II CONDITEC
CONGRESSO INTERNACIONAL DE DIREITO E TECNOLOGIA

ADMISSIBILIDADE DO MALWARE COMO MEIO DE OBTENÇÃO DE PROVA NO PROCESSO PENAL PORTUGUÊS

Congresso Internacional de Direito e Tecnologia, 2ª edição, de 06/06/2022 a 09/06/2022
ISBN dos Anais: 978-65-81152-63-5

LARANJINHO; Sérgio Manuel Maneiras Laranjinho [1]

RESUMO

Introdução Se as tecnologias de informação trouxeram inegáveis benefícios para o desenvolvimento cultural, social e económico, a verdade é que vieram também permitir que a criminalidade no ambiente digital se desenvolvesse a um ritmo alarmante, ritmo esse que o Direito tem, por natureza, dificuldade em acompanhar. O rápido e constante progresso e desenvolvimento tecnológico que se tem verificado nas últimas décadas coloca, cada vez mais, problemas práticos ao nível da investigação criminal, tornando mais complexa a recolha e a valoração dos meios de prova, nomeadamente no que diz respeito às atividades criminais que se têm vindo a desenvolver no espaço digital. A utilização de *malware* enquanto meio de obtenção de prova possibilita, genericamente, a observação e vigilância em tempo real e a cópia dos dados presentes no sistema informático em causa. O presente estudo centra-se no tema da investigação criminal em ambiente digital, nomeadamente sobre a eventual possibilidade de utilização de *malware* como meio oculto de obtenção de prova. O problema que nos propusemos tratar resulta, assim, da conjugação de duas questões essenciais: (1) pode o *malware* ser utilizado em processo penal? (2) com que pressupostos e limitações? **2. Objetivo(s)** Pretendemos com o presente estudo procurar saber se existe já base legal para fundamentar o recurso a *malware* como meio de obtenção de prova e se, por outro lado, é admissível a sua utilização e em que termos à luz dos princípios fundamentais do Estado de Direito Democrático português [art.º 2.º Constituição da República Portuguesa (CRP)]. **3. Métodos** No que se refere ao método, nesta investigação foram utilizados essencialmente o método analítico, através da análise documental da legislação e da jurisprudência e, no método crítico, presente sobretudo na reflexão tecida sobre as implicações legais da utilização de *malware* como meio oculto de obtenção de prova no processo pena. **4. Resultados** Os meios ocultos de obtenção de prova, nomeadamente utilização de malware, contribuem para uma tensão cada vez maior e mais evidente entre a eficácia no combate ao crime e a proteção dos direitos fundamentais dos cidadãos, bem como para um esbater na fronteira entre prevenção e pressão criminal. A aplicação da inovação tecnológica na criação de novos meios de obtenção de prova é suscetível de trazer formas de ingerência nos direitos fundamentais cada vez mais graves. **5. Conclusão** O recurso a *malware* para fins de

[1] Universidade Aberta , sergiolaranjinho@gmail.com

investigação criminal tem obrigatoriamente que ser expressamente prevista por lei, definindo-se claramente e de forma precisa os casos e em que termos essa utilização é possível. Ainda, à luz do artigo 32.º n.º 4 da CRP, a autorização do uso deste método oculto terá que estar sujeita a "reserva de juiz (de Instrução)" com o objetivo principal de assegurar uma tutela preventiva de direitos fundamentais, já que o próprio visado não o pode fazer, por desconhecer da aplicação da medida. Mais, exige-se que seja dado conhecimento aos suspeitos, arguidos ou visados após a realização da medida oculta, *in casu* da utilização de *malware*, para que os mesmos controlem a legalidade da mesma.

PALAVRAS-CHAVE: malware, meio de obtenção de prova, métodos ocultos de investigação, processo penal

[1] Universidade Aberta , sergiolaranjinho@gmail.com