Sumário

AGRADECIMENTOS 7

INTRODUÇÃO 15

1. *Hacking* governamental como mecanismo de acesso ao conteúdo legível de dados sem enfraquecimento da criptografia forte necessária para segurança da informação na atual era digital 27

1.1. O que é criptografia, para que serve e sua relevância na atual era digital 27

1.1.1. Tipos e formas de criptografia 30

1.1.2. *Crypto Wars* e a necessidade de prevalência da criptografia forte 32

1.2. Alternativas à proibição da criptografia para acesso ao conteúdo legível de dados criptografados 39

1.2.1. Limitação ao uso da criptografia forte 40

1.2.2. Obrigação de licença ou autorização para o oferecimento e/ou utilização da criptografia 41

1.2.3. *Mandatory key escrow* 42

1.2.4. Obrigação de assistência 44

1.2.5. Obtenção de chaves criptográficas 46

1.2.6. Acesso por força bruta 48

1.2.7. Mecanismos de acesso excepcional 49

1.2.8. Exploração de vulnerabilidades 52

1.3. *Hacking* como alternativa para acesso ao conteúdo legível de dados criptografados 53

1.3.1. *Hacking* governamental 57

1.3.1.1. Definição de *hacking* governamental, suas finalidades e modalidades 57

1.3.1.2. Elementos, ferramentas e possíveis ações do *hacking* governamental 60

1.3.1.2.1. Exploração de vulnerabilidades conhecidas ou desconhecidas 60

1.3.1.2.2. Utilização de *software* malicioso 62

1.3.1.2.3. Meios de entrega do *software* malicioso 68

1.3.1.3. Vantagens e preocupações em relação ao *hacking* governamental 71
1.3.1.3.1. Não enfraquecimento da criptografia 71
1.3.1.3.2. Eficiência 72
1.3.1.3.3. Invasividade 73
1.3.1.3.4. Afetação de terceiros 74
1.3.1.3.5. Comercialização e comoditização de vulnerabilidades 75
1.3.1.3.6. Divulgação de vulnerabilidades para fabricantes ou fornecedores 78
1.3.1.3.7. Notificação do sujeito-alvo 80
1.3.1.3.8. Divulgação das vulnerabilidades aos usuários afetados e ao público em geral 81
1.3.1.3.9. Vazamentos e furtos de ferramentas de *hacking* detidas por autoridades governamentais 81
1.3.1.3.10. Período de duração 83
1.3.1.3.11. Integridade das redes, dos sistemas e dos dispositivos eletrônicos afetados, bem como dos dados coletados 83
1.3.1.3.12. Custo 84

2. Parâmetros internacionais e estrangeiros para a prática de medidas ocultas de investigação ou monitoramento que atinjam dados pessoais nas quais se inclui o *hacking* governamental 87
2.1. Parâmetros estabelecidos pelas cortes interamericana e europeia de direitos humanos para a prática de medidas ocultas de investigação ou monitoramento que atinjam dados pessoais 87
2.1.1. Legalidade e garantias mínimas a serem estabelecidas em lei 97
2.1.1.1. Natureza das ofensas que podem dar origem à autorização de medidas ocultas de investigação ou monitoramento que atinjam dados pessoais 106
2.1.1.2. Pessoas ou categorias de pessoas que podem ser alvo dessas medidas 108
2.1.1.3. Tipos de medidas e ações que podem ser empregadas ... 110
2.1.1.4. Limite temporal para duração dessas medidas 110
2.1.1.5. Procedimento para coleta, armazenamento e uso dos dados coletados pelas autoridades 112
2.1.1.6. Circunstâncias nas quais os dados coletados podem e/ou devem ser apagados/destruídos 115
2.1.1.7. Procedimento para compartilhamento dos dados coletados com terceiros 116
2.1.2. Fim legítimo a ser alcançado 118

2.1.3. Necessidade, adequação e proporcionalidade **121**
2.1.4. Mecanismos de controle e supervisão **124**
2.1.4.1. Necessidade de autorização prévia **124**
2.1.4.2. Necessidade de supervisão da execução **129**
2.1.4.2.1. Transparência **133**
2.1.4.3. Revisão após o término e notificação do alvo **134**
2.2. Aplicação dos parâmetros das Cortes Interamericana e Europeia de Direitos Humanos para disciplina em lei do *hacking* governamental no direito estrangeiro **141**
2.2.1. Legalidade e garantias mínimas a serem estabelecidas em lei **143**
2.2.1.1. Natureza das ofensas que podem dar origem à autorização de *hacking* governamental **153**
2.2.1.2. Pessoas ou categorias de pessoas que podem ser alvo de *hacking* governamental **158**
2.2.1.3. Tipos de medidas e ações que podem ser empregadas para a prática de *hacking* governamental **161**
2.2.1.4. Limite temporal para duração do *hacking* governamental **167**
2.2.1.5. Procedimento para coleta, armazenamento e uso dos dados coletados por meio do *hacking* governamental **170**
2.2.1.6. Circunstâncias nas quais os dados coletados podem e/ou devem ser apagados/destruídos **177**
2.2.1.7. Procedimento para compartilhamento dos dados coletados com terceiros **180**
2.2.2. Fim legítimo a ser alcançado **182**
2.2.3. Necessidade, adequação e proporcionalidade **184**
2.2.4. Mecanismos de controle e supervisão **189**
2.2.4.1. Necessidade de autorização prévia **189**
2.2.4.2. Necessidade de supervisão da execução **201**
2.2.4.2.1. Transparência **205**
2.2.4.3. Revisão após o término e notificação do alvo **208**
2.3. Exemplo de país que autoriza a prática de *hacking* governamental sem disciplina em lei específica, em desacordo com os parâmetros das Cortes Interamericana e Europeia de Direitos Humanos: Estados Unidos da América **212**
2.3.1. Panorama geral e exemplos da prática de *hacking* governamental por autoridades de investigação norte-americanas **213**
2.3.2. Respaldo legal utilizado para requerimentos e autorizações de *hacking* governamental nos Estados Unidos da América: *Wiretap Act* e *Rule 41* das *Federal Rules of Criminal Procedure* **220**

2.3.3. Possível enquadramento do *Wiretap Act* e da *Rule 41* das *Federal Rules of Criminal Procedure*, nos parâmetros das Cortes Interamericana e Europeia de Direitos Humanos, para autorização, por analogia, do *hacking* governamental **227**

2.3.3.1. Legalidade e garantias mínimas a serem estabelecidas em lei **227**

2.3.3.1.1. Natureza das ofensas que podem dar origem à autorização das medidas **228**

2.3.3.1.2. Pessoas ou categorias de pessoas que podem ser alvo das medidas **229**

2.3.3.1.3. Tipos de medidas e ações que podem ser empregadas **230**

2.3.3.1.4. Limite temporal para duração das medidas .. **231**

2.3.3.1.5. Procedimento para coleta, armazenamento e uso dos dados coletados pelas autoridades ... **232**

2.3.3.1.6. Circunstâncias nas quais os dados coletados podem e/ou devem ser apagados/destruídos **234**

2.3.3.1.7. Procedimento para compartilhamento dos dados coletados com terceiros **234**

2.3.3.2. Fim legítimo a ser alcançado **235**

2.3.3.3. Necessidade, adequação e proporcionalidade **236**

2.3.3.4. Mecanismos de controle e supervisão **237**

2.3.3.4.1. Necessidade de autorização prévia **237**

2.3.3.4.2. Necessidade de supervisão da execução e transparência **240**

2.3.3.4.3. Revisão após o término e notificação do alvo ... **241**

2.3.4. Impossibilidade de o *Wiretap Act* e a *Rule 41* das *Federal Rules of Criminal Procedure* servirem como base legal para autorização, por analogia, do *hacking* governamental **245**

2.3.5. *Vulnerabilities Equity Process* (VEP): regramento norte-americano para divulgação de vulnerabilidades usadas para a prática de *hacking* governamental **250**

3. Admissibilidade do *hacking* governamental como meio de obtenção de prova no processo penal brasileiro **259**

3.1. Taxatividade (ou não) dos meios de obtenção de prova no processo penal brasileiro **259**

3.2. Direitos fundamentais afetados pela execução do *hacking* governamental como meio de obtenção de prova para fins de investigação criminal e/ou instrução processual penal **271**

3.2.1. Inviolabilidade do domicílio **273**

3.2.2. Inviolabilidade do sigilo das comunicações 277
3.2.3. Direito à privacidade 282
3.2.4. Proteção dos dados pessoais e autodeterminação informacional ... 286
3.2.5. Liberdade de expressão 291
3.2.6. Grau de afetação de direitos fundamentais e a necessária taxatividade do *hacking* governamental como meio de obtenção de prova para fins de investigação criminal e/ou instrução processual penal 292
3.3. Meios de obtenção de prova disciplinados em lei no Processo Penal brasileiro e a sua possível aplicação analógica ao *hacking* governamental 294
3.3.1. Interceptações telefônica e telemática 295
3.3.2. Interceptação ambiental de sinais eletromagnéticos, ópticos e acústicos 302
3.3.3. Infiltração virtual de agentes 307
3.3.4. Busca e apreensão domiciliar 315
3.3.5. Possíveis novos meios de obtenção de prova e a eventual disciplina em lei do *hacking* governamental no processo penal brasileiro 319
3.4. Consequências atuais da prática do *hacking* governamental, por autoridades de investigação e persecução penal, para obtenção de prova no processo penal brasileiro 331

4. Disciplina em lei do *hacking* governamental no processo penal brasileiro 337
4.1. Legalidade e garantias mínimas a serem estabelecidas em lei 337
4.1.1. Natureza das ofensas que podem dar origem à autorização de *hacking* governamental 339
4.1.2. Pessoas ou categorias de pessoas que podem ser alvo de *hacking* governamental 342
4.1.3. Tipos de medidas e ações que podem ser empregadas para a prática de *hacking* governamental 344
4.1.4. Limite temporal para duração do *hacking* governamental 346
4.1.5. Procedimento para coleta, armazenamento e uso dos dados coletados por meio do *hacking* governamental 349
4.1.6. Circunstâncias nas quais os dados coletados podem e/ou devem ser apagados/destruídos 355
4.1.7. Procedimento para compartilhamento dos dados coletados com terceiros 359
4.2. Fim legítimo a ser alcançado 361
4.3. Necessidade, adequação e proporcionalidade 362
4.4. Mecanismos de controle e supervisão 363
4.4.1. Necessidade de autorização prévia 363

4.4.2. Necessidade de supervisão da execução **367**
4.4.2.1. Transparência **369**
4.4.3. Revisão após o término e notificação do alvo **371**
4.5. Proposta legislativa compilada para disciplina do *hacking* governamental no processo penal brasileiro **375**
4.6. Regramento administrativo sobre aquisição e divulgação de vulnerabilidades e de ferramentas tecnológicas para a prática de *hacking* governamental **386**

CONCLUSÃO **393**

REFERÊNCIAS **399**