Alemanha limita uso de spyware policial a crimes graves

Data: 2025-08-09 09:27:11

Autor: Inteligência Against Invaders

Alemanha limita uso de spyware policial a crimes graves

O principal tribunal da Alemanha decidiu que a polícia pode usar spyware apenas para crimes puníveis com pelo menos três anos de prisão.

O principal tribunal da Alemanha decidiu que a polícia só pode usar spyware para monitorar dispositivos em casos envolvendo crimes com pena máxima de pelo menos três anos.

“A interferência tanto no direito fundamental de proteção dos sistemas informáticos como no artigo 10.º, n.º 1, da Lei Fundamental, causada pela vigilância das telecomunicações de origem nos termos do § 100a(1) segunda frase do Código de Processo Penal, não pode ser justificada na medida em que essa vigilância das telecomunicações de origem seja permitida para a investigação de atos criminosos que acarretam uma pena máxima de prisão de três anos ou menos e, portanto, se enquadram na categoria de criminalidade básica.” afirma o tribunal superior da Alemanha.

O principal tribunal da Alemanha analisou um caso da Digitalcourage desafiando as regras de 2017 que permitem que a polícia use spyware para espionar bate-papos e mensagens criptografadas.

Os demandantes argumentaram que as regras permitiam que o spyware monitorasse as comunicações criptografadas de indivíduos que não estavam sob investigação. O tribunal concordou, restringindo seu uso a casos graves.

O principal tribunal da Alemanha decidiu que uma mudança de 2017 no código de processo penal carecia de clareza sobre quando o spyware poderia ser usado. Ele determinou que tais ferramentas são apropriadas apenas para investigar crimes graves e podem expor os cidadãos a atividades de vigilância que representam uma intrusão “muito grave” na privacidade. A decisão limita o uso de software de vigilância, que pode monitorar comunicações criptografadas, para casos que atendam a um alto limite de gravidade criminal.

“Quando considerada em uma avaliação geral, a vigilância de telecomunicações de origem causa uma interferência muito grave tanto no Art.10 (1) da Lei Básica quanto no direito fundamental de proteção dos sistemas de TI. A forma e o âmbito da recolha de dados, que ocorre de forma dissimulada e através da evasão directa dos mecanismos de segurança, intensificam, por si só, a ingerência nos direitos fundamentais, uma vez que a vigilância das telecomunicações de origem permite o acesso a registos de dados que, em termos de volume e variedade, podem exceder em muito as fontes tradicionais de informação. A vigilância de telecomunicações de origem permite a interceptação e análise de todos os dados brutos trocados e, portanto, tem um alcance excepcional, particularmente dadas as realidades da tecnologia da informação moderna e sua importância para

as relações de comunicação", conclui o comunicado. "Os dados que podem ser interceptados não apenas carregam uma grande variedade de tipos de comunicações eletrônicas, que podem ser analisadas. Dada a utilização ubíqua e diversificada dos sistemas informáticos, todas as formas de actividade dos indivíduos e de interacção humana reflectem-se cada vez mais nos sinais electrónicos e, por conseguinte, tornam-se acessíveis através da vigilância das telecomunicações de origem, em particular. Além disso, a integridade de um sistema de TI é afetada negativamente e sua confidencialidade está em risco."

Siga-me no Twitter:@securityaffairseLinkedineMastodonte

PierluigiPaganini

(Assuntos de Segurança–hacking,spyware)