

SUMÁRIO

INTRODUÇÃO	21
CAPÍTULO 1 – MEIOS DE OBTENÇÃO DE PROVA	25
1.1 Terminologia.....	25
1.2 A formação do conjunto de elementos de prova	29
1.3 Meios lícitos e ilícitos.....	36
1.4 Prova ilegal, prova ilegítima e prova ilícita.....	51
1.5 Meios típicos, atípicos e irrituais	58
1.6 A cadeia de custódia da prova.....	61
CAPÍTULO 2 – MEIOS DE OBTENÇÃO DE PROVA E OS DIREITOS FUNDAMENTAIS.....	67
2.1 Compreensão dominante na doutrina sobre os meios atípicos de obtenção de prova	68
2.2 Necessária releitura crítica da instrumentalidade do processo penal.....	71
2.2.1 Justiça, verdade e prova penal	71
2.2.2 A segurança como razão legitimadora do Estado ...	83
2.2.3 Ordem pública e segurança pública.....	84
2.2.4 Teoria geral dos direitos fundamentais	91
2.3 Meios atípicos de obtenção de prova e os direitos fundamentais	103
2.3.1 A analogia.....	107

2.3.2	Análise de constitucionalidade da atipicidade como óbice ao emprego de meio atípico de obtenção de prova	121
2.3.3	Critérios para admissão de meio atípico de obtenção de prova	124
2.3.4	Exemplo de aplicação da teoria	135

CAPÍTULO 3 – DIFICULDADES PROBATÓRIAS NO CONTEXTO DO CRIME ORGANIZADO..... 145

3.1	Características do crime organizado.....	146
3.2	Compromissos internacionais sobre o crime organizado	150
3.3	Conceito legal de organização criminosa	152
3.4	Exemplos de criminalidade organizada no Brasil.....	157
3.4.1	Jogo do bicho.....	158
3.4.2	Tráfico de drogas	160
3.4.3	Milícias	166
3.4.4	Criminalidade política	168
3.5	Dificuldades probatórias na investigação de organizações criminosas no Brasil.....	171
3.6	Insuficiência dos meios típicos frente à criminalidade organizada.....	181

CAPÍTULO 4 – A INVASÃO DE SISTEMA INFORMÁTICO COMO MEIO DE OBTENÇÃO DE PROVA..... 183

4.1	Importância dos dados digitais para investigação	183
4.2	Dificuldades probatórias no universo digital: as medidas antiforenses.....	185
4.3	Características da invasão de dispositivo informático.....	186
4.4	A questão em outros ordenamentos jurídicos	190
4.4.1	Portugal	191
4.4.2	Alemanha	193
4.4.3	Itália.....	194
4.4.4	Estados Unidos.....	199

CAPÍTULO 5 – A INVASÃO DE DISPOSITIVO INFORMÁTICO NA INVESTIGAÇÃO DO CRIME ORGANIZADO 205

5.1	Bens atingidos pela existência da organização criminosa...	205
5.2	Direitos e garantias dos investigados usualmente sujeitos à restrição na utilização da invasão de sistema informático como meio de obtenção de prova.....	208
5.2.1	Direito à privacidade	209
5.2.2	Direito à palavra falada.....	210
5.2.3	Direito à imagem	211
5.2.4	Direito à inviolabilidade do domicílio.....	211
5.2.5	Direito ao sigilo das comunicações	212
5.2.6	Direito à autodeterminação informacional.....	214
5.2.7	Direito à confidencialidade e integridade dos sistemas técnicos-informacionais.....	215
5.2.8	Direito a não produzir prova contra si mesmo.	217
5.2.9	Contraditório	219
5.2.10	Presunção de inocência.....	220
5.2.11	Dignidade da pessoa humana.....	221

CAPÍTULO 6 – ANÁLISE DA ADMISSIBILIDADE DA INVASÃO DE SISTEMA INFORMÁTICO NA INVESTIGAÇÃO DE CRIME ORGANIZADO 223

6.1	A tipificação da conduta de invasão de dispositivo informático.....	223
6.2	Análise da admissibilidade da invasão conforme a funcionalidade empregada	232
6.2.1	Captação ambiental de sinais óticos ou acústicos ...	235
6.2.2	O monitoramento do fluxo de comunicação ou de dados	238
6.2.3	A obtenção de mensagens privadas armazenadas.....	239
6.2.4	Captação de dados referentes à localização do investigado.....	245

6.2.5	Captação de dados de identificação de conexão ..	248
6.2.6	Captação dos demais dados (arquivados, senhas digitadas etc.).....	251
CONCLUSÃO		257
REFERÊNCIAS BIBLIOGRÁFICAS		261