313 projetos de reconhecimento facial em andamento no país. Lima apontou a falta de transparência na contratação dessas tecnologias, muitas vezes realizadas sem avaliação prévia de impacto ou regulamentação.

Para a pesquisadora, o uso indiscriminado de ferramentas como o reconhecimento facial pode exacerbar desigualdades sociais e discriminações, especialmente em um contexto onde essas tecnologias são frequentemente direcionadas a comunidades vulneráveis. Lima citou a necessidade de analisar as escolhas políticas por trás dessas aquisições, questionando por que o investimento é priorizado em vigilância, e não em áreas como educação e saúde.

Inspirando-se na citação Deleuze, Lima afirmou que as máquinas não operam de forma neutra e precisam ser analisadas em seus contextos sociais e políticos. “As máquinas, por si só, não explicam nada. Elas refletem escolhas humanas e políticas, e precisamos compor junto a elas com reflexão crítica”, concluiu.

O Painel 2 destacou um ponto crucial: a tecnologia sozinha não resolve os desafios do sistema de justiça, sendo necessário um equilíbrio entre inovação, ética e governança. Desde a proteção de metadados até o descarte de vestígios digitais e

o uso de tecnologias de vigilância em massa, as exposições apontaram para a necessidade de regulamentações claras, que respeitem os direitos fundamentais e garantam a transparência.

Mais do que uma discussão técnica, o debate sobre IA e vigilância é também uma questão política e social, que exige reflexão coletiva sobre o tipo de sociedade que queremos construir. A implementação de novas tecnologias precisa estar alinhada a princípios democráticos, protegendo a privacidade e os direitos individuais, ao mesmo tempo em que fortalece a eficiência e a equidade no sistema de justiça criminal.