

Impactos da nova decisão sobre interceptação telefônica e provas digitais

O EncroChat foi um provedor de serviços de comunicação que, supostamente, era utilizado por organizações criminosas para planejar atividades ilícitas. Entre junho e julho de 2020, a plataforma foi infiltrada pela polícia durante uma operação simultânea em diversos países europeus, sem autorização judicial adequada, caracterizando abuso e ilegalidade.

O serviço funcionava em dispositivos Android com funcionalidades como GPS, câmera e microfone permanentemente desativadas, dificultando a geolocalização e a coleta de provas periciais. O EncroChat oferecia um aplicativo de mensagens criptografadas que roteava comunicações por um servidor central. Havia também um “botão de pânico” que, ao ser ativado por um PIN específico, apagava automaticamente todos os dados do dispositivo.

A descoberta do sistema criptografado ocorreu em 2017 pela Gendarmerie francesa, que apreendeu dispositivos durante operações contra o crime organizado. Posteriormente, com o apoio técnico da Agência Nacional de Crimes, autoridades francesas e holandesas conseguiram interceptar mensagens através de um “dispositivo técnico” inserido nos servidores do EncroChat na França. Esses dados foram distribuídos pela Europol e utilizados para identificar suspeitos ao analisar milhões de mensagens e imagens.

Em 20 de dezembro de 2024, a 25ª Câmara Criminal do Tribunal Regional de Berlim proferiu uma decisão marcante: um réu foi absolvido em um processo baseado exclusivamente em dados do EncroChat. O tribunal concluiu que a coleta e o compartilhamento desses dados violaram legislações nacionais e europeias, incluindo normas sobre interceptação telefônica e cadeia de custódia de provas digitais, além de infringir direitos fundamentais e constitucionais.

Parâmetros para legalidade do uso de dados

O Tribunal de Justiça da União Europeia (TJUE) já havia estabelecido parâmetros essenciais para a legalidade do uso de tais dados, que foram seguidos pelo Tribunal de Berlim. A decisão ressaltou que a defesa foi prejudicada, pois as autoridades não forneceram informações detalhadas sobre a coleta de dados ou os arquivos completos da investigação. O TJUE destacou a necessidade de apresentar o material bruto e originário para assegurar um julgamento justo.

Além disso, o tribunal berlinense considerou injustificado o monitoramento indiscriminado de todos os usuários da plataforma, caracterizando o ato como abusivo e ilegal. O TJUE sugeriu que investigações mais direcionadas contra suspeitos específicos ou operadores das plataformas, como EncroChat e Sky ECC, poderiam ter sido realizadas em vez de uma vigilância em massa.

A decisão reforça os limites da vigilância estatal e a importância dos direitos fundamentais na era digital. O Tribunal de Berlim reiterou que a proteção jurídica prevista no artigo 31º da Diretiva 2014/41 da União Europeia é crucial em casos envolvendo dados de telecomunicações coletados transnacionalmente. Segundo o TJUE, um país que solicita dados de outro deve garantir que os direitos fundamentais dos cidadãos sejam preservados de forma equivalente à proteção oferecida em seu próprio território.

Falta de proporcionalidade em abordagem de autoridades

A decisão destaca a falta de proporcionalidade e subsidiariedade na abordagem das autoridades no caso EncroChat, bem como em operações similares, como Sky ECC. Não foi comprovada a razoabilidade de considerar todos os usuários da plataforma como suspeitos de crimes graves ou de que não havia alternativas menos invasivas para obtenção de provas.

Embora a decisão escrita ainda não tenha sido publicada, o parecer oral sugere que o artigo 31º desempenhou um papel central na fundamentação. Isso pode influenciar outros processos envolvendo





provas digitais baseadas em plataformas criptografadas na União Europeia e, possivelmente, em outras jurisdições, como o Brasil.

Essa decisão representa um marco para o Estado de Direito na Europa, enfatizando o equilíbrio entre segurança e liberdades civis. Ela aponta para a necessidade de investigações que respeitem os direitos fundamentais, especialmente em casos que envolvem provas digitais obtidas de forma controversa. Esse precedente pode servir de exemplo para outros países que enfrentam desafios semelhantes no combate ao crime organizado na era digital.

Fonte: <https://conjur.jumps.com.br/2024-dez-30/impactos-da-nova-decisao-sobre-interceptacao-telefonica-e-provas-digitais/>