

DUARTE RODRIGUES NUNES

OS MEIOS
DE OBTENÇÃO
DE PROVA PREVISTOS NA
**LEI DO
CIBERCRIME**

.....

2.^A EDIÇÃO
REVISTA E ATUALIZADA

 **GESTLEGAL**

ÍNDICE

Prefácio à 2.^a edição	5
Abreviaturas	7
1. Introdução	11
2. Conceito de cibercrime	37
3. A prova digital.....	47
4. A conjugação das disposições processuais da Lei n.º 109/2009 com o art. 189.º do CPP e com o regime da Lei n.º 32/2008.....	57
5. A preservação expedita de dados (art. 12.º da Lei n.º 109/2009).....	75
5.1. Generalidades.....	75
5.2. Direitos fundamentais restringidos por via do recurso à preservação expedita de dados.....	83
5.3. Catálogo de crimes que permitem o recurso à preservação expedita de dados.....	84
5.4. O grau de necessidade exigido para a autorização do recurso à preservação expedita de dados.....	84
5.5. O grau de suspeita exigido para a autorização do recurso à preservação expedita de dados.....	85
5.6. A admissibilidade do recurso à preservação expedita de dados sem a prévia utilização de outros meios de obtenção de prova menos lesivos.	86
5.7. A admissibilidade da cumulação da preservação expedita de dados com outros meios de obtenção de prova.....	87
5.8. As pessoas que poderão ser alvo de preservação expedita de dados.	88
5.9. A admissibilidade do recurso à preservação expedita de dados relativos a pessoas que se possam recusar validamente a depor.....	91
5.10. A competência para autorizar o recurso à preservação expedita de dados.....	91
5.11. A preservação expedita de dados como medida cautelar e de polícia e a posterior valoração das provas obtidas por essa via.....	92

•

5.12. A ordem de preservação dirigida a entidades privadas estrangeiras que não possuam qualquer representação em Portugal. Necessidade de recurso aos mecanismos de cooperação judiciária internacional?.....	93
5.13. Requisitos formais da ordem de preservação e duração máxima da preservação expedita de dados	94
6. A revelação expedita de dados de tráfego (art. 13.º da Lei n.º 109/2009).	97
6.1. Generalidades.....	97
6.2. Direitos fundamentais restringidos por via do recurso à revelação expedita de dados de tráfego.....	101
6.3. Catálogo de crimes que permitem o recurso à revelação expedita de dados de tráfego	102
6.4. A admissibilidade do recurso à revelação expedita de dados de tráfego sem a prévia utilização de outros meios de obtenção de prova menos lesivos	102
6.5. A admissibilidade da cumulação da revelação expedita de dados de tráfego com outros meios de obtenção de prova	102
6.6. As pessoas que poderão ser alvo de revelação expedita de dados de tráfego	104
6.7. A admissibilidade do recurso à revelação expedita de dados de tráfego relativos a pessoas que se possam recusar validamente a depor	104
7. A injunção para apresentação ou concessão do acesso a dados (art. 14.º da Lei n.º 109/2009).....	105
7.1. Generalidades.....	105
7.2. Direitos fundamentais restringidos por via do recurso à injunção para apresentação ou concessão do acesso a dados.....	118
7.3. A obtenção dos dados de localização celular de todos os telefones móveis/cartões que acionaram um determinado conjunto de antenas de telecomunicações no lapso de tempo em que o crime sob investigação terá sido praticado para posterior identificação dos seus autores	120
7.4. Catálogo de crimes que permitem o recurso à injunção para apresentação ou concessão do acesso a dados	130
7.5. O grau de necessidade exigido para a autorização do recurso à injunção para apresentação ou concessão do acesso a dados.....	131
7.6. O grau de suspeita exigido para a autorização do recurso à injunção para apresentação ou concessão do acesso a dados	131
7.7. A admissibilidade do recurso à injunção para apresentação ou concessão do acesso a dados sem a prévia utilização de outros meios de obtenção de prova menos lesivos.....	132
7.8. A admissibilidade da cumulação da injunção para apresentação ou concessão do acesso a dados com outros meios de obtenção de prova.....	132

•

•

7.9. As pessoas que poderão ser alvo da injunção para apresentação ou concessão do acesso a dados	134
7.10. A admissibilidade do recurso à injunção para apresentação ou concessão do acesso a dados relativos a pessoas que se possam recusar validamente a depor	136
7.11. A competência para autorizar o recurso à injunção para apresentação ou concessão do acesso a dados.....	146
7.12. A injunção para apresentação ou concessão do acesso a dados dirigida a entidades privadas estrangeiras que não possuam qualquer representação em Portugal. Necessidade de recurso aos mecanismos de cooperação judiciária internacional?.....	148
7.13. Requisitos formais da injunção para apresentação ou concessão do acesso a dados	149
8. A pesquisa de dados informáticos (art. 15.º da Lei n.º 109/2009)	153
8.1. Generalidades.....	153
8.2. Direitos fundamentais restringidos por via do recurso à pesquisa de dados informáticos	167
8.3. Catálogo de crimes que permitem o recurso à pesquisa de dados informáticos.....	175
8.4. O grau de necessidade exigido para a autorização do recurso à pesquisa de dados informáticos.....	176
8.5. O grau de suspeita exigido para a autorização do recurso à pesquisa de dados informáticos.....	177
8.6. A admissibilidade do recurso à pesquisa de dados informáticos sem a prévia utilização de outros meios de obtenção de prova menos lesivos	178
8.7. A admissibilidade da cumulação da pesquisa de dados informáticos com outros meios de obtenção de prova	179
8.8. As pessoas que poderão ser alvo de pesquisa de dados informáticos	181
8.9. A admissibilidade do recurso à pesquisa de dados informáticos relativamente a pessoas que se possam recusar validamente a depor	182
8.10. A competência para autorizar o recurso à pesquisa de dados informáticos.....	208
8.11. O âmbito da autorização da pesquisa de dados informáticos	210
8.12. A pesquisa de dados informáticos realizada sem autorização prévia da autoridade judiciária.....	216
8.13. O acesso transfronteiriço a sistemas informáticos situados em países estrangeiros sem recurso aos mecanismos de cooperação judiciária internacional	234
8.14. Requisitos formais e procedimentais da pesquisa de dados informáticos.....	244

•

•

9. A apreensão de dados informáticos (art. 16.º da Lei n.º 109/2009)	259
9.1. Generalidades	259
9.2. A apreensão de criptomoedas	265
9.3. Direitos fundamentais restringidos por via da apreensão de dados informáticos	267
9.4. Admissibilidade da apreensão de dados informáticos pessoais ou íntimos	269
9.5. Catálogo de crimes que permitem a apreensão de dados informáticos...	277
9.6. O grau de necessidade exigido para a autorização do recurso à apreensão de dados informáticos	278
9.7. O grau de suspeita exigido para a autorização do recurso à apreensão de dados informáticos	279
9.8. A admissibilidade da apreensão de dados informáticos sem a prévia utilização de outros meios de obtenção de prova menos lesivos	281
9.9. A admissibilidade da cumulação da apreensão de dados informáticos com outros meios de obtenção de prova	281
9.10. As pessoas que poderão ser alvo de uma apreensão de dados informáticos	283
9.11. A admissibilidade do recurso à apreensão de dados informáticos relativos a pessoas que se possam recusar validamente a depor	285
9.12. A competência para autorizar a apreensão de dados informáticos .	303
9.13. O âmbito da apreensão de dados informáticos. <i>Plain view?</i>	306
9.14. A apreensão de dados informáticos realizada sem autorização prévia da autoridade judiciária	317
9.15. Requisitos procedimentais da apreensão de dados informáticos. Os modos de apreensão de dados informáticos	319
10. A apreensão de correio eletrónico e de registos de comunicação de natureza semelhante (art. 17.º da Lei n.º 109/2009)	329
10.1. Generalidades	329
10.2. Direitos fundamentais restringidos pela apreensão de correio eletrónico e de registos de comunicação de natureza semelhante	349
10.3. Catálogo de crimes que permitem apreensão de correio eletrónico e de registos de comunicação de natureza semelhante	351
10.4. O grau de necessidade exigido para a apreensão de correio eletrónico e de registos de comunicação de natureza semelhante	352
10.5. O grau de suspeita exigido para a apreensão de correio eletrónico e de registos de comunicação de natureza semelhante	353
10.6. A admissibilidade da apreensão de correio eletrónico e de registos de comunicação de natureza semelhante sem a prévia utilização de outros meios de obtenção de prova menos lesivos	354

•

10.7. A admissibilidade da cumulação da apreensão de correio eletrônico e de registos de comunicação de natureza semelhante com outros meios de obtenção de prova.....	355
10.8. As pessoas que poderão ser alvo da apreensão de correio eletrônico e de registos de comunicação de natureza semelhante.....	356
10.9. A admissibilidade da apreensão de correio eletrônico e de registos de comunicação de natureza semelhante relativos a pessoas que se possam recusar validamente a depor.....	357
10.10. A competência para autorizar a apreensão de correio eletrônico e de registos de comunicação de natureza semelhante. A apreensão de correio eletrônico e de registos de comunicação de natureza semelhante como medida cautelar e de polícia e a posterior valoração das provas obtidas por essa via.....	359
10.11. Requisitos procedimentais da apreensão de correio eletrônico e de registos de comunicação de natureza semelhante.....	361
11. A interceção de comunicações (art. 18.º da Lei n.º 109/2009).....	363
11.1. Generalidades.....	363
11.2. A vigilância nas fontes (<i>Quellenüberwachung</i>).....	368
11.3. A obtenção dos dados de tráfego de todos os telefones móveis/cartões que acionaram um determinado conjunto de antenas de telecomunicações no lapso de tempo em que o crime sob investigação terá sido praticado para posterior identificação dos seus autores.....	378
11.4. Direitos fundamentais restringidos por via do recurso à interceção de comunicações.....	386
11.5. Catálogo de crimes que permitem o recurso à interceção de comunicações.....	388
11.6. O grau de necessidade exigido para a autorização do recurso à interceção de comunicações.....	401
11.7. O grau de suspeita exigido para a autorização do recurso à interceção de comunicações.....	401
11.8. A admissibilidade do recurso à interceção de comunicações sem a prévia utilização de outros meios de obtenção de prova menos lesivos....	404
11.9. A admissibilidade da cumulação da interceção de comunicações com outros meios de obtenção de prova.....	406
11.10. As pessoas que poderão ser alvo de uma interceção de comunicações.....	407
11.11. A admissibilidade do recurso à interceção de comunicações a pessoas que se possam recusar validamente a depor.....	409
11.12. A competência para autorizar o recurso à interceção de comunicações. Os procedimentos <i>ex abrupto</i>	417
11.13. Requisitos formais e procedimentais da interceção de comunicações	418

•

•

12. As ações encobertas em ambiente informático-digital ou online (art. 19.º da Lei n.º 109/2009).....	427
12.1. Generalidades.....	427
12.2. Os vários “atores” das ações “encobertas”.....	438
12.3. Direitos fundamentais restringidos por via do recurso às ações encobertas em ambiente informático-digital	453
12.4. Catálogo de crimes que permitem o recurso às ações encobertas em ambiente informático-digital	455
12.5. O grau de necessidade exigido para a autorização do recurso às ações encobertas em ambiente informático-digital	458
12.6. O grau de suspeita exigido para a autorização do recurso às ações encobertas em ambiente informático-digital	459
12.7. A admissibilidade do recurso às ações encobertas em ambiente informático-digital sem a prévia utilização de outros meios de obtenção de prova menos lesivos	459
12.8. A admissibilidade das ações encobertas em ambiente informático-digital com outros meios de obtenção de prova.....	460
12.9. O “interrogatório” do agente infiltrado ao arguido ou a pessoas que possam recusar a prestação de depoimento sem os advertir da faculdade de recusar o depoimento.....	461
12.10. A identidade fictícia do agente infiltrado	466
12.11. O depoimento do agente infiltrado. O valor probatório do relato da ação encoberta.....	467
12.12. O cometimento de crimes pelo agente infiltrado e a sua relevância no plano da prova.....	471
12.13. As pessoas que poderão ser alvo de ações encobertas em ambiente informático-digital.....	475
12.14. A admissibilidade do recurso às ações encobertas em ambiente informático-digital visando pessoas que se possam recusar validamente a depor	476
12.15. A competência para autorizar o recurso às ações encobertas em ambiente informático-digital	477
12.16. Requisitos procedimentais das ações encobertas em ambiente informático-digital.....	479
13. A busca <i>online</i> (arts. 15.º e 18.º da Lei n.º 109/2009).....	481
Bibliografia	513
Documentos e artigos de imprensa consultados	533
Jurisprudência	535
Índice	543



GESTLEGAL

www.gestlegal.pt • editora@gestlegal.pt