Pós-Graduação em Ciência da Computação

DANIELLE NOVAES DE SIQUEIRA VALVERDE

EVIDÊNCIAS CRIMINAIS ELETRÔNICAS EM NUVEM E SUA COLETA EXTRATERRITORIAL NO PROCESSO PENAL

Universidade Federal de Pernambuco
posgraduacao@cin.ufpe.br
www.cin.ufpe.br/~posgraduacao

Recife
2018

Danielle Novaes de Siqueira Valverde

EVIDÊNCIAS CRIMINAIS ELETRÔNICAS EM NUVEM E SUA COLETA EXTRATERRITORIAL NO PROCESSO PENAL

Tese de Doutorado submetida ao Programa de Pós-graduação em Ciência da Computação do Centro de Informática da Universidade Federal de Pernambuco, como requisito parcial para obtenção do grau de Doutor em Ciência da Computação.

Área de concentração: Multidisciplinar

Orientador: Prof. Dr. Ruy José Guerra Barretto de Queiroz

Recife
2018

Catalogação na fonte
Bibliotecária Monick Raquel Silvestre da S. Portes, CRB4-1217

V215e Valverde, Danielle Novaes de Siqueira
Evidências criminais eletrônicas em nuvem e sua coleta extraterritorial no processo penal / Danielle Novaes de Siqueira Valverde. – 2018.
292 f.: il., fig., tab.

Orientador: Ruy José Guerra Barretto de Queiroz.
Tese (Doutorado) – Universidade Federal de Pernambuco. CIn, Ciência da Computação, Recife, 2018.
Inclui referências, glossário, apêndice e anexo.

1. Ciência da computação. 2. Computação em nuvem. I. Queiroz, Ruy José Guerra Barretto de (orientador). II. Título.

004 CDD (23. ed.) UFPE- MEI 2019-005

Danielle Novaes de Siqueira Valverde

Evidências Criminais Eletrônicas em Nuvem e sua Coleta Extraterritorial no Processo Penal

Tese de Doutorado apresentada ao Programa de Pós-Graduação em Ciência da Computação da Universidade Federal de Pernambuco, como requisito parcial para a obtenção do título de Doutor em Ciência da Computação.

Aprovado em: 19/02/2018.

_____

Orientador: Prof. Dr. Ruy José Guerra Barretto de Queiroz

BANCA EXAMINADORA

_____

Prof. Dr. Kiev Santos da Gama
Centro de Informática / UFPE

_____

Prof. Dr. Carlos André Guimarães Ferraz
Centro de Informática / UFPE

_____

Prof. Dr. Roberto Wanderley Nogueira
Faculdade de Direito / UFPE

_____

Profa. Dra. Maria Amália Oliveira de Arruda Camara
Faculdade de Direito / UPE

_____

Profa. Dra. Cinthia Obladen de Almendra Freitas
Escola de Direito / PUC/PR

Ao meu pai, José de Siqueira Silva,
que sempre iluminou meu caminho, no
estudo do Direito Penal.

AGRADECIMENTOS

O desafio de escrever uma Tese de Doutorado é imenso, a ponto de conduzir o estudante ao exílio social e familiar. Mas é extremamente gratificante chegar ao fim, e o apoio dos amigos e da família foi fundamental nessa jornada. Meus sólidos laços familiares permitiram suportar os momentos mais difíceis e seguir em frente. Nesse momento, cumpre-me externar toda a minha gratidão aos que, direta ou indiretamente, auxiliaram-me nessa conquista.

Aos meus pais e irmãos, pelo carinho e apoio. Ao meu pai, em particular, obrigada pelos agradáveis e enriquecedores momentos de discussão que levaram à propositura final desta Tese. Foi ele que, em sua sabedoria, disse: “o ruim é inaceitável, o perfeito é impossível, mas o bom é satisfatório; está na hora de colocar um ponto final”.

Ao meu esposo, Francisco Valverde, obrigada pela compreensão da minha ausência, por me substituir (muito bem) em atividades que a mim cabiam, por estar ao meu lado, como amigo e companheiro, sempre, e pelas críticas e sugestões, na sua visão leiga de professor de Odontologia.

À minha filha, Adélia Valverde, nunca desista! Mesmo diante de grandes obstáculos que a vida coloca no nosso caminho, mesmo diante da incompreensão de muitos, siga em frente, cumpra sua missão, termine o que foi iniciado.

Ao meu orientador, o Professor Dr. Ruy de Queiroz, pelos ensinamentos e pelo exemplo de amor ao estudo, de honestidade intelectual e de simplicidade para enfrentar comigo temas complexos do Direito. Obrigada também pela paciência e, sobretudo, pelas palavras de força, perseverança e apoio, proferidas em momentos de extrema provação. Peço a Deus que lhe propicie longos anos de saúde, paz e juventude intelectual.

Aos colegas policiais, especialmente a George Fragoso, pela dedicação de seus valiosos minutos para a leitura dos escritos, contribuindo com críticas e sugestões. Também não posso olvidar outros colegas policiais e magistrados, que pacientemente me ouviram.

À Evandro Curvelo, pelas horas de discussão sobre computação em nuvem e segurança cibernética. Espero ter desatado o “nó górdio”.

Muitas instituições e pessoas, que conheci apenas na virtualidade do espaço cibernético, contribuíram para que essa jornada fosse concluída. O Conselho da Europa, o *Digital Watch Observatory*, as Nações Unidas e seu Escritório para Drogas e Crime; os colaboradores que responderam às minhas solicitações ou compartilharam seus escritos (Thomas Dowling: *OATD Organization*, Agnes Kasper, Bruce Sterling); muito obrigada.

Por fim, agradeço a Deus e a Nossa Senhora, pelo presente de estar aqui, com saúde e força para iniciar novos desafios.

RESUMO

Computação em nuvem, em termos gerais, refere-se ao modelo tecnológico que permite, de forma onipresente, conveniente e sob demanda, o compartilhamento de recursos computacionais configuráveis, que podem ser rapidamente alocados e liberados com o mínimo de esforço de gerenciamento ou interação do provedor de serviço. Quando aplicado sobre a Internet, facilmente a distribuição dos recursos ultrapassam as fronteiras territoriais dos países, desenhando arquiteturas multinacionais de prestação de serviços. Esse modelo distribuído vem evoluindo e oferecendo vantagens à sociedade da tecnologia da informação e comunicação. Nos primórdios da Internet, por exemplo, o usuário costumava armazenar *e-mails* em seus computadores pessoais. Com a disseminação do *webmail*, passou a conservá-los na nuvem, pela facilidade de poder acessá-los, a partir de qualquer dispositivo, independentemente de onde estivesse. A computação em nuvem trouxe o estado da arte da mobilidade dos dados. Por diversas razões, provedores de computação em nuvem particionam, replicam dados, armazenando-os em *data centers* geograficamente distribuídos sob as mais variadas jurisdições nacionais, trazendo implicações à investigação criminal, quando as evidências se encontram nesse ambiente, mas em território de Estado estrangeiro. Os desafios aos agentes de persecução criminal são muitos. Os dados digitais são intangíveis e voláteis, tornando o tempo um adversário a uma apuração criminal exitosa. As leis processuais penais são informadas pelo princípio da territorialidade absoluta, que impede um Estado de exercer seu poder soberano além da sua própria soberania. Os tratados de assistência judiciária em matéria penal não têm se mostrado efetivos na coleta de evidências criminais, quando armazenadas em nuvem, sobre território estrangeiro. Os desafios aos provedores de serviço decorrem principalmente da insegurança jurídica relativa ao cumprimento de medidas processuais penais. Aos usuários, essas lacunas acarretam a sensação de vulnerabilidade na proteção de seus direitos fundamentais. Apesar da natureza transnacional da computação em nuvem e de suas repercussões à investigação criminal, até hoje há uma vacuidade normativa, uma ausência de regramento internacional global que as Convenções regionais não preenchem, de forma a evitar imperativos conflitantes e procedimentos controvertidos. Essa Tese se insere nessa problemática do direito processual penal e do direito internacional, e tem por objetivo propor a negociação de instrumento jurídico internacional que viabilize a cooperação direta entre Estado soberano e empresa provedora de serviço de computação em nuvem pública, para permitir que autoridades de persecução criminal possam requisitar evidências eletrônicas, relativas a pessoas investigadas por prática de crimes graves, diretamente a provedor de serviço sediado em território de outro Estado Parte, sem a obrigatoriedade de formalizar acordo bilateral de assistência judiciária em matéria penal, simplificando os procedimentos persecutórios, de forma que não se inviabilizem pela burocracia e morosidade contraproducente à apuração das infrações penais.

Palavras-chaves: Evidência eletrônica. Extraterritorialidade. Computação em nuvem. Persecução criminal. Direito internacional.

ABSTRACT

Cloud computing, in general terms, refers to the technological model that enables ubiquitous, convenient and on demand sharing of configurable computing resources that can be quickly allocated and released with minimal management effort or interaction of the service provider. When applied over the Internet, resource allocation easily transcends the territorial boundaries of countries, designing multinational architectures of service delivery. This distributed model has been evolving and offering advantages to the information and communication technology society. In the early days of the Internet, for example, the users would store e-mails on their personal computers. With the spread of *webmail*, they started to save them in the cloud due to the ease of being able to access them from any device, no matter where the users were. Cloud computing has brought the state of the art of data mobility. For various reasons, cloud computing providers partition, replicate data, and store them in geographically distributed *data centers* across a wide range of national jurisdictions, with implications for criminal investigation when evidence is available in that environment but in foreign State territory. The challenges to criminal prosecution agents are many. Digital data are intangible and volatile, making time an adversary to successful criminal scrutiny. Criminal procedural laws are informed by the principle of absolute territoriality, which prevents a State from exercising its sovereign power beyond its own sovereignty. The legal aid treaties in criminal matters have not been effective in collecting criminal evidence, when stored in the cloud, over foreign territory. The challenges to service providers stem primarily from legal uncertainty regarding compliance with criminal procedural measures. To users, such gaps create a sense of vulnerability in protecting their fundamental rights. Despite the transnational nature of cloud computing and its repercussions on criminal investigation, today there is still a normative vacuum, an absence of global international regulation that Regional Conventions do not fulfill in order to avoid conflicting imperatives and controversial procedures. This thesis is part of the issue regarding criminal procedural law and international law, and aims to propose the negotiation of an international legal instrument that enables direct cooperation between the sovereign State and the public cloud computing service provider, in order to allow criminal prosecution authorities to request electronic evidence concerning persons investigated for committing serious crimes directly to a service provider based in the territory of another State Party without the obligation to formalize a bilateral agreement on legal assistance in criminal matters, thus simplifying the prosecution procedures so that they are not made unfeasible by the bureaucracy and slowness which are counterproductive to the investigation of criminal offenses.

Keywords: Electronic evidence. Extraterritoriality. Cloud computing. Criminal prosecution. International law.

LISTA DE ABREVIATURAS E SIGLAS

AES	*Advanced Encryption Standard*
AWS	*Amazon Web Services*
BDTD	Biblioteca Digital Brasileira de Teses e Dissertações
Capes	Coordenação de Aperfeiçoamento de Pessoal de Nível Superior
CCDCOE	*Cooperative Cyber Defense Centre of Excellence*
CCTV	*Closed-circuit television* / Circuito Fechado de Televisão
CEG	*Cloud Evidence Group /* Grupo de Evidências em Nuvem
Cert.br	Centro de Estudo, Resposta e Tratamento de incidentes de Segurança no Brasil
CIJ/ICJ	Corte Internacional de Justiça*/International Court of Justice*
CIS/CEI	*Commonwealth of Independent States* / Comunidade dos Estados Independentes
D.K.O.M	*Direct Kernel Object Manipulation*
DDoS	*Distributed Denial-of-Service*
DEI	Decisão Europeia de Investigação
DNS	*Domain Name System*
DOJ	*Departamento of Justice* (dos Estados Unidos da América)
DSA	*Digital Signature Algorithm*
ECPA	*Electronic Communications Privacy Act*
ECS	*Electronic Communication Service*
ETS	*European Treaty Series*
Eurojust	*The European Union's Judicial Cooperation Unit*
Europol	*European Union Agency for Law Enforcement Cooperation*
FAPESP	Fundação de Amparo à Pesquisa do Estado de São Paulo

FBI	*Federal Bureau of Investigation*
FISA	*Foreign Intelligence Surveillance Act*
FMI	Fundo Monetário Internacional
G8	*Group of Eight / Grupo dos Oito*
IaaS	*Infrastructure as a Service* / Infraestrtura como Serviço
IBICT	Instituto Brasileiro de Informação em Ciência e Tecnologia
ICPA	*International Communications Privacy Act*
IEEE	*Institute of Electrical and Electronics Engineers*
Interpol	*International Criminal Police Organization*
IP	*Internet Protocol* (protocolo Internet)
ISP	*Internet Service Provider / Provedor de Serviço Internet*
LEA	Liga dos Estados Árabes
MCP	*Multinacional Cloud Service Provider*
MEC	Ministério da Educação
MEC	Ministério da Educação
MLAT	*Mutual Legal Assistence Treaty*
MSP	*Mobile Service Provider* / Provedor de serviços móveis
NATO/OTAN	*North Atlantic Treaty Organization* / Organização do Tratado do Atlântico Norte
NDLTD	*Networked Digital Library of Theses and Dissertations*
NIST	*National Institute of Standards and Technology*
OATD	*Open Access Theses and Dissertations*
OCDE	Organização de Cooperação e Desenvolvimento Econômico
OCLC	*Online Computer Library Center*
OEA	Organização dos Estados Americanos
OIT	Organização Internacional do Trabalho

ONU	Organização das Nações Unidas
OSCE	*Organization for Security and Cooperation in Europe*
OUA	Organização de Unidade Africana
PaaS	*Plataform as a Service* / Plataforma como Serviço
PC-CY	*Committee of Experts on Crime in Cyber-space*
PEB	*Process Environment Block*
RCS	*Remote Computing Service*
SaaS	*Software as a Service* / *Software* como Serviço
SCA	*Stored Communications Act*
SCO	*Shanghai Cooperation Organization*
SOCTA	*Serious and Organised Crime Threat Assessment*
SSRN	*Social Science Research Network*
STF	Supremo Tribunal Federal
STJ	Superior Tribunal de Justiça
TCP	*Transmission Control Protocol*
T-CY	Comitê da Convenção de Budapeste sobre o Cibercrime / *Cybercrime Convention Committee*
TFUE	Tratado sobre o Funcionamento da União Europeia
TOR	*The Onion Router*
TRF	Tribunal Regional Federal
TUE	Tratado da União Europeia
UA/AU	União Africana/*African Union*
Unesco	*United Nations Educational, Scientific, Cultural Organization* / Organização das Nações Unidas para a Educação, a Ciência e a Cultura
UNODC	*United Nation Office on Drugs and Crime*
UPU	União Postal Universal

URL	*Uniform Resource Locator*
URSS	União das Repúblicas Socialistas Soviéticas

LISTA DE TABELAS

Tabela 1 - Categorias antiforenses, por Harris (2006) 69

Tabela 2 - Requisitos para acesso pelo Estado a informações de usuários de provedores de serviço, nos termos do SCA e do Wiretap Act 81

Tabela 3 - Principais peças do processo *Microsoft Ireland Case* 88

Tabela 4 - Normas de direito internacional concernentes ao combate às infrações intensivas em tecnologias da informação e comunicação 135

Tabela 5 - Características entre as normas internacionais analisadas 160

Tabela 6 - Comparação entre requisitos analisados nas normas internacionais 160

Tabela 7 - Infrações penais em tratados internacionais 211

Tabela 8 - Características gerais das propostas analisadas, em comparação ao modelo apresentado 222

Tabela 9 - Comparação entre os tipos de dados, ofensividade e diligências propostas 223

Tabela 10 - Comparação entre os requisitos de adesão ao tratado 224

Tabela 11 - Restrições na requisição de dados digitais 224

Tabela 12 - Exigências para requisitar diretamente ao provedor de computação em nuvem 225

Tabela 13 - Bibliotecas digitais utilizadas na busca por trabalhos científicos 266

Tabela 14 - Palavras-chaves utilizadas para compor a expressão de busca 267

Tabela 15 - Resultados para as expressões “electronic evidence” e filtro “extraterritorial” 270

Tabela 16 - Resultados de interesse ao estudo, para as expressões “electronic evidence” e filtro “cloud” 272

Tabela 17 - Resultados relevantes ao estudo, para as expressões “electronic evidence” e filtro “cross-border” 275

Tabela 18 - Resultados para as expressões “digital evidence” + “cloud” e “digital evidence” + “crime”, não listados anteriormente. 276

Tabela 19 - Resultados relevantes ao estudo, para a expressão “Microsoft ireland case”. 276

Tabela 20 - Resultados de interesse para a expressão da Figura 10 278

Tabela 21 - Expressões lógicas de busca com as palavras-chaves de interesse, sobre a biblioteca digital Springer 279

Tabela 22 - Publicações disponíveis e de interesse ao estudo, retornadas pelo uso das expressões lógicas da Tabela 21 279

Tabela 23 - Publicação retornada, e disponível, pelo uso das palavras-chaves transborder, cross-border, extraterritorial, evidence, digital, electronic, criminal, relevantes ao processo de revisão. 280

Tabela 24 - Expressões lógicas de busca com as palavras-chaves de interesse, sobre o Banco de Teses e Dissertações da Capes 280

Tabela 25 - Publicação de interesse ao estudo, retornada pelo uso das expressões lógicas da Tabela 24. 281

Tabela 26 - Expressões lógicas de busca com as palavras-chaves de interesse, sobre o BDTD/IBICT 281

Tabela 27 - Expressões lógicas de busca com as palavras-chaves de interesse, sobre o OATD 282

Tabela 28 - Publicações de interesse ao estudo, retornadas pelo uso das expressões lógicas da Tabela 27. 282

Tabela 29 - Publicações de interesse ao estudo, retornadas pelo uso expressão “Microsoft ireland case”, na Public Version of WorldCat 283

Tabela 30 - Publicações do Comitê para a Convenção do Cibercrime, do Conselho da Europa 284

LISTA DE ILUSTRAÇÕES

Figura 1 - Gráfico de evolução das três ocorrências policiais mais registradas na Delegacia de Repressão ao Crime Cibernético de Pernambuco 54

Figura 2 - Etapas do processo de investigação forense (KENT et al., 2006, p.3-1) 57

Figura 3 - Modelo tridimensional da *cloud forensics* 58

Figura 4 - Reprodução do sítio eletrônico do aplicativo Facebook, destinado a solicitações *on-line* para autoridades de aplicação da lei 125

Figura 5 - Estrutura do Capítulo II da Convenção de Budapeste sobre o Cibercrime 142

Figura 6 - Estrutura do Capítulo III da Convenção de Budapeste sobre o Cibercrime 142

Figura 7 - Estrutura normativa da Convenção da União Africana sobre Segurança Cibernética e Proteção de Dados Pessoais 154

Figura 8 - Processo de tramitação, nos Estados Unidos, de uma requisição realizada nos termos de Acordo de Assistência Judiciária em Matéria Penal - MLAT. 186

Figura 9 - Diagrama da proposta do Departamento de Justiça dos Estados Unidos 186

Figura 10 - Expressão booleana com as palavras-chaves de interesse, sobre a IEEE Xplore 278

SUMÁRIO

1 INTRODUÇÃO 23

2 OS DESAFIOS AO ACESSO EXTRATERRITORIAL A EVIDÊNCIAS CRIMINAIS EM NUVEM COMPUTACIONAL 32

2.1 O problema do acesso transfronteiriço a evidências criminais em nuvem 32

2.2 Justificativa 39

2.3 Objetivos 40

2.4 Delimitação da abordagem 41

2.4.1 Evidências criminais eletrônicas 41

2.4.2 As diligências para a produção de prova 42

2.4.3 O ambiente de computação em nuvem 44

2.4.4 Crime cibernético 46

2.4.5 Guerra cibernética 47

2.4.6 A investigação criminal na *Dark Web* 48

2.4.7 Escopo negativo da pesquisa 51

2.5 Perguntas de pesquisa 51

2.6 Hipóteses 52

2.7 Metodologia 52

3 A FORENSE DIGITAL EM NUVEM COMPUTACIONAL 55

3.1 A Forense digital 55

3.2 As fases da forense digital 56

3.3 A forense digital em nuvem computacional 58

3.3.1 Os desafios da computação em nuvem à forense digital 61

3.3.2 *Frameworks* para a forense digital em nuvem computacional 62

3.4 Antiforense digital 68

3.4.1 Destruição de dados 69

3.4.2 Ocultação de dados 70

3.4.2.1 Criptografia 70

3.4.2.2 Esteganografia 72

3.4.3 Eliminação da fonte 72

3.4.4 Falsificação 73

3.5 Técnicas de investigação criminal em nuvem computacional 73

3.6 Contribuições à pesquisa 75

4 O CASO *MICROSOFT IRELAND* 76

4.1 O *Electronic Communications Privacy Act* *76*

4.2 O *Stored Communications Act* 77

4.3. Os projetos de lei para alterar o SCA 82

4.3.1 O *Law Enforcement Access to Data Stored Abroad Act* *82*

4.3.2 O *E-mail Privacy Act* 82

4.3.3 O *International Communications Privacy Act* *83*

4.4 *Microsoft Ireland Case*: *Microsoft Corporation* versus *United States of America* 85

4.4.1 Descrição dos fatos 85

4.4.2 O Mandado (*Warrant 13 MAG 2814*) e a resposta da Microsoft 87

4.4.3 Resposta dos Procuradores do *U.S. District Court for the Southern District of New York* sobre a decisão da Microsoft 89

4.4.3.1 O SCA não admite recusa a cumprimento de mandado judicial 89

4.4.3.2 Provedor de serviço norte-americano deve cumprir mandado de produção de informações, independentemente de onde os dados estejam armazenados 90

4.4.3.3 O SCA-Warrant é diferente do mandado de busca convencional. 90

4.4.3.4. O SCA Warrant não tem natureza extraterritorial 91

4.4.3.5 A política da Microsoft impede a coleta de evidências criminais armazenadas no exterior 91

4.4.4 Argumentos da Microsoft em resposta aos Procuradores da *United States District Court for the Southern District of New York* 92

4.4.4.1 Tribunal norte-americano não tem competência para expedir mandado extraterritorial. 93

4.4.4.2 O *Warrant* expedido tem natureza extraterritorial. 93

4.4.4.3. A cooperação internacional é o meio adequado para requisitar os dados 93

4.4.5 Resposta do *Magistrate Judge* James C. Francis IV 94

4.4.5.1 O SCA-Warrant não viola o princípio da extraterritorialidade. 94

4.4.5.2 A história legislativa do SCA ampara a ordem 95

4.4.5.3 Limitação territorial traz prejuízos à investigação criminal 95

4.4.5.4 O SCA não presume a extraterritorialidade 96

4.4.6 Resposta da *Chief Judge* ao recurso da Microsoft 96

4.4.7 A decisão da *United States Court of Appeals for the Second Circuit* 97

4.4.8 Contribuições dos *amicus curiae* 99

4.5 A situação atual do processo 100

4.6 Contribuições à pesquisa 100

5 O ESPAÇO CIBERNÉTICO NO DIREITO INTERNACIONAL 102

5.1 Considerações iniciais sobre o Direito Internacional Público 102

5.2 Os elementos do Estado no Direito Internacional 103

5.2.1 A comunidade de indivíduos 104

5.2.2 O território 104

5.2.3 Um governo autônomo e independente 106

5.2.4 A finalidade e a capacidade de manter relações com outros Estados .. 108

5.3 A Aplicação da lei processual penal no espaço: o exemplo do Brasil 108

5.4 Os territórios *nullius* 111

5.5 Um enfoque territorial sobre o espaço cibernético no Direito Internacional 113

5.6 O princípio da territorialidade e a coleta de evidências criminais eletrônicas 118

5.7 A transnacionalidade do crime, seus efeitos na disposição das evidências eletrônicas e os princípios condicionantes da jurisdição 120

5.7.1 O exemplo da justiça penal brasileira 123

5.8 A incidência da lei sobre a territorialização dos dados eletrônicos 124

5.9 O Brasil e a Federação Russa: a normatização interna sobre os dados eletrônicos 126

5.10 Contribuições à pesquisa 127

6 AS EVIDÊNCIAS CRIMINAIS ELETRÔNICAS NAS NORMAS INTERNACIONAIS 129

6.1 Considerações iniciais sobre tratado internacional 129

6.2 As organizações internacionais intergovernamentais e as normas de direito internacional sobre o crime cibernético 132

6.3 Acordo de Cooperação entre os Estados Membros da Comunidade dos Estados Independentes para o Combate a Infrações Relacionadas à Informação Computacional 137

6.3.1 A Comunidade dos Estados Independentes 137

6.3.2 A estrutura normativa do Acordo 137

6.3.3 Alterações em andamento 139

6.4 A Convenção de Budapeste sobre o Cibercrime 139

6.4.1 O Conselho da Europa e a elaboração da Convenção de Budapeste sobre o Cibercrime 139
6.4.2 Estrutura normativa da Convenção 141
6.4.3 O acesso transfronteiriço a dados armazenados 143
6.4.4 Alterações em andamento 147
6.5 Acordo entre os Governos dos Estados Membros da Organização para Cooperação de Xangai sobre a Cooperação no campo da Segurança da Informação Internacional 147
6.5.1 A Organização para Cooperação de Xangai 147
6.5.2 A estrutura normativa do Acordo 148
6.6 A Convenção da Liga dos Estados Árabes sobre o Combate às Ofensas contra a Tecnologia da Informação 149
6.6.1 A Liga dos Estados Árabes 149
6.6.2 Estrutura normativa da Convenção 149
6.6.3 O acesso transfronteiriço a dados armazenados 151
6.7 Convenção da União Africana sobre Segurança Cibernética e Proteção de Dados Pessoais 152
6.7.1 A União Africana 152
6.7.2 A estrutura normativa da Convenção 153
6.7.3 O acesso transfronteiriço a dados armazenados 155
6.8 Acordo entre os Estados Unidos da América e a União Europeia sobre a Proteção dos Dados Pessoais no Âmbito da Prevenção, Investigação, Detecção e Repressão de Infrações Penais 156
6.8.1 A estrutura normativa do Acordo 156
6.9 Organização das Nações Unidas 157
6.10 Contribuições à pesquisa 159
7 O ESTADO DA ARTE SOBRE A COLETA EXTRATERRITORIAL DE EVIDÊNCIAS CRIMINAIS ELETRÔNICAS 161

7.1 Os desafios para uma solução jurídica 162

7.2 A necessidade de elaboração de tratado internacional 163

7.3 A proposta do Segundo Protocolo Adicional à Convenção de Budapeste 163

7.3.1 Assistência judiciária mútua mais efetiva 165

7.3.2 Cooperação direta com provedores de serviço em outras jurisdições. 167

7.3.3 Estruturas explícitas e garantias robustas para o acesso extraterritorial a evidências criminais em nuvem 169

7.3.4 Salvaguardas e requisitos de proteção de dados. 170

7.3.5 Outras medidas oriundas do Conselho da Europa 172

7.4 Requisição de evidências criminais diretamente a provedor de computação em nuvem 173

7.5 A reformulação do MLAT 182

7.6 Proposta do Departamento de Justiça dos Estados Unidos para o acesso extraterritorial a evidências de crimes graves, inclusive o terrorismo 185

7.7 Um modelo de investigação criminal para as autoridades policiais 189

7.7.1 A Jurisdição investigativa 189

7.7.2 Teste multifatorial 190

7.7.3 Afastar a territorialidade 190

7.7.4 Uma nova estrutura para definir a jurisdição 191

7.8 A solução é harmonizar o direito substantivo 191

7.9 Enunciado no Direito Brasileiro 192

7.10 Mecanismos alternativos de cooperação internacional 193

7.11 Uma nova abordagem para avaliar a jurisdição dos mandados expedidos nos termos do SCA 194

7.12 Uma analogia interpretativa com o direito de perseguição 196

7.13 Contribuições à pesquisa 198

8 COOPERAÇÃO DIRETA ENTRE ESTADO E PROVEDOR DE COMPUTAÇÃO EM NUVEM EM OUTRA JURISDIÇÃO 199

8.1 Discussões preliminares 199

8.2 Delineamento da proposta 205

8.3 Premissas que orientam a proposta 206

8.4 Descrição dos requisitos da proposta 207

8.4.1 O mecanismo jurídico a ser utilizado 207

8.4.2 Os tipos de evidências criminais eletrônicas suscetíveis de serem requisitadas 209

8.4.3 Os crimes graves 210

8.4.4 Os requisitos para um Estado aderir ao tratado internacional 212

8.4.5 O principal compromisso dos Estados Parte 213

8.4.6 As condições que autorizam a requisição direta ao provedor de nuvem 213

8.4.7 As exigências legais por tipo de dados 214

8.4.8 As restrições 215

8.4.9 Os mecanismos de auditoria e transparência 215

8.4.10 A proteção de dados e respeito à privacidade 216

8.4.11 Proteção da soberania 219

8.4.12 Penalidades 219

8.5 Processo participativo para a elaboração do tratado internacional 219

8.6 Comparação entre o modelo proposto a os pesquisados 221

9 CONSIDERAÇÕES FINAIS 226

9.1 Respostas às perguntas de pesquisa 227

9.2 Recomendações para trabalhos futuros 228

9.3 Conclusão final 229

REFERÊNCIAS 231

GLOSSÁRIO 261

APÊNDICE A – PROTOCOLO DE REVISÃO SISTEMÁTICA 264

ANEXO A - OCORRÊNCIAS REGISTRADAS NA DELEGACIA DE POLÍCIA DE REPRESSÃO AO CRIME CIBERNÉTICO DE PERNAMBUCO, DE JANEIRO/2014 A OUTUBRO/2017 285

1 INTRODUÇÃO

O progresso a que chegaram os meios de comunicação, nos últimos cem anos, incluindo-se entre eles a Internet, trouxe inquestionáveis benefícios à humanidade, tais como o avanço da ciência e da tecnologia a serviço da saúde, da paz, do bem-estar da sociedade.

Descobertas científicas, que outrora teriam requerido enorme esforço, dedicação e tempo, tiveram facilitado o percurso das investigações, a realização das pesquisas, a comprovação das experiências, por meio de intercâmbio cultural em tempo recorde e em espaço global, que aceleraram a produção de conhecimento e aumentaram o rigor da produção científica de forma vertiginosa.

A Internet, valendo-se da informática, dos computadores, conduziu, como um dos principais instrumentos de evolução e aprimoramento técnico-científico, as transformações operadas no mundo, em seguimento que parece inesgotável, interminável, sem fim.

Culturalmente, permitiu o ensino, a pesquisa, o aprendizado à distância, difundiu mundialmente a arte, a literatura, a música, permitiu a evolução dos instrumentos e invenções a serviço do homem, aprimorando o trato da saúde, as condições de segurança, transportes, produção de alimentos, de energia renovável ou não renovável, em proporções inimagináveis, no início do século passado.

As relações sociais também experimentaram extremo influxo de mudanças, em detalhes mínimos, como a obsolescência da correspondência epistolar pelos correios, a assimilação de costumes de regiões distantes e o abandono de usos locais de longa tradição.

A grande rede oferece, por excelência, um ambiente único para o compartilhamento de ideias e informações, favorecendo o exercício da liberdade de expressão, que é direito fundamental positivado no parágrafo 2º do artigo 19 do Pacto Internacional sobre Direitos Civis e Políticos, de 1966[1].

[1] O Pacto Internacional sobre Direitos Civis e Políticos foi adotado pela XXI Sessão da Assembleia-Geral das Nações Unidas, em 16 de dezembro de 1966, e promulgado no Brasil, por força do Decreto nº 592, de 06 de julho de 1992 (BRASIL, 1992).

A Internet surge numa década de grandes conquistas científicas. A competição econômica e tecnológica entre países, mas sobretudo a disputa de poder entre eles, o desejo de sobrepor-se uns aos outros, dominarem-se pela força das armas e do conhecimento, e o temor de serem superados, subjugados, submetidos à hegemonia uns dos outros, em idos do século XX, em tempo imediatamente posterior à Segunda Guerra Mundial, gerou uma tensão internacional, polarizada pelos Estados Unidos da América e a então União das Repúblicas Socialistas Soviéticas (URSS), clima de ameaça velada que se denominou de Guerra Fria.

Nesse estado de medição de forças, de aterrorização recíproca, de guerra iminentemente próxima e não desejada, surgiu, como esforço de um espírito guerreiro, a busca de capacitar-se tecnologicamente para superar países opositores, a descoberta de que era possível aprimorar e agilizar a produção do conhecimento científico para fins bélicos, de fortalecimento do poder soberano, iniciando-se uma corrida entre as nações, com fins que foram de muito ultrapassados em favor da humanidade.

Na corrida pela conquista do espaço sideral, a URSS foi pioneira: em 1957, lança à órbita terrestre o primeiro satélite artificial, denominado *Sputnik 1*; em 1961, o russo Iuri Gagarin foi o primeiro ser humano a alcançar a órbita geocêntrica. Em resposta ao triunfo russo, no dia 20 de julho de 1969, sob intensa cobertura jornalística, astronautas americanos pousaram na Lua. Mas foi em dezembro desse mesmo ano que uma experiência, realizada na Califórnia/Estados Unidos e pouco divulgada à época, marcou o futuro das tecnologias da informação e das comunicações na sociedade global: entrou no ar uma rede experimental de computadores com 04 (quatro) nós, conectando as *University of California*, *Los Angeles* (UCLA), *University of California*, *Santa Barbara* (UCSB), *Stanford Research Institute*, *California* (SRI) e *University of Utah*, *Salt Lake City* (LEINER et al, 2012; TANENBAUM; WETHERALL, 2011; ZACON, 1997). Era o início da Internet.

Essa pequena rede de computadores foi o resultado inicial do programa do Departamento de Defesa dos Estados Unidos - DARPA[2], intitulado *Resource Sharing*

[2] *Defence Advanced Research Projects Agency*. Inicialmente chamada de ARPA, foi criada em 1958 pelo Presidente Eisenhower, dos Estados Unidos da América, em resposta ao lançamento do *Sputnik* 1 e por outras realizações soviéticas, que indicavam estarem os norte-americanos à retaguarda dos rivais da Guerra Fria, especialmente nas tecnologias de combate e defesa em conflitos bélicos (DARPA. Innovation at DARPA. July, 2016. Disponível em: <http://www.darpa.mil/attachments/DARPA_Innovation_2016.pdf. Acesso em: 20 jul. 2016.).

Computer Networks, que ficou internacionalmente conhecida como Arpanet (BOLT BERENEK AND NEWMAN, 1981).

Internet, para o *United States Federal Networking Council* (1995), é termo utilizado para designar o sistema global de informações que:

> *(i) is logically linked together by a globally unique address space based on the Internet Protocol (IP) or its subsequent extensions/follow-ons;*
> *(ii) is able to support communications using the Transmission Control Protocol/Internet Protocol (TCP/IP) suite or its subsequent extensions/follow-ons, and/or other IP-compatible protocols; and*
> *(iii) provides, uses or makes accessible, either publicly or privately, high level services layered on the communications and related infrastructure described herein.*[3]

Para Kahn e Cerf (1999), a Internet fundamenta-se na interconexão global de centenas de milhares de diferentes computadores, entidades de comunicação e sistemas de informações heterogêneos, sendo possível sua implementação graças ao uso comum de um conjunto de padrões de comunicação, procedimentos e formatos. A comunicação entre os vários tipos de dispositivos, de fabricantes diversos e sistemas operacionais distintos, é realizada por meio de protocolos comuns, sendo os dois iniciais chamados *Transmission Control Protocol* / *Internet Protocol* (TCP/IP), que constituíram a principal base de operação da rede.

Trata-se de um sistema incomum, no sentido de não ter sido planejado nem ser controlado por qualquer governo, instituição pública ou privada (TANENBAUM; WETHERALL, 2011, p.33).

A Internet sofreu mudanças ao longo dos tempos. Seu tamanho aumentou consideravelmente com o surgimento do *World Wide Web* (WWW), no início da década de 1990, e com a abertura de sua exploração comercial, pelo Governo dos Estados Unidos, em 1991(KUROSE; ROSS, 2010). Nesse mesmo ano, foi realizada no Brasil a primeira conexão, por meio da Fundação de Amparo à Pesquisa do Estado de São Paulo – Fapesp (CARVALHO, 2006), sendo sua abertura para fins comerciais realizada apenas em 1994, por meio da Embratel. Em janeiro de 1993, quando o *Internet System Consortium* iniciou a pesquisa de Domínio Internet, o número de *hosts*

[3] Livre tradução da autora: (i) é logicamente conectado por um espaço de endereçamento global único baseado no Protocolo Internet (IP) ou suas subsequentes extensões/seguintes; (ii) é capaz de fornecer comunicações usando o conjunto Protocolo de Transmissão e Controle/Protocolo Internet (TCP/IP) ou suas subsequentes extensões, e/ou outro protocolo IP compatível; e (iii) fornece, usa ou torna acessível, tanto de forma pública ou privada, serviços de alto nível baseados em comunicações e na infraestrutura descrita acima.

visíveis era de aproximadamente 1 milhão. Em julho de 2017, esse número já superava a marca de 1 (um) bilhão[4].

O número de usuários da Internet mais do que triplicou em uma década: de 1 (um) bilhão, em 2005, para cerca de 3,2 bilhões, no final de 2015, o equivalente a cerca de 40% da população mundial. Nos países em desenvolvimento, apenas 31% da população acessavam-na em 2014, em comparação com 80% nos países de renda alta (BANCO MUNDIAL, 2016). Na lista de países com maior número de usuários da Internet, a China ocupa a primeira posição, com 705 milhões, seguida pela Índia (333 milhões), Estados Unidos (242 milhões) e Brasil (120 milhões) (UNCTAD, 2017). Em nível mundial, o telefone celular é a principal forma de acesso à Internet dos habitantes de países em desenvolvimento. Entre os 20% dos domicílios mais pobres, quase sete de cada 10 têm telefone celular (BANCO MUNDIAL, 2016). No Brasil, no ano de 2016, em 60,3% dos domicílios, o acesso à Internet ocorria por meio do telefone celular (PESQUISA NACIONAL POR AMOSTRA DE DOMICÍLIO CONTÍNUA, 2017).

E há previsão de crescimento. Estima-se que o mundo terá 5,8 bilhões de assinantes de serviços móveis em 2020, o equivalente a 70% da população do planeta. Do total desses assinantes, 524 milhões estarão na América Latina, sendo que 262 milhões, quase metade, conectados à Internet 3G e 4G. O Brasil vai liderar o uso de *smartphones* na região. Em 2015, o país tinha aproximadamente 248 milhões de assinantes móveis. A previsão para 2020 é de 304 milhões, sendo que 80% usuários de celulares inteligentes conectados à Internet[5]. Todo esse movimento abre espaço para o desenvolvimento de aplicações em computação em nuvem para alimentar a grande malha de dispositivos conectados às redes de comunicação. No Brasil, dentre os aplicativos mais usados estão o *Whatsapp*, *Facebook*, *Instagram*, *Facebook Messenger* e *Twitter*[6]. As estatísticas são um indício da inserção da computação em nuvem na vida das pessoas e das empresas, que a utilizam para entregar serviços *on-line*, bem como para suportar seus processos de negócios. Essa característica mostra mais uma inovação na Internet, cujas aplicações disponíveis nos

[4] Internet Systems Consortium (ISC). Internet Domain Survey. Number of Hosts advertised in the DNS. Jul, 2017. Disponível em: <https://ftp.isc.org/www/survey/reports/current/>. Acesso em: 16 out. 2017.
[5] GSMA. The Mobile Economy. 2016. Disponível em: <https://www.gsmaintelligence.com/research/?file=97928efe09cdba2864cdcf1ad1a2f58c&download>. Acesso em: 20 jun. 2017.
[6] CONECTA. WhatsApp é o aplicativo de rede social mais usado pelos internautas brasileiros. A pesquisa foi realizada com 2.000 internautas, em junho de 2017. Disponível em: < http://conecta-i.com/?q=pt-br/whatsapp-%C3%A9-o-app-de-rede-social-mais-usado-pelos-internautas-brasileiros>. Acesso em: 20 set. 2017.

primórdios da rede eram basicamente a transferência de arquivos (*ftp*), o *login* remoto (*telnet*) e o correio eletrônico (*e-mail*) (LEINER et al, 2012).

No entanto, nessa instrumentalização benéfica, subjacentes ocorrem, justificando a assertiva de que ao inventor não é dado controlar os efeitos todos e usos de seus inventos, muitos riscos, males e danos, não queridos pelos que promoveram ou promovem as possibilidades cada vez maiores de emprego da Internet em benefício do ser humano. Por ser global, instantânea, digital, intrinsecamente transnacional, e ter a capacidade de processar dados, oferecendo um ambiente propício à prática de crimes em que sistemas informáticos são meios ou alvos de ataques, a Internet desperta o interesse especial da criminologia (KOOPS, 2010).

Proliferam os crimes, o terrorismo, instrumentalizados pela tecnologia da informação e comunicação. Crimes multinacionais, organizações criminosas transnacionais, ou nacionais com efeitos internacionais, constituem uma ofensa à tranquilidade pública, à paz social, à economia, que se erige em preocupação dos povos, cuja prevenção passa pela possibilidade técnica e jurídica de desvendar essas infrações penais e sua autoria.

O crime cibernético vem se tornando cada vez mais hostil. Se antes o criminoso evitava o confronto com a vítima, utilizando-se da dissimulação, persuasão (engenharia social) como subterfúgio para obter vantagem indevida, hoje ele ameaça, extorque, amedronta suas vítimas, viola os direitos mais fundamentais do homem, como vem ocorrendo em casos de exploração sexual, pornografia infantil, sequestro de dados (*ransomware*), ataque distribuído por negação de serviço (DDoS[7]). O modelo de negócio baseado no crime como serviço (*Crime-as-a-Service - CaaS*) proporciona acesso relativamente fácil a produtos ilegais e a contratação de serviços ilícitos (EUROPOL, 2015). Os mercados *on-line* sobre a *Darknet* são plataformas usadas para anunciar e vender todos os tipos de drogas, gerando lucros de aproximadamente 24 bilhões de Euros, por ano (EUROPOL, 2017b).

E a cada ano, o crime cibernético vem se reinventando. No final de 2016, foi registrado o primeiro ataque maciço proveniente de dispositivos Internet das Coisas (IoT), que foram tranformados em *botnet* para ataques distribuídos de negação de serviço (DDoS), pelo *malware Mirai*. Foram cerca de 150.000 (cento e cinquenta mil)

[7] *Distributed Denial-of-Service*

roteadores e câmeras de circuito fechado de televisão (CCTV) infectados pelo *malware*, causando inclusive situações vexatórias na costa oeste dos Estados Unidos (EUROPOL, 2017a).

Trata-se ainda de uma criminalidade que não reconhece fronteiras nem respeita soberania estatal, seja pelos métodos de seu planejamento, organização e execução, seja pelo alcance dos danos gerados, seja ainda pela capacidade de movimentação dos recursos ilícitos auferidos nos sistemas econômicos, oficiais ou não, de diversas nações e organizações (WEBER, 2011). Essa característica transnacional frequentemente traz desafios aos sistemas criminais dos Estados, por ser o Direito Penal tradicionalmente expressão da jurisdição territorial de onde a ofensa ocorreu (CLOUGH, 2011).

Novas arquiteturas tecnológicas, como a computação em nuvem, vêm contribuindo sobremaneira para o surgimento de incertezas acerca da efetividade dos tratados internacionais que visam a proteção da sociedade contra a criminalidade intensiva no uso da tecnologia da informação e comunicação.

É característica dessa arquitetura a fragmentação da conta de usuário e a distribuição do conteúdo das comunicações, dos metadados, dos dados pessoais entre os vários *data centers* da empresa, em geral espalhados geograficamente por diversas regiões do mundo, com o fim de proporcionar qualidade dos serviços prestados, com a diminuição da latência da rede. Consequentemente, questiona-se sobre a possibilidade de uma autoridade estatal poder utilizar-se unicamente do devido processo legal interno no seu país para requisitar dados extraterritoriais para constituir prova no processo penal.

O incremento significativo do armazenamento de arquivos pessoais e de comunicações no ambiente da computação em nuvem está diretamente relacionado com a facilidade de gerenciamento desses dados. O crescimento de servidores de *e-mail* é um exemplo. Nos tempos em que foi lançado, os usuários armazenavam os *e-mails* localmente, nos computadores pessoais. Então, quando um *e-mail* era enviado, o remetente mantinha o original armazenado em seu computador e o destinatário recebia uma cópia. Assim, os dados existiam em dois lugares: no computador do remetente e no computador do destinatário da mensagem. Servidores intermediários poderiam manter temporariamente uma cópia, embora a responsabilidade pelo armazenamento fosse exclusivamente dos envolvidos na comunicação, ou seja, o destinatário e o remetente.

No entanto, esse modelo apresentava algumas desvantagens. Para ler o *e-mail*, o destinatário ou o remetente precisavam acessar o computador onde se encontrava instalado o aplicativo de correio eletrônico. O *webmail* (aplicativo de correio eletrônico na *web*) veio superar essa limitação, alterando um serviço que era local para um serviço baseado na computação em nuvem. O mesmo ocorreu com o armazenamento de arquivos digitais em geral, como fotos, vídeos, músicas, filmes.

Ademais, o aumento da criptografia ponto-a-ponto, inviabilizando a interceptação telemática em alguns aplicativos, também fez aumentar o número de requisições para divulgação de dados protegidos por sigilo e armazenados fora dos limites territoriais da jurisdição interessada (SWIRE; HEMMINGS; VERGNOLLE, 2016).

Acredita-se que o direito internacional, por meio da edição de normas internacionais de caráter vinculante, uniformizadoras de procedimentos, pode contribuir para aperfeiçoar a segurança jurídica das atividades forenses relativas ao acesso a evidências criminais eletrônicas, armazenadas em Estado estrangeiro, garantindo-lhe o valor probatório no processo penal.

Ao longo dessa pesquisa, diversos modelos de procedimentos relativos à forense digital em ambiente de computação em nuvem foram apresentados, esbarrando todos, no entanto, em limitações legais impostas pela característica multijurisdicional da tecnologia analisada, e que lhe impulsiona e diferencia dos modelos anteriores existentes. Hoje, é impensável exigir das empresas de tecnologia da informação e comunicação que retrocedam a modelos de negócio ou tecnológico na Internet, atrelados à territorialização dos dados digitais, no intuito de facilitar o exercício das atribuições do Estado, inclusive no dever de apurar o delito e punir os infratores da lei.

O presente trabalho insere-se nessa problemática do direito internacional, do direito processual penal e da ciência da computação, e visa contribuir com as discussões interdisciplinares nas áreas do direito e da ciência da computação acerca de questões legais relacionadas à localização, preservação, produção, acesso, busca e apreensão extraterritorial de evidências eletrônicas de crime, quando armazenadas em ambiente de computação em nuvem, sobre território estrangeiro.

Além da presente seção, esta Tese está organizada em mais oito:

a) OS DESAFIOS AO ACESSO EXTRATERRITORIAL A EVIDÊNCIAS CRIMINAIS EM NUVEM COMPUTACIONAL, que tem o propósito de

descrever os problemas que motivaram a realização dessa pesquisa, bem como visa apresentar a justificativa, os objetivos, as perguntas de pesquisa, hipóteses e a metodologia empregada, além de delimitar a abordagem conceitual;

b) A FORENSE DIGITAL EM NUVEM COMPUTACIONAL, com o objetivo apresentar conceitos básicos atinentes à computação forense, bem como *frameworks* utilizados pelos peritos no exame de dados digitais, em busca de evidências da prática de crimes, para constituir prova no processo penal;

c) O CASO *MICROSOFT IRELAND*, que analisa peças do processo judicial instaurado para dirimir litígio entre a empresa *Microsoft Corporation* e os Estados Unidos, relativamente ao cumprimento extraterritorial de mandado de busca e apreensão de evidências criminais eletrônicas, armazenadas em ambiente de computação em nuvem, sobre território de Estado estrangeiro;

d) O ESPAÇO CIBERNÉTICO NO DIREITO INTERNACIONAL, que apresenta uma abordagem acerca do espaço cibernético, no contexto do direito internacional, enfatizando os desafios trazidos pela computação em nuvem à persecução criminal;

e) AS EVIDÊNCIAS CRIMINAIS ELETRÔNICAS NAS NORMAS INTERNACIONAIS, que objetiva identificar, por meio da análise dos tratados internacionais de abrangência regional, relativos ao controle da criminalidade cibernética, o tratamento legal conferido à localização, preservação, acesso, produção, busca e apreensão de evidências criminais, localizadas em território de outro Estado Parte;

f) O ESTADO DA ARTE SOBRE A COLETA EXTRATERRITORIAL DE EVIDÊNCIAS CRIMINAIS ELETRÔNICAS, que apresenta os caminhos para onde estão seguindo as propostas existentes, elaboradas com o fim de superar os desafios trazidos pela computação em nuvem à coleta extraterritorial de evidências criminais eletrônicas;

g) COOPERAÇÃO DIRETA ENTRE ESTADO E PROVEDOR DE COMPUTAÇÃO EM NUVEM EM OUTRA JURISDIÇÃO, que apresenta a proposta final dessa Tese, atinente à elaboração de tratado internacional,

com a finalidade de disciplinar a requisição remota de dados extraterritoriais, armazenados em ambiente de computação em nuvem;

h) CONSIDERAÇÕES FINAIS, que apresenta as principais conclusões obtidas a partir desse estudo, bem como as recomendações de temas para trabalhos futuros.

2 OS DESAFIOS AO ACESSO EXTRATERRITORIAL A EVIDÊNCIAS CRIMINAIS EM NUVEM COMPUTACIONAL

A presente seção tem o propósito de descrever os problemas que motivaram a realização desta pesquisa, enfatizando os desafios enfrentados pelas autoridades de persecução criminal e por peritos forenses nas atividades de localização, preservação, produção, acesso, busca e apreensão extraterritorial a evidências criminais eletrônicas, armazenadas em ambiente de computação em nuvem.

Não apenas os agentes públicos, mas a sociedade civil e os usuários da tecnologia em comento também externam preocupações quanto à legalidade dos atos praticados pelas referidas autoridades, que podem resultar em possível violação de direitos fundamentais.

Também são apresentados nesta seção a justificativa para a escrita da tese, os objetivos a que se pretende alcançar, a delimitação do tema, com ênfase no escopo negativo, além das perguntas de pesquisa, hipóteses e metodologia utilizada.

2.1 O problema do acesso transfronteiriço a evidências criminais em nuvem

A computação em nuvem é uma tecnologia relativamente recente, implementada em meados da década dos anos 2000. Dentre as facilidades técnicas oferecidas, que se revestem em benefícios aos usuários, estão a virtualização do ambiente e a distribuição da infraestrutura por lugares distantes, as vezes envolvendo países distintos, ocasionando assim um verdadeiro fenômeno de internacionalização dos dados, com tendência de crescimento. A empresa norte-americana Google LLC, por exemplo, possui 15 (quinze) *data centers*[8], dos quais 07 (sete) estão fora dos

[8] https://www.google.com/about/datacenters/inside/locations/index.html. Acesso em: 13 dez. 2017.
Américas: Berkeley County (Carolina do Sul), Council Bluffs (Iowa), Douglas County (Georgia), Condado de Jackson (Alabama), Lenoir (Carolina do Norte), Mayes County (Oklahoma), Condado de Montgomery(Tennessee), Quilicura (Chile), The Dalles (Oregon); Ásia: Changhua County, (Taiwan), Cingapura; Europa: Dublin (Irlanda), Eemshaven (Holanda), Hamina (Finlândia), St Ghislain(Bélgica).

Estados Unidos, além de manter representação comercial em cerca de 50 (cinquenta) países[9].

A internacionalização dos dados é especialmente verdadeira para os usuários dos serviços de computação em nuvem fora dos Estados Unidos. Empresas norte-americanas, por exemplo, são responsáveis por 7 dos 10 *websites* mais populares no Brasil[10], 8 dos 10 em Portugal[11], 4 dos 10, na Rússia[12], todos os 10 primeiros, na Índia[13].

Essa internacionalização dos dados traz consequências de ordem prática e jurídica.

As consequências de natureza prática relacionam-se, por exemplo, à segurança das informações. Entre 2013 e 2014, 47% dos adultos nos Estados Unidos tiveram suas informações pessoais, armazenadas em ambiente de computação em nuvem, comprometidas (BAUTISTA, 2014).

Os efeitos legais referem-se tanto ao alcance da aplicação da lei quanto aos novos procedimentos da investigação criminal e à forense digital.

Hoje, mais do que nunca, crimes são praticados no território de um Estado e seus efeitos se propagam para Estados distantes (UNODC, 2017; GUILLOT, 2014; UNODC, 2013; ITU, 2009; ITU, 2012; COSTA, 2011; KOOPS, 2010; FERREIRA, 2007; FERREIRA, 2005). A pluralidade de jurisdições envolvidas levanta conflitos na aplicação do direito que, apesar de sempre existirem, estão mais frequentes, motivados pela globalização da tecnologia da informação e comunicação. As controvérsias aumentam quando uma atividade é permitida no Estado onde foi praticada e ilegal onde seus efeitos se manifestam.

É comum entre usuários da Internet a compreensão de que uma lei interna, vigente em seu país de residência e editada para regular relações no mundo físico, excepcionalmente alcance os atos praticados no espaço cibernético. No entanto, é questionada a aplicação de lei estrangeira, editada em países com os quais o usuário não mantém qualquer vínculo no mundo físico, para regular o comportamento dele no espaço cibernético, mesmo que fisicamente o usuário se encontre em seu país.

[9] https://www.google.com.br/about/our-story/. Acesso em: 22 nov. 2017.
[10] https://www.alexa.com/topsites/countries/BR. Acesso em: 22 nov. 2017.
[11] https://www.alexa.com/topsites/countries/PT. Acesso em: 22 nov. 2017.
[12] https://www.alexa.com/topsites/countries/RU. Acesso em: 22 nov. 2017.
[13] https://www.alexa.com/topsites/countries/IN. Acesso em: 22 nov. 2017.

Parece um equívoco que a mera presença cibernética em outra jurisdição seja suficiente para desencadear a aplicação do direito estrangeiro (REED, 2012).

As leis são editadas para regular não apenas as atividades desenvolvidas no interior das fronteiras físicas de um Estado, mas alcançam também as ações praticadas fora de sua jurisdição, quando efeitos relevantes ao direito se fazem sentir dentro do território nacional, como nos casos de extraterritorialidade da lei penal brasileira, constantes no art. 7º do Código Penal Brasileiro (BRASIL, 1940).

Na época pré-globalização, esses efeitos transnacionais constituíam preocupação unicamente de grandes empresas multinacionais, cujas subsidiárias espalhavam-se por diversas localidades mundo afora, sujeitando-se a diferentes jurisdições. Na atual sociedade globalizada, e especialmente com a realidade do espaço cibernético, essa preocupação vem se refletindo tanto nas médias e pequenas empresas quanto para os usuários, individualmente.

Nesse ambiente globalizado e cibernético, na medida em que os litígios transnacionais vêm aumentando, legislações domésticas vêm sendo editadas para regular condutas extraterritoriais, bem como decisões judiciais vêm sendo proferidas nos casos em que os efeitos do crime são sentidos internamente (REED, 2012).

Em 1996, empresa sediada nos Estados Unidos e segunda maior provedora de serviços *on-line* a época, a *Compuserve*, bloqueou o acesso de seus usuários a mais de 200 grupos de discussão na Internet, em cumprimento a ordem decorrente de uma investigação criminal, que estava sendo conduzida por Procurador do Estado da Bavária, na Alemanha, relacionada à publicação de registros pornográficos, envolvendo crianças. Segundo entendimento do Procurador, a empresa provedora de serviço seria corresponsável pela publicação do material (NASH, 1996). Em resposta, ativistas em favor da liberdade de expressão protestaram contra o que intitularam ser uma exportação dos padrões morais germânicos para o mundo. A empresa restabeleceu o acesso para a maioria dos grupos, exceto para os assinantes da Alemanha. Em 1997, o Gerente Geral da *CompuServe,* em Munique, foi indiciado por distribuição de pornografia pela Internet (GREWLICH, 1999, p. 275), sendo inocentado dois anos mais tarde[14].

[14] ANDREWS, E.L.. German Court Overturns Pronography Rules Against Compuserve. The New York Times, United States of America, 18 nov. 1999. International Business. Disponível em: <http://www.nytimes.com/1999/11/18/business/international-business-german-court-overturns-pornography-ruling-against.html>. Acesso em: 10 out. 2016.

A internacionalização dos dados também se constitui em desafios às autoridades de investigação criminal e à forense computacional. Em paralelo ao crescimento da utilização da nuvem computacional para o armazenamento de arquivos, vem sendo registrado um aumento no número de evidências criminais encontradas nesse ambiente, ensejando na necessidade de considerar aspectos legais para a requisição extraterritorial, a natureza volátil e a facilidade de alteração e exclusão dos dados digitais (BECHTEL, 2013).

O primeiro desafio ao agente de investigação criminal, quando se depara com evidências de crimes no ambiente de computação em nuvem, é identificar sob qual provedor de serviço Internet o dado encontra-se armazenado para, em seguida, definir se o referido provedor de serviço é nacional ou estrangeiro. Sendo nacional ou estrangeiro com representação comercial no país, o agente poderá requisitar a diligência diretamente ao provedor. Caso não haja representação comercial[15] ou seja negada resposta à requisição de coleta dos dados digitais, o agente poderá utilizar-se de instrumentos da cooperação internacional com instituições de aplicação da lei no Estado estrangeiro ou com instituições internacionais, como Interpol, Europol *(European Union Agency for Law Enforcement Cooperation)* ou Eurojust (*The European Union's Judicial Cooperation Unit*) (OSULA, 2015a), para solicitar apoio nas investigações e na preservação das evidências eletrônicas que, facilmente, podem ser alteradas, apagadas (OSULA, 2015a).

Quando exigido, utilizar-se-á de cooperação jurídica internacional[16], por meio de acordo bilateral de assistência judiciária em matéria penal (*Mutual Legal Assistence Treaty* – MLAT)[17] ou através de carta rogatória (OSULA, 2015a; OSULA, 2015b;

[15] Algumas propostas apresentadas na seção 7 referem-se ao contato direto com o provedor de serviços de nuvem, independentemente da representação comercial no país.

[16] A cooperação jurídica internacional (ou ainda assistência, ajuda ou auxílio mútuo internacional) é definida como um conjunto de atos que regulamenta o relacionamento entre dois ou mais Estados, ou ainda entre Estados e Tribunais Internacionais, tendo em vista a necessidade gerada a partir das limitações territoriais de soberania. A amplitude da expressão abrange o intercâmbio não somente entre órgãos judiciais, mas também entre órgãos judiciais e administrativos de Estados distintos. Ademais, a expressão "cooperação jurídica internacional" não abrange apenas a cooperação judicial ou jurisdicional, mas também a cooperação administrativa entre órgãos investigatórios, que igualmente produzem efeitos jurídicos. A qualificação da cooperação como jurídica está mais associada aos efeitos que desta possam advir do que propriamente à natureza do objeto da cooperação ou à qualidade de quem coopera (BECHARA, 2011). Em sentido estrito, a cooperação administrativa internacional não está vinculada a uma demanda ou feito criminal, mas a necessidade de aprimoramento tecnológico, compartilhamento de informações, estratégias de atuação entre os órgãos envolvidos (WEBER, 2011).

[17] Nos Estados Unidos da América, são conhecidos como *Mutual Legal Assistence Treaty* – MLAT. Os Governos do Brasil e dos Estados Unidos da América mantém Acordo de Assistência Judiciária em Matéria Penal, promulgado por força do Decreto nº 3.810, de 02 de maio de 2001 (BRASIL, 2001).

WALDEN, 2011). Segundo pesquisa da Organização das Nações Unidas (ONU), cerca de 70% dos países que responderam ao questionamento, informaram o MLAT como o principal instrumento jurídico formal de cooperação internacional, para a obtenção de evidências criminais (UNODC, 2013).

O contato com provedor de serviço (nacional ou estrangeiro) em geral é realizado através de algum meio de comunicação convencional (telefone, fax, formulário, *e-mail*, sistema *on-line*). Ao receber a requisição, a instituição decidirá se atende ou não, caso acredite de "boa-fé que a lei [os] obriga a fazer isso"[18].

Eventualmente, as dificuldades para obter evidências criminais eletrônicas, incluindo a negativa por parte de empresas provedoras de computação em nuvem, mesmo perante instrumento de cooperação jurídica internacional formalmente estabelecido, podem estimular agências de investigação criminal a recorrerem a práticas unilaterais invasivas (CURRIE; 2017, SVANTESSON, 2016a) que, na maioria das vezes, são desonestas e ilegais, por violarem direitos humanos fundamentais, podendo constituir crime a sua prática, a depender da legislação interna do país.

A ausência de regramento internacional, da mesma forma, pode favorecer à extensão transnacional de poderes de investigação, comprometendo assim proteções processuais no curso da persecução criminal e favorecendo a perseguições pessoais em países onde a promoção e a proteção dos direitos humanos são deficitárias (CYBERCRIME CONVENTION COMMITTEE, 2014). De acordo com relatório do Comitê da Convenção de Budapeste sobre o Cibercrime (2014), um número cada vez maior de países da União Europeia está adotando medidas unilaterais para obter acesso extraterritorial a dados armazenados no estrangeiro, com a finalidade de proteger seus nacionais. Em contraposição, é interesse da sociedade civil organizada manter a Internet livre e aberta, protegendo os direitos fundamentais dos usuários e de terceiros (SWIRE; HEMMINGS, 2015).

Ocorre que, esse meio tradicional de cooperação jurídica internacional vem sendo questionado quanto a sua efetividade, quando envolve a busca extraterritorial de evidências eletrônicas de crime, em ambiente de computação em nuvem (CURRIE, 2017; KRISHNAMURTHY, 2016; SVANTESSON, 2016a; CYBERCRIME CONVENTION COMMITTEE, 2016b; JAYCOX; TIEN, 2015; OSULA, 2015a; OSULA, 2015b; CYBERCRIME CONVENTION COMMITTEE, 2015),

[18] De acordo com a política de dados do Facebook (https://pt-br.facebook.com/privacy/explanation) e do Whatsapp (https://www.whatsapp.com/legal/?l=pt_br#privacy-policy-managing-your-information), por exemplo.

Para Krishnamurthy (2016), a natureza volátil e intangível dessas evidências e sua localização na nuvem computacional dificilmente se compatibilizará com os termos usualmente constantes nos acordos bilaterais de assistência judiciária, em matéria penal e processual penal, por três razões:

a) os dados que podem interessar à persecução penal em um determinado país podem ter sido armazenados em provedores de serviço de computação nuvem multinacionais (*Multinacional Cloud Service Provider* - MCP), que operam em outros países;
b) por razões de desempenho e confiabilidade, os MCPs particionam os dados de uma conta em pequenos pacotes que são armazenados e recuperados, total ou parcialmente, nos servidores situados em diferentes países, dificultando a localização precisa da informação requerida;
c) tanto as autoridades do país requerente quanto os técnicos do próprio MCP não têm como precisar que interesses privados podem ser violados com a busca digital, até que esta seja realizada. Ao contrário das evidências físicas encontradas no mundo real, referentes a indivíduos, via de regra, identificáveis, a propriedade de uma conta eletrônica muitas vezes só pode ser determinada após devassa de seu conteúdo.

Consequentemente, o autor questiona sobre a possibilidade de uma autoridade policial poder utilizar-se unicamente do devido processo legal vigente em seu país, para requisitar dados a um MCP, fisicamente localizado em território estrangeiro, uma vez que não sabe precisar onde os fragmentos dos dados da conta do usuário suspeito encontram-se armazenados.

Nos termos atuais da cooperação internacional, teoricamente seriam necessários tantos acordos de assistência judiciária em matéria penal quanto o número de países envolvidos no armazenamento distribuído dos dados.

Ademais, a computação em nuvem é dinâmica, podendo haver novas fragmentações e mudanças na alocação dos recursos, com vistas a atender requisitos de alta disponibilidade, alta performance, segurança e resiliência, o que torna extremamente difícil a coleta dessas evidências.

Num exemplo fictício, um Policial Federal brasileiro que, durante uma investigação criminal, chega a um suspeito de nacionalidade alemã, cujos dados relevantes ao processo encontram-se armazenados em servidores na própria Alemanha, mas com cópias de segurança na Dinamarca, poderá requisitar

diretamente ao provedor de serviço de computação em nuvem (que mantém escritório no Brasil) ou poderá também, legitimamente, requisitar os dados à Dinamarca? Questionamentos como esses têm sido frequentes e ainda não estão pacificados por normas internacionais.

Requisitos internos das legislações vigentes nos países demandados também precisam ser observados, o que enseja mais tempo para a resposta ao pleito, podendo comprometer o resultado esperado. Nos Estados Unidos, por exemplo, o *Stored Communications Act*[19], que é objeto de estudo na seção 4, estabelece os requisitos autorizadores da quebra de sigilo de dados dos usuários dos serviços de comunicações armazenadas. Decorre desse requisito legal a necessidade de processamento dos pedidos externos, feitos por meio de acordo bilateral de cooperação jurídica em matéria penal ou através de carta rogatória, no sentido de passar à apreciação de autoridade competente norte-americana a requisição de dados localizados em servidores nos Estados Unidos. Compete ao Departamento de Justiça dos Estados Unidos (DOJ) obter a autorização cabível. Em média, o processamento de pedidos dessa natureza se estende por cerca de 09 (nove) meses (KRISHNAMURTHY, 2016).

Embora os acordos bilaterais de assistência judiciária em matéria penal sejam os instrumentos legais que possibilitam o acesso formal a evidências eletrônicas armazenadas em Estado estrangeiro, quando o fator tempo é crítico para o sucesso da investigação criminal, os procedimentos atinentes ao MLAT vêm se mostrando burocráticos, pois seguem uma estrutura de procedimentos pré-estabelecida (OSULA, 2015b), morosos (SVANTESSON, 2016a, CYBERCRIME CONVENTION COMMITTEE, 2016b), ineficientes (OSULA, 2015b; JAYCOX; TIEN, 2015; KRISHNAMURTHY, 2016; CYBERCRIME CONVENTION COMMITTEE, 2016b), dificultando a investigação criminal. E a situação tende a se agravar, com o aumento de requisição registradas nos últimos anos, em sede do Departamento de Justiça dos Estados Unidos (UNITED STATES, 2016b).

Além do tempo como fator crítico para o acesso à evidência eletrônica, a dificuldade em estabelecer o local onde o dado se encontra armazenado, em razão

[19] *United States Code Title 18 - Crimes and Criminal Procedure, Chapter 121 - Stored Wire and Electronic Communications and Transactional Records Access*.

do fenômeno da perda da localização[20], inerente à mobilidade dos dados, característica da computação em nuvem, também constitui desafio adicional às investigações criminais (OSULA, 2017).

No contexto da problemática descrita, merece destaque o processo judicial travado entre a empresa *Microsoft Corporation* e os Estados Unidos, que ficou popularmente conhecido como *Microsoft Ireland Case*[21], que trouxe à tona intensas discussões acerca da possibilidade de autoridades públicas norte-americanas compelirem empresas daquele país a produzirem informações a partir de dados armazenados em servidores de computação em nuvem, situados em Estado estrangeiro.

No Brasil, situações semelhantes têm sido observadas, com ênfase em duas decisões proferidas no âmbito do Superior Tribunal de Justiça e do Tribunal Regional Federal da 4ª Região, que são abordadas na seção 5.

2.2 Justificativa

A presente Tese insere-se na lacuna de uma problemática multidisciplinar, envolvendo a ciência da computação, o direito processual penal e o direito internacional, pertinente ao exercício da prova, relativa à materialidade de crimes e sua autoria, quando as evidências são digitais e estão armazenadas em servidores de computação em nuvem, sobre solo estrangeiro.

Justifica-se à ciência da computação por nela principiar, pois é onde se registra a ocorrência das condutas criminosas perpetradas com o uso da tecnologia da informação e comunicação, e por meio dela é apurada, usando metodologias e ferramentas da forense digital. Assim, gera-se o crime na informática; deixa-se o rastro de sua passagem nela; apura-se sua ocorrência e responsabilidade penal por meio dela. O direito opera na interdisciplinariedade dos fatos criminosos de cuja prevenção não se pode excluir nem a importância da norma jurídica nem da informática. Justifica-

[20] Perda da localização ou *loss of location* refere-se à situação na qual não é possível precisar a localização do dado. A mobilidade e o espelhamento dos dados fazem com que, em algumas situações, seja extremamente difícil precisar a localização exata dos dados, até mesmo para os provedores de computação em nuvem (COUNCIL OF EUROPE, 2010; CYBERCRIME CONVENTION COMMITTEE, 2016b).

[21] O caso *Microsoft Ireland* será abordado na seção 4.

se aqui o interesse do direito processual penal e, subsidiariamente, também do direito penal.

Por fim, no âmbito do direito internacional está justificado o presente trabalho, pela possibilidade de envolver múltiplas jurisdições na solução de entraves legais, no curso da persecução criminal. Aparentemente, a questão situar-se-ia quase que exclusivamente no ordenamento jurídico dos países em que ocorreram os crimes e daqueles sobre cujo território, sob cuja soberania estão armazenados ou são processados dados que potencialmente podem se constituir em provas de fatos criminosos. No entanto, o aspecto distribuído da infraestrutura tecnológica em comento pode envolver o conflito de soberanias, de princípios e direitos dos usuários dos sistemas informáticos, bem como o interesse jurídico e legítimo dos Estados e da sociedade de prevenir as infrações penais, evitando a impunidade dos delinquentes.

Nesse contexto, portanto, a ciência da computação e a ciência do direito são indissociáveis, o que justifica o aspecto multidiciplinar da abordagem nessa Tese.

2.3 Objetivos

O objetivo principal dessa Tese é contribuir com as discussões interdisciplinares nas áreas do direito internacional, direito processual penal e da ciência da computação acerca de questões legais relacionadas à localização, preservação, produção, acesso, busca e apreensão extraterritorial de evidências eletrônicas de crimes, quando armazenadas em ambiente de computação em nuvem, sobre território estrangeiro.

São objetivos específicos:

a) avaliar tratados internacionais, relativamente à coleta extraterritorial de evidências criminais;
b) propor uma estrutura de requisitos para servir de reflexão na elaboração de documento internacional, de caráter multilateral e vinculante, que estabeleça normas disciplinadora das diligências para produção de provas no processo penal, quando as evidências são eletrônicas e estão armazenadas em servidores de computação em nuvem, sobre território estrangeiro.

2.4 Delimitação da abordagem

Interessam a esta pesquisa questões de direito processual penal, de direito internacional e da ciência da computação, relativas à localização, preservação, produção, acesso, busca e apreensão extraterritorial de evidências criminais eletrônicas armazenadas em ambiente de computação em nuvem, no contexto delimitado segundo os critérios relacionados a seguir.

2.4.1 Evidências criminais eletrônicas

Evidências digitais ou eletrônicas[22] são definidas pelo *Scientific Working Group on Digital Evidence*[23] como informações de valor probatório que estão armazenadas ou são transmitidas em formato digital, sendo relevantes tanto ao processo penal quanto na solução de litígios cíveis.

No processo penal, o ambiente digital apresenta-se como uma nova dimensão à investigação das infrações penais. Os dados eletrônicos, armazenados ou em trânsito, podem ser utilizados como evidências, tanto para justificar quanto para refutar versões sobre a reconstituição histórica de uma conduta possivelmente delituosa. Ademais, são capazes de indicar a intenção ou tentativa de prática criminosa, bem como de confirmar ou refutar um álibi (CASEY, 2011). Esses dados são apresentados sob diversas formas, como texto, imagem, vídeo, áudio, e podem estar presentes em vários sistemas computacionais.

A coleta de provas no processo civil e na arbitragem é orientada por princípios diferentes dos que regem o processo penal (LAURITS; KASPER, 2016). Para o presente estudo, serão de interesse apenas as abordagens atinentes ao processo penal.

---

[22] Ao longo do texto, as terminologias “evidência digital” e “evidência eletrônica” serão utilizadas como sinônimos para referir todas as evidências no formato digital ou eletrônico.

[23] *Scientific Working Group on Digital Evidence* (SWGDE). Digital Evidence: Standards and Principles. *FBI - Forensic Science Communication*, United States of America, n. 2, v. 2, abril 2000. https://www.swgde.org

2.4.2 As diligências para a produção de prova

As dificuldades enfrentadas pelas autoridades de persecução criminal, na obtenção de evidências em outras jurisdições, não é novidade ao processo penal. Frequentemente, a requisição de evidências e a troca de informações relevantes ao fato investigado ocorrem por meio de acordo de assistência judiciária em matéria penal (MLAT).

Conforme ressaltado na subseção 2.1, estudos recentes apontam para a ineficiência dos tradicionais meios de cooperação jurídica internacional (MLAT, Carta Rogatória), quando a coleta de eviências criminais eletrônicas é extraterritorial, motivando, inclusive, tentativas unilaterais para obtê-las e, em atitude extrema, o abandono das investigações (CURRIE, 2017).

Dessa maneira, é compreensível que os Estados procurem formas alternativas para obter as evidências de que necessitam, como por meio de cooperação internacional informal entre agências de aplicação da lei, de redes de ponto de contatos 24/7 que funcionam em instituições policiais, do envio de requisições diretamente a empresas provedoras de serviço de Internet, de ferramentas para acesso direto a dados armazenados remotamente, independentemente da definição de onde se encontrem contidos (OSULA, 2017), ferramentas de análise e inteligência sobre dados públicos (OSULA, 2017; WENDT; BARRETO, 2013).

A abordagem nessa Tese está limitada à regulação legal, em nível internacional, dos seguintes meios de investigação e prova no processo penal: localização, preservação, produção, acesso e busca e apreensão de evidências criminais eletrônicas, quando armazenadas em servidor de computação em nuvem, localizado em território estrangeiro. Nesse contexto, é importante ressaltar que a localização física do dado é de difícil precisão, tendo em conta o fenômeno da “perda da localização”.

A localização do dado implica em precisar sua existência e posicionamento, não obstante a impossibilidade de sua determinação quando mobilizados em trânsito, hipótese em que somente podem ser interceptados.

A preservação refere-se à conservação de dados específicos, incluindo dados relativos ao tráfego, armazenados por meio de um sistema informático, nomeadamente nos casos em que existem motivos para pensar que os mesmos são susceptíveis de perda ou alteração. Essa medida aplica-se a dados já existentes ou

em curso de armazenamento, não se referindo à recolha em tempo real nem a conservação de futuros dados de tráfego, ou à interceptação das comunicações.

A produção de dados refere-se a poderes necessários para compelir o provedor de serviço a fornecer dados armazenados específicos ou a prestar informações relativas aos subscritores. Não inclui dados ainda não existentes, tais como dados de tráfego ou de conteúdo relacionados com comunicações futuras.

O acesso é a possibilidade de, mediante o consentimento da pessoa legalmente autorizada a divulgar esses dados, conhecer o ambiente virtual da computação em nuvem, onde se supõe estejam contidos os vestígios eletrônicos de crimes investigados, com o fim de periciá-los. A pessoa legalmente autorizada pode ser o próprio usuário ou o técnico do provedor de serviço Internet, desde que para cumprir determinação legal.

A busca e apreensão é o termo utilizado para referir a "diligência que se realiza objetivando a procura de alguma coisa ou de alguém para apreendê-la" (TOURINHO FILHO, 2007, p. 580). A rigor, "a busca é a procura, a diligência que objetiva encontrar o que se deseja, ao passo que a apreensão é medida de constrição, para acautelar, pôr em custódia determinado objeto ou pessoa" (TÁVORA; ALENCAR, 2009, p. 390). Embora tradicionalmente a busca e apreensão refira-se a objetos tangíveis, na Convenção de Budapeste sobre o Cibercrime, o termo "busca" significa procurar, ler, inspecionar ou rever dados, incluindo a noção de pesquisa e de análise desses dados[24]. O termo "apreender" significa efetuar e guardar uma cópia dos dados ou informações, incluindo, ainda, a utilização ou apreensão de programas necessários ao acesso aos dados objeto da busca e apreensão[25] (COUNCIL OF EUROPE, 2001a).

No direito brasileiro, o termo busca e apreensão vem sendo usado extensivamente para referir também dados digitais, como é possível observar em decisões judiciais (STJ, 2014) e na doutrina (BRASIL, 2017).

As diligências de localização, preservação, produção, busca e apreensão, em geral, são executadas pelo provedor de serviço Internet, em atendimento à ordem ou requisição de autoridade legalmente competente, empenhada no esclarecimento e na apuração de infração penal.

---

[24] Parágrafo 191, do Relatório Explicativo da Convenção de Budapeste sobre o Cibercrime (COUNCIL OF EUROPE, 2001b).
[25] Parágrafo 197, do Relatório Explicativo da Convenção de Budapeste sobre o Cibercrime (COUNCIL OF EUROPE, 2001b).

2.4.3 O ambiente de computação em nuvem

É incerto quando a terminologia “computação em nuvem” foi utilizada pela primeira vez (MARTINI; QUICK; CHOO, 2013). Kaufman (2009) sugere que sua origem está no mundo das telecomunicações dos anos 1990, quando os provedores começaram a utilizar o serviço de rede privada virtual (*virtual private network* - VPN), nas comunicações de dados. Na academia, um dos registros mais remotos para o termo foi trazido pelo professor de sistemas de informação, Ramnath Chellappa[26], no ano de 1997. Comercialmente, parece que a primeira referência encontrada, em março de 2006, foi a oferta do serviço *Amazon Web Services* (AWS) pela empresa Amazon.com Inc., como plataforma de serviços em nuvem para processamento computacional, armazenamento de banco de dados, distribuição de conteúdo e outras funcionalidades[27].

Uma definição amplamente aceita para computação em nuvem, e adotada nesta Tese, é provida pela agência do governo norte-americano *National Institute of Standards and Technology* – NIST[28]:

> Cloud computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. This cloud model promotes availability and is composed of five essential characteristics (On-demand self-service, Broad network access, Resource pooling, Rapid elasticity, Measured Service) (MELL; GRANCE, 2011, p.2). [29]

Para Armbrust *et al* (2010), computação em nuvem refere-se à entrega de aplicações sobre a Internet como serviço, por meio de extenso e complexo sistema de *hardware* e *software*, denominado *data center*. Comercialmente, esses serviços vêm sendo oferecidos nas modalidades de *Software* como Serviço - SaaS, ou

[26] http://www.dell.com/learn/br/pt/brbsdt1/sb360/social_cloud
[27] https://aws.amazon.com/pt/what-is-aws/
[28] http://www.nist.gov/
[29] Livre tradução da autora: “A computação em nuvem é um modelo para habilitar o acesso por rede, conveniente e sob demanda, a um conjunto compartilhado de recursos de computação (como redes, servidores, armazenamento, aplicações e serviços) que possam ser rapidamente provisionados e liberados com o mínimo de esforço de gerenciamento ou interação com o provedor de serviços.”

Plataforma como Serviço – PaaS, ou ainda Infraestrutura como Servico – IaaS. O *data center* (*hardware* e *software*) é o que comumente nomina-se de nuvem ou *cloud*.

De acordo com o modelo de implantação, a computação em nuvem pode ser classificada como Nuvem Pública, quando está disponível para o uso do público em geral; Nuvem Privada, para se referir ao *data center* de organização privada, não disponível para o público em geral; Nuvem Comunitária, quando infraestrutura é compartilhada e gerenciada por várias organizações; e a Nuvem Híbrida, que consiste na combinação de dois ou mais modelos de computação em nuvem (VERAS, 2015; BECHTEL, 2013).

O conceito de computação em nuvem ainda se aprimora. A ideia inicial associada a essa nova arquitetura de tecnologia da informação e comunicação era a de processar as aplicações e armazenar os dados fora do ambiente corporativo (ou seja, em *data centers)*, otimizando o uso de recursos. Atualmente, os serviços de computação em nuvem pública são fornecidos, em sua maioria, por grandes empresas multinacionais, como Microsoft Corporation, Google LLC., Amazon.com, Rackspace Inc., Dropbox Inc. (VERAS, 2015).

Essa pluralidade de modelos e tecnologias impacta diretamente na coleta de evidências criminais eletrônicas, especialmente porque os dados estão geograficamente distribuídos e armazenados em múltiplas jurisdições, simultaneamente (IGLESIAS; NICHOLLS; TRAVIS, 2012).

Não se pode olvidar também os desafios técnicos e legais trazidos pela computação em nuvem aos peritos forenses. Tecnicamente, é difícil estabelecer o acesso direto dos peritos, seja físico ou virtual, ao ambiente do *data center* onde as evidências encontram-se armazenadas ou são processadas (MARTINI; CHOO, 2014). Os desafios jurídicos estão relacionados à necessidade de expedição de mandado ou requisição, por autoridade competente, levando-se em conta a natureza do dado a ter o sigilo violado, o crime investigado (QUICK; CHOO, 2014).

Do ponto de vista da computação forense, essas peculiaridades importam na necessidade de normatizar e reescrever procedimentos clássicos alusivos à coleta de evidências eletrônicas, compatíveis com o novo ambiente, bem como desenvolver ferramentas adequadas, atendendo aos novos requisitos trazidos pelo ambiente da computação em nuvem (BECHTEL, 2013; MARTINI; CHOO, 2014).

Para o contexto deste trabalho, são de interesse apenas os dados armazenados em ambiente de computação em nuvem pública, pois a política de privacidade e proteção de dados adotada pela empresa que implementa o modelo de nuvem privada, bem como o controle exercido sobre o ambiente e seus usuários facilitam as respostas a demandas judiciais, o que não ocorre com aquela (IGLESIAS; NICHOLLS; TRAVIS, 2012).

Também não serão tratadas aqui as evidências criminais eletrônicas encontradas em mídias óticas (CDs, DVDs, Blue-Ray), *pendrive*, cartões de memória ou qualquer outro dispositivo que possibilite o armazenamento local da evidência.

2.4.4 Crime cibernético

Não existe consenso, seja em nível internacional ou interno, relativo a uma definição legal ou doutrinária para o crime cibernético, nem tampouco acerca da padronização terminológica para os crimes praticados por meio da tecnologia da informação e comunicação. Doutrinadores do direito, representantes do setor privado, da área de segurança da informação, do Estado, apresentam definições diversificadas, em nível de abrangência e de especificidade (FINKLEA; THEOHARY, 2015).

As convenções e os tratados internacionais relativos ao crime cibernético, via de regra, incumbem à doutrina o papel de defini-lo. A Convenção de Budapeste sobre o Cibercrime (COUNCIL OF EUROPE, 2001a), a Convenção da Liga dos Estados Árabes para o Combate a Ofensas relacionadas à Tecnologia da Informação (LEAGUE OF ARAB STATES, 2010) e a Convenção da União Africana para a Segurança Cibernética e Proteção de Dados Pessoais (AFRICA UNION, 2014) não trazem qualquer definição para o termo cibercrime ou a expressão “crime cibernético”. O Acordo de Cooperação entre os Estados Membros da Comunidade dos Estados Independentes, para o Combate a Infrações Relacionadas à Informação Computacional *(*COMMONWEALTH OF INDEPENDENT STATES*,* 2001), em seu art. 1(a), alude a ofensas relacionadas a informações de computador. Todos esses tratados regionais serão estudados na seção 6.

Em relação à legislação interna, menos de 5% dos países, que foram consultados em pesquisa realizada pela ONU (UNODC, 2013), utilizam o termo ‘*cybercrime’* no título ou na nominação jurídica de suas disposições. São mais

frequentes, no entanto, o uso das expressões como '*computer crimes'*, '*electronic communications'*, '*information technologies*' ou '*high tech crimes*' (UNODC, 2013, p.12).

No âmbito do presente estudo, a definição formal, diferenças, semelhanças entre as expressões e os termos acima apresentados devem ser compreendidos em sentido mais amplo, vez que as evidências criminais eletrônicas poderão subsidiar a investigação de qualquer ação criminosa, desde que seu autor tenha utilizado recursos da tecnologia da informação e comunicação, deixando evidências em ambiente de computação em nuvem.

Não confundir o conceito de crime cibernético com a tipificação de cada crime dessa natureza, a cargo da legislação dos diversos países, lembrando que o tipo penal é a definição legal individualizada das condutas criminosas. A violação das condutas aos bens jurídicos a serem protegidos pelo direito penal não se aprimorou ao ponto de chegar a unificação de entendimento e proteção universal uniforme, por força de fatores vários condicionantes, entre eles a diversidade cultural que desafia e vence a globalização.

2.4.5 Guerra cibernética

O Manual de Tallinn (SCHMITT, 2013) apresenta um estudo sobre a aplicação do direito internacional, relativamente à guerra cibernética, compreendendo o *jus ad bellum*, definido como o direito de fazer a guerra quando esta parece justa, e o *jus in bello*, conjunto de normas, primeiro costumeiras, depois convencionais, que floresceram no domínio do direito das gentes, quando a guerra era uma opção lícita para resolver conflitos entre Estados (RESEK, 2014).

Embora as atividades de inteligência cibernética, operações *cyber-to-cyber* em sentido estrito[30] e outras relacionadas à guerra cibernética possam também deixar evidências no mundo digital, a legalidade de sua coleta extraterritorial não será abordada na presente pesquisa, sobretudo porque o que é crime ou deixa de ser nas relações entre países implica em correlação de forças e de poder no confronto das soberanias, cuja consideração extrapola ao objeto do presente estudo.

[30] São exemplos de operações *cyber-to-cyber,* em sentido estrito, as operações cibernéticas contra infraestrutura crítica estatal e o ataque cibernético a sistema de comando e controle do inimigo (SCHIMITT, 2013).

Do mesmo modo, está excluída do contexto dessa Tese a análise sobre o acesso extraterritorial a dados digitais em nuvem pública, para fins de vigilância de inteligência. Nos Estados Unidos, por exemplo, sob a égide do *Foreign Intelligence Surveillance Act* (FISA), de 1978 (UNITED STATES, 1978), que integra o *50 United States Code* (*50 U.S.C - War and National Defense*), é lícito realizar vigilância de inteligência, inclusive quando a pessoa sob vigilância não é um nacional norte-americano ou que esteja em outro país, nos termos do *50 U.S. Code § 1881a - Procedures for targeting certain persons outside the United States other than United States persons* (UNITED STATES, 1978). Justifica a ativação do FISA, por exemplo, quando existir causa provável que o alvo da vigilância seja um "poder estrangeiro". Após os atentados terroristas de 11 de setembro de 2001, o *Patriotic Act* alterou o FISA, incluindo o terrorismo no contexto da definição de "poder estrangeiro", possibilitando a vigilância de alvo contra o qual se suspeite de envolvimento com o terrorismo, mesmo que não tenha praticado qualquer atividade criminosa (VAILE et al, 2013).

Van Hoboken, Arnbak e Van Eijk (2013) consideram preocupantes esses dispositivos legais, pois é suficiente para justificar a coleta o fato de as informações serem potencialmente relevantes à vigilância, não importando a pessoa do estrangeiro investigado nem a natureza dos dados a ele associados. Decorre do FISA o poder do Estado para compelir empresas provedoras de serviço, sediadas nos Estados Unidos, a contribuir com as operações de vigilância, sem que esse mandamento do Governo contrarie a Constituição norte-americana. Segundo os autores, essa possibilidade constitui um risco, por exemplo, a segurança dos contratos comerciais estabelecidos com as empresas, relativamente à confiança e garantia do sigilo dos dados armazenados nesse ambiente, como os segredos industriais.

2.4.6 A investigação criminal na *Dark Web*

A *Dark Web* é uma rede global e privada de computadores que permite aos usuários realizarem transações anonimamente, ocultando evidências que possibilitem a sua localização e identificação, bem como o rastreamento das operações realizadas. A anonimização é garantida por meio do emprego de diversos tipos de ferramentas,

como *The Onion Router* (TOR), I2R, *freenet*, e de métodos, a exemplo dos protocolos de criptografia (GHAPPOUR, 2017).

Em razão dessa característica, tornou-se um facilitador para o crime e o terrorismo. Dentre as atividades criminosas facilitadas pela *Dark Web* estão a exploração da pornografia infantil, o tráfico ilícito de drogas, de armas de fogo, de seres humanos, fraudes com cartões de crédito, comércio ilegal de *malwares*. De acordo com o relatório de avaliação de ameças do crime organizado na União Europeia[31] - 2017, 57% (cinquenta e sete por cento) das páginas da *Darknet* apresentam conteúdo ilegal (EUROPOL, 2017a).

A *Dark Web* está inserida na *Deep Web*, que inclui a parte da Internet que é inalcançável por meio de motores de busca convencionais, sendo o acesso realizado apenas através de ferramentas específicas (como TOR, I2P), configurações e autorizações próprias (GREENBERG, 2014).

A *Silk Road* foi um dos exemplos de serviço em favor do crime que ocorreu sobre a *Dark Web*. Criada em 2011, por Ross William Ulbricht, usando o pseudônimo de *Dread Pirate Roberts*, funcionou como um mercado global de venda e troca de bens e serviços ilícitos, e de contrabando de mercadorias, onde comprador e vendedor podiam se encontrar anonimamente. Embora qualquer tipo de produto ilícito ou de venda controlada pudesse ser encontrado no ambiente, a principal mercadoria comercializada era a droga (lícita controlada ou ilícita), com mais de 13 mil anúncios de venda. A única forma de pagamento aceita era por meio de *Bitcoin*, que é uma moeda digital que permite às partes trocarem fundos, sob forte proteção de privacidade (GOODMAN, 2015). O fundador e mantenedor do serviço foi preso em 2013 e condenado a cumprir prisão perpétua, após anos de investigação do *Federal Bureau of Investigations* (FBI), que foi baseada principalmente na infiltração policial e na prática de *hacking*, por meio do envio de *malwares* a computadores remotos, no intuito de coletar dados. Essas duas técnicas, a infiltração policial e o *hacking*, em geral são utilizadas por autoridades policiais que procedem investigação criminal em rede que pratica a anonimização, como a *Dark Web.*

No Brasil, a Lei nº 13.441, de 08 de maio de 2017 (BRASIL, 2017), aprovou alteração no Estatuto da Criança e do Adolescente, para prever a infiltração de agentes de polícia na Internet, com o fim de investigar crimes contra a dignidade

31 The European Union (EU) Serious and Organised Crime Threat Assessment (SOCTA) 2017.

sexual de crianças e de adolescentes. Nos termos da lei, a infiltração será precedida de autorização judicial, devidamente circunstanciada e fundamentada, que estabelecerá os limites da infiltração para obtenção de prova, ouvido o Ministério Público. Trata-se de medida excepcional, somenta admitida se a prova não puder ser obtida por outros meios. A norma preceitua ainda que não comete crime o policial que oculta a sua identidade para, por meio da Internet, colher indícios de autoria e materialidade dos crimes. Quem deixar de observar a estrita finalidade da investigação, porém, pode responder pelos excessos praticados.

Nos Estados Unidos, a infiltração, para fins de investigação criminal, é permitida e deve ser precedida de um *Warrant* (mandado judicial). Ocorre que, até pouco tempo, alguns magistrados se negavam a conceder o referido instrumento, sob o argumento de que, sendo a localização do computador incerta ou desconhecida, não seria possível precisar a Corte Distrital competente para expedi-lo, contrariando assim a norma que disciplina a busca e apreensão[32] e a Quarta Emenda à Constituição dos Estados Unidos (UNITED STATES, 2013). Alterações no código (processo penal) norte-americano permitiram a presunção de territorialidade para os casos em que a localização do dispositivo tenha sido ocultada por meios tecnológicos, sem, no entanto, autorizar o magistrado a expedir mandados de busca e apreensão fora do território norte-americano.

Quanto ao *hacking*, o uso pelas autoridades de investigação criminal de técnicas de *hacking* para perseguir, na *Dark Web,* indivíduos suspeitos de prática de ato criminoso, vem sendo entendido como uma operação *cyber-exfiltration* no exterior, com potencial para violar a soberania de outras nações (GHAPPOUR, 2017).

Aspectos legais das técnicas de investigação criminal no ambiente de rede onde predomina a prática da anonimização, como a *Deep Web*, *Dark Web* ou *Dark net*, não serão objeto de discussão nesta Tese, embora se trate de um tema instigante e desafiador.

[32] A diligência de busca e apreensão, no direito norte-americano, é disciplinada pela Regra 41, do Código de Processo Criminal Federal (*United States Federal Rules of Criminal Procedur*e, de 1944 (UNITED STATES, 1944).

2.4.7 Escopo negativo da pesquisa

Diante do esposto, não serão objeto de estudo na presente tese:

a) a coleta de provas para o processo civil e para a arbitragem, pois é orientada por princípios diferentes dos que regem o processo penal;
b) no ambiente de Nuvem Privada ou Comunitária, pois o controle mais rigoroso exercido sobre o ambiente facilita a coleta de evidências criminais;
c) em mídias óticas (CDs, DVDs, Blue-Ray) ou magnéticas (disco rígido, fita megnética) ou *pendrive*, cartões de memória ou qualquer outro dispositivo que possibilite o armazenamento local da evidência eletrônica;
d) as operações *cyber-to-cyber* em sentido estrito e outras relacionadas à guerra cibernética, que possam também deixar evidências no mundo digital, pois o direito da guerra é regido por normas próprias reguladoras de um estado de exceção;
e) a vigilância de inteligência, mesmo que destinada à prevenção da violência criminal, por se orientar em legislações específicas;
f) os ambientes onde predomina a prática da anonimização, como a *Deep Web*, *Dark Web* ou *Dark net*, pois as técnicas de investigação empregadas diferem das utilizadas na Internet convencional.

2.5 Perguntas de pesquisa

A pergunta central a que se pretende responder ao final da pesquisa é:

Qual é a solução da ciência da computação e da ciência jurídica para a localização, preservação, acesso, produção, busca e apreensão de evidências criminais, armazenadas em ambiente de computação em nuvem, em território de Estado estrangeiro?

Outras indagações também são consideradas:

a) as normas internacionais, em matéria de segurança da informação e criminalidade cibernética, são adequadas à localização, preservação, acesso, produção, busca e apreensão extraterritorial de evidências criminais, armazenadas em servidor de computação em nuvem?
b) que tratados internacionais multilaterais abordam a questão e como se desenham as previsões executórias?

c) quais são os requisitos orientadores na elaboração de norma internacional atinente à localização, preservação, acesso, produção, busca e apreensão de evidências criminais, armazenadas em ambiente de computação em nuvem, em território de Estado Parte estrangeiro?

2.6 Hipóteses

São as hipóteses inicialmente levantadas:

a) faz-se necessário atualização ou edição de tratado internacional multilaterais atinente à localização, preservação, acesso, produção, busca e apreensão extraterritorial de evidências eletrônicas, de forma a superar os desafios próprios do espaço cibernético, tais como a volatilidade dos dados e a natureza transnacional;
b) a multiplicidade de convenções internacionais sobre crime cibernético contribui para a cooperação internacional regionalizada, em oposição à natureza universal do crime cibernético.

2.7 Metodologia

Esta Tese foi desenvolvida através de pesquisa exploratória, elaborada por meio de levantamento bibliográfico e análise de documentos. Os conceitos relativos ao tema são apresentados mediante levantamento bibliográfico realizado em livros e periódicos da doutrina jurídica e da ciência da computação. O estado da arte, relativamente às propostas que vem sendo apresentadas para enfrentar os problemas alusivos à localização, preservação, acesso, produção, busca e apreensão extraterritorial de evidências criminais, quando armazenadas em ambiente de computação em nuvem, foi buscado por meio de revisão sistemática de literatura, cujo protocolo encontra-se no Apêndice A.

Na pesquisa documental, foram analisados tratados internacionais, de abrangência regional, sobre segurança da informação e crimes cibernéticos, com o objetivo de identificar as disposições processuais alusivas ao problema descrito.

Outros documentos também subsidiaram a revisão de literatura, como diversas peças jurídicas do caso *Microsoft Corporation versus* Estados Unidos da

América, também conhecido como *Microsoft Ireland Case* (que é abordado na seção 4), além de relatórios do Conselho da Europa e da ONU.

É oportuno ressaltar que, no início da elaboração desse trabalho, ainda na fase de qualificação da proposta, foram realizadas entrevistas com autoridades de persecução criminal no Estado de Pernambuco, como magistrados, policiais civis, policiais federais, policiais militares, promotores de justiça e peritos criminais. Ocorre que, no curso do levantamento dos dados, que subsidiariam ainda mais a feitura da Tese, percebeu-se que os desafios enfrentados pelos profissionais em comento pouco ultrapassavam as fronteiras do país, uma vez que predominava, internamente, a prática de delitos informáticos perpetrados por brasileiros, contra brasileiros e/ou utilizando-se de recursos tecnológicos localizados em solo pátrio, o que é corroborado por pesquisas divulgadas pela Europol, que destaca a preferência do delinquente brasileiro pela Internet navegável (e não da *deep web*) (EUROPOL, 2016) e pela prática do *phishing* bancário e de outras estratégias de ataques baseadas em engenharia social, dentro do território nacional (EUROPOL, 2015).

Ratificam também as conclusões obtidas com esse levantamento preliminar os dados apresentados pela Secretaria de Defesa Social, em resposta a requisição da autora, realizada por meio do sítio Internet de acesso à informação[33]. De acordo com os dados fornecidos, os delitos “estelionato/fraude”, “difamação” e “invasão de dispositivo informático” representam, juntos, cerca de 65% das ocorrências registradas na Delegacia de Polícia de Repressão ao Crime Cibernético, da Polícia Civil de Pernambuco, no período compreendido entre janeiro de 2014 a outubro de 2017 (ANEXO A). A Figura 1 apresenta a evolução dessas três principais ocorrências, no período considerado.

As entrevistas visaram identificar, com base na experiência profissional dos entrevistados, qual seria a solução mais adequada para resolver o problema em estudo.

Durante as entrevistas, a obrigação de territorialização dos dados no Brasil, por parte de empresa provedoras de serviço Internet que implementam computação em nuvem no país ou que atuam em território nacional, foi a opção que predominou, embora o escasso conhecimento técnico (em informática) dos policiais em geral e a carência de recusos tecnológicos tenham sido ressaltados como os principais

[33] URL: http://www.portaisgoverno.pe.gov.br/web/ouvidoria/formularios-lai.

problemas enfrentados pelas instituições. Aliás, os próprios entrevistados não se mostravam familiarizados com o problema, obrigando essa autora a explicar e exemplificar, previamente.

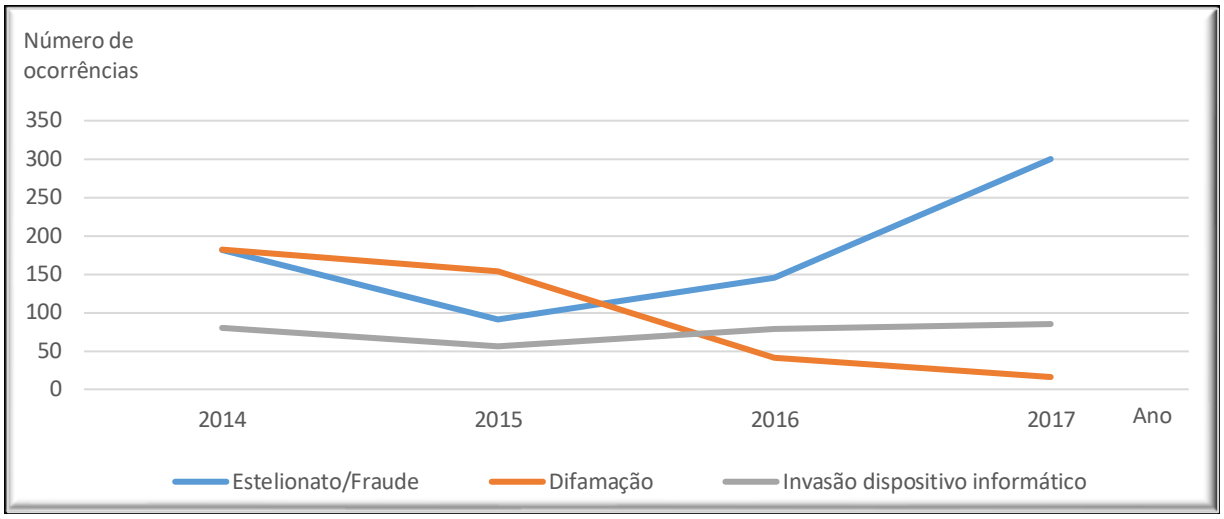

Figura 1 - Gráfico de evolução das três ocorrências policiais mais registradas na Delegacia de Repressão ao Crime Cibernético de Pernambuco

Fonte: Secretaria de Defesa Social de Pernambuco, novembro/2017.

Outrossim, embora alguns processos judiciais no país (estudados ao longo do trabalho) aludam ao problema investigado, não parece que este seja um óbice à persecução criminal, pelo menos no Estado de Pernambuco.

Por essas razões, esse levantamento foi abandonado.

3 A FORENSE DIGITAL EM NUVEM COMPUTACIONAL

Tecnicamente, há várias maneiras através das quais o ambiente da computação em nuvem pode ser explorado, com o intuito de localizar, preservar, produzir, acessar, buscar e apreender evidências eletrônicas de crime.

A presente seção tem por objetivo apresentar conceitos básicos atinentes à computação forense, bem como *frameworks* utilizados pelos peritos no exame de dados digitais em busca de evidências da prática de crimes, para constituir prova no processo penal.

3.1 A Forense digital

A forense digital (ou forense computacional ou computação forense ou forense eletrônica) é uma área relativamente recente da ciência forense (MARTINI; QUICK; CHOO, 2013; McKEMMISH, 1999), surgida na década de 1980, em resposta aos primeiros casos de vírus de computador que se espelhavam por redes de comunicações. Nos anos seguintes, evoluiu para a investigação de condutas ilícitas relacionadas à pedofilia e, posteriormente, no combate a crimes cibernéticos, quando a popularização da Internet e o uso de computadores pessoais e outros dispositivos eletrônicos criaram oportunidades para a prática de atividades ilegais. O termo forense significa “pertinente à lei” e refere-se à busca minuciosa por informações relativas a eventos passados, atinentes a uma investigação criminal (DELLA VECCHIA; WEBER; ZORZO, 2013).

A forense digital é referida como um elemento facilitador na limitação da prática de delitos digitais (DIDONÉ, 2011), podendo ser conceituada como uma ciência multidisciplinar que visa à preservação, coleta, validação, identificação, análise, interpretação, documentação e apresentação de evidências digitais, de maneira científica e legalmente válida, permitindo a reconstrução de eventos passados e colaborando na investigação de crimes, comportamentos ilegais ou inapropriados, cometidos em meio virtual (DFRWS, 2001). Aliás, o aspecto

multidisciplinar da forense digital é também destacado por DIDONÉ (2011), Ruan *et al.* (2011), US-Cert (2008), McKemmish (1999), SLAY *et al* (2009).

O US-Cert (2008) define forense computacional como:

> the discipline that combines elements of law and computer science to collect and analyze data from computer systems, networks, wireless communications, and storage devices in a way that is admissible as evidence in a court of law.[34]

Tem como objetivo principal determinar a dinâmica, a materialidade e a autoria de ilícitos relacionados à área da informática, apresentando como questão principal a identificação e o processamento de evidências digitais em provas materiais de crime, por meio de métodos técnico-científicos, conferindo-lhes validade probatória em juízo (ELEUTÉRIO; MACHADO, 2010). A garantia da validade das provas no processo penal depende da utilização de um conjunto de técnicas e procedimentos, fundamentados em conhecimentos científicos, para coletar, analisar e apresentar evidências digitais perante um tribunal (NOLAN *et al*, 2005).

3.2 As fases da forense digital

Tradicionalmente, McKemmish (1999) alude a quatro fases da computação forense, que são: a identificação, a preservação, a análise e a apresentação das evidências digitais.

A identificação da evidência digital, que é o primeiro passo do processo, alude à determinação de que evidências são necessárias à investigação, sua localização, tipo e formato, de maneira a definir a tecnologia apropriada para a sua extração.

A preservação é um elemento crítico à forense digital, consistente na garantia de sua inalterabilidade ou, em última instância, a alteração mínima possível.

A fase de análise inclui a extração, o processamento e a interpretação dos dados coletados (em nível de *bits*) nas duas fases anteriores, transformando-os em evidências apresentáveis a um tribunal.

Por fim, a apresentação da evidência digital, como prova no processo penal, geralmente é realizada pelo perito forense.

---

[34] Tradução da autora: “a disciplina que combina elementos do Direito e da Ciência da Computação para coletar e analisar dados de sistemas computacionais, redes, comunicações sem fio e dispositivos de armazenamento, de modo que possam constituir evidências admissíveis num tribunal”.

Outro ciclo de procedimentos é apresentado por Kent *et al*. (2006), sendo ilustrado na Figura 2. Os dados digitais extraídos a partir das mídias digitais são examinados, transformando-se em informações relevantes à investigação. Essas informações, depois de analisadas, poderão constituir evidências criminais.

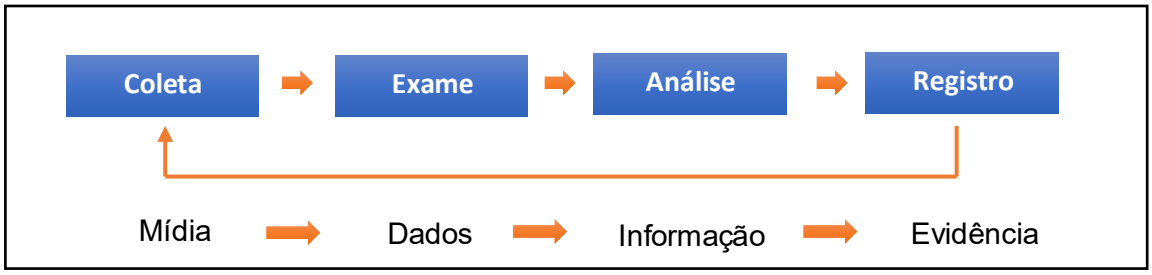

Figura 2 - Etapas do processo de investigação forense (KENT *et al*., 2006, p. 3-1)

A forense digital pode ser realizada tanto em sistema computacional ainda em execução (*Live Forensics*) como em equipamento desligado (perícia convencional ou estática).

A *Live Forensics* permite ao investigador analisar elementos indisponíveis durante a perícia convencional, como o conteúdo da memória de acesso randômico (memória RAM), portas abertas, conexões ativas de rede, programas em execução, chaves criptográficas, conteúdos não criptografados. A vantagem da *Live Forensics* é a simplicidade dos procedimentos e a resposta imediata. No entanto, depois de desligada a máquina, não existe possibilidade de reprodução nem de realização de novos exames, caso surjam outros questionamentos. Na perícia estática, é providenciada uma cópia forense do dispositivo de armazenamento para, a partir daí, a imagem ser analisada em laboratório de informática, utilizando-se sistema operacional e aplicações forenses confiáveis (MESQUITA, HOELZ; RALHA, 2011).

O ambiente de computação em nuvem apresenta desafios novos tanto à perícia *Live* quanto à perícia estática, inviabilizando-as em determinadas situações. Nesta última, por exemplo, para realizar a clonagem do disco rígido seria necessário desligar (*shutting down*) o sistema, o que seria impensável se diversas máquinas virtuais compartilhassem essa mesma infraestrutura física, considerando que aplicações críticas podem estar em funcionamento e a privacidade de usuários não investigados, sujeita à violação, ilegal e desnecessariamente (SIBIYA; VENTER; FOGWILL, 2012).

3.3 A forense digital em nuvem computacional

A forense digital em nuvem computacional, também conhecida como *Cloud Forensics*, é definida como a aplicação da ciência forense digital nos modelos da computação em nuvem, constituindo assim uma subárea de *Network Forensics* (RUAN *et al*, 2011).

A multidisciplinaridade da forense computacional é herdada pela *Cloud Forensics*, uma vez que aspectos técnicos e legais devem ser levados em consideração, além da cooperação entre as partes envolvidas, que no trabalho de Ruan *et al* (2011) é designado como questão organizacional, envolvendo os usuários, o provedor da computação em nuvem e, conforme os objetivos das investigações, as autoridades de investigação criminal.

O modelo tridimensional apresentado por Ruan *et al* (2011) para a definição de computação em nuvem (Figura 3) demonstra o lado multidimensional da disciplina, estendendo a definição de *Cloud Forensics* entre três dimensões: técnica, legal e organizacional.

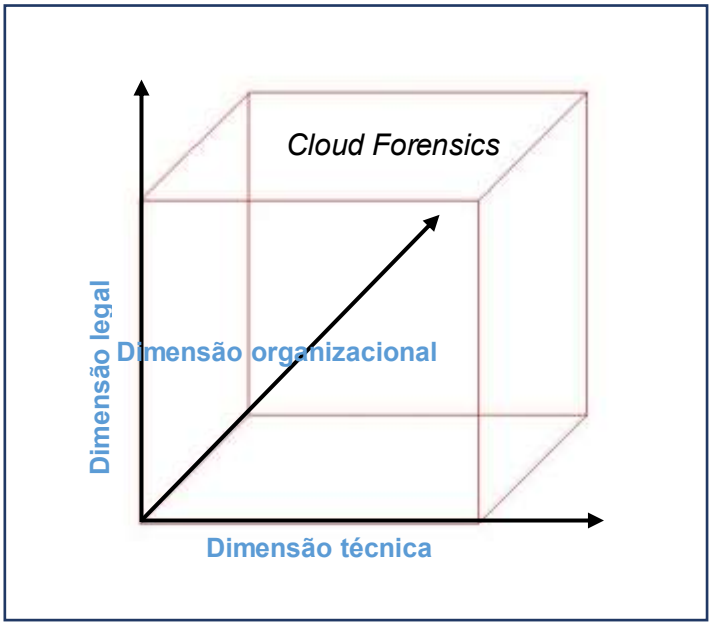

Figura 3 - Modelo tridimensional da *Cloud Forensics*
Fonte: Ruan *et al* (2011, p.5)

A dimensão técnica envolve um conjunto de ferramentas, procedimentos e metodologias para a realização do processo forense em ambientes de computação em nuvem. Os autores elencam os seguintes procedimentos:

a) coleta de dados: trata-se do processo de identificação, rotulação, registro e aquisição de dados no ambiente de computação em nuvem. As fontes de dados tanto podem estar do lado do cliente quanto do provedor de nuvem. A coleta deverá incluir procedimentos que garantam a integridade dos dados, ser realizada dentro dos limites legais, respeitando a jurisdição do Estado onde se encontram armazenados e a privacidade de inquilinos ou usuários não investigados;
b) elasticidade, perícia estática e *Live Forensics*: sendo uma das características da computação em nuvem a elasticidade, as ferramentas de forense digital nesse ambiente também precisam ser elásticas, trabalhando com grande quantidade de dados;
c) segregação de evidências: outra característica essencial na computação em nuvem é o *pooling* de recursos, que permite o compartilhamento de recursos e, consequentemente, a redução do custo em tecnologia da informação. Por outro lado, o ambiente multi-inquilino (*multi-tenant*) provoca a segregação da evidência, sendo necessários procedimentos e ferramentas para separar os dados dos múltiplos usuários, nos seus diferentes métodos de implantação e modelos de serviço;
d) investigação em ambiente virtualizado: a virtualização é a tecnologia chave da implementação da computação em nuvem. Nesse ambiente, faz-se necessário ferramentas e procedimentos para localizar e rastrear fisicamente os dados, num determinado período de tempo, respeitando as jurisdições envolvidas;
e) proatividade: medidas proativas podem ser adotadas para facilitar a investigação forense, tais como sistemas elaborados para recolher dados tanto a partir do provedor quanto do lado do cliente.

A dimensão legal envolve aspectos do Direito que legitimam a execução da *Cloud Forensics*. Referem-se, por exemplo, à jurisdição, ao compartilhamento de recursos, a acordos de nível de serviços (entre clientes e fornecedores de serviços):

a) multijurisdição e multi-usuário: trata-se de aspectos que são exacerbados na computação em nuvem. Regulações e acordos legais precisam ser estabelecidos para assegurar que as atividades forenses não violem jurisdição de Estado estrangeiro onde os dados se encontram

armazenados, nem tampouco atente contra a privacidade de usuários não investigados;

b) acordo de nível de serviço: definem acordos entre os provedores de computação em nuvem e os clientes do serviço. Os autores recomendam que algumas disposições que facilitem o trabalho da perícia forense sejam incluídas nos termos desses acordos. São exemplos: (1) serviços prestados, técnicas suportadas, acesso concedido pelo provedor de computação em nuvem ao usuário, em relação à investigação forense; (2) limites confiáveis, ressaltando funções e responsabilidades entre o provedor de computação em nuvem e o cliente, em relação à investigação forense; (3) como as investigações forenses são protegidas em um ambiente com múltiplas jurisdições, em termos de regulamentações legais, confidencialidade dos dados e políticas de privacidade; (4) como as investigações forenses são protegidas em um ambiente compartilhado, em termos legais, de confidencialidade dos dados e de política de privacidade.

Na dimensão organizacional, as investigações forenses envolvem os investigadores, profissionais de tecnologia da informação e comunicação, tratadores de incidentes, consultores legais, assistência externa, cabendo-lhes as seguintes funções:

a) investigadores: tanto do lado dos provedores de computação em nuvem quanto do lado do cliente são responsáveis por um trabalho colaborativo. Também é esperado que compreendam as capacidades forenses das partes com as quais interagem e a separação de funções entre elas;

b) profissionais de tecnologia da informação e comunicação: esse grupo inclui administradores de sistema, de rede de computadores e de segurança, e outros profissionais técnicos capazes de contribuir com o seu conhecimento para a investigação, facilitando o acesso dos investigadores à cena do crime, e à coleta dos dados de interesse;

c) tratadores de incidentes: refere-se do grupo que responde a incidentes de segurança na nuvem computacional, tais como acesso não autorizado, vazamento acidental e perda de dados, violação da confidencialidade, uso inadequado do sistema, infecções por códigos maliciosos, ataques internos maliciosos, ataques de negação de serviço, dentre outros. Os

autores recomendam que a empresa provedora de computação em nuvem mantenha um plano de atuação em caso de incidentes de segurança;

d) consultores legais: em razão do aspecto multidisciplinar da forense digital no ambiente de computação em nuvem, herdado da forense computacional, é importante ter à disposição especialistas na ciência jurídica que estejam familiarizados com aspectos legais sobre a perícia forense, com destaque a questões relacionadas à possibilidade de envolver múltiplas jurisdições;
e) assistência externa: é desejável que a empresa provedora da computação em nuvem mantenha equipes terceirizadas para apoiá-la nas atividades técnicas de forense digital, estabelecendo previamente as ações que devem ser executadas pelas mesmas, registrando em políticas, diretrizes e acordos, de forma transparente para seus clientes e para os agentes de aplicação da lei, quando necessário.

3.3.1 Os desafios da computação em nuvem à forense digital

O ambiente de computação em nuvem reveste-se de novos desafios à forense digital. Sibiya, Venter e Fogwill (2012) destacam os seguintes:

a) identidade: é difícil estabelecer um liame entre dados armazenados na nuvem computacional e o seu usuário;
b) encriptação: dados podem ser criptografados pelo cliente antes de enviá-los, e/ou pelo provedor de serviço em nuvem, antes de armazená-los;
c) jurisdição: acesso a dados armazenados em jurisdição estrangeira pode configurar violação à soberania de outros países. Ademais, segundo Dykstra e Sherman (2012), a natureza distribuída da computação em nuvem pode levar ao armazenamento de dados em diversos países, dificultando a obtenção dos mesmos, em especial quando inexistem acordos de cooperação entre os Estados envolvidos;
d) distribuição: os dados podem estar distribuídos em *data centers* situados em vários países.

Além do aspecto multijurisdicional possível de ocorrer durante a perícia forense digital, Martini, Quick e Choo (2013) acrescentam que a volatilidade dos dados digitais pode dificultar a investigação.

Também se constitui em obstáculo à perícia forense a característica de multi-inquilinato, que dificulta a obtenção do *hardware* que executa as aplicações de interesse, pois, como ele é compartilhado por vários usuários, não seria viável removê-lo para análise (FONTE II; SIMPLÍCIO JR., 2017).

Combinadas, tais características dificultam a coleta de evidências com a credibilidade necessária para que elas possam ser usadas em processos legais, que exigem o respeito à privacidade, à jurisdição, e à cadeia de custódia[35], bem como a reprodutibilidade do processo de coleta (FONTE II; SIMPLÍCIO JR., 2017).

Sang (2013) apresenta como desafios à forense digital no ambiente de computação em nuvem:

a) os modelos de computação em nuvem (*IaaS*, *PaaS*, *SaaS*), que apresentam diferentes níveis de complexidade;
b) dificuldade em dimensionar o conteúdo do *hardware* e das aplicações de interesse que funcionam na nuvem computacional, pois elas podem estar em qualquer parte do mundo ou até mesmo em nenhuma máquina real, pois funcionam em máquinas virtuais;
c) a natureza dinâmica e escalável característica da nuvem computacional faz aumentar as chances de perder informações.

Para o modelo *IaaS*, é possível coletar informações exatamente como a lista da máquina virtual. Caso não implemente máquinas virtuais, a coleta pode ser realizada por meio de *Live Forensics*. No entanto, para os modelos *SaaS* e *PaaS*, a maioria dos itens mostrados na lista não estão disponíveis, tornando a análise das máquinas virtuais impraticável, sem o apoio técnico dos provedores. Como as máquinas virtuais para *SaaS* e *PaaS* podem ter um sistema de armazenamento enorme e conter muitos outros aplicativos, os dados massivos constituem um grande desafio para à forense digital em nuvem computacional (SANG, 2013).

3.3.2 *Frameworks* para a forense digital em nuvem computacional

Ao longo dos anos, vários modelos de forense digital foram propostos, conforme apresentado por SLAY *et al* (2009). No entanto, as metodologias estudadas

[35] Cadeia de custódia é um processo usado para manter e documentar a história cronológica da evidência, para garantir a idoneidade e o rastreamento das evidências utilizadas em processos judiciais (LOPES; GABRIEL; BARETA, 2006).

pelos autores, específicas à forense digital, dificilmente se adequam ao ambiente de computação em nuvem. Existem padrões, regras e procedimentos comuns aos diversos ambientes digitais, que devem ser observados pelos peritos forenses. No entanto, há procedimentos específicos para a computação em nuvem que, via de regra, não se aplicam à perícia convencional em dispositivos informáticos.

As quatro fases da investigação na forense computacional propostas por McKemmish (1999) e aludidas acima, pressupõem um desdobramento linear, difícil de aplicar à forense digital no ambiente de computação em nuvem. Neste, um examinador não deve parar a análise de evidências digitais já apreendidas para aguardar que os dados armazenados na nuvem sejam preservados e fornecidos para apreciação. O perito deve continuar analisando as evidências digitais disponíveis e, quando os dados da nuvem forem fornecidos, devem ser inseridos no contexto da análise. É possível que a análise dos dados da nuvem possa identificar mais dados que precisam ser periciados. Nesse sentido, o processo forense digital deve ser considerado cíclico (QUICK; CHOO, 2014).

Para garantir que as evidências digitais sejam aceitas como prova no processo criminal, faz-se necessário o desenvolvimento de rigorosas metodologias que incluam procedimentos válidos no curso de uma investigação criminal (MARTINI; QUICK; CHOO, 2013). Ao mesmo tempo, devem ser esses processos flexíveis, de maneira a permitir o retorno a etapas anteriores, durante a fase de análise (QUICK; CHOO, 2014).

Vários *frameworks* foram propostos, como: Fonte II e Simplício Jr. (2017), Quick e Choo (2014), Martini, Quick e Choo (2013), Sang (2013), Ibiya, Venter e Fogwill (2012).

Fonte II e Simplício Jr. (2017) apresentam um modelo para a coleta de evidências forenses em ambiente de computação em nuvem, enfatizando a reprodutibilidade do processo de coleta, o estabelecimento de vínculo entre e evidência coletada e sua origem, e a preservação da jurisdição e da privacidade dos usuários não investigados.

Denominada *Dizang*, a solução proposta pelos autores utiliza contêineres Linux (LXC), uma vez que, em sistemas desenvolvidos sobre infraestrutura virtual, em especial quando esta é auto-escalável, os recursos computacionais são altamente voláteis e, portanto, podem deslocar-se a qualquer momento. Embora o contêiner seja um *software* e, portanto, também volátil, cada imagem compilada e sua execução na

forma de contêiner são normalmente atreladas a um *hash* que identifica univocamente essa relação. O contêiner permite identificar com mais precisão a fonte da evidência, uma vez que é possível dividir as partes de um sistema em contêineres, como por exemplo, um contêiner para o motor de páginas dinâmicas, outro com a lógica de negócios e um terceiro para um banco de dados.

A solução proposta pelos autores tem como foco a coleta de informações de memória no espaço do usuário (*user space*), não abrangendo o espaço *kernel* (*kernel space*). Assim, o *Dizang* não provê suporte a técnicas de investigação de *malware,* que se baseiam em informações do *kernel space*, como, por exemplo, a comparação de informações do bloco do ambiente do processo (*Process Environment Block* – PEB), que ficam no *user space*, com informações do descritor de endereços de memória virtual (*Virtual Address Descriptor* – VAD), localizado no *kernel space*. Análise de ameaças que realizam manipulação direta dos objetos do *kernel* (D.K.O.M.– *Direct Kernel Object Manipulation*) também não se beneficiam da solução proposta.

Outro *framework* é apresentado por Quick e Choo (2014), baseado na análise de dados remanescentes, deixados pelos usuários em dispositivos informáticos (celulares, computadores pessoais etc), após acessarem o referido ambiente, de forma a identificar se o dado digital suspeito está armazenado remotamente, estabelecendo inclusive a associação entre os mesmos e o usuário investigado[36].

Para os autores, constituem as fases da forense digital no ambiente de computação em nuvem as seguintes:

a) inicial, quando é delineado o escopo da pesquisa ou da investigação;
b) preparação e resposta, nas quais são providenciados os *hardwares* e *softwares* a serem utilizados na perícia forense, como a criação de máquinas virtuais, instalação de *browsers*, dentre outros;
c) identificação e coleta, na qual os arquivos de interesse são identificados e coletados;
d) preservação (cópia forense), na qual são feitas cópias dos dados constantes nos dispositivos de armazenamento virtuais de cada máquina virtual criada, bem como dos arquivos de memória e de rede de

[36] O aplicativo de nuvem computacional analisado pelos autores foi o *Google Drive*, e os dispositivos informáticos explorados foram computadores portáteis e Iphone. Ressaltam os autores que a solução apresentada é flexível o bastante para ser aplicada a qualquer ambiente de armazenamento em nuvem.

computadores, utilizando *softwares* específicos para essa finalidade, como *Encase Forensic*, *X-Way Evidence File Container*, não olvidando usar *hash* para garantir a integridade dos dados;

e) análise, quando a cópia forense dos discos virtuais, memória e rede de computadores é examinada, usando ferramentas de análise forense, como *X-Ways Forensic*, *Guidance Software EnCase*, *AccessData FTK*, *Network Miner*, *Internet Evidence Finder*, *RegRipper*, dentre outras;

f) apresentação, quando os resultados são apresentados e novas requisições podem ser identificadas (outros dados protegidos por senhas), ensejando inclusive em novas diligências;

g) retorno ou *feedback*, constitui a fase onde são identificados os pontos negativos e positivos da investigação, que proporcionará a equipe de peritos forenses consolidar o conhecimento na área, para implementar melhorias em processos de investigação futuros;

h) finalização, que é a conclusão da investigação.

Trata-se de um processo cíclico e interativo, no qual o perito forense pode retornar a fases anteriores durante a investigação para realizar novos exames, sem comprometer as atividades em execução.

Um outro framework, proposto por Martini, Quick e Choo (2013), foi inspirado no modelo originalmente apresentado por McKemmish (1999) e baseado em ciclo de análise de inteligência, sendo que aplicado ao ambiente de computação em nuvem. Assim, o modelo compreende os seguintes elementos:

a) escopo inicial;

b) preparação;

c) identificação e preservação das fontes de evidência;

d) coleta;

e) exame e análise;

f) apresentação, e

g) finalização.

No início de uma investigação, é importante delinear o seu escopo, a natureza e o ambiente da análise, de maneira a estabelecer as fronteiras da apuração. Os investigadores e peritos forenses precisam identificar “o que”, “onde”, “quando”, “quem”, “por que” e “como”, devendo todas as ações serem documentadas, incluindo as pessoas envolvidas, evidências apreendidas, identificada qualquer requisição

urgente, dentre outros aspectos. Geralmente, o escopo inicial é genérico, sendo refinado no desenrolar das investigações.

A fase seguinte é a de preparação, que se assemelha a fase homônima do *framework* de Quick e Choo (2014), na qual os investigadores e peritos forenses utilizam para compreender os requisitos e garantir a disponibilidade de recursos para a realização da perícia forense.

A identificação e preservação das fontes de evidência digital potencialmente relevante é a próxima etapa do *framework* em comento. Trata-se de uma fase crítica, considerando a volatilidade característica do ambiente de computação em nuvem. Geralmente, a análise da nuvem decorre de indícios encontrados em dispositivos pessoais (como *smatphones*, *tablets*, computadores). Uma vez identificadas as fontes, o próximo passo é localizar (eletrônica e fisicamente) o provedor do serviço para, em seguida, adotar providências legais no sentido de autorizar a violação do sigilo dos dados pessoais e dos arquivos digitais do investigado, passando então a fase seguinte, que é a de coleta.

A coleta no ambiente de computação em nuvem traz vários desafios, relacionados à localização do dado digital e à tecnologia empregada.

A localização física do dado digital torna-se desfavorável às investigações quando o armazenamento se encontra em servidores situados em jurisdições distintas daquela que apura os fatos, pois há necessidade de medidas legais adicionais que viabilizem a perícia ou a requisição em terras estrangeiras.

Mesmo que as evidências digitais estejam na jurisdição onde se processam as investigações, as tecnologias associadas à computação em nuvem podem introduzir questões relevantes, se comparadas aos tradicionais procedimentos de coleta, realizados em computadores pessoais. A inviabilidade de apreensão do *hardware*, a dinâmica das máquinas virtuais, os sistemas de *storages* são algumas características da tecnologia que trazem à perícia forense nova dinâmica de acesso às evidências digitais. Na nuvem, a coleta de evidências pode ser realizada diretamente pelo perito forense, usando uma máquina cliente com credenciais criadas para esse fim ou o próprio ambiente do usuário. Também é possível que o provedor de serviço execute as operações, em atenção a requisições do Poder Judiciário. Em todo caso, os autores recomendam a elaboração de um plano formal, orientador das ações.

O exame e análise das evidências digitais coletadas constituem a etapa subsequente e utilizam *softwares* e *hardwares* adequados a cada situação. Procedimentos comuns no exame dos dados coletados são: aplicação de filtros, busca por palavras-chaves, recuperação de dados excluídos, dentre outros. Na análise, que em geral é realizada manualmente, os peritos buscam por evidências digitais que respondam a testes de hipóteses, relativamente à investigação criminal. A qualquer momento, novas evidências digitais podem ser incluídas para exame e análise.

Na fase de apresentação, os procediemtnso são idênticos aos já referidos nos *frameworks* anteriores.

Quando a investigação envolve um volume grande de dados digitais e múltiplos investigados, a cadeia de custódia com detalhamento dos registros de *logs* torna-se crítica, pois precisa ser apresentada de forma legalmente aceitável. Tanto o provedor de serviço Internet quanto o provedor de serviços móveis (MSP) podem fornecer informações relevantes sobre conexões estabelecidas pelo investigado com o ambiente de computação em nuvem, constituindo assim potenciais fontes de evidências forenses.

Ainda, antes de finalizar uma investigação, os autores recomendam que os peritos forenses se certifiquem sobre a necessidade de aprofundar a análise dos dados coletados, com base nas considerações dos investigadores ou das autoridades para as quais os resultados foram apresentados. Não havendo mais dados digitais a serem analisados nem novas evidências a serem anexadas às investigações, o caso é dado por encerrado, devendo os dados serem arquivados de maneira que possam ser acessados posteriormente, se possível e quando necessário.

Sang (2013) propõe um modelo baseado em *logs*, para construir um sistema forense computacional amigável, que permita coletar rapidamente dados digitais na nuvem computacional, enfatizando a garantia da cadeia de custódia no transporte da evidência. A solução aplica-se unicamente à fase de coleta de dados.

Sibiya, Venter e Fogwill (2012) desenvolveram um *framework* denominado *Live digital forensic framework for a cloud*, projetado para resolver problemas de associação dos dados armazenados no ambiente de computação em nuvem ao usuário que de fato é o seu proprietário. São características da solução proposta:

a) a realização de perícia *Live*, ou seja, em máquinas virtuais de ambiente de computação em nuvem, a extração de dados para a busca de evidências criminais deve ser realizada enquanto o sistema está em funcionamento;

b) buscar a associação entre o usuário o os dados, considerando que, em ambiente de nuvem computacional, os dados dos usuários são armazenados remotamente. Mesmo que os dados sejam identificados, ainda será um desafio associá-los ao usuário investigado;
c) utilização de técnicas de mineração de dados (*data mining*), possibilitando a extração de dados de arquivos de *log* em locais de interesse, como área de trabalho remota hospedada ou o dispositivo cliente acessado;
d) emprego de técnicas de inteligência artificial para inferir relacionamentos entre os dados e o usuário investigado.

Nesse sentido, o *framework* indica mecanismos que podem ser utilizados para a coleta de evidências digitais em aplicações virtualizadas, sendo implementado servidor virtual, utilizando-se de algoritmos para descobrir arquivos de *log* de locais considerados relevantes, como a área de trabalho remota hospedada ou o dispositivo cliente acessado. Quando acionado, executa a análise forense entre duas organizações virtuais e monitora a interação.

3.4 Antiforense digital

A antiforense digital é um conjunto de métodos utilizados para impedir a ação da ciência forense na coleta de evidências digitais que resultem em violação de privacidade individual ou exposição de segredos industriais, podendo se manifestar por meio de destruição, ocultação, eliminação da fonte ou falsificação dos dados digitais (Tabela 1). As evidências podem ser destruídas para evitar que sejam encontradas ou que sejam úteis, caso sejam localizadas. Podem ser ocultadas para impedir que sejam casualmente expostas ou dificultar a sua identificação. Possíveis fontes de evidências podem ser destruídas para garantir que nunca estejam disponíveis, ou ainda manipuladas, para distribuir a culpa ou corromper a sua validade, de modo que não possam ser utilizadas como prova no processo penal (HARRIS; 2006).

Tabela 1 - Categorias antiforenses, por Harris (2006)

Nome	Destruição	Ocultação	Eliminação da fonte	Falsificação
Alterações MACE	Destruir a informação MACE ou sobrescrever com dados aleatórios.			Reescrever com dados aleatórios para confundir investigadores.
Remover/ esterilizar arquivo	Reescrever o conteúdo com dados aleatórios	Excluir o arquivo		
Encapsulamento de dados		Ocultar um arquivo em outro		
Sequestro de contas				Criar evidência para comprometer a análise da imagem
Desabilitar *logs*			Não são disponibilizadas informações sobre atividades realizadas.	

Fonte: Harris (2006, p. S45)

O resultado antiforense pode ser obtido com o uso de ferramentas ou métodos maliciosos, muitos de conhecimento público, ou simplesmente pelo uso de proteções legítimas, como senhas e criptografia. Embora diversos estudos sejam realizados sobre a detecção de ações antiforense, é importante estabelecer processos bem definidos de identificação e avaliação de riscos, de forma a evitar que evidências digitais deixem de ser recuperadas por falta de tratamento adequado (MAUÉS; HOELZ, 2016).

3.4.1 Destruição de dados

O principal objetivo da destruição de dados é impossibilitar que seu conteúdo seja recuperado ou possa expor a privacidade de pessoas ou eventualmente causar impacto no mercado corporativo. Trata-se de um processo irreversível que exige procedimentos adequados, tanto lógicos quanto físicos, que garantam a efetiva destruição das informações e resguardem os responsáveis de possíveis sanções legais.

De acordo com Della Vecchia, Weber e Zorzo (2013), a destruição física consiste em causar danos estruturais ao dispositivo de armazenamento, inviabilizando

sua reutilização pelos meios convencionais para os quais foi projetado. Pode ser realizada por meio de procedimentos relativamente simples, como a utilização de materiais abrasivos (lixa) para remover a camada magnética que reveste os discos de armazenamento, trituradores ou fragmentadores de alumínio, incineração, fundição de metais, agentes químicos. Os procedimentos de destruição lógica inviabilizam o acesso ao dado, mas conserva as funcionalidades da mídia, possibilitando assim uma melhor relação de custo/benefício. São exemplos a sobrescrita (*wiping* ou *shredding*) e a desmagnetização (*degaussing*), que consiste na remoção ou redução do campo magnético, esterilizando o disco ou qualquer outra mídia magnética.

3.4.2 Ocultação de dados

A ocultação de dados objetiva proteger informações privadas ou confidenciais contra a exposição indevida por descuido ou ação de intrusos. Existem diversas técnicas orientadas para a proteção de dados sensíveis, com diferentes procedimentos de ocultação e controle. Algumas não escondem a existência da informação, porém impõem dificuldades na interpretação do conteúdo (criptografia), enquanto outras privilegiam a ocultação da própria existência da informação (esteganografia) (DELLA VECCHIA; WEBER, ZORZO; 2013).

3.4.2.1 Criptografia

O dicionário *on-line* de Oxford[37] define criptografia como a arte de escrever ou decifrar códigos[38]. Nos dias atuais, essa definição é insuficiente para abranger a essência da criptografia moderna, que, a partir do final do século 20, por volta dos anos 80, despontou com novas teorias, o que permitiu o estudo rigoroso da criptografia como ciência.

A criptografia clássica tinha como cerne o sigilo das comunicações. Era considerada uma arte, pois se valia da criatividade e de habilidades pessoais para construir ou decifrar códigos. Era um trabalho intuitivo, por haver poucas referências sobre como elaborar um bom código. Era usada principalmente para atender fins militares e de inteligência organizacional (KATZ; LINDELL, 2007).

---

[37] https://en.oxforddictionaries.com/definition/cryptography.
[38] Livre tradução da autora para: "*The art of writing or solving codes*".

A criptografia moderna abrange muito mais do que comunicações secretas. Inclui autenticação de mensagens, assinaturas digitais, protocolos para troca de chaves secretas, protocolos de autenticação, leilões eletrônicos, eleições, moedas digitais. Além do mais, dedica-se à solução de problemas que possam surgir em qualquer computação distribuída que esteja sob ataque interno ou externo. Nesse sentido, a criptografia moderna é definida como o estudo científico sobre técnicas para proteger informações digitais, transações e computação distribuída. Nos dias de hoje, a criptografia está presente em grande parte do mundo digital, nas várias transações *on-lines* e nas comunicações entre pessoas comuns (KATZ; LINDELL, 2007).

Na criptografia moderna, o segredo não está no algoritmo, mas nas chaves utilizadas para cifrar e decifrar a mensagem. Existem, portanto, duas técnicas tradicionais (sem considerar princípios de física quântica), que são a criptografia simétrica e a criptografia assimétrica (DELLA VECCHIA; WEBER, ZORZO; 2013).

A criptografia simétrica é a forma mais comum e a de mais simples entendimento. Os dados a serem protegidos são alimentados a um algoritmo que recebe uma chave secreta e fornece como saída o dado criptografado. A informação é então transmitida ao receptor (ou armazenada para uso posterior). Para obter os dados originais, a informação criptografada é alimentada a um algoritmo que realiza um procedimento inverso e, se fornecida a mesma chave secreta, tem como saída os dados originais. Nesse modelo, a mesma chave é utilizada para codificar e decodificar. São exemplos de algoritmos de criptografia simétrica o AES (*Advanced Encryption Standard*), *Blowfish*, RC4 (DELLA VECCHIA; WEBER, ZORZO; 2013).

A criptografia assimétrica ou criptografia de chave pública utiliza duas chaves distintas, sendo uma para codificar e a outra para decodificar a mensagem cifrada. Os algoritmos de criptografia assimétrica são em geral baseados em problemas de difícil solução, como curvas elípticas, logaritmos discretos, fatoração de números primos. São exemplos de técnicas de criptografia assimétrica o protocolo *Diffie-Hellman* de troca de chaves, o algoritmo RSA e o padrão DSA (*Digital Signature Algorithm*).

Uma das desvantagens da criptografia assimétrica é o custo computacional dos algoritmos, mais lentos que os da criptografia simétrica, mesmo se implementados em *hardware* (DELLA VECCHIA; WEBER, ZORZO; 2013).

A criptografia pode ser realizada por *hardware* ou por *software*. Para armazenamento de informações de maneira segura, por *software*, Della Vecchia, Weber e Zorzo (2013) recomendam a criação de um arquivo (contêiner) em um disco

rígido e montar este arquivo em um *drive* virtual. Todas as informações do *drive* virtual são armazenadas no contêiner, de forma cifrada. A criptografia por *hardware* pode ser utilizada, por exemplo, por meio de *chips* da família MAXQ® (DeepCover® Secure Microcontroller) ou por *smartcards,* como *Javacards*, produzidos pela empresa NXP.

3.4.2.2 Esteganografia

Esteganografia é a técnica de ocultar, esconder informações (inclusive arquivos completos) em arquivo contendo texto, imagem, som, vídeo ou qualquer outro tipo de conteúdo, de tal forma que a presença das informações escondidas não seja percebida. O arquivo que contém as informações escondidas é chamado de hospedeiro ou portador (DELLA VECCHIA; WEBER, ZORZO; 2013).

Várias técnicas de esteganografia utilizam representações digitais de imagens ou áudios como arquivos hospedeiros. Um exemplo de técnica aplicada a imagens, que se encontra entre as mais difíceis de ser detectada, é a LSB (*Least Significant Bit*), na qual os dados a serem escondidos utilizam o *bit* menos significativo de cada canal de cada *pixel*. O *Hide & Reveal*, *SilentEye*, *OpenPuff* são exemplos de *softwares* que implementam essa técnica (DELLA VECCHIA; WEBER, ZORZO; 2013).

3.4.3 Eliminação da fonte

Refere-se à neutralização de possíveis fontes de evidências. Nesse caso, não há necessidade de destruir provas, uma vez que não foram criadas. No mundo físico, a utilização luvas de borracha para cometer um crime é um exemplo de eliminação de fontes de evidência. No entanto, pode ocorrer que o próprio ato de eliminação gere evidências. Assim, as luvas de borracha usadas para segurar a arma podem se tornar evidências.

Além disso, a falta de evidência pode se tornar evidência. Isso parece contra-intuitivo, no entanto, uma arma completamente desprovida de impressões digitais, pode levar o investigador a presumir que o crime foi cuidadosamente planejado. Essas observações também se aplicam ao mundo digital.

3.4.4 Falsificação

A falsificação de evidências é o ato de criar uma versão "falsificada" da evidência, indicando a prática de crime diverso do que ocorreu. Isso inclui criar evidências que funcionem como um ataque contra o processo ou ferramentas, envolvendo a edição seletiva de evidências existentes ou a criação de evidências inválidas para corromper a validade da evidência real. A evidência pode estar à vista de todos, não ter sido destruída e ainda ser inválida.

Outras das categorias antiforenses podem precisar ser combinadas com essa evidência de falsificação para que o resultado pretendido seja alcançado. No mundo físico, por exemplo, provas poderiam ser criadas para fazer um homicídio parecer um suicídio.

No mundo digital, a falsificação pode incluir o uso da conta de outra pessoa ou o de roteamento remoto para lançar ataques de negação de serviço, imputando, assim, a culpa a terceiro, que não foi quem efetivamente praticou o delito.

3.5 Técnicas de investigação criminal em nuvem computacional

Tecnicamente, há várias maneiras através das quais podem ser realizadas pesquisas no ambiente da computação em nuvem. Geralmente, em investigações dessa natureza, os agentes de investigação criminal e peritos criminais geralmente estão interessados em *e-mails* e arquivos pessoais armazenados. Eventualmente, quando o ambiente de tecnologia da informação e comunicação é o alvo do ataque, pode interessar também os diversos registros de atividades do invasor, como os registros de conexão, os registros de acesso a aplicações, os registros de atividades em banco de dados, dentre outros.

Koops e Goodwin (2014) introduzem duas técnicas utilizadas por peritos forenses para vasculhar o ambiente de computação em nuvem. A primeira é baseada no modelo cliente-servidor, no qual o computador da agência de investigação criminal funciona como o cliente, e o servidor é o computador do provedor da computação em nuvem. Assim, quando devidamente autorizado, o cliente utiliza-se de protocolos e aplicativos que possibilitam o acesso e a comunicação com os diversos ambientes a serem explorados. Para o acesso à plataforma *web*, por exemplo, seria empregado o protocolo HTTP; para a transferência de arquivos, o protocolo FTP; para o *e-mail*, os

protocolos POP3 ou SMTP, ou equivalentes. As credenciais para o acesso do cliente ao servidor podem ser voluntariamente cedidas pelo investigado ou criadas pelo provedor do serviço de nuvem.

Uma segunda técnica descrita pelos autores refere-se ao acesso ao ambiente, por meio de “ataque de força bruta” (com o intuito de evidenciar as credenciais de acesso), ou através da exploração de vulnerabilidades de segurança (por meio de varredura de portas – *port scan*), ou ainda se utilizando da instalação de *softwares* maliciosos (*backdoor*). A legalidade desses procedimentos de investigação criminal vem sendo questionada (GHAPPOUR, 2017). No Brasil, esses procedimentos invasivos violam o ordenamento jurídico, podendo inclusive constituir-se em crime.

Independentemente de autorização, a resposta do servidor, nesse modelo cliente-servidor, depende da configuração instalada e do recurso utilizado. Um acesso autorizado, por exemplo, pode ensejar em atendimento ou negação às solicitações enviadas, ou simplesmente ser ignorado. A varredura de portas, por sua vez, afetará significativamente o funcionamento do sistema.

Realizado o acesso ao ambiente, os dados podem ser copiados, alterados, apagados, além de ser possível também o registro da situação do servidor naquele momento (*snapshots*), semelhante ao registro que é feito por satélites sobre alvos na superfície terrestre, como objetos, áreas, fenômenos (KOOPS; GOODWIN, 2014). No entanto, diferentemente de um satélite, o simples fato de entrar em um sistema informático já lhe provoca alterações.

Outra estratégia de utilização da tecnologia da informação e comunicação na investigação criminal e na busca de provas para o processo penal é apresentada por Wendt e Barreto (2013, p. 3), sob a denominação de inteligência digital. Para os autores, trata-se de um processo baseado na utilização de todos os meios tecnológicos, digitais, telemáticos e de interceptação de sinais, com a finalidade de obter e analisar os dados, propiciando a produção de conhecimentos e/ou provas a respeito de assuntos de interesse da inteligência de segurança pública e, especificamente, da prática de delitos sob investigação policial ou, ainda, a responsabilidade penal de seus autores.

O objetivo principal da inteligência digital é auxiliar na produção do conhecimento, facilitanto sua concepção e seu aprimoramento, principalmente com base em fontes abertas, porém sem olvidar as fontes restritas, cujo acesso exige autorização de autoridade competente.

Nesse sentido, a inteligência digital tanto se desenvolve sobre dados abertos, ou seja, disposíveis na Internet para livre acesso de todos, quanto sobre dados protegidos por sigilo, como por senhas ou por qualquer outra restrição de acesso. O problema de pesquisa nessa Tese não alcança dos dados abertos, cujo acesso é irrestrito.

3.6 Contribuições à pesquisa

Esta seção demonstra a importância do aspecto multidisciplinar da ciência forense, em todas as suas subáreas, inclusive a digital, que requer do perito conhecimento profundo na sua área de atuação e compreensão dos limites impostos pela lei, no exercício do seu labor.

No caso da forense digital, o direito ampara, legitima, limita todas as fases de levantamento de evidências criminais eletrônicas. Não há como dissociar as atividades técnicas, desenvolvidas pelos peritos forenses, das normas processuais que as disciplinam, sob pena de invalidá-las como prova no processo penal.

O aspecto multijurisdicional da computação em nuvem foi apontado por vários autores como um desafio ao trabalho dos peritos. Entendem que, em sendo identificada a localização do dado em jurisdição distinta da que processa o crime, os trabalhos dependerão de acordo de cooperação internacional, que permitam a requisição de diligências a autoridades de outros Estados, por meio das quais são demandadas as empresas provedoras de serviço para a divulgação de dados protegidos por sigilo.

4 O CASO *MICROSOFT IRELAND*

O processo judicial relativo à controvérsia entre a empresa *Microsoft Corporation* e o Governo dos Estados Unidos da América, conhecido popularmente como *Microsoft Ireland Case*, ressaltou os desafios à persecução criminal (na qual prevalece o princípio da territorialidade), trazidos pela computação em nuvem (que implementa o estado da arte da mobilidade dos dados). O referido caso provocou intensa discussão entre estudiosos do direito e da ciência da computação, empresas provedoras de computação em nuvem, instituições não governamentais de defesa dos direitos humanos, autoridades de persecução criminal, peritos forenses e até mesmo representações estatais, como o Governo da República da Irlanda.

Não se pretende utilizar o rigor metodológico de estudo de caso, uma vez que não se constitui objetivo dessa Tese aprofundar a investigação qualitativa do caso, mas tão somente buscar, nas argumentações das partes e dos *amicus curiae*[39]*,* identificar os fundamentos defendidos e sua possível contribuição à proposta de solução apresentada adiante. Mesmo assim, as fases da referida metodologia foram observadas: a exploratória (delimitando o foco da abordagem), a coleta de dados (nas peças processuais) e a análise (com base nos documentos recolhidos).

Esta seção apresenta o caso *Microsoft Ireland*, iniciando com uma breve abordagem acerca da legislação criminal dos Estados Unidos, concernente ao caso em estudo. Em seguida, são analisadas as principais peças do processo, com o objetivo de identificar as teses defendidas pelas partes e por instituições, como *amicus curiae*.

4.1 O *Electronic Communications Privacy Act*

O *Electronic Communications Privacy Act* (ECPA) é uma lei federal dos Estados Unidos, editada em 1986, atualizando o *Federal Wiretap Act*, de 1968, que se referia à interceptação telefônica, mas silenciava quanto às comunicações

[39] Expressão em latim para designar “amigos da Corte” ou “amigos do Tribunal”.

realizadas por meio de computadores ou de outros dispositivos eletrônicos e digitais (DEPARTMENT OF JUSTICE, 2013).

De modo geral, o ECPA protege a privacidade das comunicações eletrônicas, seja enquanto são produzidas ou transmitidas, seja quando se encontram armazenadas em meio digital. Seus dispositivos integram o *United States Code Title 18 (18 U.S.C)* (UNITED STATES, 1986), e estão distribuídos por três Títulos:

a) Título I, geralmente referido como *Wiretap Act*, protege todas as formas de comunicações contra a interceptação indevida, inclusive na forma tentada. Nesse caso, é necessário que os dados estejam em trânsito entre servidores (STEPHENSON, 1999). Também proíbe a utilização indevida, em instrução probatória, de dados obtidos em desacordo com a lei. Está codificado no *18 U.S.C Chapter 119 - Wire and Electronic Communications Interception and Interception of Oral Communications*, §§ 2510 a 2522;
b) Título II, também conhecido como *Stored Communications Act - SCA*, protege o sigilo do conteúdo das comunicações e dos arquivos, ambos armazenados em provedores de serviço, e também dos registros relacionados aos assinantes, como nome, endereço IP, dados de pagamento. Está codificado no *18 U.S.C Chapter 121 - Stored Wire and Electronic Communications and Transactional Records Access*, §§ 2701 a 2712.
c) Título III, conhecido como *Pen Register Act*, protege informações relativas à origem e destinação de comunicações (DEPARTMENT OF JUSTICE, 2013). Está codificado no *18 U.S.C Chapter 206 - Pen Registers and Trap and Trace Devices*, §§ 3121 a 3127.

É relevante ao contexto desse trabalho o *Title II - Stored Communications Act.*

4.2 O *Stored Communications Act*

O *Stored Communications Act* (SCA) é a parte do ECPA especialmente destinada à proteção dos dados armazenados em dois tipos de serviços eletrônicos.

Trata-se do *Electronic Communications Service* – ECS[40], que, via de regra, oferece serviço de envio de mensagens eletrônicas sobre linhas de telefonia, e o *Remote Computing Service* – RCS[41], que provê acesso remoto a computadores para processamento de dados. Tanto o ECS quanto o RCS serão referidos aqui como provedores de serviço, fazendo a distinção apenas quando estritamente necessário. Para ambos, o SCA impõe a obrigação de sigilo dos dados (ORTON; ALVA; ENDICOTT-POPOVSKY, 2012; KERR, 2004), embora excepcionalmente autorize a divulgação a autoridades de justiça criminal, nas condições estabelecidas pelo próprio SCA.

É relevante destacar que o SCA entrou em vigor no ano de 1986 e, desde então, não ocorreram alterações nesses dois conceitos. Na época em que o SCA foi editado, a diferença entre o ECS e o RCS estava tecnicamente evidente nas implementações das redes de computadores. Nos dias atuais, com o advento da Internet, da computação em nuvem e de outras tecnologias da informação e comunicação, essa diferença tornou-se transparente. No entanto, a determinação da natureza do serviço, se proveniente de um ECS ou de um RCS, continua sendo determinante para definir a medida cabível à quebra do sigilo dos dados. Sendo assim, os Tribunais, quando precisam aplicar o SCA, procuram identificar previamente a intenção do legislador, a partir dos princípios que nortearam a edição do texto original, considerando também a história legislativa da norma, atualizando-a quanto às novas plataformas tecnológicas disponíveis (ROBISON, 2010). A estrutura dos dispositivos do SCA é complexa (GRAY, 2016; ORTON; ALVA; ENDICOTT-POPOVSKY, 2012) e, em algumas situações, acarreta interpretações ambíguas (GRAY, 2016).

O SCA está codificado no *18 U.S.C Chapter 121 - Stored Wire and Electronic Communications and Transactional Records Access*, §§ 2701 a 2712. A Seção *18 U.S.C § 2703* do SCA - *Required disclosure of customer communications or records*, dispõe sobre requisitos para o Estado requerer ao provedor de serviço a entrega de dados e informações relativos a um determinado cliente, além de estabelecer instrumentos jurídicos para esse fim, quais sejam: a intimação administrativa

[40] 18 U.S. Code § 2510 – Definitions – (15) *"electronic communication service" means any service which provides to users thereof the ability to send or receive wire or electronic communications*;
[41] 18 U.S. Code § 2711 - *Definitions for chapter - (2) the term "remote computing service" means the provision to the public of computer storage or processing services by means of an electronic communications system*;

(*Administrative Subpoena*), a ordem judicial (*Court Order*) e o mandado (*Warrant*)[42]. O tipo de registro que o provedor de serviço irá produzir, associado a requisitos específicos, indicará a escolha do instrumento a ser utilizado (UNITED STATES, 2014c).

A *Administrative Subpoena* (autorizada por estatuto Federal ou Estadual, ou Grande Júri Federal ou Estadual) é utilizada para a obtenção das seguintes categorias de informações:

a) registros e outras informações pertinentes ao usuário (nome, endereço, forma de pagamento pelo serviço) e algumas informações transacionais (registros de ligações telefônicas locais e de longa distância, duração e tipo de serviços utilizados, registro de conexões IP), nos termos do 18 U.S.C § 2703 (c)(1)(E)(2). Nesse contexto, não estão incluídos os conteúdos das comunicações;
b) conteúdo de comunicações recuperadas e outros arquivos armazenados pelo provedor de serviços RCS (como *e-mail*s abertos, independentemente de tempo), desde que a entidade governamental emita aviso prévio ao cliente ou assinante, conforme 18 U.S.C §§ 2703 (b)(1)(B)(i) e (b)(2)), e
c) conteúdo de comunicações não recuperadas e armazenadas com o provedor de serviço (como *e-mail*s não abertos), por mais de 180 dias, desde que precedida de aviso prévio emitido pela entidade governamental ao cliente ou assinante (18 U.S.C § 2703 (a)).

É exigência para a expedição de uma *Court Order* que a entidade governamental requisitante demonstre que os dados solicitados são relevantes à identificação do sujeito ativo e à formação da materialidade do crime investigado, nos termos da 18 U.S.C § 2703 (d). Uma *Court Order* autoriza o provedor a entregar:

a) todos os registros que podem ser produzidos por meio de *Administrative Subpoena*;
b) outros registros relativos ao usuário, como os endereços eletrônicos com os quais o assinante se comunicou. Não inclui o conteúdo das comunicações.

[42] Ao longo do texto, optou-se por manter a terminologia original (*Administrative Subpoena, Court Order e warrant),* em razão da dificuldade em associá-las a designações correspondentes no direito brasileiro.

Por fim, o *Warrant* impõe ao provedor de serviço de comunicação eletrônica (ECS) a obrigação de produzir os seguintes registros:

a) todos aqueles extraídos sob o manto do 18 U.S.C § 2703 (d);
b) o conteúdo de comunicações eletrônicas, como *e-mails* não abertos, armazenadas com o provedor de serviço por menos de 180 dias (18 U.S.C § 2703 (a)).

Em alguns processos judiciais que tramitaram em tribunais distritais, magistrados fizeram distinção entre *e-mails* abertos e *e-mails* não abertos, argumentando que, uma vez acessado, o *e-mail* não estaria em ECS, e sim em RCS, o que autorizaria o acesso por meio de *Administrative Subpoena*, não necessitando de um *Warrant* (SWIRE; HEMMINGS; VERGNOLLE, 2016).

A expedição de um *Warrant* pelo Tribunal segue as normas estabelecidas no *Federal Rules of Criminal Procedures* (UNITED STATES, 1946) ou, no caso da justiça estadual, obedece aos procedimentos constantes em estatutos locais (18 U.S.C § 2703 (a)(b)).

A expedição de um *Warrant* exige, da autoridade requisitante, a apresentação de fundadas razões que justifiquem a excepcionalidade da violação ao direito fundamental à privacidade, vez que nenhum mandado será expedido, a não ser mediante indícios de culpabilidade confirmados por juramento ou declaração, nos termos da Quarta Emenda à Constituição dos Estados Unidos[43].

A Tabela 2 sumariza as exigências para a divulgação de dados dos usuários, nos termos do SCA e do *Wiretap Act*.

Observa-se, a partir da interpretação do SCA, o tratamento diferenciado dispensado aos dados de conteúdo e aos que caracterizam a comunicação e permitem a identificação do usuário, ou seja, os metadados. Quando um *e-mail* é enviado, por exemplo, o corpo do *e-mail*, o assunto e os anexos são considerados dados de conteúdo. Os metadados referentes ao *e-mail* são os endereços eletrônicos do destinatário e do remetente, os endereços IP associados, o dia e a hora em que o

[43] Amendment IV (1791): The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized (UNITED STATES, 1789). Tradução: Emenda IV (1791): O direito do povo à inviolabilidade de suas pessoas, casas, papéis e haveres contra busca e apreensão arbitrárias não poderá ser infringido; e nenhum mandado será expedido a não ser mediante indícios de culpabilidade confirmados por juramento ou declaração, e particularmente com a descrição do local da busca e a indicação das pessoas ou coisas a serem apreendidas.

e-mail foi enviado, as informações de cobrança e outros que facilitem a identificação do usuário (KERR, 2004).

Tabela 2 - Requisitos para acesso pelo Estado a informações de usuários de provedores de serviço, nos termos do SCA e do *Wiretap Act*

Tipo de comunicação	Requisito divulgação ao Estado	Amparo legal
***E-mail* em trânsito**	*Warrant*	18 U.S.C § 2516 (*Wiretap Act*)
***E-mail* armazenado em computador doméstico**	*Warrant*	4ª Emenda à Constituição dos Estados Unidos
***E-mail* aberto e armazenado remotamente**	*Administrative Subpoena*	18 U.S.C § 2703 (SCA)
***E-mail* não aberto, armazenado remotamente, por até 180 dias.**	*Warrant*	18 U.S.C § 2703 (SCA)
***E-mail* não aberto, armazenado remotamente, por mais de 180 dias.**	*Administrative Subpoena*	18 U.S.C § 2703 (SCA)

Fonte: *Electronic Privacy Information Center*[44]

O caso *Microsoft Ireland* motivou a apresentação de projetos de lei ao Congresso norte-americano, voltados a promover alterações no ECPA, em reconhecimento à necessidade de atualização legal ante a mudanças trazidas pela tecnologia da informação e comunicação (como a Internet, a computação em nuvem), proporcionando assim segurança jurídica a todos os atores envolvidos (Estado, provedores de serviço, vítimas, infratores, sociedade), por ocasião da coleta, no estrangeiro, de evidências criminais eletrônicas. De acordo com Daskal (2017a), nenhuma proposta satisfará plenamente a todos os interesses, embora haja um consenso de que o estado atual é inadequado à segurança e à privacidade dos usuários, e para as empresas provedoras de serviço.

Nesse sentido, foram apresentados os seguintes projetos:

a) o *Law Enforcement Access to Data Stored Abroad Act* (2015), que propõe alterar o *18 U.S. Code*, para proteger os dados armazenados fora dos Estados Unidos;

b) o *E-mail Privacy Act;*

c) o *International Communications Privacy Act.*

[44] Electronic Privacy Information Center (United States of America). Electronic Communications Privacy Act (ECPA). Disponível em: <https://epic.org/privacy/ecpa/>. Acesso em: 16 ago. 2016.

4.3. Os projetos de lei para alterar o SCA

4.3.1 O *Law Enforcement Access to Data Stored Abroad Act*

O projeto de lei denominado *Law Enforcement Access to Data Stored Abroad Act* (LEADS) foi apresentado em 12 de fevereiro de 2015, durante a 1ª sessão da 114ª legislatura (de 06 de janeiro de 2015 a 03 de janeiro de 2017) (CONGRESS, 2015). O projeto não tramita mais no Congresso, vez que ultrapassou a legislatura, que é de dois anos e recebe a denominação de *Congress* (114º *Congress*, por exemplo).

As mudanças propostas pelo LEADS incidiam principalmente sobre questões procedimentais do MLAT. Quanto à divulgação de informações, era obrigatória a expedição de um *Warrant* para autorizar a produção de todas as informações de conteúdo, independentemente do período de armazenamento ou se se tratava de *e-mail* aberto ou não lido. Não havia previsão de mudanças, no entanto, em relação aos metadados.

O objetivo da lei era minimizar a reação de Estados estrangeiros, surpreendidos pelo cumprimento de mandando judicial em seu território, expedido por autoridade norte-americana, nos termos do SCA, bem como garantir aos cidadãos estrangeiros que não haveria violação de privacidade de seus dados, por parte dos Estados Unidos (SCHULTHEIS, 2015).

4.3.2 O *E-mail Privacy Act*

Trata-se de um projeto de lei que tramita no Congresso norte-americano, propondo alterações no ECPA, com o fim de atualizar as proteções de privacidade para as comunicações eletrônicas armazenadas em provedores de serviço e, ao mesmo tempo, atender aos requisitos relativos à aplicação da lei.

O projeto de lei foi apresentado primeiramente em maio de 2013, durante o 113º *Congress* (referência: H.R. 1852), sendo reapresentado em abril de 2016, ao 114º *Congress* (referência: H.R. 699) e ao 115º *Congress* (referência: H.R. 387), em janeiro de 2017 (CONGRESS, 2017a).

Dentre as medidas propostas está a eliminação dos diferentes critérios exigidos à quebra de sigilo dos dados armazenados pelos provedores de serviço. Assim, pretende-se que a divulgação de qualquer conteúdo das comunicações seja

realizada apenas através de *Warrant,* expedido por Tribunal, independentemente do tempo em que esteja armazenada ou se a informação é buscada de um ECS ou RCS.

Na perspectiva do poder judiciário, tratamento igualitário entre dados e metadados facilitaria a aplicação do SCA, podendo contribuir para aumentar a eficiência da persecussão criminal, além de dirimir incertezas quanto à natureza dos dados requeridos e à proteção conferida pela Quarta Emenda à Constituição dos Estados Unidos. Do ponto de vista do poder legislativo, permitiria assegurar uniformidade ao tratamento à privacidade do usuário, submetendo-os aos mesmos padrões e regras de divulgação. Ademais, evitaria que os provedores de serviço tivessem que adotar procedimentos diversos (a depender do tipo de dado solicitado) para atender, ou não, as requisições judiciais (GRAY, 2016).

Outra medida refere-se à notificação do usuário, relativamente à divulgação do conteúdo de suas comunicações. Caberá ao órgão responsável pela persecução criminal que recebeu as informações, no prazo de 10 (dez) dias, ou a outra entidade governamental, no prazo de 03 (três dias), fornecer ao usuário cuja conta foi violada uma cópia do mandado, notificando-o acerca da quebra do sigilo. É permitido ao Estado pleitear a prorrogação do referido prazo, caso a divulgação comprometa a investigação.

4.3.3 O *International Communications Privacy Act*

O projeto de lei denominado *International Communications Privacy Act* (ICPA) foi originalmente apresentado ao 114º *Congress*, em 25 de maio de 2016, com a referência de S.2986 (*Senate*), sendo reapresentado ao 115º *Congress*, em 27 de julho de 2017, como S.1671 (*Senate*). Outro projeto de lei idêntico também foi apresentado à *House of Representative*, com a referência HR. 3718, em 08 de setembro de 2017 (CONGRESS, 2017b).

O referido projeto de lei altera o código penal federal norte-americano para:

> […] allowing a governmental entity to require providers of electronic communication services or remote computing services to disclose the contents of communications in electronic storage (e.g., the cloud), regardless of where those communications are located. Thus, a governmental entity may obtain a warrant for electronic communications stored outside of the United States if certain conditions for obtaining the warrant are met (CONGRESS, 2017b)[45]

Ainda de acordo com o projeto de lei, o acesso ao conteúdo das comunicações depende de comprovação, por parte da instituição governamental interessada na divulgação dos dados, de que a pessoa investigada seja norte-americana, residente nos Estados Unidos ou um nacional de país estrangeiro com o qual os Estados Unidos mantenham acordo de cooperação policial. A autoridade policial deverá demonstrar ao Tribunal que adotou todas as medidas cabíveis para determinar a nacionalidade e a localização do usuário ou cliente.

O projeto de lei prevê inclusive alterações nos procedimentos do MLAT, como a elaboração de um aplicativo *on-line* a ser disponibilizado no site eletrônico do Departamento de Justiça dos Estados Unidos, padronizando a requisição de evidências criminais eletrônicas em território norte-americano.

Caberá também ao Departamento de Justiça manter relatórios periódicos de atividades relacionadas ao MLAT, com o número de requisições recebidas, atendidas, bem como realizadas pelo próprio Governo norte-americano a Estado estrangeiro.

O Congresso entende que a imposição de localização ou territorialização dos dados, por parte de Estados estrangeiros, a provedores de serviço, é incompatível com a natureza transnacional da Internet, constitui um impedimento à inovação, além de ser prescindível à persecução criminal (de acordo com o *Sec. 5. Sense of Congress*, do projeto de lei (CONGRESS, 2017b)).

[45] Livre tradução da autora: "[...] permitir que uma entidade governamental exija que os provedores de serviços de comunicação eletrônica ou serviços de computação remota divulguem o conteúdo das comunicações armazenadas eletronicamente (por exemplo, na nuvem), independentemente de onde estejam localizadas. Assim, uma entidade governamental pode obter um mandado para comunicações eletrônicas armazenadas fora dos Estados Unidos se determinadas condições forem atendidas."

4.4 *Microsoft Ireland Case*: *Microsoft Corporation* versus *United States of America*

4.4.1 Descrição dos fatos

O caso em análise ficou popularmente conhecido como *Microsoft Ireland Case,* sendo formalmente intitulado "*In the Matter of a Warrant to Search a Certain E-Mail Account Controlled and Maintained by Microsoft Corporation".*

Em 4 de dezembro de 2013, agentes federais dos Estados Unidos, que conduziam uma investigação criminal relativamente a tráfico de drogas, obtiveram do *Magistrate Judge* James C. Francis IV, do *United States District Court for the Southern District of New York,* com fundamento no *SCA*, mandado de busca e apreensão de informações *(Warrant)* associadas a uma determinada conta de *e-mail*, controlada e mantida pela *Microsoft Corporation* (Microsoft), empresa multinacional sediada naquele país, na cidade de Redmond, Estado de Washington (UNITED STATES, 2014d; UNITED STATES, 2014f).

Na Microsoft, as requisições relacionadas à violação de privacidade são processadas pelo *Microsoft´s Global Criminal Compliance Team,* a partir de escritórios da empresa na Califórnia e Washington. Primeiramente, a equipe técnica identifica a localização dos dados e, caso estejam armazenados em território norte-americano, procedem a recuperação (MICROSOFT CORPORATION, 2014a).

A empresa atendeu as requisições contidas no mandado relativamente às informações da conta não relacionadas a conteúdo[46], vez que se encontravam armazenadas em servidores nos Estados Unidos (ELLINGSEN, 2016; HARVARD LAW REVIEW, 2015; MICROSOFT CORPORATION, 2013). No entanto, recusou-se a fornecer o conteúdo dos *e-mails*, vez que os dados se encontravam armazenados em *data center* da Corporação em Dublin, República da Irlanda, operado e mantido pela subsidiária irlandesa *Microsoft Ireland Operations Limited,* entendendo, portanto, o Microsoft que nenhum Tribunal nos Estados Unidos seria competente para expedir mandado extraterritorial de busca e apreensão de informações, bem como carecia o

[46] São duas as categorias de dados de mensagens de *e-mail*: a) informações de conteúdo, como as constantes no corpo do *e-mail*, anexos ou em suas linhas de assunto; b) informações não relacionadas a conteúdo, como o endereço do emitente, do destinatário, data e hora da transmissão, catálogo de endereços (MICROSOFT CORPORATION, 2013).

Governo norte-americano de autoridade para executá-lo (MICROSOFT CORPORATION, 2013; MICROSOFT CORPORATION, 2014a).

Para a Microsoft (2013), a Regra 41 (busca e apreensão) das Regras Federais de Procedimentos Criminais[47] ou qualquer outro estatuto ou norma de direito processual penal norte-americano, incluindo o SCA, não autorizam a emissão de mandados com alcance extraterritorial. Ademais, é entendimento da Corte Suprema norte-americana que, quando um estatuto não dispõe explicitamente acerca da aplicação extraterritorial de uma medida judicial, é porque esta não existe, conforme asseverado no caso *Morrison v. National Australian Bank*, de 2010.

Reforça ainda a tese defendida pela Microsoft a instrução contida no manual do Departamento de Justiça dos Estados Unidos (DEPARTMENT OF JUSTICE, 2009), orientando os agentes federais, em caso de coleta extraterritorial de evidências criminais, a solicitarem previamente a conservação dos dados relevantes à investigação, enquanto é formalizado o pedido de assistência judiciária com o país onde se encontrem armazenadas essas evidências de crime.

Durante todo o caso, a Microsoft recebeu apoio de profissionais da ciência da computação e de várias instituições[48] que, na qualidade de *amicus curiae*, apresentaram ao Tribunal suas contribuições.

Em julho de 2016, o *United States Court of Appeals for the Second Circuit*[49], por unanimidade, decidiu que a Microsoft não estaria obrigada a fornecer informações armazenadas em servidores de subsidiária irlandesa da empresa, localizados em Dublin. Em junho de 2017, o Departamento de Justiça dos Estados Unidos impetra ação na Suprema Corte, requerendo deliberação acerca da possibilidade de um provedor de serviços de *e-mail*, sediado nos Estados Unidos, cumprir mandado baseado em causa provável, emitido nos termos do 18 USC. 2703 - *Required*

---

[47] *Federal Rules of Criminal Procedures - Title VIII. Supplementary and Special Proceedings - Rule 41. Search and Seizure*

[48] Brennan Center for Justice, New York; Electronic Frontier Foundation, San Francisco; American Civil Liberties Union, New York; The Constitution Project; Applec Inc.; BSA The *Software* Alliance; Center for Democracy and Technology; Chamber of Commerce of the United States; The National Association of Manufacturers; ACT|The APP Association; Anthony J. Colangelo, International Law Scholar; AT&T Corp.; Rackspace US, Inc.; Computer & Communications Industry Association; I2 Coalition; Application Developers Alliance, Washington DC; Ireland; Amazon.com, Inc.; Accenture PLC; Verison Communications Inc., New York, NY; Cisco System Inc., San Jose, CA; eBay Inc.; Hewlett-Packard Co.; Salesforce.com, Inc., San Francisco, CA; Media Organizations, Washington, DC; Computer and Data Science Experts; Jan Philipp Albrecht, Member of the European Parliament (UNITED STATES, 2016a).

[49] Corte de Apelação competente para receber os recursos oriundos de processos que tramitam na *United States District Court Southern District of New York*

disclosure of customer communications or records, mediante violação de sigilo, nos Estados Unidos, de comunicações eletrônicas sobre as quais mantenha controle, mesmo que o provedor tenha decidido armazenar os dados em território estrangeiro.

A Tabela 3 apresenta, em ordem cronológica, as principais peças que compõem o caso *Microsoft Ireland*, até a setembro de 2017.

A seguir, serão apresentadas as teses que subsidiaram a defesa das partes envolvidas no processo.

4.4.2 O Mandado (*Warrant 13 MAG 2814*) e a resposta da Microsoft

O *Warrant*[50]*,* que obrigava a Microsoft a fornecer dados armazenados em servidores da empresa, foi expedido em 4 de dezembro de 2013, pelo *Magistrate Judge* James C. Francis IV, do *United States District Court for the Southern District of New York,* em atenção à requisição de agentes federais norte-americanos que conduziam uma investigação criminal relativamente a tráfico de drogas.

O *Warrant* estava fundamentado no *SCA* e determinava que a Microsoft fornecesse informações associadas a uma determinada conta de *e-mail*, controlada, mantida e operada pela empresa (UNITED STATES, 2014g).

Especificamente, foram solicitadas as seguintes informações:

a) o conteúdo de todos os *e-mails* armazenados na conta do investigado, inclusive o conteúdo dos *e-mails* enviados;
b) os registros e outras informações que possibilitassem a identificação do usuário (como nome completo, endereço físico, número de telefone etc), registros relacionados a data de criação da conta, registros de movimentação, os tipos de serviços utilizados, os endereços IP associados, os endereços IP dos logins relativamente a cada sessão estabelecida, *e-mails* alternativos, *logs* de arquivos, métodos de conexão;
c) os registros e informações associados à conta, como agenda de contatos, imagens e arquivos armazenados;

[50] Cópia do *Warrant* encontra-se anexada ao "*Government's Brief in Support of The Magistrate Judge's Decision to Uphold a Warrant Ordering Microsoft to Disclose Records Within Its Custody and Control*" (UNITED STATES, 2014d).

d) os registros relacionados à comunicação entre a conta investigada e qualquer outro indivíduo, incluindo contato com serviços de suporte e registros de ações.

Tabela 3 - Principais peças do processo *Microsoft Ireland Case*

Data	Identificação da peça	Autoria
04/12/2013	*Warrant* 13 MAG 2814	*Magistrate Judge* James C. Francis IV
18/12/2013	*Memorandum in Support of Microsoft´s Motion to Vacate in Part na SCA Warrant Customer Information located Outside the United States*	Microsoft Corporation
14/02/2014	*Governments' Memorandum of Law in Opposition to Microsoft´s Motion to Vacate Email Account Warrant*	Preet Bharara, *US Attorney for Southern District of New York*
14/03/2014	*Reply Memorandum in Support of Microsoft´s Motion to Vacate in Part na SCA Warrant Seeking Customer Information located Outside the United States.*	Microsoft Corporation
25/04/2014	*Memorandum and Order*	*Magistrate Judge* James C. Francis IV
06/06/2014	*Microsoft's Objections to the Magistrate's Order Denying Microsoft's Motion to Vacate in Part a Search Warrant Seeking Customer Information Located Outside the United States*	Microsoft Corporation
10/06/2014	*Memorandum of law in Support of Verizon Communications Inc.´s Motion to Participate as amicus curiae and Microsoft Inc.´s Motion to Vacate Search Warrant.*	*Verizon Communications Inc.*
11/06/2014	*Memorandum of law of amicus curiae AT&T Corp. In Support of Microsoft Corporation.*	*AT&T Corporation*
12/06/2014	*Brief Amicus Curiae of Electronic Frontier Foundation in support of Microsoft Corporation*	*Electronic Frontier Foundation*
13/06/2014	Memorandum of law in Support of Motion by Apple Inc. and Cisco System Inc. to Participate as *amicus curiae* and Microsoft Inc.´s Motion to Vacate Search Warrant.	Apple Inc. and Cisco System Inc.
09/07/2014	*Government's Brief in Support of The Magistrate Judge's Decision to Uphold a Warrant Ordering Microsoft to Disclose Records Within Its Custody and Control.*	Preet Bharara, *US Attorney for Southern District of New York*
29/08/2014	*Memorandum and Order*	*Chief Magistrate* Loretta A. Preska
08/12/2014	*Brief for Appellant (United States Court of Appeals for the Second Circuit)*	Microsoft Corporation
15/12/2014	*Brief for Amici Curiae Brennan Center for Justice at NYU School of Law, American Civil Liberties Union, the Constitution Project, and Electronic Frontier Foundation in Support of Appellant.*	*Electronic Frontier Foundation et al.*
23/12/2014	*Brief for Amicus Curiae Ireland*	Governo da Irlanda.
09/03/2015	*Brief for the United States of America*	Preet Bharara, *US Attorney for Southern District of New York*
08/04/2015	*Reply Brief for Appellant*	Microsoft Corporation
14/07/2016	*Decision of United States Court of Appeals for the Second Circuit*	*US Court of Appeals for the Second Circuit*
23/06/2017	*On Petition for a Writ of Certiorari to The United States Court of Appeals for the Second Circuit. Petition for a Writ of Certiorari.*	Departamento de Justiça dos Estados Unidos
09/2017	*On Petition for a Writ of Certiorari to the United States Court of Appeals for the Second Circuit* (DEPARTMENT OF JUSTICE, 2017).	Departamento de Justiça dos Estados Unidos

Fonte: Direta

As informações armazenadas em território norte-americano foram entregues aos agentes federais. No entanto, os conteúdos das comunicações, que se encontravam armazenados em território de Estado estrangeiro, não foram produzidos (MICROSOFT CORPORATION, 2013).

4.4.3 Resposta dos Procuradores do *U.S. District Court for the Southern District of New York* sobre a decisão da Microsoft

Em resposta a recusa da Microsoft em fornecer as informações requisitadas, os advogados do *U.S. District Court for the Southern District of New York* apresentaram Memorando (UNITED STATES, 2014f), contestando os argumentos apresentados. Foi incorporado ao processo em 14 de fevereiro de 2014.

A principal tese defendida nesse documento foi a de que o mandado corretamente exigia da Microsoft a produção de informações, a partir de registros que se encontravam sob sua posse, controle e custódia, independentemente de onde estivessem fisicamente armazenados.

Para os Procuradores, houve um equívoco da Microsoft na interpretação dos termos do mandado, pois:

a) o SCA não admite recusa a cumprimento de mandado judicial;
b) provedor de serviço norte-americano deve cumprir o *SCA-Warrant*[51], independentemente de onde os dados requisitados estejam armazenados;
c) o *SCA-Warrant* é diferente do mandado de busca convencional;
d) o SCA-*Warrant* não tem a natureza extraterritorial;
e) a política da Microsoft impede a coleta de evidências criminais armazenadas no exterior.

As seções seguintes apresentam uma breve descrição desses argumentos.

4.4.3.1 O SCA não admite recusa a cumprimento de mandado judicial

De acordo com o Procurador, não há indicação no texto ou na estrutura do SCA que permita a um provedor de serviço, sediado nos Estados Unidos, recusar-se

[51] O termo *SCA-Warrant* foi muito utilizado pelo Estado, embora não exista previsão explícita no SCA, sendo objeto inclusive de contra-argumentação por parte da Microsoft e de fundamento à decisão da Corte de Apelação. Sendo assim, optou-se por preservar o termo cunhado pelo Estado, ao invés da sua tradução para o vernáculo escolhido para a escrita desta tese.

a cumprir mandado judicial de busca de dados armazenados em seus servidores, mesmo que localizados no exterior. O SCA confere ao magistrado autoridade para expedir ordem ou mandado de busca (*SCA-Warrant*) onde tenha jurisdição sobre a ofensa investigada, sendo a localização física do registro irrelevante.

4.4.3.2 Provedor de serviço norte-americano deve cumprir mandado de produção de informações, independentemente de onde os dados estejam armazenados

A empresa norte-americana provedora de serviço deve cumprir mandado de busca de informações que estejam sob o seu controle, independentemente da localização física dos dados. Registros eletrônicos e outros dados que estejam sob posse, custódia ou controle de empresa localizada nos Estados Unidos devem ser a este entregues, quando requisitados por força de mandado judicial, para subsidiar investigação criminal, independentemente de onde estejam fisicamente armazenados, pois a produção de registros é determinada pelo controle dos dados, não pela sua localização (UNITED STATES, 2014f, p.10).

4.4.3.3 O SCA-Warrant é diferente do mandado de busca convencional.

Segundo os Procuradores, a Quarta Emenda à Constituição dos Estados Unidos não se aplica a buscas em águas internacionais nem limita a capacidade do Estado em reunir evidências criminais em país estrangeiro.

A Microsoft sugere que as limitações relativas aos mandados convencionais (expedidos para busca e apreensão de evidências em instalações físicas), conforme estabelecido na Regra 41 (busca e apreensão) das Regras Federais de Procedimentos Criminais, também se apliquem ao *SCA-Warrant*. No entanto, há diferenças que variam desde a competência para expedi-los quanto a sua execução.

Tem competência para expedir um *SCA-Warrant* qualquer Tribunal que apresente jurisdição sobre a ofensa investigada (18 U.S.C § 2711 – (3)(A)(i)), independentemente de onde estejam fisicamente armazenados os dados, se dentro ou fora do distrito que o expediu. Ademais, não há obrigação de solicitar ao tribunal distrital onde se encontre sediado o provedor de serviço[52].

[52] Em 2001, o Congresso norte-americano alterou o SCA no sentido de eliminar a dependência da localização física do dado para a determinação de que Tribunal Distrital seria competente para expedir o mandado de busca baseado no SCA (*SCA-Warrant*). Essa alteração foi trazida pelo Ato Patriótico ou

Os mandados convencionais, por sua vez, obedecem às limitações impostas pela Regra 41 (busca e apreensão) das Regras Federais de Procedimentos Criminais. Destarte, são expedidos pelo tribunal do distrito onde se encontre a pessoa procurada ou a propriedade a ser vasculhada (UNITED STATES, 2014f, p.13). Quanto a execução, um mandado convencional é cumprido por agentes da lei, diferentemente do *SCA-Warrant* que, de acordo com o 18 U.S.C. § 2703 (g), não será exigida a presença de agente da lei para acompanhar a produção dos registros.

4.4.3.4. O SCA Warrant não tem natureza extraterritorial

O *SCA-Warrant* não tem a natureza de extraterritorialidade, pois não se refere à devassa de local físico fora do país, mas é dirigido a um provedor de serviço de comunicação, localizado em território norte-americano. Para os Procuradores, o *SCA-Warrant* não se destina a explorar local físico em busca de evidências físicas, nem tampouco é executado por um agente da lei. Funcionalmente, assemelha-se a uma *Administrative Subpoena* ou a outra requisição dirigida a um provedor de serviço, obrigando-o a produzir as informações requeridas, com base nos dados armazenados em seus servidores.

Assim, a Microsoft poderia determinar a seus técnicos que procedessem, remotamente (a partir dos Estados Unidos), a recuperação dos dados, utilizando-se de rotinas de *software* específicas, mesmo estando os dados armazenados no *data center* da empresa, na República da Irlanda.

4.4.3.5 A política da Microsoft impede a coleta de evidências criminais armazenadas no exterior

Segundo os Procuradores, a política de criação e manutenção de contas da Microsoft, que reflete diretamente na distribuição do conteúdo das comunicações dos usuários, baseada na mera declaração de residência do usuário, é contrária às mudanças incorporadas ao SCA, em 2001, que visaram proporcionar aos agentes da

---

Lei Patriótica dos Estados Unidos, em 2001 (*Uniting And Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism - USA Patriot Act* (UNITED STATES, 2001)*)*, nos termos do § 220(a)(2). Um dos objetivos dessa medida foi minimizar as demandas direcionadas aos Tribunais situados em *Eastern District of Virginia* e *Northern District of California*, onde se concentra a maior parte dos provedores de serviço do país (UNITED STATES, 2014f).

lei ferramentas eficazes e segurança jurídica para a condução de investigações criminais.

Os argumentos da Microsoft sugerem que a recuperação do conteúdo de *e-mail* dependa exclusivamente do Estado em cujo território o provedor de serviço de comunicação escolheu para armazenar o dado. Informações eletrônicas, como as requeridas no mandado, podem ser mantidas em qualquer local no mundo e movidas facilmente entre os diversos *data centers* da empresa, a qualquer tempo e por diversas razões.

É estratégia da empresa armazenar o conteúdo dos *e-mails* em *data center* situado próximo ao local onde o assinante declara residir.

Nessas circunstâncias, não seria surpresa se alguém, com intenção de cometer crime, deliberadamente elegesse outro país como moradia "virtual", de modo a armazenar o conteúdo de suas comunicações longe do alcance rápido dos agentes da lei norte-americanos, que serão obrigados a se utilizarem de instrumentos de cooperações jurídica internacional morosos e burocráticos, como o *Mutual Legal Assistance Treaties* (MLAT) ou a carta rogatória.

4.4.4 Argumentos da Microsoft em resposta aos Procuradores da *United States District Court for the Southern District of New York*

A resposta da Microsoft ao Memorando detalhado na seção anterior foi protocolada ao processo em 14 de março de 2014. De acordo com a empresa, o Estado insiste em obrigá-la a, indiretamente, executar o que o Estado não tem a autoridade de fazer diretamente, isto é, cumprir um *SCA-Warrant* fora dos limites territoriais do país (MICROSOFT CORPORATION, 2014a). Defende ainda a Microsoft que o SCA não instituiu um novo tipo de mandado, o *SCA-Warrant*, com funcionalidades equivalentes a *Administrative* S*ubpoena*.

Por fim, a Microsoft requereu ser desobrigada de produzir as informações solicitadas, pelos seguintes motivos:

a) Tribunal dos Estados Unidos não tem competência para expedir mandado extraterritorial;
b) o *SCA-Warrant* expedido tem natureza extraterritorial;
c) a cooperação internacional é o meio adequado para requisitar os dados.

4.4.4.1 Tribunal norte-americano não tem competência para expedir mandado extraterritorial.

A Microsoft não questiona se a Quarta Emenda à Constituição dos Estados Unidos proíbe o Governo de coletar evidências em solo estrangeiro sem a devida autorização, mas se o *SCA-Warrant,* expedido nesse caso, tem o poder de obrigá-la a prestar apoio em busca extraterritorial de evidências criminais. Além do mais, nenhuma lei norte-americana autoriza a expedição de mandado para ser executado fora do alcance da jurisdição nacional (MICROSOFT CORPORATION, 2014a).

4.4.4.2 O *Warrant* expedido tem natureza extraterritorial.

O instrumento expedido foi um *Warrant*, não uma *Administrative Subpoena* ou qualquer outra forma compulsória de obtenção de dados com base no SCA.

Em discordância com os argumentos dos Advogados, que sustentaram não ter o *SCA-Warrant* natureza extraterritorial, vez que foi dirigido à Corporação sediada nos Estados Unidos, a Microsoft apresentou precedente de julgamento (*United States* v. *Gorshkov*, 2001), indicando que a busca de dados eletrônicos deve ocorrer no local onde se encontram armazenados, não em local de onde seja possível acessá-lo, remotamente. Nesses termos, estando os dados na República da Irlanda, estaria caracterizada a extraterritorialidade do mandado.

Ademais, ao editar o SCA, o Congresso norte-americano não criou um novo tipo de mandado, o *SCA-Warrant*, cuja funcionalidade assemelha-se a uma *Administrative Subpoena* e com poderes para compelir empresa nacional a produzir ou recuperar informação armazenada no exterior.

4.4.4.3. A cooperação internacional é o meio adequado para requisitar os dados

De acordo com a Microsoft, o Estado não pode obrigá-la a violar o sigilo de dados armazenados fora do território dos Estados Unidos. Para obtê-los, o Governo deve observar o disposto no *Mutual Legal Assistance Treaty* (MLAT) vigente entre os dois países, que entrou em vigor em 11 de agosto de 2009. O Estado ignorou essa opção quando afirmou que tanto o MLAT quanto da carta rogatória são instrumentos morosos e burocráticos (MICROSOFT CORPORATION, 2014a).

4.4.5 Resposta do *Magistrate Judge* James C. Francis IV

Em resposta à defesa da Microsoft, o magistrado que expediu o *Warrant* ratificou a ordem e determinou a entrega imediata dos dados requisitados, por meio de *Memorandum and Order,* expedido em 25 de abril de 2014 (UNITED STATES, 2014d).

Nessa resposta, o magistrado fundamentou sua decisão no princípio da nacionalidade, segundo o qual é possível a aplicação extraterritorial das leis penais norte-americanas a empresas que estão sujeitas à jurisdição do país, no sentido de obrigá-las a produzirem evidências criminais, mesmo que a partir de dados armazenados em servidores de subsidiárias da empresa, em Estado estrangeiro. Ratificaram ainda a decisão do magistrado as alterações no SCA, trazidas pelo *Patriot Act* (PECORARO, 2017).

São os principais pressupostos defendidos pelo magistrado:

a) *o SCA-Warrant* não viola o princípio da extraterritorialidade*;*

b) a história legislativa do SCA ampara a ordem;

c) limitação territorial traz prejuízos à investigação criminal;

d) o SCA não presume a extraterritorialidade.

4.4.5.1 O SCA-Warrant não viola o princípio da extraterritorialidade.

O magistrado negou o pleito da Microsoft, fundamentando que o *SCA-Warrant* não violava o princípio da extraterritorialidade, uma vez que foi expedido contra empresa sediada em território norte-americano, para que fossem produzidas informações que se encontravam sob sua custódia, posse e controle, independentemente de onde estivessem armazenadas.

Apesar do SCA utilizar o termo *Warrant*, na prática não se trata de um mandado convencional, mas de uma ordem híbrida: parte *Search Warrant*, parte *Administrative subpoena.*

Como *Search Warrant*, é expedido por magistrado e exige do agente da lei demonstrar indícios de culpabilidade, confirmados por juramento ou declaração. Por outro lado, a sua execução dar-se-á de forma semelhante a uma A*dministrative Subpoena*, pois é cumprida diretamente pelo provedor de serviço que tem a posse, custódia e controle dos dados requeridos, dispensando a presença física de um

agente da lei nas instalações da empresa, para apreender o *hardware* ou executar ele mesmo o mandado, como ocorre na busca e apreensão de evidências físicas.

Essa estrutura ampara o entendimento do Estado no sentido de que mandado expedido nos termos do SCA (*SCA-Warrant*), não enseja aplicação do princípio da extraterritorialidade. Via de regra, tem sido entendimento usual que a *Administrative Subpoena* obrigue o recebedor a produzir informações sob sua custódia, posse ou controle, independentemente de onde estejam armazenadas.

4.4.5.2 A história legislativa do SCA ampara a ordem

A história legislativa do SCA oferece suporte à posição do magistrado.

Em 2001, o *Patriotic Act* (UNITED STATES, 2001) alterou o SCA para permitir que Tribunal, com jurisdição sobre uma investigação, tenha competência para expedir diretamente *SCA-Warrant*, sem a necessidade de solicitar ao Tribunal do Distrito onde se encontre sediado o provedor de serviço. Um dos objetivos dessa medida foi aliviar os Tribunais situados em *Eastern District of Virginia* e *Northern District of California*, onde se concentra a maior parte dos provedores de serviço (UNITED STATES, 2014d).

4.4.5.3 Limitação territorial traz prejuízos à investigação criminal

A imposição de limitações territoriais ao cumprimento de mandados expedidos nos termos do SCA pode trazer sérios prejuízos à investigação criminal.

Primeiramente, como o provedor de serviço não tem obrigação de validar a informação fornecida pelo assinante ou cliente, no momento em que uma conta é criada, alguém com a intenção de praticar ações criminosas poderá escolher como residência um país diferente dos Estados Unidos, ficando assim fora do alcance de um eventual *SCA-Warrant*.

Em segundo lugar, se um *SCA-Warrant* tiver o mesmo tratamento que um mandado de busca convencional, sua execução no exterior apenas poderá ser realizada mediante cooperação jurídica internacional, podendo inclusive o Estado requerido se negar a prestar assistência, a exemplo dos termos constantes nos

MLATs Estados Unidos e Canadá, Estados Unidos e Reino Unido, Estados Unidos e Brasil[53].

Por fim, podem ainda existir situações que envolvam países com os quais os Estados Unidos não celebraram acordo de assistência jurídica. E, excepcionalmente, pode haver casos em que o dado esteja armazenado em servidores localizados em território que não esteja sob jurisdição de qualquer país (território *nullius*). A Google, por exemplo, externou sua intenção de instalar servidores *offshore* no mar (em local sem jurisdição de qualquer nação), mesmo que o objetivo estivesse relacionado à busca por tecnologias de refrigeração dos equipamentos e energias alternativas[54].

4.4.5.4 O SCA não presume a extraterritorialidade

Os requisitos que contribuem para a presunção de extraterritorialidade não estão presentes no *SCA-Warrant*, pois (UNITED STATES, 2014d, p.21):

a) não criminaliza conduta que ocorre em outro país;
b) não envolve a participação de um agente da lei na sua execução;
c) não requer a presença física do técnico da empresa no local onde o dado se encontra fisicamente armazenado;
d) o provedor de serviço pode executar o mandado remotamente, a partir dos Estados Unidos.

Por fim, o magistrado contestou os argumentos da Microsoft quanto à extraterritorialidade, alegando que a jurisprudência referida pela empresa tratava de mandados expedidos sob o fundamento de outras leis, que não o SCA.

4.4.6 Resposta da *Chief Judge* ao recurso da Microsoft

Da decisão do *Magistrate Judge* James C. Francis IV, a Microsoft recorreu, em 06 de junho de 2014 (MICROSOFT CORPORATION, 2014b), à *Chief Judge of the*

[53] No MLAT firmado entre o Brasil e os Estados Unidos, promulgado por meio do Decreto nº 3.810, de 2 de maio de 2001, a Autoridade Central do Estado Requerido poderá negar assistência, nos termos do Artigo III. "Restrições à Assistência: 1. A Autoridade Central do Estado Requerido poderá negar assistência se: a) a solicitação referir-se a delito previsto na legislação militar, sem, contudo, constituir crime comum; b) o atendimento à solicitação prejudicar a segurança ou interesses essenciais semelhantes do Estado Requerido; ou c) a solicitação não for feita de conformidade com o Acordo."

[54] PALOU,Nacho. Google podría instalar sus servidores en alta mar para ahorrar energía. Microsiervos, Ed Economia, Ecologia, 15 set. 2008. Disponível em: <www.microsiervos.com/archivo/ecologia/google-instalar-servidores-alta-mar-ahorrar-energia.html>. Acesso em: 13 de dezembro de 2017.

U.S. District Court for the Southern District of New York, Loretta A. Preska, que, em 29 de agosto de 2014, ratificou a decisão original, exarada pelo magistrado, sob o argumento de que, implicitamente, o SCA autorizava a busca extraterritorial de evidências eletrônicas em processo criminal, devendo prevalecer o entendimento de que se trata de uma questão de controle de dados, e não de sua localização. Portanto, tendo a Microsoft o controle sobre os *e-mail*s do usuário, podendo inclusive acessá-los remotamente, somado ao fato de se tratar de uma investigação para apurar crime doméstico, seria injustificável a negação ao cumprimento da ordem judicial (UNITED STATES, 2014e).

Em 09 de julho de 2014, os Procuradores pela *United States District Court for the Southern District of New York* (UNITED STATES, 2014g) apresentaram apoio ao *Magistrate Judge* James C. Francis IV, ratificando os argumentos apresentados na subseção 4.4.3 e, ao final, opinando pelo indeferimento da moção apresentada pela Microsoft, em 06 de junho de 2014.

Em 08 de dezembro de 2014, a Microsoft apelou à *United States Court of Appeals for the Second Circuit* (UNITED STATES, 2014a), sendo deliberado pelo colegiado de Juízes, em 14 de julho de 2016 (UNITED STATES, 2016a), conforme será detalhado na próxima subseção. Para instruir o processo, em 09 de março de 2015, o *United States District Court for the Southern District of New York* apresentou resposta à apelação da Microsoft (UNITED STATES, 2015b), sendo a réplica da empresa apresentada em 08 de abril de 2015 (UNITED STATES, 2015a).

4.4.7 A decisão da *United States Court of Appeals for the Second Circuit*

A decisão da *United States Court of Appeals for the Second Circuit* foi proferida em 14 de julho de 2016, favorecendo o entendimento defendido pela Microsoft, no sentido de não ser obrigada a produzir informações, a partir de dados armazenados em território estrangeiro (UNITED STATES, 2016a). Participaram do julgamento três magistrados.

A decisão do órgão reconheceu a jurisdição territorial sobre os dados, baseado no critério da localização física dos mesmos, e não na localização do provedor de serviço (DASKAL, 2016b).

A análise da Corte de Apelação concentrou-se principalmente em verificar se o SCA autoriza o cumprimento de mandado judicial para a coleta de evidências

criminais eletrônicas, armazenadas em servidores localizados em território estrangeiro.

A Corte de Apelação entendeu que o ECPA não traz qualquer dispositivo que indique a intenção do Congresso em admitir a possibilidade de aplicação extraterritorial do SCA. Fundamentou a análise da Corte a decisão da Corte Suprema dos Estados Unidos, no caso *Morrison* v. *National Australia Bank* (UNITED STATES, 2010), onde ficou assentado que uma lei necessita dispor explicitamente acerca da possibilidade de aplicação extraterritorial, não se admitindo a sua presunção. Assim, uma lei aprovada pelo Congresso, a menos que disponha de forma contrária, aplicar-se-á tão somente no âmbito da jurisdição territorial dos Estados Unidos.

A Corte de Apelação reconheceu também a relevância do *Warrant* como instrumento por meio do qual o Estado exerce seu poder, nos termos da Quarta Emenda à Constituição dos Estados Unidos.

A história legislativa do SCA, relativamente às alterações ocorridas após sua promulgação em 1986, sustenta o entendimento dos magistrados de que o Congresso teve a intenção de estender ao termo *Warrant* do SCA as mesmas conotações relativas ao mandado convencional, inclusive a limitação de alcance apenas em nível doméstico.

Assim, quando o Congresso alterou o 18 U.S.C § 2703 para mitigar requisitos constantes na Regra 41 das Regras Federais de Procedimentos Criminais, relativamente ao *SCA-Warrant*, foi para permitir que magistrados expedissem mandados a serem executados dentro de outro distrito. Nenhuma alteração, porém, alude à possibilidade de transpor fronteiras internacionais.

Ademais, as discussões no Congresso não refletem qualquer expectativa de que o material a ser pesquisado e produzido esteja em local diferente de onde o provedor de serviço está localizado. Pressupõe-se, então, que o provedor de serviço Internet onde se encontra a conta do usuário está localizado nos Estados Unidos.

A Corte de Apelação rejeitou também o entendimento do Estado no sentido de que o *SCA-Warrant*, na prática, tratava-se de uma ordem híbrida, parte *Warrant*, parte A*dministrative Subpoena.* Os *Warrants* e as A*dministrative Subpoena* são instrumentos legais distintos. O 18 U.S.C § 2703 não usa os termos de forma intercambiável nem a palavra “híbrido”. Não há justificativa razoável para inferir que foi propósito do Congresso conferir ao termo *Warrant* o significado do termo

A*dministrative Subpoena*, ou substituir o mandado tradicional por um novo instrumento com alcance extraterritorial.

Por fim, concluem os magistrados, que o Estado, ao obrigar o provedor de serviço a auxiliá-lo na busca e apreensão de dados, este se investe das funções inerentes a um agente público e, como tal, deve observar o disposto na Quarta Emenda à Constituição dos Estados Unidos.

A decisão do *United States Court of Appeals for the Second Circuit* evidenciou que o direito à privacidade vigente no mundo físico também se aplica ao mundo digital. Então, se leis domésticas não alcançam evidências físicas que estejam em Estado estrangeiro, também não podem alcançar evidências eletrônicas armazenadas em servidores dispostos fora do território do país (BUTLER, 2017).

4.4.8 Contribuições dos *amicus curiae*

Várias instituições, profissionais e acadêmicos posicionaram-se em alinhamento com as argumentações apresentadas pela Microsoft. A *Verizon Communications Inc*. (UNITED STATES, 2014c) foi a primeira empresa que se apresentou como *amicus curiae* em apoio à Microsoft, por ocasião do recurso ao US *District Court for the Southern District of New York.* Outras empresas também se apresentaram, como *Electronic Frontier Foudation* (2014), *Brennan Center for Justice at NYU School of Law, American Civil Liberties Union* e *the Constitution Project (*BRENNAN CENTER FOR JUSTICE et al, 2014), At&t *Corporation*, Apple Inc. e Cisco System, Inc. (UNITED STATES, 2014b).

O Governo na República da Irlanda apresentou suporte à Microsoft, como *amicus curiae*, enfatizando a inadmissibilidade de tribunal estrangeiro desrespeitar a soberania irlandesa (ou de qualquer outro Estado soberano), independentemente de a Irlanda ser parte ou não do processo (IRELAND, 2014).

Outras instituições também prestaram apoio à Microsoft, tais como: BSA The *Software* Alliance; Center for Democracy and Technology; Chamber of Commerce of the United States; The National Association of Manufacturers; ACT|The APP Association; Anthony J. Colangelo, International Law Scholar; Rackspace US, Inc.; Computer & Communications Industry Association; I2 Coalition; Application Developers Alliance, Washington DC; Ireland; Amazon.com, Inc.; Accenture PLC; San Jose, CA; eBay Inc.; Hewlett-Packard Co.; Salesforce.com, Inc., San Francisco,

CA; Media Organizations, Washington, DC; Computer and Data Science Experts; Jan Philipp Albrecht, Member of the European Parliament (UNITED STATES, 2016a).

Na Suprema Corte, apresentaram apoio ao peticionante (Governo dos Estados Unidos), como *amici curiae*, os Estados de Vermont, Alabama, Arizona, Arkansas, Connecticut, Delaware, Hawaii, Idaho, Illinois, Indiana, Iowa, Kansas, Kentucky, Louisiana, Maine, Maryland, MassachuSetts, Michigan, Montana, Nebraska, New Hampshire, New Mexico, New York, North Carolina, Ohio, Oregon, Pennsylvania, South Carolina, South Dakota, Texas, Utah, Virginia, Wyoming e a Comunidade de Puerto Rico (UNITED STATES, 2017b).

4.5 A situação atual do processo

Em 16 de outubro de 2017, a Suprema Corte norte-americana decidiu conhecer o *writ of certiorari*, impetrado pelo Departamento de Justiça dos Estados Unidos, por meio de petição apresentada em 23 de junho de 2017, pleiteando a análise e deliberação sobre: se provedor de serviço de *e-mail*, localizado nos Estados Unidos, é obrigado a cumprir mandado (*Warrant*), expedido com base em causa provável, nos termos do 18 USC § 2703 do SCA, para violar sigilo de comunicações eletrônicas sob o controle do provedor, mesmo que esse provedor tenha decidido por armazenar os dados em território estrangeiro (UNITED STATES, 2017a).

Até 25 de dezembro de 2017, o processo encontrava-se pendente de julgamento. A deliberação a ser prolatada pela Corte Suprema dos Estados Unidos reveste-se da expectativa de referencial importante, na medida em que esse país contribui, abrigando grande concentração de provedores mundiais de computação em nuvem.

4.6 Contribuições à pesquisa

O estudo do caso *Microsoft Ireland* monstrou-se bastante relevante à pesquisa, pois constitui-se na referência que iniciou um amplo debate mundial em torno de tema, envolvendo inclusive o país onde se encontra sediada grande parte das empresas de tecnologia da informação que prestam serviços por meio da implementação da computação em nuvem, que são os Estados Unidos da América.

A relevância do caso é tamanha que chegou à Suprema Corte norte-americana o questionamento sobre a possibilidade de um provedor de serviço do país, que decidiu armazenar em território estrangeiro conteúdo de comunicações sobre as quais ainda mantém controle, é obrigado a cumprir mandado judicial, expedido nos termos do Título 18 do Código dos Estados Unidos (18 USC. 2703).

Além disso, até janeiro de 2018, 03 (três) projetos de lei foram apresentados ao Congresso norte-americano, no intuito de disciplinar, de alguma forma, o acesso ou a coleta extraterritorial a evidências criminais eletrônicas em nuvem computacional. Junte-se a esse conjunto a proposta de lei do Departamento de Justiça dos Estados Unidos, encaminhada ao Congresso, no final de 2017.

Optou-se por analisar diretamente os autos do processo, com a finalidade de identificar os principais argumentos que fundamentam as teses defendidas pelas partes no litígio.

Observa-se que os argumentos constantes nos autos foram desenvolvidos, predominantemente, em torno do amparo legal para legitimar ou coibir o cumprimento de medidas processuais penais (no caso, mandado de busca e apreensão de evidências criminais eletrônicas), em servidor de computação em nuvem de empresa norte-americana (a *Microsoft Corporation*), localizado em território estrangeiro (na República da Irlanda), considerando o fato da Microsoft possuir o controle sobre os dados requeridos. Trata-se de argumentos que são levados em conta por ocasião da proposta apresentada ao final desta Tese.

As empresas de tecnologia da informação e comunicação e a sociedade civil organizada sustentam que qualquer solicitação para recuperar dados armazenados em servidores localizados em solo estrangeiro deve ser encaminhada às autoridades daquele país, por meio de instrumento de cooperação judiciária internacional em matéria penal.

Por outro lado, as autoridades públicas entendem que, se a empresa provedora do serviço é norte-americana, mantém e controla os dados, independente de se encontrarem remotamente armazenados, devem atender a mandado judicial, mesmo que estejam em solo estrangeiro.

Outros casos semelhantes ocorreram em nível mundial, inclusive aqui no Brasil, como será referido adiante.

5 O ESPAÇO CIBERNÉTICO NO DIREITO INTERNACIONAL

Esta seção tem o objetivo de apresentar uma abordagem acerca do espaço cibernético no contexto do direito internacional, enfatizando os desafios trazidos pela computação em nuvem, como ambiente virtual que implementa o estado da arte da mobilidade dos dados eletrônicos, à persecução criminal, informada primordialmente pelo princípio da territorialidade.

Inicialmente, são tratados os elementos constitutivos do Estado, em razão de sua relevância à definição de critérios para estabelecer a competência jurisdicional estatal incidente sobre o espaço em comento.

Em seguida, é considerada a territorialidade do espaço cibernético, no tocante ao Direito Internacional, e suas repercussões diretas na atividade probatória de fato criminoso, com vestígios contidos em servidores de computação em nuvem, localizados em Estado estrangeiro.

5.1 Considerações iniciais sobre o Direito Internacional Público

O Direito Internacional Público é um conjunto de princípios e regras jurídicas costumeiras e convencionais que disciplinam e regem a atuação e a conduta da sociedade internacional (formada pelos Estados, pelas organizações internacionais intergovernamentais e também pelos indivíduos), visando alcançar as metas comuns da humanidade e, em última análise, a paz, a segurança e a estabilidade das relações internacionais (MAZZUOLI, 2015).

Trata-se de um sistema jurídico autônomo, regulador das relações entre Estados soberanos. Também conhecido como *direito das gentes*, no sentido de direito das nações ou dos povos, repousa sobre o consentimento, ou seja, os Estados não se subordinam senão ao direito que livremente reconhecem ou constituem (REZEK, 2014).

A aceitação e a obrigatoriedade do Direito Internacional Público perante a sociedade internacional são fundamentadas na norma *pacta sunt servanda*[55], segundo a qual todo tratado em vigor obriga as partes e deve ser cumprido por elas de boa fé.

Outras correntes existem e fundamentam o Direito Internacional Público sob enfoques diversos. Para a corrente voluntarista, por exemplo, a obrigatoriedade do Direito Internacional decorre sempre do consentimento (vontade) comum dos Estados. A corrente objetivista, por sua vez, apregoa que essa obrigatoriedade advem da existência de princípios e normas superiores aos do ordenamento jurídico estatal, uma vez que a sobrevivência da sociedade internacional depende de valores que devem ter prevalência sobre as vontades e os interesses domésticos dos Estados (RESEK, 2014).

5.2 Os elementos do Estado no Direito Internacional

O Estado, sob a perspectiva do Direito Internacional Público, é um ente jurídico, dotado de personalidade internacional, formado por uma comunidade humana, estabelecida de maneira permanente em um determinado território, sob a autoridade de um governo independente e com a finalidade precípua de zelar pelo bem comum daqueles que o habitam (MAZZUOLI, 2015).

A Convenção Panamericana sobre Direitos e Deveres dos Estados, assinada em Montevidéu a 26 de dezembro de 1933[56], acrescenta mais um requisito ao conceito, que é a capacidade de entrar em relações com os demais Estados.

Em resumo, são elementos constitutivos do Estado a comunidade de indivíduos, o território, o governo autônomo e independente, a finalidade e a capacidade de manter relações com os demais Estados.

A seguir, são apresentados suscintamente todos esses elementos, uma vez que a localização, preservação, acesso, coleta, produção, busca e apreensão extraterritorial de evidências criminais, em ambiente de computação em nuvem, implica necessariamente em lidar com a autoridade de vários Estados, considerando

[55] A norma *pacta sunt servanda* foi positivada no art. 26 da Convenção de Viena sobre o Direito dos Tratados, que foi promulgada no Brasil por meio do Decreto nº 7.030, de 14 de dezembro de 2009 (BRASIL, 2009).
[56] A Convenção foi promulgada pelo Brasil por meio do Decreto nº 1.570, de 13 de abril de 1937 (BRASIL, 1937).

que, tanto para requisitar qualquer medida de persecução criminal em território de Estado estrangeiro, quanto autorizá-las internamente, constituem expressões de soberanias estatais diversas.

5.2.1 A comunidade de indivíduos

A dimensão humana do Estado soberano é a comunidade nacional, formada pelos nacionais e estrangeiros residentes. Sobre os últimos, o Estado exerce sua jurisdição territorial; sobre os nacionais distantes, o Estado exerce jurisdição pessoal, fundada no vínculo de nacionalidade e independente do território onde se encontrem (REZEK, 2014).

5.2.2 O território

Trata-se do elemento material do conceito de Estado, que se consubstancia na fração delimitada do planeta em que este se assenta com sua população e demais elementos (MAZZUOLI, 2015). Compreende a superfície terrestre (solo e subsolo) com limites reconhecidos, as águas territoriais (fluviais, lacustres, marítimas) e o espaço aéreo correspondente (BITENCOURT, 2009).

Por força de uma ficção jurídica, alguns autores, como Bitencourt (2009), consideram território nacional – por extensão ou flutuante – as aeronaves e as embarcações. Em sentido contrário, Mazzuoli (2015, p. 489) defende que, “se um navio militar fosse realmente território de um Estado a que sua bandeira representa, as leis sanitárias e os regulamentos portuários não poderiam jamais ser-lhe aplicados”.

E o espaço cibernético, existe como pura virtualidade? Essa virtualidade é sinônimo de idealidade ou o virtual é concreto? O espaço virtual existe fora do espaço estatal ou precisa de um espaço físico, sobre o qual incida a soberania estatal? Não se pode olvidar que Estado e soberania, apesar da existência concreta imaginável, não deixam de ser abstração, virtualidade, dado que o ente Estado, a entidade soberania, são intangíveis, tão inapalpáveis quanto o espaço cibernético.

Sobre seu território, o Estado exerce todas as competências de ordem legislativa, administrativa e jurisdicional (jurisdição geral) e, nesse exercício, não enfrenta a concorrência de qualquer outra soberania (jurisdição exclusiva) (REZEK,

2014). Nos Estados nacionais modernos, a jurisdição é uma das expressões da soberania (CARNEIRO, 2005).

O Direito Internacional reconhece, em acepção própria, que a jurisdição é dividida em 03 (três) categorias: jurisdição prescritiva ou legislativa, jurisdição executiva e a jurisdição judicial ou adjudicatória (CURRIE, 2017; SVANTESSON, 2016a; WOODS, 2016; WESTMORELAND; KENT, 2015; KOOPS; GOODWIN, 2014; SCASSA; CURRIE, 2011; BROWNLEE, 2010).

A jurisdição prescritiva ou legislativa (*prescriptive or legislative jurisdiction*) refere-se à supremacia de um Estado para regular seus interesses, editando leis e normas vinculantes dentro de seu território, sem interferências externas.

A jurisdição executiva (*enforcement jurisdiction*), consistente no poder do Estado em fazer cumprir suas normas e as decisões proferidas por seus Tribunais, via de regra não pode ser exercida em território de Estado estrangeiro. O confisco de bens, a detenção de indivíduos e a coleta de evidências criminais, por exemplo, em razão do caráter invasivo, não podem ser exercidos por agentes de um Estado no território de outro Estado, a menos que este consinta, sob pena de constituir violação a normas internacionais (SVANTESSON, 2016a).

A jurisdição judicial ou adjudicatória (*judicial ou adjudicative jurisdiction)* refere-se aos poderes que possuem os Tribunais de um Estado para julgar processos que envolvam pessoas, bens, fatos ou eventos (SVANTESSON, 2016a). Refere-se à aplicação das leis de um Estado, por meio de decisões judiciais.

Via de regra, o Poder Legislativo do Estado exerce a jurisdição prescritiva ou legislativa, a Polícia Judiciária, durante a persecução criminal, exerce a jurisdição executiva, e a jurisdição adjudicativa ou judicial é exercida pelo Poder Judiciário, quando o magistrado ou o Tribunal prolata decisões (SCASSA; CURRIE, 2011).

Além da jurisdição legislativa, da jurisdição executiva, e da jurisdição adjudicatória, Svantesson (2016a) propõe que seja reconhecido, pela comunidade internacional, que o acesso extraterritorial a evidências eletrônicas, no curso de uma investigação criminal, seja entendido não como uma forma de jurisdição executiva, mas sim de “jurisdição investigativa”.

No contexto dos dados digitais, a jurisdição prescritiva está relacionada à capacidade de o Estado editar leis que estebeleçam as circunstâncias que autorizam o Governo acessar dados de usuários, armazenados em empresas privadas. O poder dos Tribunais para processar e julgar sob a égide dessas leis refere-se à jurisdição

adjudicativa. A jurisdição de execução diz respeito ao poder de aplicação dessas leis, mesmo que compulsoriamente, ou seja, executando mandados de busca ou prendendo criminosos (WESTMORELAND; KENT, 2015).

A natureza jurídica do espaço cibernético para o Direito Internacional, no contexto da apuração de fatos criminosos, será objeto de estudo na subseção 5.5, pela importância que representa à presente pesquisa.

5.2.3 Um governo autônomo e independente

O elemento político do conceito de Estado é o governo autônomo e independente, assim entendido aquele capaz de decidir de modo definitivo dentro de seu território, sem a intromissão de qualquer outra autoridade exterior, bem como de participar das relações internacionais e de conduzir as suas políticas interna e externa, sem a interferência de terceiros Estados (MAZZUOLI, 2015).

O conceito de Estado autônomo e independente induz à ideia de Estado soberano, sendo a soberania, hoje uma afirmação do Direito Internacional positivo, nos termos da Carta das Nações Unidas[57], da Declaração Relativa aos Princípios do Direito Internacional Referentes às Relações Amistosas e à Cooperação entre Estados, conforme a Carta das Nações Unidas[58], da Carta da Organização dos Estados Americanos[59].

A Carta das Nações Unidas traz, em seu art. 2º, §1º, que a organização "é baseada no princípio da igualdade de todos os seus Membros" (ONU, 1945).

A Declaração Relativa aos Princípios do Direito Internacional Referentes às Relações Amistosas e à Cooperação entre Estados, conforme a Carta das Nações Unidas, dispõe que todos os Estados soberanos são iguais perante a ordem jurídica internacional, independentemente das diferenças de seus sistemas políticos, econômicos e sociais ou de seus níveis de desenvolvimento (ONU, 1970).

A Carta da Organização dos Estados Americanos, em seu art. 3º, letra b), assenta que "a ordem internacional é constituída essencialmente pelo respeito à personalidade, soberania e independência dos Estados e pelo cumprimento fiel das

[57] Promulgada pelo Brasil por meio do Decreto nº 19.841, de 22 de outubro de 1945 (BRASIL, 1945).
[58] Livre tradução da autora para: *Declaration on Principles of International Law concerning Friendly Relations and Co-operation among States in accordance with the Charter of the United Nations*.
[59] Promulgada pelo Brasil por força do Decreto nº 30.544, de 14 de fevereiro de 1952 (BRASIL, 1952a).

obrigações emanadas dos tratados e de outras fontes do direito internacional" (OEA, 1948).

A soberania é referida nos documentos acima no contexto do princípio da igualdade soberana, resultando no entendimento de que a soberania moderna tem limites encontrados nas próprias normas internacionais gerenciadoras das atividades dos Estados, não mais se podendo falar em soberania absoluta. Por isso, segundo Mazzuoli, 2015, o terceiro elemento constitutivo do Estado não é a "soberania", mas o "governo autônomo e independente".

A igualdade soberana, inclusive, garante serem invioláveis a integridade territorial e a independência política de um Estado, mesmo quando a integridade territorial é infringida com a finalidade de autoproteção (ou *self-help*) ou em resposta a ações ou omissões de outro Estado (KOOPS; GOODWIN, 2014).

Acerca da autoproteção, a Corte Internacional de Justiça (CIJ/ICJ) decidiu, no caso *Corfu Channel*[60], em 1949, que a operação de varredura de minas no Estreito de Corfu, realizada pelo Reino Unido da Grã-Bretanha e Irlanda do Norte (Reino Unido) sob o argumento de autoproteção, constituiu uso ilegal da força contra a integridade territorial da Albânia, mesmo tendo responsabilizado a Albânia pelos danos causados a navios da Marinha Real Britânica, decorrentes da colisão com minas dispostas em águas albanesas.

[60] Em 22 de outubro de 1946, no Estreito de Corfu, 02 (dois) navios *destroyers* da Marinha Real Britânica sofreram avarias após colidirem com minas submarinas dispostas em águas albanesas, resultando inclusive em mortes e ferimentos em oficiais e marinheiros da equipagem. Diante do ocorrido, o Governo do Reino Unido enviou notificação à Albânia, expressando sua intenção de proceder a retirada de minas no Estreito de Corfu. Em resposta, o governo albanez expressou consentimento para as operações realizadas tão somente fora das águas territoriais do país. No entanto, nos dias 12 e 13 de novembro de 1946, a Marinha Real Britânica retirou 22 (vinte e duas) minas em águas territoriais albanesas e dentro do referido canal, não obstante formal oposição da Albânia. O Reino Unido apresentou o caso ao Conselho de Segurança das Nações Unidas, que, mediante Resolução expedida em 9 de abril de 1947, recomendou que os dois governos submetessem a controvérsia à Corte Internacional de Justiça. Em 25 de março de 1948, após a admissibilidade da Corte, as partes apresentaram um acordo do compromisso, solicitando a apreciação de duas questões: a) a Albania seria responsável pelas explosões e, por isso, teria a obrigação de indenizar o Reino Unido? b) o Reino Unido violou leis internacionais ao, primeiramente, realizar manobras em águas albanesas, em 22 de outubro de 1946, quando ocorreram as explosões, e, em seguida, nos dias 12 e 13 de novembro de 1946, quando procederam a retirada de minas do Estreito de Corbu, em águas albanesas, sem o consentimento deste? Quanto a primeira questão, a Corte decidiu (11 votos contra 05) que a Albânia seria responsável pelos danos causados à Marinha Real Britânica. Quanto a segunda questão, a Corte decidiu (14 votos contra 02) que o Reino Unido não violou a soberania da Albânia enquanto navegava pelo Estreito de Corfu, no dia 22 de outubro de 1946. Finalmente, por unanimidade, a Corte declarou que as ações de varredura realizadas pela Marinha Real Britânica no Canal de Corfu, nos dias 12 e 13 de novembro de 1946, violara a soberania da Albânia (RANGEL, 1976; INTERNATIONAL COURT OF JUSTICE, 1949).

Aliás, o respeito à igualdade soberana e a não interferência externa a um Estado autônomo e independente é requisito à garantia da paz mundial, sendo essa uma das funções do Direito Internacional (KOOPS; GOODWIN, 2014).

5.2.4 A finalidade e a capacidade de manter relações com outros Estados

Esse elemento constitutivo do conceito traduz a ideia de que o Estado deve sempre perseguir uma finalidade, direcionada a buscar o bem comum de cada um dos indivíduos que o compõe (MAZZUOLI, 2015).

Um governo autônomo e independente garante a capacidade de um Estado para manter relações internacionais com outros Estados, nos termos do art. 1º da Convenção Panamericana sobre Direitos e Deveres dos Estados, assinada em Montevidéu a 26 de dezembro de 1933[61].

5.3 A Aplicação da lei processual penal no espaço: o exemplo do Brasil

Estão aqui apresentados os princípios relativos à aplicação das normas de direito processual penal no espaço, tomando por base o ordenamento jurídico brasileiro. Eventualmente, normas de direito internacional são referidas.

Tradicionalmente, as leis processuais penais no Brasil são informadas pelo princípio da territorialidade absoluta. Logo, têm aplicação a todos os processos em trâmite no território nacional - *locus regit actum*[62] (TÁVORA; ALENCAR, 2009). Sendo o Processo Penal o meio de que se valem os órgãos jurisdicionais penais para a solução das lides penais, e seus órgãos jurisdicionais representam parcela do poder soberano de um Estado, não pode este exercer seu poder soberano além da sua própria soberania. Por essa mesma razão, fica excluída a possibilidade de ser

[61] De acordo com o artigo 1º da Convenção, o Estado como pessoa de Direito Internacional deve reunir os seguintes requisitos: I. População permanente; II. Território determinado; III. Governo; IV. Capacidade de entrar em relações com os demais Estados.
[62] Livre tradução da autora a partir do latim: “a lei do lugar é que rege os atos”.

aplicada a lei processual penal de um outro país em território nacional (TOURINHO FILHO, 2012).

Mesmo que atos processuais precisem ser executados no exterior, como ouvida de testemunha, busca e apreensão, intimação, citação etc, aplicável será a lei penal do país onde tais atos são realizados. É o domínio da *lex fori*[63].

Na mesma linha, o cumprimento, no Brasil, de atos processuais referentes às relações jurisdicionais com autoridades estrangeiras, deve observar as leis pátrias.

Nesse sentido, o Código Penal Militar brasileiro (BRASIL, 1969), cominando pena gravíssima, criminalizou, nos arts. 138 e 139, as condutas de "praticar o militar, indevidamente, no território nacional, ato de jurisdição de país estrangeiro, ou favorecer a prática de ato dessa natureza" e "violar o militar território estrangeiro, com o fim de praticar ato de jurisdição em nome do Brasil", respectivamente.

A regra de territorialidade é oriunda do Direito Internacional Privado que, para a forma dos atos e negócios jurídicos, estabeleceu o referido princípio, que foi transplantado para o Direito Processual, notadamente o Civil, resultando que *ordo judicii regitur legibus loci, ubi causa agitur*[64] (TOURINHO FILHO, 2012).

Não obstante, a lei processual penal de um Estado pode ter aplicação extraterritorial (LIMA, 2011), quando:

a) se tratar de território *nullius*[65], que se encontra detalhado na subseção 5.4;

b) houver autorização do Estado onde deva ser praticado o ato processual;

c) houver guerra, em território ocupado.

No Brasil, excepcionalmente, a lei autoriza a incidência de outros diplomas normativos, como os tratados, as convenções e as regras do direito internacional, nos termos do art. 1º, inc. I, do Código de Processo Penal Brasileiro[66].

O referido inciso é peculiar porque trata de uma hipótese de exclusão da jurisdição pátria, em atenção aos tratados e às regras de Direito Internacional, dando prevalência a própria ordem internacional, onde infrações aqui ocorridas não serão julgadas em território nacional, como ocorre com a imunidade diplomática, positivada

[63] Livre tradução da autora a partir do latim: "Lei do foro".
[64] Livre tradução da autora a partir do latim: "O processo é regido pelas leis do lugar onde a causa deve ser julgada".
[65] Livre tradução da autora a partir do latim: "Nulo".
[66] Art. 1º Código Processo Penal: O processo penal reger-se-á, em todo o território brasileiro, por este Código, ressalvados: I - os tratados, as convenções e regras de direito internacional;

no artigo 31 Convenção de Viena de 1961[67], promulgada no Brasil por meio do Decreto nº 56.435, de 8 de junho de 1965 (BRASIL, 1965), e com os crimes cometidos a bordo de navios ou aeronaves privadas estrangeiras, em trânsito pelo Brasil.

Assim, Chefes de Governo estrangeiro ou de Estado estrangeiro, suas famílias e membros de comitivas, embaixadores e suas famílias, funcionários estrangeiros de corpos diplomáticos e suas famílias, funcionários de organizações internacionais em serviço (Organização das Nações Unidas, Organização dos Estados Americanos) gozam de imunidade diplomática, que consiste na prerrogativa de responder no seu país de origem por delito praticado no Brasil.

Quanto ao cônsul, este goza de imunidade em relação aos crimes funcionais, nos termos do art. 41[68] da Convenção de Viena sobre Relações Consulares de 1963, promulgada pelo Brasil por meio do Decreto nº 61.078, de 26 de julho de 1967 (BRASIL, 1967).

As sedes das embaixadas ou legações são consideradas territórios do país onde se acham situadas, tanto que os crimes aí praticados por pessoas alheias às imunidades sujeitam-se à jurisdição do Estado onde se encontra a embaixada. Apesar disso, como consequência da inviolabilidade e imunidade concedidas aos agentes diplomáticos, considera-se também inviolável a sede das embaixadas.

Ademais, dispõe o art. 369 do Código de Processo Penal que as citações que houverem de ser feitas em legações estrangeiras serão efetuadas mediante carta rogatória. Entende Tourinho Filho (2012) que assim procedeu o legislador pátrio não porque o Brasil entenda que as sedes das embaixadas sejam território estrangeiro, mas tão somente por cortesia.

---

[67] Artigo 31. 1. O agente diplomático gozará de imunidade de jurisdição penal do Estado acreditado.[...]; 4. A imunidade de jurisdição de um agente diplomático no Estado acreditado não o isenta da jurisdição do Estado acreditante.

[68] Artigo 41 - Inviolabilidade pessoal dos funcionários consulares. 1. Os funcionários consulares não poderão ser detidos ou presos preventivamente, exceto em caso de crime grave e em decorrência de decisão de autoridade judiciária competente. 2. Exceto no caso previsto no parágrafo 1 do presente artigo, os funcionários consulares não podem ser presos nem submetidos a qualquer outra forma de limitação de sua liberdade pessoal, senão em decorrência de sentença judiciária definitiva. 3. Quando se instaurar processo penal contra um funcionário consular, êste será obrigado a comparecer perante as autoridades competentes. Todavia, as diligências serão conduzidas com as deferências devidas à sua posição oficial e, exceto no caso previsto no parágrafo 1 dêste artigo, de maneira a que perturbe o menos possível o exercício das funções consulares. Quando, nas circunstâncias previstas no parágrafo 1 deste artigo, for necessário decretar a prisão preventiva de um funcionário consular, o processo correspondente deverá iniciar-se sem a menor demora.

Quanto aos crimes cometidos a bordo de navios ou aeronaves privadas estrangeiras, em águas territoriais e espaço aéreo brasileiros, não se aplicam a lei penal nem a lei processual penal pátrias, salvo se a infração for praticada por ou contra brasileiro, ou se afetar ou ameaçar a ordem pública nacional.

5.4 Os territórios *nullius*

O território *nullius* designa os espaços cuja utilização suscita o interesse de mais de um Estado soberano – às vezes de toda comunidade internacional - ainda quando sujeitos à incidência de determinada soberania. Cuida-se do mar, dos rios internacionais, do espaço aéreo, do espaço extra-atmosférico e do continente antártico (RESEK, 2014). São considerados também patrimônio comum da humanidade (KOOPS; GOODWIN, 2014).

O direito do mar é parte elementar do direito internacional público, e suas normas, durante muito tempo, foram unicamente costumeiras. Atualmente, a Convenção das Nações Unidas sobre o Direito do Mar, instituída em Montego Bay/Jamaica, em 10 de dezembro de 1982, traz 320 (trezentos e vinte) artigos e diversos anexos. Em interpretação analógica ao direito de perseguição, constante na referida Convenção, Vargas-Leon (2016) entendeu que a nenhum Estado é permitido acessar diretamente evidências criminais eletrônicas, armazenadas em território estrangeiro.

O rio internacional é todo curso d´água que banha mais de um Estado soberano. São exemplos o rio Amazonas, o rio Reno, o rio Danúbio. O interesse pelos rios internacionais está relacionado ao valor econômico da navegação, a produção de energia elétrica, a irrigação, o proveito industrial (RESEK, 2014). Regimes jurídicos são estabelecidos por meio de tratados multilaterais ou unilaterais, como o Tratado de Cooperação da Amazônia, que reúne Bolívia, Brasil, Colômbia, Equador, Guiana, Peru, Suriname e Venezuela.

O espaço aéreo e o espaço extra-atmosférico apresentam regimes jurídicos distintos. O regime jurídico relativo ao espaço aéreo é determinado em função de qual seja a superfície terrestre ou hídrica subjacente, enquanto o do espaço extra-atmosférico é uniforme e apresenta semelhança com o alto-mar.

Sobre os ares situados acima de seu território, o Estado exerce soberania plena, projetando-se o mesmo regime jurídico da superfície subjacente. Mas é livre a

navegação aérea, civil ou militar, sobre os espaços onde não incide qualquer soberania estatal, como o alto-mar (incluindo o polo norte) e o continente antártico.

Referenciam o direito à navegação aérea as Convenções de Chicago de 1944, formada por 03 (três) convenções principais e vários textos ancilares.

O direito relativo ao espaço extra-atmosférico começou a ser forjado entre dois acontecimentos histórico: a colocação em órbita do primeiro satélite artificial – o *Sputnik* – pela União Soviética, em 4 de outubro de 1957, e o primeiro pouso de nave terrestre tripulada na Lua, por astronautas norte-americanos, em 20 de julho de 1969.

O Tratado sobre Princípios Reguladores das Atividades dos Estados na Exploração e Uso do Espaço Cósmico, Inclusive a Lua e Demais Corpos Celestes, foi aberto à assinatura em Londres, Moscou e Washington, a 27 de janeiro de 1967, sendo promulgado no Brasil, através do Decreto nº 64.362, de 17 de abril de 1969 (BRASIL, 1969a).

Diz o acordo internacional que a exploração e uso do espaço cósmico deve ter em mira o interesse de todos os países, além do que pode ser explorado e utilizado livremente por todos os estados, sem qualquer discriminação em condições de igualdade e em conformidade com o direito internacional, com liberdade de acesso a todas as regiões dos corpos celestes (art. 1º).

O espaço cósmico, inclusive a Lua e demais corpos celestes, não pode ser objeto de apropriação nacional por proclamação de soberania, por uso ou ocupação, nem por qualquer outro meio (art. 2º).

E finalmente, a Antártica é uma ilha que domina todo o círculo pólar antártico, sendo coberta de gelo em quase toda a sua extensão. O interesse econômico e estratégico motivou alguns Estados a pretendê-la, com base em teorias diversas. A Argentina, por exemplo, aventou, como fundamento da sua pretensão, a teoria da *continuidade da massa geológica*; países europeus de tradição navegatória reivindicaram a teoria da *descoberta*; os Estados Unidos preferiram prestigiar a teoria da atividade de *controle do litoral antártico*, embora não formulasse nenhuma reivindicação concreta nem reconhecesse reivindicação alheia; pela teoria dos setores, se aplicada à Antártica, haveria de dividir o continente em diversas fatias triangulares resultantes da projeção não apenas de litorais próximos (como Chile, África do Sul ou Austrália), mas também alguns situados mais distante, como México, Paquistão ou até mesmo a Islândia (RESEK, 2014).

O Tratado da Antártica, firmado em Washington no ano de 1959 e promulgado pelo Brasil por meio do Decreto nº 75.963, de 11 de julho de 1975 (BRASIL, 1975), tem por objetivo assegurar que a Antártida seja usada para fins pacíficos, para cooperação internacional na pesquisa científica, e não se torne cenário ou objeto de discórdia internacional. São proibidas, no entanto, quaisquer medidas de natureza militar, tais como o estabelecimento de bases e fortificações, a realização de manobras militares, assim como as experiências com quaisquer tipos de armas.

Analogamente, se o espaço sideral, os mares e rios internacionais, as terras de ninguém têm suas convenções regulatórias dos interesses sociais, políticos, ecinômicos, científicos, é difícil compreender que o espaço cibernético ainda não haja sido regulado pelo *jus gentium*. Ele é de interesse comum à humanidade, não se submete ao senhorio de qualquer Estado, não pode ser apropriado por qualquer deles, mas todos têm o direito ou o interesse indeclinável de acessá-lo, ninguém pode ser excluído dele, porque se o fosse, estaria alijado das intercomunicações e do progresso.

O espaço cibernético não tem dono, mas é de todos; não pode submeter-se ao domínio de uma soberania, porque transcende dela, nem existiria uma bastante ampla para contê-lo; não pode, também, excluir qualquer uma delas.

5.5 Um enfoque territorial sobre o espaço cibernético no Direito Internacional

O conceito de território no Direito Internacional é repleto de significados. Em particular, quando se trata de espaço cibernético as discussões são travadas no sentido de entendê-lo como “espaço” ou como “lugar”. Embora esses termos sejam utilizados literalmente como referência a alguma área física, o termo “espaço” tende a incorporar a abstração de um ambiente com propósitos definidos.

Doutrinariamente, costuma-se dividir as concepções acerca do espaço cibernético em duas Escolas.

Primeiro, a Escola dos excepcionalistas, que consideram o espaço cibernético apartado do mundo real, com características próprias e, por isso, justificaria novos princípios e o tratamento jurídico diferenciado. Em sentido contrário, a Escola dos não-excepcionalistas consideram-no tão real quanto o mundo físico, vez que é concebido pela conexão entre vários dispositivos físicos, além de ser utilizado por indivíduos de um mundo real (KOOPS; GOODWIN, 2014).

A história do espaço cibernético como um lugar passível de ser legalmente protegido tem uma de suas primeiras referências no início dos anos 90, com os "*cyberlibertarians*"[69], que propugnavam ser o espaço cibernético um ambiente apartado do mundo físico e, por isso, deveria usufruir de independência em relação às soberanias do mundo real. Assim, em retórica intencionalmente exagerada, na Declaração de Independência do Ciberespaço[70], Barlow afirmou:

> *Governments of the Industrial World, you weary giants of flesh and steel, I come from Cyberspace, the new home of Mind. On behalf of the future, I ask you of the past to leave us alone. You are not welcome among us.* [...].[71]

Antes mesmo dessa assertiva, modelos de regulamentação para a Internet já haviam sido propostos.

Em 1994, Hardy (1994) sugeriu que as transações *on-line* fossem reguladas aos moldes da *Lex Mercatoria*, privilegiando os termos contratuais pactuados entre as partes, ao invés de submetê-las a normas ditadas por uma autoridade central. A *Lex Mercatoria* teve sua origem no continente europeu durante a Idade Média e chamava atenção por seu caráter transnacional e pela fidelidade aos usos e costumes mercantis, que eram aplicados pelos próprios mercadores ou pelas corporações de ofício, em processo célere e informal (VIDIGAL, 2010).

Em 1995, Post (1995) afirmou ser a Internet *multi-jurisdictional* - vez que dados originados num determinado Estado poderiam transitar por diversas jurisdições intermediárias, onde houvesse servidores conectados à rede, antes de chegarem ao destino final - e quase *a-jurisdictional*, pois as fronteiras físicas de um país seriam irrelevantes ao ambiente da rede mundial de computadores, sendo essa autonomia resultante da natureza eletrônica das mensagens e da topologia descentralizada da Internet. Como a Internet é considerada a rede das redes de computadores, os problemas que lhe ocorressem deveriam ser resolvidos com a mínima interferência na liberdade dos indivíduos em escolher sob que regras desejariam estar submetidos enquanto utilizam o ambiente.

---

[69] *Cyberlibertarian*: "*A person who opposes government regulation of the Internet*" (de acordo com o *English Oxford Living Dictionaries*. Powered by Oxford University Press. 2017. Disponível em: <https://en.oxforddictionaries.com>. Acesso em: 25 mai. 2017).

[70] BARLOW, John Perry. A Declaration of the Independence of Cyberspace. Davos, Suíça, 8 fev.,1996. Disponível em: <https://www.eff.org/cyberspace-independence>. Acesso em: 20 mai. 2017.

[71] Livre tradução da autora: "Governos do Mundo Industrial, vocês gigantes aborrecidos de carne e aço, eu venho do espaço cibernético, o novo lar da Mente. Em nome do futuro, eu peço a vocês do passado que nos deixem em paz. Vocês não são benvindos entre nós."

Sob o argumento metafórico de que o espaço cibernético era um “espaço” e, por isso, deveria ser regulado independentemente das fronteiras físicas e geográficas das jurisdições estatais, resultou, entre os anos de 1996 e 1997, em forte tendência de estudiosos em entendê-lo como um ambiente autônomo. E nesse contexto, alguns autores defendiam, enquanto outros condenavam, o modelo de autorregulamentação.

Em 1996, Johnson e Post (1996) patrocinaram o movimento de autorregulamentação do espaço cibernético, sob o argumento de que a Internet desafiava o poder dos Estados para regular o comportamento *on-line*, bem como a sua legitimidade para fazê-lo num ambiente globalizado, pois não haveria forma clara que vinculasse uma transação eletrônica a uma determinada jurisdição estatal. Sendo assim, concluíram que o espaço cibernético deveria ser deixado para desenvolver suas próprias estruturas regulatórias, o que obrigaria os Estados soberanos, em algumas circunstâncias, a se submeterem a esse novo ambiente legal.

Em oposição à Johnson e Post (1996), Lessig (1996) contestava essa soberania do espaço cibernético em relação ao mundo real, sugerindo, por sua vez, que a regulamentação do ambiente fosse realizada por meio de codificações escritas na forma de *Software*, que definiriam os termos de acesso e utilização dos ativos do sistema. Nesse modelo, a lei estaria escrita sob a forma de código-fonte.

A partir de 1998, novas teorias surgiram em discordância à autorregulamentação.

Nesse sentido e sob o argumento de que as transações no espaço cibernético eram funcionalmente idênticas às processadas no mundo real, Goldsmith (1999, p. 37) concluiu que,

> There is no general normative argument that supports the immunization of cyberspace activities from territorial regulation. And there is every reason to believe that nations can exercise territorial authority to achieve significant regulatory control over cyberspace transactions. Resolution of the choice-of-law problems presented by cyberspace transactions will be challenging, but no more challenging than similar problems raised in other transnational contexts.[72]

[72] Livre tradução da autora: “Não há um argumento normativo geral que ampare a imunidade das atividades do ciberespaço da regulamentação territorial. E há razão para acreditar que as nações podem exercer autoridade territorial para garantir um controle regulatório sobre as transações do ciberespaço. A solução do problema de escolha de lei a ser aplicada às transações no ciberespaço será desafiadora, mas não mais provocadora do que problemas semelhantes levantados em outros contextos transnacionais.”

Ainda em contraposição aos *cyberlibertarians*, Netanel (2000) afirmou ser o espaço cibernético anárquico e contrário aos princípios democráticos liberais, vez que favoreceria à prevalência de maiorias, à inviolabilidade do ambiente, a invasões sistemáticas de privacidade, à desigualdade na distribuição de requisitos para o exercício da cidadania. Para garantir a proteção e a promoção de ideais liberais, seria desejável a regulação seletiva pelo Estado liberal.

A essa altura é relevante ressaltar que, tanto para os excepcionalistas quanto para os não-excepcionalistas, a metáfora do "espaço cibernético como lugar" não foi objeto de discussão, pois, implicitamente, assim as Escolas o consideravam.

No entanto, em contraposição a esse entendimento, Andrew Shapiro e Timothy Wu apresentaram novos argumentos. Para Shapiro, o espaço cibernético não era um espaço real, mas um meio passível de ser controlado. Para Wu, a Internet não se desenvolve em outro mundo, mas se trata de uma rede de computadores que suporta a execução de várias aplicações do mundo real (apud HUNTER, 2003).

As discussões sobre a metáfora do espaço cibernético como "espaço" ou como "lugar", aliadas à dicotomia conceitual apresentada pelas Escolas excepcionalista e não-excepcionalista, trazem consequências diretas à regulamentação da Internet e à persecução criminal.

Aos Estados, parece prevalecer a visão não-excepcionalista (KOOPS; GOODWIN, 2014), como se observa no exercício da jurisdição prescritiva, por meio da qual os Estados legislam acerca da parte da Internet que consideram sob sua esfera de poder, fundamentados na localização física dos dispositivos informáticos ou dos equipamentos de comunicação e processamento de dados. E são vários os exemplos de territorialização dos dados. Dentro dessa concepção, o Brasil, ao sancionar o Marco Civil da Internet (BRASIL, 2014), dispôs que qualquer operação de coleta, armazenamento, guarda e tratamento de registros, de dados pessoais ou de comunicações por provedores de conexão e de aplicações de Internet em que pelo menos um desses atos ocorra em território nacional, deverão ser obrigatoriamente respeitados a legislação brasileira e os direitos à privacidade, à proteção dos dados pessoais e ao sigilo das comunicações privadas e dos registros (art. 11). A Federação Russa, igualmente, aprovou, em 2013, legislação de proteção de dados que pressupõem a exigência de territorialização dos dados pessoais dos cidadãos russos (MEDVEDEV, 2016).

A visão não-excepcionalista do espaço cibernético também prevalece na expedição de mandados judiciais, que respaldam os procedimentos investigatórios alusivos à persecução criminal, e em decisões judiciais. Dentre as questões discutidas no caso *Microsoft Ireland,* por exemplo, está a legalidade do alcance extraterritorial de um mandado judicial para produção de evidências criminais, cujas particularidades estão apresentadas na seção 4.

No Brasil, merecem destaque duas decisões proferidas no âmbito do Superior Tribunal de Justiça e do Tribunal Regional Federal da 4ª Região.

No Superior Tribunal de Justiça, a Ministra relatora do curso do Inquérito nº 784/DF defrontou-se com a negativa da empresa Google Brasil Internet LTDA em cumprir ordem judicial, no sentido de quebrar o sigilo das comunicações pessoais de indivíduo brasileiro, suspeito de ter cometido crime grave em território brasileiro e sem qualquer conexão com Estado estrangeiro, sob o argumento de que os dados em questão estariam armazenados em solo norte-americano e, por isso, sujeitos à legislação daquele país, indicando a via diplomática (Acordo de Assistência Judiciária em Matéria Penal entre o Governo da República Federativa do Brasil e o Governo dos Estados Unidos da América - Decreto nº 3.810, de 02.05.2001) para a obtenção dessas informações. Em questão de ordem suscitada, a relatora posicionou-se, e foi seguida pela maioria dos Ministros da Corte Especial, no sentido de obrigar a empresa a cumprir a ordem emanada de autoridade pátria, sob o fundamento de que,

> [...] é irrecusável que o fato de esses dados estarem armazenados em qualquer outra parte do mundo não os transformam em material de prova estrangeiro, a ensejar a necessidade da utilização de canais diplomáticos para transferência desses dados. Trata-se, evidentemente, de elemento de prova produzido, transmitido e recebido em território brasileiro, repito. Nada tem a ver com terras alienígenas, a não ser pelo fato de, por questões estratégico-empresariais, estarem armazenadas nos Estados Unidos (STJ, 2013).

Outra decisão que merece destaque foi a proferida em voto, no mandado de segurança[73] impetrado pela empresa Google Brasil Internet LTDA, contra ato do Juízo da 2ª Vara Federal Criminal de Curitiba/PR, no sentido de obrigar o impetrante a fornecer conteúdo de mensagens eletrônicas enviadas e recebidas por uma conta de usuário aberta no serviço Gmail.

[73] MS n° 2009.04.00.011335-1/PR, da C. 7ª Turma do TRF-4ª Região (STJ, 2013).

Foi alegado pelo impetrante a impossibilidade de cumprir a ordem, posto que o conteúdo das mensagens se encontrava em servidores localizados nos Estados Unidos, onde há legislação de proteção ao sigilo das comunicações, pelo que seu fornecimento poderia ser considerado crime naquele país. Explicou que a solicitação das mensagens deveria ocorrer conforme o procedimento previsto no Acordo de Assistência Judiciária em Matéria Penal, mantido entre os dois países e citado acima. A relatora, Juíza Federal Salise Monteiro, julgou improcedente, ressaltando que,

> [O] dever legal de prestar informações recai sobre a empresa sediada em território nacional, devendo esta tomar as medidas necessárias para o cumprimento da ordem emanada da autoridade judiciária brasileira – fornecimento de dados relativos à quebra de *e-mail* (Gmail) –, sendo descabida a invocação de leis americanas para se esquivar de atendimento à requisição judicial, quando o fato investigado foi praticado por brasileiro em território nacional. (BRASIL, 2013).

Tanto as determinações do Poder Judiciário quanto a negativa da empresa em atendê-las, reforçam a visão do espaço cibernético como “lugar” ou território, em detrimento da ideia de espaço, associada a um ambiente virtual desprovido de fronteiras físicas limitantes da livre circulação de dados digitais.

5.6 O princípio da territorialidade e a coleta de evidências criminais eletrônicas

A natureza dos dados digitais vem provocando incertezas no cumprimento ao princípio da territorialidade. Enquanto a aplicação desse princípio depende da definição de onde a evidência encontra-se fisicamente disposta, os dados estão em toda parte e em qualquer lugar. Portanto, como os desafios trazidos pelos dados são complexos, as soluções também são.

Tradicionalmente, duas premissas orientam o princípio da territorialidade, por ocasião da localização, preservação, produção, acesso, busca e apreensão de evidências criminais. Primeiro, as evidências físicas têm uma localização identificável e estável, dentro ou fora do território. Segundo, a localização é relevante e determinará a jurisdição competente para processar o pedido de busca e apreensão de evidências.

As evidências lógicas também enfrentam essas premissas. No entanto, por diversas razões, comportam-se diferentemente das evidências físicas.

Primeiramente, a velocidade, a facilidade e a imprevisibilidade com que os dados fluem por meio das fronteiras nacionais, bem como a divisibilidade, fazem da sua localização incerta e instável (DASKAL, 2015; BECHTEL, 2013), impossibilitando precisar onde se encontram. A esse fenômeno, os estudiosos do Conselho da Europa denominam de "*loss of location*" (COUNCIL OF EUROPE, 2010; CYBERCRIME CONVENTION COMMITTEE, 2016b). Ademais, a distância entre a localização do dado e o seu proprietário, que, em geral, desconhece onde aqueles estão armazenados, prejudica o significado normativo da localização do dado (DASKAL, 2015).

É característica da computação em nuvem o gerenciamento dos recursos, de modo a garantir alta performance e alta disposibilidade das transações eletrônicas. Como estratégia de processamento, de armazenamento, de segurança, de resiliência, os dados são divididos, particionados e copiados para mais de um servidor físico, que podem estar espalhados por diversas jurisdições, inclusive em localidades bem distantes do usuário.

O controle e o gerenciamento das partes da evidência digital são realizados pelo provedor do serviço de computação em nuvem. De acordo com a política da *Microsoft Corporation*, por exemplo, os dados pessoais dos usuários são armazenados em *data center* nos Estados Unidos e o conteúdo das comunicações, em *data center* próximo ao local onde o usuário indicou como sua residência (UNITED STATES, 2014f). Cópias de segurança podem estar num terceiro *data center*. Por sua vez, quando a evidência criminal é física (uma arma de fogo, por exemplo) mesmo que fracionada, todas as partes permanecem sob o controle direto do proprietário.

Em segundo lugar, o acesso independe da localização do dado. Diferentemente da evidência física, que exige a presença do agente de investigação criminal para a busca e apreensão da evidência, na computação em nuvem o dado eletrônico pretendido pode ser acessado e apreendido remotamente, não coincidindo, necessariamente, o local de acesso com o local de armazenamento.

Na abordagem relativamente aos dados, a Escola dos excepcionalistas defende que a intangibilidade, a mobilidade, a divisibilidade e a fungibilidade dos dados digitais, bem como a distância que os separa de seu proprietário, justificam o tratamento legal diferenciado (WOODS, 2016).

Por outro lado, os não-excepcionalistas entendem que essas carcaterísticas, de uma forma ou de outra, estão presentes no mundo dos bens físicos, não tendo os

tribunais encontrado dificuldades para julgar fatos que envolvam quaisquer desses aspectos, a exemplo de litígios relacionados à propriedade imaterial e ao comércio internacional. Ademais, os dados digitais têm uma localização física e, consequentemente, uma presença territorial, onde quer que estejam armazenados, sugerindo que os mesmos sejam bem mais tangíveis do que os excepcionalistas acreditam ser (WOODS, 2016). O argumento de que os dados são a-territoriais é decorrente das características de mobilidade, divisibilidade e por estarem juntos com outros dados. Como os dados são intangíveis, não é necessário que estejam vinculados a uma determinada localização, o que lhes confere independência de localização em relação ao usuário (DASKAL, 2015).

5.7 A transnacionalidade do crime, seus efeitos na disposição das evidências eletrônicas e os princípios condicionantes da jurisdição

A jurisdição prescritiva ou legislativa, aquela concernente à competência dos Estados para editar leis sem interferências externas, é orientada pelo princípio da territorialidade. Os Estados são soberanos, em seu território e sobre os seus nacionais, para regular os atos praticados internamente ou atuar na investigação de fatos que envolvam seus cidadãos, sejam como vítimas ou como autores de práticas delituosas (SCASSA; CURRIE, 2011).

Ocorre que, no contexto da jurisdição criminal, é possível que um delito possa ocorrer em mais de um Estado, seja quando é praticado num local e tem seus efeitos sentidos em outros, seja quando é praticado simultaneamente em vários Estados. Os ataques distribuídos de negação de serviço (DDoS) e os ataques para sequestro de dados (*ramsonware*) são exemplos de como ações criminosas, perpetradas por meio da Internet, facilmente alcançam dimensões mundiais.

Em 2007, a Estônia foi alvo de um dos maiores ataques cibernéticos já registrados, que durou 22 (vinte de dois) dias, de 17 de abril a 18 de maio (HERZOG, 2011). Diversas instituições públicas e privadas tiveram suas atividades paralisadas, em razão de ataques distribuídos de negação de serviço, que resultaram em degradação temporária ou perda de serviço, em muitos servidores comerciais e governamentais. Enquanto a maioria dos ataques tinha por objetivo atingir serviços Internet amplamente utilizados pela população, como sites públicos e de *e-mail*, outros se concentraram em ambientes de atividades críticas, como instituições financeira,

hospitais, servidores de domínio – DNS (OTTIS, 2008). O ataque foi desencadeado quando o governo da Estônia determinou a realocação da estátua do Soldado de Bronze de Tallin, que representava a vitória soviética sobre o nazismo, do Parque Tõnismägi para o Cemitério Militar de Tallin (HERZOG, 2011). A autoria dos ataques foi atribuída a cidadãos russos residentes no país e na Rússia, embora não tenha sido confirmada a participação do Governo nas ações (HERZOG, 2011; OTTIS, 2008).

Em 12 de maio de 2017, ocorreu um ataque global de *ransomware*, em escala sem precedentes. De acordo com a Europol, o *ransomware WannaCry* infectou rapidamente trezentas mil vítimas, em mais de 150 (cento e cinquenta) países, incluindo o Brasil, atingindo alvos de alto perfil, como o Serviço Nacional de Saúde do Reino Unido, a empresa espanhola de telecomunicações Telefónica e a empresa de logística Fed-Ex (EUROPOL, 2017b).

Os exemplos acima motivam o estudo do princípio da terriorialidade qualificada, que é uma subclasse do princípio da territorialidade e se aplica quando uma ação ou conduta, que ultrapassa as fronteiras nacionais, apresenta conexões suficientes com um Estado, fazendo-o considerar afeto à sua jurisdição (SCASSA; CURRIE, 2011), sem excluir a jurisdição dos demais, cuidando-se para não ofender ao princípio do *ne bis in idem*[74], segundo o qual ninguém pode ser punido, mais de uma vez, pelo mesmo crime.

Nesse contexto, quatro princípios conquistaram aceitação do direito internacional, como suporte à ação extraterritorial. Trata-se do princípio da nacionalidade, do princípio da proteção, do princípio universal e do princípio da nacionalidade passiva[75] (SCASSA; CURRIE, 2011; BROWNLEE, 2010; BLAKESLEY; STIGAL, 2004).

O princípio da nacionalidade é aquele segundo o qual os Estados podem afirmar a jurisdição sobre os atos praticados por seus nacionais, independentemente de onde tenham ocorrido o fato criminoso.

De acordo com o princípio da proteção ou da defesa ou real, os Estados podem afirmar a jurisdição sobre os atos cometidos no exterior, inclusive por cidadãos

[74] Livre tradução da autora, a partir do latim, no contexto do Direito Penal: “Não pode ser punido duas vezes pelo mesmo fato”.
[75] Na doutrina brasileira, o princípio da nacionalidade referido pelos autores estrangeiros coincide com o princípio da nacionalidade ativa; o princípio da proteção equivale ao princípio da defesa ou real; o princípio universal coincide com o princípio da justiça penal universal; e do princípio da nacionalidade passiva apresenta a mesma terminologia empregada no direito pátrio (BRANDÃO, 2008).

estrangeiros (BROWNLEE, 2010), que comprometam sua segurança, integridade territorial e independência política (SCASSA; CURRIE, 2011). Esse princípio é invocado quando o bem jurídico violado pelo crime está diretamente relacionado à existência do Estado, porque a sua conservação é tida como um interesse vital da própria nação (BRANDÃO, 2008; BLAKESLEY; STIGAL, 2004). São exemplos os crimes de traição, espionagem, falsificação de moedas (SCASSA; CURRIE, 2011).

Pelo princípio universal ou da justiça penal universal, que é bastante controverso e relativamente recente (KONTOROVICH, 2008), os Estados podem afirmar a jurisdição sobre determinados crimes graves, mesmo que não mantenham qualquer relação direta com a ofensa, seja em relação à localização do fato ou à cidadania das vítimas ou dos autores. O exercício dessa jurisdição baseia-se na afirmação de que certos crimes são tão hediondos que afetam o sistema jurídico internacional ou a humanidade como um todo (BROWNLEE, 2010). Os delitos sujeitos à jurisdição universal, bem como os requisitos e restrições concernentes ao seu exercício, ainda não foram estabelecidos pelo direito internacional. No entanto, há o entendimento de que indivíduos que pratiquem tortura, genocídio, crimes de guerra, crimes contra a humanidade (KONTOROVICH, 2008), pirataria clássica (SCASSA; CURRIE, 2011; BLAKESLEY; STIGAL, 2004) poderão ser processados e julgados por qualquer Estado que invocar o princípio da justiça penal universal.

Embora poucos Estados já tenham exercido essa jurisdição, o conceito geral vem conquistando o apoio da comunidade internacional (KONTOROVICH, 2008). Os Estados Unidos, por exemplo, têm expandido o alcance de sua jurisdição para processar e julgar crimes hediondos transnacionais ou internacionais[76], como o terrorismo, a lavagem de capitais, o tráfico de drogas, o tráfico de seres humanos (BLAKESLEY; STIGAL, 2004).

Blakesley e Stigal (2004) defendem também o alcance extraterrirorial das leis norte-americanas para processar e julgar pessoas pela prática de crimes relacionados à exploração sexual de menores, independentemente da nacionalidade das vítimas ou dos autores, bem como do local onde tenham sido praticados ou de onde seus efeitos tenham se manifestado, pois a exploração sexual de menores aberra contra o senso ético-jurídico da humanidade.

---

[76] Crime transnacional é aquele que viola o bem jurídico de dois ou mais países. Crime internacional, por sua vez, é o que viola bens jurídicos universais e que se caracterizam pela ação generalizada ou sistemática (BECHARA, 2011).

Por fim, segundo o princípio da nacionalidade passiva, os Estados podem afirmar jurisdição sobre delitos praticados contra seus cidadãos, independentemente de onde tenham ocorrido. Dentre os princípios citados, esse é o que mais enfrenta resistência em nível internacional e, por isso, geralmente tem sido aplicado subsidiariamente. Os Estados Unidos utilizam frequentemente esse princípio, nos julgamentos de casos de terrorismo (SCASSA; CURRIE, 2011).

5.7.1 O exemplo da justiça penal brasileira

O lesgilador brasileiro dispôs acerca da aplicação extraterritorial da lei penal, vez que o princípio da territorialidade, isoladamente, não seria suficiente para fundamentar e explicar todo o alcance espacial da lei penal.

As hipóteses de aplicação extraterritorial da lei penal são reunidas, segundo o Código Penal Brasileiro, em dois subgrupos. No primeiro, estão previstos os casos de aplicação extraterritorial incondicionada ou absoluta da lei penal brasileira, referindo aos delitos praticados fora do território nacional. No segundo, estão previstas as hipóteses de aplicação extraterritorial da lei penal, condicionada aos requisitos trazidos pelo Código Penal (BRANDÃO, 2008).

Nos casos da extraterritorialidade incondicionada ou absoluta, o simples cometimento de um delito que se enquadre nas hipóteses previstas no ordenamento jurídico brasileiro justifica a aplicação da lei penal brasileira, mesmo que cometidos no estrangeiro. Essas hipóteses estão alicerçadas no princípio da proteção ou da defesa ou real e no princípio da justiça penal universal.

O princípio da defesa fundamenta os dispositivos legais trazidos pelo art. 7º, inc. I, “a”, “b”, “c” do Código Penal (BRASIL, 1940).

O princípio da justiça penal universal fundamenta a aplicação extraterritorial da lei penal em face da significação que o delito tem para a ordem jurídica internacional, a exemplo do crime de genocídio, quando o sujeito ativo é brasileiro ou domiciliado no Brasil (art. 7º inc. I, “d”).

As hipóteses de extraterritorialidade condicionada são fundamentadas nos princípios da nacionalidade, da bandeira (art. 7º, Inc. II, “c”) e da justiça penal universal (art. 7º, Inc. II, “a”).

De acordo com princípio da nacionalidade, o Estado tem legitimidade para aplicar a sua lei penal ao seu cidadão que pratica um crime, ainda que se dê fora de

suas fronteiras (princípio da nacionalidade ativa), bem como o Estado se julga competente para aplicar sua lei penal sempre que o crime seja praticado contra seus nacionais (princípio da nacionalidade passiva), com as restrições trazidas pela lei (art. 7º, §3º do Código Penal).

5.8 A incidência da lei sobre a territorialização dos dados eletrônicos

As excepcionalidades relativamente ao alcance extraterritorial da lei trazem à tona a possibilidade de regulamentar internamente a jurisdição sobre os dados armazenados fisicamente em território nacional, como expressão da soberania estatal.

Nesse sentido, Woods (2016) sugere que alguns critérios de referência possam ser utilizados como fundamento na regulamentação interna sobre a jurisdição dos dados digitais no ambiente de nuvem computacional. São eles: a localização do dado, o local onde o dano se fez sentir, a nacionalidade do suspeito, a nacionalidade da vítima, a sede da empresa provedora do serviço de computação em nuvem computacional.

A jurisdição sobre o dado, estabelecida com base no local onde se encontra armazenado, é o critério que parece prevalecer nos embates jurídicos travados nos tribunais, tanto no Brasil como no estrangeiro. O cenário criado por esse entendimento favorece, em grande escala, os Estados Unidos, vez que concentra o maior número de *hosts*[77] do mundo.

Os Estados têm interesse em garantir que suas leis sejam aplicadas, em caso de lesão ao direito interno. Por essa razão, seria relevante sustentar que o Estado onde o crime foi praticado ou que sofreu seus efeitos tem interesse em obter acesso à evidência criminal, independentemente de onde esteja armazenada. Esse foi o sentido das decisões iniciais no caso *Microsoft Ireland*, que é abordado na seção 4.

Os critérios baseados na cidadania do suspeito e da vítima refletem o interesse do Estado em proteger seus nacionais. Quando o critério é estebelecido com base na cidadania do suspeito, algumas questões colocam-se como empecilhos. Primeiramente, será difícil, no início da persecução criminal, determinar a nacionalidade da pessoa investigada. Aliás, identificá-la será o grande desafio.

[77] https://www.cia.gov/library/publications/the-world-factbook/rankorder/2184rank.html http://world.bymap.org/InternetHosts.html. Acesso em: 13 dez. 2017.

Ademais, é bem provável que, para se proteger ou se esconder, o usuário escolha provedores de nuvem que armazenem seus dados pessoais e de suas comunicações em países que possuam legislações mais rigorosas em relação à proteção à privacidade.

A sede da empresa provedora do serviço de nuvem também pode ser usada por um Estado como fundamento para determinar a jurisdição sobre os dados. Esse parece ter sido o entendimento que prevalece nas decisões nos Estados Unidos, como no caso *Microsoft Ireland*, bem como na definição da política de uso dos serviços e da proteção à privacidade de grandes provedores de serviço Internet, como o Facebook Inc., que, no seu espaço eletrônico, destinado à requisição de evidências de crimes, expressa que o atendimento às solicitações por quebra de sigilo dar-se-á nos termos do *Stored Communications Act*, lei norte-americana (vide Figura 4).

Figura 4 - Reprodução do sítio eletrônico do aplicativo Facebook, destinado a solicitações *on-line* para autoridades de aplicação da lei

Além dos critérios acima, é oportuno acrescentar, com base em julgado no Reino da Bélgica (CURRIE, 2017), a jurisdição estabelecida com fundamento nos serviços prestados no país, pela empresa provedora de serviço, mesmo que não mantenha representação comercial em seu território. Nesse caso, entendeu a Corte de Cassação (*Cour de Cassation*) belga, que o simples fato de os dados serem transmitidos pelo do território do país, usando o idioma local, explorando o domínio *.be*, apresentando publicidades locais, justificariam as autoridades locais a compelir o provedor a fornecer os dados relativos a um cidadão belga, investigado por prática de crime, sem a necessidade de estabelecer cooperação jurídica internacional com o Estado sede da empresa ou com o Estado onde se encontravam armazenados (SCHRIJVER; DAENENS, 2013).

Coincide o entendimento do Poder Judiciário belga com o sentido conferido pelo legislador brasileiro, ao artigo 11 do Marco Civil da Internet (BRASIL, 2014).

5.9 O Brasil e a Federação Russa: a normatização interna sobre os dados eletrônicos

Em 2014, o Brasil aprovou o Marco Civil da Internet (BRASIL, 2014), disciplinando, no artigo 11, que, nas operações de coleta, armazenamento, guarda e tratamento de registros, de dados pessoais e/ou de comunicações por provedores de conexão e de aplicações de Internet em que pelo menos um desses atos ocorra em território nacional, deverão ser obrigatoriamente respeitados a legislação brasileira e os direitos à privacidade, à proteção dos dados pessoais e ao sigilo das comunicações privadas e dos registros.

O disposto no artigo aplica-se aos dados coletados em território nacional e ao conteúdo das comunicações, desde que pelo menos um dos terminais esteja localizado no Brasil, abrangendo inclusive os casos em que as atividades sejam realizadas por pessoa jurídica sediada no exterior, desde que oferte serviço ao público brasileiro ou pelo menos uma integrante do mesmo grupo econômico possua estabelecimento no Brasil.

No entanto, estando os dados armazenados em *data center* nos Estados Unidos, mesmo que todos os requisitos estabelecidos pela legislação brasileira sejam observados, as autoridades norte-americanas têm sinalizado para o entendimento de

que a divulgação de dados pessoais deve, obrigatoriamente, respeitar a legislação vigente nos Estados Unidos. Conflitos de leis entre países sempre existiram, não sendo o espaço cibernético o primeiro nem o último a provocar a disputa por interesses antagônicos, tampouco a justificar submissão ou obediência à legislação de Estado estrangeiro, em razão de seu poderio tecnológico, econômico, bélico.

Na Federação Russa, a Lei Federal nº 242-FZ, de 21 de julho de 2014[78], alterou a lei de proteção de dados, introduzindo a obrigação a todos os operadores de dados de garantir que o registro, a sistematização, a acumulação, o armazenamento, a alteração e a extração de dados pessoais de cidadãos russos sejam realizados em território da Federação Russa, no curso da coleta de dados pessoais relevantes dos indivíduos, inclusive por meio da Internet. Embora não esteja explícito, significa que qualquer dado pessoal de cidadão russo precisará estar armazenado em servidores, *data centers* ou sistemas de tecnologia da informação e comunicação, localizados em território da Federação Russa (MEDVEDEV, 2016). A nova lei, no entanto, não proíbe o acesso a servidores, *data centers* ou sistemas de tecnologia da informação e comunicação localizados em território russo, a partir de dispositivos instalados em Estado estrangeiro, nem impõe qualquer restrição a tranferências de dados pessoais de cidadãos russos, nem tampouco impede a duplicação, em Estado estrangeiro, dos referidos dados pessoais (MEDVEDEV, 2016). Em 2016, o Governo da Federação Russa obrigou o Twitter, Inc. a cumprir as normas de localização de dados no país[79].

5.10 Contribuições à pesquisa

A importância dessa seção reside no trato conceitual dos elementos essenciais do Estado, entre eles o território e a soberania, inevitavelmente envolvidos no conflito de natureza jurídico-internacional, de corrente da pretensão punitiva de um Estado, atinente a crime ocorrido em seu território, cuja punição depende de prova armazenada em nuvem computacional, sobre território estrangeiro.

---

[78] Entrou em vigor em 01 de setembro de 2015 (MEDVEDEV, 2016).

[79] BLAGOV, Sergei. Russia to Twitter: Comply with Data Localization. **Bloomberg BNA**. Bloomberg Law: Privacy & Data Security. 25 jan., 2016. Disponível em: < https://www.bna.com/russia-twitter-comply-n57982066518>. Acesso em 25 set. 2017.

É relevante considerar as contribuições das discussões sobre a compreensão do espaço cibernético como “lugar” ou “espaço” e as consequências práticas e legais decorrentes, a territorialização dos dados, que são aspectos delimitantes da proposta final desta Tese.

6 AS EVIDÊNCIAS CRIMINAIS ELETRÔNICAS NAS NORMAS INTERNACIONAIS

Inexiste tratado internacional, multilateral, de caráter vinculante e de alcance universal, concernente à prevenção e ao controle da criminalidade cibernética. A Convenção de Budapeste sobre o Cibercrime (COUNCIL OF EUROPE, 2001a) é considerada o tratado internacional mais proeminente sobre o assunto. Embora admita adesões de países que não são membros do Conselho da Europa, é exigido convite formal, precedido de anuência unânime de todos os Estados Membros, o que reforça o seu caráter regional.

Além dessa Convenção, existem outros tratados internacionais, também de abrangência regional, reunindo Estados em torno do interesse comum de proteger a sociedade contra a criminalidade intensiva no uso da tecnologia da informação e comunicação, que por vezes apresentam alcance extraterritorial.

O propósito desta seção é identificar, na análise desses instrumentos normativos internacionais, o tratamento legal conferido à localização, preservação, acesso, produção, busca e apreensão de evidências criminais em servidores de computação em nuvem, localizados em território de outro Estado Parte. Outrossim, aspectos complementares ao cerne desse trabalho serão ressaltados, como: solicitação direta a provedor de serviço, pedidos de urgência, cooperação direta entre as autoridades judiciárias.

6.1 Considerações iniciais sobre tratado internacional

O desenvolvimento da sociedade internacional e a intensificação das relações internacionais fizeram aumentar a edição de tratados internacionais, atualmente considerados a fonte mais segura e concreta das relações entre os sujeitos do Direito Internacional Público (MAZZUOLI, 2015).

A Convenção de Viena sobre o Direito dos Tratados, concluída em 23 de maio de 1969[80], é um importante documento que regula aspectos concenentes à edição de tratados internacionais firmados entre Estados (artigo 1º), desde questões pré-negociais até o processo de formação dos tratados, sua entrada em vigor, aplicação provisória, observância, interpretação, assim como a nulidade, extinção e suspensão de sua execução. Entre as regras basilares, está a norma *pacta sunt servanda* (artigo 26) e o corolário segundo o qual o Direito interno não pode legitimar a inexecução de um tratado (artigo 27).

A Convenção de Viena sobre o Direito dos Tratados (1969) não dispôs sobre os tratados concluídos entre Estados e organizações internacionais ou entre organizações internacionais, que foi objeto de outra convenção específica, concluída em 1986 e intitulada Convenção de Viena sobre Direito dos Tratados entre Estados e Organizações Internacionais ou entre Organizações Internacionais.

Tratado é um termo genérico para designar todo acordo formal concluído entre pessoas jurídicas de Direito Internacional Público, e destinado a produzir efeitos jurídicos (RESEK, 2014). De acordo com a Convenção de Viena sobre o Direito dos Tratados de 1969, tratado significa “um acordo internacional concluído por escrito entre Estados e regido pelo Direito Internacional, quer conste de um instrumento único, quer de dois ou mais instrumentos conexos, qualquer que seja sua denominação específica”, nos termos do artigo 2, parágrafo 1, letra a (BRASIL, 2009).

A Convenção não faz referência às diferentes denominações que por ventura possam ter os tratados internacionais. Na prática convencional, são identificadas diversas denominações que recebem os tratados, dependendo do assunto por eles abordados, de sua finalidade, da qualidade das partes, do número de participantes etc. A doutrina vem se esforçando para delinear os contornos de cada um desses tipos de instrumentos, levando em conta a denominação que recebem. Para Mazzuoli (2015), por exemplo, os termos e acepções mais comumente empregados nas práticas das relações internacionais são:

a) *Tratado*, para designar normalmente os ajustes solenes concluídos entre Estados e/ou organizações internacionais cujo objeto, finalidade, número e poderes das partes têm maior importância. São exemplos os tratados de paz, de amizade, de arbitragem, de cooperação, de navegação etc.;

[80] Promulgada pelo Brasil por meio do Decreto nº 7.030, de 14 de dezembro de 2009 (BRASIL, 2009).

b) *Convenção*, que denota tratado solene e multilateral, oriundo de conferências internacionais que versem sobre assuntos de interesse geral, sendo a vontade das partes paralela e uniforme. Um exemplo é a Convenção de Budapeste sobre o Cibercrime;
c) *Pacto*, expressão utilizada para restringir o objeto político de um tratado, como o Pacto do Aço, de 1939. As Nações Unidas utilizam o termo para designar os dois dos mais importantes tratados internacionais de direitos humanos: o Pacto Internacional dos Direitos Civis e Políticos, e o Pacto Internacional dos Direitos Econômicos, Sociais e Culturais, celebrados em Nova York, em 1966. Uma ressalva interessante é a troca de denominação que ocorre com a Convenção Americana sobre Direitos Humanos (1969), que é conhecida também como Pacto de San José da Costa Rica;
d) *Acordo*, que é comumente empregado para designar tratados de natureza econômica, financeira, comercial ou cultura, podendo, contudo, dispor sobre segurança recíproca, projetos de desarmamento, questões sobre fronteiras, arbitragem, questões de ordem política etc. Podem ser bilaterais ou multilaterais, geralmente com número reduzido de participantes e de relativa importância. São exemplos o Acordo entre os Governos dos Estados Membros da Organização para Cooperação de Xangai sobre a Cooperação no Campo da Segurança da Informação Internacional (2009) e o Acordo de Cooperação entre os Estados Membros da Comunidade dos Estados Independentes para o Combate a Infrações Relacionadas à Informação Computacional (2001);
e) *Carta*, geralmente empregada para estabelecer os instrumentos constitutivos de organizações internacionais (Carta da Nações Unidas (ONU, 1945), que criou a Organização das Nações Unidas (ONU), por exemplo), podendo ser empregada também para tratados solenes que estabeleçam direitos e deveres dos Estados-partes, como a Carta Social Europeia;
f) *Protocolo*, para designar acordos menos formais que os tratados, acordos complementares, suplementos a acordos pré-existentes ou já estabelecidos. O Protocolo Adicional à Convenção sobre o Cibercrime Relativo à Incriminação de Atos de Natureza Racista e Xenófoba

Praticados através de Sistemas Informáticos (COUNCIL OF EUROPE, 2003) é suplementar à Convenção de Budapeste sobre o Cibercrime;

g) *Ato* ou *Ata*, que é empregado quando se estabelecem regras que incorporam o resultado de uma conferência ou de um acordo entre as partes. Existem também *Atos* que não são tratados (por exemplo, a Ata final de Helsinque, de 1975), uma vez que seu caráter vinculante é apenas moral, e não jurídico;

h) *Declaração,* que é utilizada para designar atos que estebelecem regras e princípios jurídicos, ou ainda para as normas de direito internacional indicativas de uma política comum de interesse coletivo. São exemplos a Declaração de Paris (1856), a Declaração de Haia (1907), a Declaração do México (1945).

Além dos citados, outros termos e acepções são empregados nas relações internacionais, mas geralmente para referir acordos temporários (*modus vivendi*, Arranjo), ou para designar compromissos de menor relevância (Ajuste ou Acordo Complementar, Convênio), e ainda expressões pouco empregadas (Código, Regulamento, Contrato, Constituição, Termo de Referência).

Essa abordagem inicial é relevante às análises que são realizadas nas seções seguintes, bem como na estruturação da proposta apresentada na Tese.

6.2 As organizações internacionais intergovernamentais e as normas de direito internacional sobre o crime cibernético

A crescente necessidade de cooperação internacional, nos mais diversos campos de aplicação do Direito, fez levar à criação e desenvolvimento de instituições internacionais, capazes de coordenar os interesses da sociedade internacional, relativamente a diversas finalidades.

As organizações internacionais intergovernamentais são um fenômeno da modernidade, tendo seus contornos contemporâneos definidos a partir do início do Século XIX (MAZZUOLI, 2015). São instituições capazes de conciliar atritos e divergências entre os Estados, contribuindo assim para a almejada conquista da paz nas relações internacionais.

Na classificação dessas organizações internacionais, Mazzuoli (2015) apresenta os seguintes critérios:

a) em relação à finalidade;

b) em relação à natureza; e

c) em relação ao âmbito territorial de atuação.

No que tange aos fins que perseguem, as organizações podem ser classificadas de fins gerais e fins específicos. São exemplos das organizações com finalidades gerais a ONU, cujos objetivos principais são a manutenção da paz e da segurança internacionais, e a Organização dos Estados Americanos (OEA), que atua em âmbito territorial mais restrito e tem por finalidade promover a solidariedade, intensificar a colaboração e defender a soberania, a integridade territorial e a independência dos Estados Americanos (artigo 1º da Carta da Organização dos Estados Americanos (OEA,1948)).

São organizações de finalidades específicas aquelas destinadas à cooperação econômica (Organização de Cooperação e Desenvolvimento Econômico – OCDE, Fundo Monetário Internacional – FMI, Banco Mundial), à cooperação social, cultural e humanitária (Organização das Nações Unidas para a Educação, a Ciência e a Cultura (Unesco) e Organização Internacional do Trabalho – OIT), à cooperação técnica (União Postal Universal – UPU), à cooperação militar (Organização do Tratado do Atlântico Norte – OTAN), além daquelas que apresentam finalidade política, atuando em situações de conflito e exercendo a influência sobre temas importantes para o Estado, como os ligados à soberania, independência e relativos a direitos humanos (Liga dos Estados Árabes, União Africana).

Quanto ao alcance e base territorial, as organizações internacionais são classificadas em universais ou regionais. A ONU é um exemplo de instituição universal, pois admite o ingresso de qualquer Estado, sem qualquer discriminação. A Liga dos Estados Árabes é referida como instituição regional, vez que permite a participação tão somente de Estados Árabes.

Outros exemplos de organizações regionais são o Conselho da Europa[81], a OEA, a União Africana (UA).

[81] O Conselho da Europa não deve ser confundido com a União Europeia. O Conselho da Europa tem sede em Estrasburgo (França) e é formado por todos os países europeus, a exceção da Bielorrúsia. A União Europeia é formada por 28 (vinte e oito) Estados; do Conselho da Europa fazem parte 47 (quarenta e sete) países (MAZZUOLI, 2015). A concepção do Conselho da Europa teve por objetivo estreitar os laços entre os diversos Estados na Europa, a fim de salvaguardar e realizar os ideais e princípios que são herança comum e favorecer o progresso econômico e social de todos eles. Dentre os organismos regionais, o de maior envergadura e projeção é a União Europeia (GUERRA, 2017).

Tais instituições tratam de problemas específicos das regiões a que pertencem, como política regional, integração cultural e econômica, assuntos militares (MAZZUOLI, 2015), bem como a violência criminal intensiva no uso da tecnologia da informação e comunicação, cujos efeitos quase sempre ultrapassam as fronteiras territoriais dos Estados

Desde o início dos anos 2000, observou-se progressos significativos na promulgação de instrumentos internacionais e regionais para facilitar a prevenção e combate ao crime cibernético, sendo a primeira editada em 2001, pelos membros da Comunidade de Estados Independentes.

O estudo da ONU sobre o crime cibernético, realizado pelo Grupo de especialistas da UNODC e publicado no ano de 2013 (UNODC, 2013), identifica 05 (cinco) grupos de normatizações internacionais, relativamente ao combate às infrações cibernéticas, quais sejam:

a) as normas elaboradas no contexto ou inspiradas pelo Conselho da Europa ou União Europeia;
b) as normas criadas no contexto da Comunidade dos Estados Independentes ou da Organização para Cooperação de Xangai;
c) as normas elaboradas no âmbito da União Africana;
d) as normas editadas pela Liga dos Estados Árabes;
e) as normas elaboradas por entidades ligadas à ONU.

A Tabela 4 apresenta os instrumentos referidos acima, ressaltando o acréscimo de mais uma Convenção atribuída à União Africana, não referida originalmente pelo estudo da ONU, vez que foi editada posteriormente à publicação do referido estudo.

Tabela 4 - Normas de direito internacional concernentes ao combate às infrações intensivas em tecnologias da informação e comunicação

Organização internacional	Normas de caráter vinculativo	Normas de caráter não vinculativo
Conselho da Europa e União Europeia	• Council of Europe Convention on Cybercrime (2001) and Additional Protocol (2003); • Council of Europe Convention on Protection of Children against Sexual Exploitation and Sexual Abuse (2007); • EU legislation including on e-Commerce (2000/31/EC), on Combating Fraud and Counterfeiting of Non-Cash Means of Payment (2001/413/JHA), on Personal Data (2002/58/EC as amended), on Attacks against Information Systems (2005/222/JHA and Proposal COM (2010) 517 final), and on Child Pornography (2011/92/EU).	• Commonwealth Model Laws on Computer and Computer-related Crime (2002) and Electronic Evidence (2002).
Comunidade dos Estados Independentes e Organização para Cooperação de Xangai	• Commonwealth of Independent States (CIS) Agreement on Cooperation in Combating Offences related to Computer Information (2001); • Shanghai Cooperation Organization Agreement on Cooperation in the Field of International Information Security (2009).	
União Africana	• (Draft) Economic Community of West African States (ECOWAS) Directive on Fighting Cybercrime (2009); • (Draft) African Union Convention on the Establishment of a Legal Framework Conducive to Cybersecurity in Africa (2012). • African Union Convention on Cyber Security and Personal Data Protection (2014)*.	• East African Community Draft Legal Framework for Cyberlaws (2008); • Common Market for Eastern and Southern Africa (COMESA) Cybersecurity Draft Model Bill (2011); • Southern African Development Community (SADC) Model Law on Computer Crime and Cybercrime (2012).
Liga dos Estados Árabes	• League of Arab States Convention on Combating Information Technology Offences (2010).	• League of Arab States Model Law on Combating Information Technology Offences (2004).
Entidades ligadas à ONU	• Optional Protocol to the United Nations Convention on the Rights of the Child on the Sale of Children, Child Prostitution and Child Pornography (2000).	• International Telecommunication Union (ITU)/Caribbean Community (CARICOM)/ Caribbean Telecommunications Union (CTU) Model Legislative Texts on Cybercrime, e-Crime and Electronic Evidence (2010); • International Telecommunication Union (ITU)/Secretariat of the Pacific Community Model Law on Cybercrime (2011).

(*) acrescentado pela autora Fonte: UNODC, 2013

Para o contexto dessa pesquisa, foram analisadas as normas de direito internacional abaixo relacionadas, escolhidas dentre as de caráter vinculativo da Tabela 4, considerando a relação com o tema em estudo, a distribuição pelas organizações internacionais e a abordagem ao crime cibernético. São elas:

a) Acordo de Cooperação entre os Estados Membros da Comunidade dos Estados Independentes para o Combate a Infrações Relacionadas à Informação Computacional[82], 2001;

b) Convenção de Budapeste sobre o Cibercrime, 2001;

c) Acordo entre os Governos dos Estados Membros da Organização para Cooperação de Xangai sobre a Cooperação no Campo da Segurança da Informação Internacional[83], 2009;

d) Convenção da Liga dos Estados Árabes sobre o Combate às Ofensas contra a Tecnologia da Informação[84], 2010;

e) Convenção da União Africana sobre Segurança Cibernética e Proteção de Dados Pessoais[85], 2014.

Considerando a contribuição ao assunto abordado, também será objeto de análise o Acordo entre os Estados Unidos da América e a União Europeia sobre a Proteção de Dados Pessoais no âmbito da Prevenção, Investigação, Detecção e Repressão de Infrações Penais, aprovado, em nome da União Européia, em dezembro do ano de 2016.

Por fim, serão apresentadas as principais atuações da Organização das Nações Unidas relativamente ao crime cibernético, com destaque para um estudo que vem sendo promovido pela organização, com vistas a identificar as melhores práticas de combate à criminalidade informática, com base na análise das legislações internas de vários países.

Adiante, são apresentadas, em ordem cronológica ascendente de data de aprovação, as normas selecionadas, enfatizando disciplinamentos relevantes ao estudo, como a localização, preservação, acesso, produção, busca e apreensão

---

[82] Livre tradução da autora para: *Agreement on Cooperation Among the States Members of the Commonwealth of Independent States in Combating Offences Relating to Computer Information*.

[83] Livre tradução da autora para: *Shanghai Cooperation Organization Agreement in the Field of International Information Security.*

[84] Livre tradução da autora para: *The League of Arab States Convention on Combating Information Technology Offences.*

[85] Livre tradução da autora para: *African Union Convention on Cyber Security and Personal Data Protection.*

transfronteiriço de evidências criminais eletrônicas; a possibilidade de solicitação direta a provedor de serviço; o atendimento de pedidos de urgência; possibilidade de cooperação direta entre as autoridades judiciárias.

6.3 Acordo de Cooperação entre os Estados Membros da Comunidade dos Estados Independentes para o Combate a Infrações Relacionadas à Informação Computacional

6.3.1 A Comunidade dos Estados Independentes

Criada em 1991, a Comunidade dos Estados Independentes (CEI) constitui-se num bloco político-econômico que reúne nove repúblicas (Armênia, Belarus, Cazaquistão, Federação Russa, Moldávia, Quirquistão, Tadjiquistão, Uzbequestão e Azerbaidjão) das quinze que formavam a antiga União das Repúblicas Socialistas Soviéticas (URSS). Originalmente, não integraram a comunidade os três países bálticos (Lituânia, Letônia e Estônia). A CEI está organizada em uma confederação de Estados que preserva a soberania interna[86].

6.3.2 A estrutura normativa do Acordo

O Acordo de Cooperação entre os Estados Membros da Comunidade dos Estados Independentes para o Combate à Criminalidade Relacionada à Informação Computacional foi escrito originalmente no idioma russo, sendo aprovado e aberto para assinatura[87], em Minsk/Bielorrússia, em 01 de junho de 2001. Entrou em vigor a partir de 14 de março de 2002 (COMMONWEALTH OF INDEPENDENT STATES, 2001).

O Acordo foi estabelecido com o objetivo de inaugurar um arcabouço legal para possibilitar a cooperação entre os Membros da Comunidade dos Estados Independentes, no combate aos crimes intensivos em tecnologia da informação e comunicação. Decorre da interpretação da norma que o bem jurídico que se pretende

---

[86] GLOBAL SECURITY. Commonwealth of Independent States (CIS). Atualizado em 27 jan., 2017. Disponível em: <https://www.globalsecurity.org/military/world/int/cis.htm>. Acesso em: 20 jun. 2017.

[87] Assinaram o Acordo: Republic of Azerbaijan, Republic of Armenia, Republic of Belarus, Republic of Kazakhstan, Kyrgyz Republic, Republic of Moldova, Russian Federation, Republic of Tajikistan, Republic of Uzbekistan, Ukraine. Deixaram de assinar: Georgia e Turkmenistan (COMMONWEALTH OF INDEPENDENT STATES, 2001).

proteger é a confidencialidade, integridade e disponibilidade dos sistemas computacionais e dos dados armazenados ou em trânsito pelos meios de comunicação (artigo 1º).

Os termos do Acordo estão dispostos em 17 (dezessete) artigos, iniciando com a definição das terminologias utilizadas ao longo do texto.

O artigo 3º abrange as disposições que criminalizam 04 (quatro) condutas relacionadas à tecnologia da informação e comunicação, quais sejam:

a) acesso ilegal à sistema computacional protegido por lei, resultando em destruição, bloqueio, alteração ou cópia de informações, ou ainda que ocasione interrupção no funcionamento do computador, do sistema computacional ou da rede de computadores;
b) criação, uso e distribuição de *softwares* maliciosos;
c) violação de direitos autorais de programas de computador;
d) ofensa a normas relacionadas ao uso de computadores, sistemas computacionais ou de redes, por pessoa com acesso autorizado aos mesmos, que da sua conduta resulte em destruição, bloqueio ou alteração de informações protegidas por lei, causando danos significativos ou consequências graves.

Os artigos 4º ao 8º tratam da cooperação entre as Partes, que será processada por meio de contato direto entre as autoridades competentes, previamente designadas por cada Estado, no ato da assinatura ou do depósito do Acordo.

A cooperação ocorrerá, nos termos do artigo 5º, visando:

a) o planejamento de operações integradas;
b) a troca de informações;
c) a organização de treinamentos conjuntos;
d) a criação de um sistema de informações em suporte às atividades de prevenção e combate à criminalidade cibernética, dentre outras.

Há previsão também de atendimento a pedidos de urgência, que podem ser realizados por comunicação eletrônica ou, até mesmo, oralmente, devendo ser confirmado, oficialmente, num prazo de 03 (três) dias (artigo 6º).

É desejável que as requisições sejam atendidas em até 30 (trinta) dias, devendo a Parte requisitante ser informada sobre quaisquer eventualidades que

ocasionem atraso na resposta (artigo 7º). Não serão atendidos os pedidos que contrariem o direito interno da Parte requisitada (artigo 8º).

O instrumento internacional em análise não faz qualquer referência à localização, preservação, acesso, coleta, produção, busca e apreensão de extraterritorial de evidências eletrônicas de crimes.

6.3.3 Alterações em andamento

Em agosto de 2017, o Presidente da Federação Russa, Vladimir Putin, aprovou a edição de um novo acordo de cooperação sobre o combate ao cibercrime, entre membros da Comunidade dos Estados Independentes (CEI), em substituição ao autal.

6.4 A Convenção de Budapeste sobre o Cibercrime

6.4.1 O Conselho da Europa e a elaboração da Convenção de Budapeste sobre o Cibercrime

A primeira iniciativa internacional para discutir o crime cibernético na Europa foi promovida pelo Conselho da Europa, em 1976, durante conferência sobre aspectos criminológicos dos crimes econômicos, em Estrasburgo (França). Nessa ocasião, diversas categorias de crimes cibernéticos foram dicutidas, como violação à propriedade intelectual de programa de computador, pedofilia, fraude eletrônica (SCHJOLBERG, 2008).

Em 1985, o Conselho da Europa nomeou uma comissão de peritos para discutir questões legais acerca da criminalidade cibernética. O resultado do trabalho foi apresentado na forma de Recomendação[88] (COUNCIL OF EUROPE, 1990), que estabeleceu diretrizes referentes à definição de novas condutas relacionadas a computadores, tais como sabotagem, acesso não autorizado a dados armazenados, interceptação não autorizada, reprodução não autorizada de programas de computadores.

---

[88] *Recommendation nº R (89) 9 on Computer-related Crime and Final Report of European Committee on Crime Problems*.

Medidas processuais penais voltadas a investigação de crimes cibernéticos foram trazidas pela Recomendação Nº R (95) 13 (COUNCIL OF EUROPE, 1995), tais como a busca e apreensão, coleta de evidências eletrônicas, uso de criptografia, cooperação internacional.

Em novembro de 1996, o Comitê Europeu para Problemas Criminais[89] (CDPC) opinou pela criação de uma comissão de especialistas para estudar o crime cibernético, que foi instituída em dezembro de 1997, pelo Comitê de Ministros do Conselho da Europa, sob a denominação de Comitê de Especialistas sobre a Criminalidade no Espaço Cibernético[90] (PC-CY). O CDPC baseou sua decisão em diversos pressupostos, inclusive no caráter transfronteiriço das infrações, vez que, quando cometidas pela Internet, em geral entra em conflito com a territorialidade das autoridades nacionais, competentes para aplicar a lei.

Os trabalhos do PC-CY perduraram pelo período compreendido entre abril de 1997 a dezembro de 2000, tendo como produto final o projeto de convenção e seu Relatório Explicativo, que foram submetidos para aprovação do CDPC, na 50ª Sessão Plenária, em junho de 2001. O texto da convenção foi aprovado pelo Comitê de Ministros do Conselho da Europa, quando foi adotado e aberto para assinatura, em novembro de 2001 (COUNCIL OF EUROPE, 2001b).

Em 01 de março de 2006, entrou em vigor o Protocolo Adicional à Convenção, com o objetivo de fazer criminalizar condutas de cunho racista e xenófobo, através de ameaças, insultos e condutas congêneres, praticadas por meio da Internet e de rede de computadores. Foi aberto a assinaturas em Estrasburgo, a 28 de janeiro de 2003 (COUNCIL OF EUROPE, 2003).

Contribuíram ainda com a elaboração da referida Convenção trabalhos técnicos realizados pela OCDE (ainda nos idos de 1982) e pelo G8 (Grupo dos Oito), com a instituição de um grupo para crimes de alta tecnologia, vinculado ao grupo de especialistas em crime organizado transnacional (SCHJOLBERG, 2008).

Hoje, é reconhecida a necessidade de aditar a referida Convenção, disciplinando aspectos que, a época da edição do texto original, não configuravam desafios à persecução criminal, por ainda se encontrarem como mera possibilidade no imaginário da academia, como a computação em nuvem. Em junho de 2017, foi aprovado pelo Conselho da Europa, o Termo de Referência que orienta a elaboração

[89] Tradução da autora para: *European Committee on Crime Problems* (CDPC).
[90] Tradução da autora para: *Committee of Experts on Crime in Cyber-space* (PC-CY).

do Segundo Protocolo Adicional à Convenção. Em 2009, Morais Neto (2009) já havia percebido a necessidade de alterações, conforme expõe:

> O combate ao cibercrime não é responsabilidade apenas da União Européia, mas de todos os países. É uma necessidade a ampliação de seu principal instrumento jurídico de combate ao cibercrime, uma vez que tem se mostrado como instrumento hábil a viabilizar a cooperação penal internacional, mediante suas disposições que tratam da definição de condutas, do estabelecimento de parâmetros para harmonização e do direito nacional e notadamente das disposições de cooperação, como as medidas de auxílio mútuo exaustivamente analisadas. Não se pode dizer que se trata de uma Convenção perfeita, mas estabelece de forma clara, as ressalvas e reservas possíveis (MORAIS NETO, 2009, p.169).

6.4.2 Estrutura normativa da Convenção

A Convenção de Budapeste sobre o Cibercrime está estruturada em 04 (quatro) Capítulos[91]:

a) Capítulo I - Terminologia;

b) Capítulo II - Medidas a tomar a nível nacional

c) Capítulo III – Cooperação internacional

d) Capítulo IV - Disposições finais

O Capítulo I, composto apenas pelo artigo 1°, traz o significado para alguns termos usados na referida Convenção, de maneira a evitar equívocos à interpretação de suas normas.

O Capítulo II estabelece as medidas a serem adotadas, em nível nacional, relativamente ao direito substantivo e ao direito processual, bem como os dispositivos que instam cada Estado Parte a estabelecer a sua competência sobre qualquer infração penal, definida em conformidade com os artigos 2º ao 11º da referida Convenção. Está dividido em três seções, conforme apresenta a Figura 5.

[91] Foi utilizada a terminologia trazida pela tradução oficial para o português, disponível no site do Conselho da Europa: https://rm.coe.int/16802fa428.

Capítulo II – Medidas a tomar a nível nacional

Secção 1 – Direito penal material

Título 1 – Infracções contra a confidencialidade, integridade e disponibilidade de sistemas informáticos e dados informáticos

Título 2 – Infracções relacionada com computadores

Título 3 – Infracções relacionadas com o conteúdo

Título 4 – Infracções relacionadas com a violação do direito de autor e direitos conexos

Título 5 – Outras formas de Responsabilidade e Sanções

Secção 2 – Direito Processual

Título 1 – Disposições comuns

Título 2 – Conservação expedita de dados informáticos armazenados

Título 3 – Injunção

Título 4 – Busca e Apreensão de dados informáticos armazenados

Título 5 – Recolha em tempo real de dados informáticos

Secção 3 – Competência

Figura 5 - Estrutura do Capítulo II da Convenção de Budapeste sobre o Cibercrime
Fonte: Convenção de Budapeste sobre o Cibercrime

O Capítulo III aborda as normas que tratam da cooperação internacional, incluindo a extradição e o auxílio mútuo em matéria penal. Compreende duas seções, organizadas conforme Figura 6:

Capítulo III – Cooperação internacional

Secção 1 – Princípios gerais

Título 1 – Princípios gerais relativos à cooperação internacional

Título 2 – Princípios relativos à extradição

Título 3 – Princípios gerais relativos ao auxílio mútuo

Título 4 – Procedimentos relativos aos pedidos de auxílio mútuo na ausência de acordos internacionais aplicáveis

Secção 2 – Disposições específicas

Título 1 – Auxílio mútuo em matéria de medidas provisórias

Título 2 – Auxílio mútuo relativamente a poderes de investigação

Título 3 - Rede 24/7

Figura 6 - Estrutura do Capítulo III da Convenção de Budapeste sobre o Cibercrime
Fonte: Convenção de Budapeste sobre o Cibercrime

Por fim, no Capítulo IV são apresentadas as disposições finais, que compreendem as tradicionais cláusulas finais constantes das Convenções adotadas no âmbito do Conselho da Europa.

As regras que disciplinam o acesso extraterritorial a dados armazenados na grande rede estão previstas no artigo 32 da referida Convenção, que integra o "Título 2 – Auxílio mútuo relativamente a poderes de investigação", da "Seção 2 - Disposições específicas", do Capítulo III, que trata da Cooperação Internacional (Figura 6). As disposições acerca da busca e apreensão de dados armazenados encontram-se no artigo 19 e são relativas apenas a medidas a serem empreendidas em nível nacional, não se aplicando à medida transfronteiriça[92] (COUNCIL OF EUROPE, 2001b).

6.4.3 O acesso transfronteiriço a dados armazenados

A Convenção de Budapeste sobre o Cibercrime disciplinou o acesso direto a dados armazenados em território estrangeiro no artigo 32. De acordo com esse dispositivo, apenas duas situações permitem a um Estado Parte, unilateralmente, o legítimo acesso e obtenção de dados armazenados fisicamente no território de um outro Estado, sem a necessidade de recorrer à formulação de um pedido de auxílio mútuo.

A primeira situação informa que não será exigida autorização prévia quando os dados requeridos são acessíveis ao público em geral (fonte aberta), independentemente da localização geográfica desses dados (artigo 32.a). Nesse contexto, cita-se como exemplo todas as informações disponíveis em sítios Internet[93], desde que não estejam protegidas por senhas ou códigos de acesso, ou quaisquer outros mecanismos de segurança. Nesse sentido, Clough (2015) conclui que as agências de persecução criminal estariam autorizadas a acessar os mesmos conteúdos que qualquer pessoa, independentemente de onde estejam localizados.

A segunda situação prevista é a permissão para acessar ou receber, por meio de um sistema informático localizado em seu território, dados informáticos armazenados no território de outra Parte, desde que obtido o consentimento voluntário

[92] Parágrafo 195 do Relatório Explicativo da Convenção de Budapeste sobre o Cibercrime (COUNCIL OF EUROPE, 2001b).
[93] A manutenção de páginas Internet públicas pressupõe o consentimento, por parte do seu respectivo titular, de que a mesma poderá ser acessada por qualquer outro usuário da rede, de acordo com o item 48 do Relatório Explicativo da Convenção sobre o Cibercrime (COUNCIL OF EUROPE, 2001b).

da pessoa com legitimidade jurídica para proceder à divulgação dos mesmos (artigo 32.b).

Num exemplo hipotético, seria lícito, nos termos do artigo 32.b, o acesso do policial ao conteúdo das caixas-postais de um suspeito de traficar drogas que, no momento da prisão, encontrava-se utilizando aplicativo de *e-mail*, de um provedor de Internet situado em outro Estado Parte, e consente, voluntariamente, que o agente público explore o ambiente.

O desafio, nesse segundo caso, é identificar quando uma pessoa tem legitimidade para proceder à divulgação.

De acordo com o Relatório Explicativo da Convenção sobre o Cibercrime (COUNCIL OF EUROPE, 2001b)[94], identificar a pessoa legalmente autorizada a divulgar os dados depende das circunstâncias de cada caso concreto, da natureza jurídica da pessoa e do direito interno de cada Estado Parte. Assim, por exemplo, um usuário de uma determinada conta de *e-mail* pode divulgar o conteúdo das mensagens ou, voluntariamente, permitir-lhes o acesso de terceiros, independentemente de onde estejam fisicamente armazenadas, se dentro das fronteiras nacionais ou no território de um outro Estado.

Delgado (2007) ressalta que o fato de uma pessoa ter acesso aos dados armazenados em um sistema informático não a autoriza a divulgá-los a outrem. Os administradores de infraestrutura de tecnologia da informação e comunicação (de rede, de sistema operacional, de banco de dados), por exemplo, podem ter acesso irrestrito às bases de dados sob sua responsabilidade, para realizar manutenções periódicas e garantir o perfeito funcionamento do mesmo. No entanto, essa possibilidade não implica em reconhecimento jurídico de poderes arbitrários. Assim, ainda que tecnicamente ele tenha permissão para acessá-los, juridicamente sua autorização estará limitada à necessidade e aos fins deste acesso e jamais alcançará a entrega dos mesmos a terceiros, sem a devida permissão legal.

E caso haja a necessidade de acesso e recuperação de dados que estejam armazenados em território estrangeiro e que não estejam disponíveis para o livre acesso do público nem foram voluntariamente entregues por pessoa legalmente autorizada? Nesse caso, deverão ser observadas as regras constantes no artigo 31,

[94] Cf. Item 294 do Relatório Explicativo da Convenção sobre o Cibercrime.

que prevê, em termos gerais, a obrigatoriedade de prévio pedido de auxílio mútuo à Parte requerida.

Nos termos do artigo 31.1, o Estado Parte poderá requerer a outro Estado Parte investigação, acesso, apreensão, obtenção, divulgação de dados armazenados por meio de sistema informático que se encontre no território dessa outra Parte, incluindo a conservação expedita de dados armazenados.

O artigo 32.2 exige da Parte requerida a respectiva capacidade de resposta. Além disso, estabelece que o atendimento a um pedido de auxílio mútuo referente à busca ou acesso, apreensão ou obtenção, e divulgação de dados informáticos armazenados, realizar-se-á por meio da aplicação das normas dispostas, não apenas na Convenção de Budapeste sobre o Cibercrime, mas também nos instrumentos internacionais sobre cooperação em matéria penal, nos acordos baseados na aplicação de legislação uniforme ou recíprocas, bem como nas leis nacionais.

Ao abrigo do artigo 31.3, a resposta a um pedido de assistência mútua deverá ocorrer numa base expedita, sempre que:

a) existam motivos para crer que os dados relevantes são especialmente vulneráveis à perda ou modificação; ou
b) os instrumentos, acordos e legislação referida no parágrafo 2º prevejam uma cooperação rápida.

Assim, no contexto da Convenção de Budapeste sobre o Cibercrime, com exceção das hipóteses expressamente definidas no seu artigo 32, o acesso extraterritorial a evidências criminais eletrônicas, poderá ser entendido como violação à soberania do país onde os dados se encontrem armazenados, configurando infração à prerrogativa exclusiva das autoridades nacionais competentes para levar a cabo investigações e procedimentos criminais em seu próprio território (DELGADO, 2007).

A Convenção de Budapeste sobre o Cibercrime encontra-se aberta à adesão por outros Estados não-membros do Conselho da Europa e que não tenham participado do seu processo de elaboração, mediante convite do Comitê de Ministros do Conselho da Europa, como prevê expressamente o art. 37 do referido instrumento:

> Após a entrada em vigor da presente Convenção, o Comitê de Ministros do Conselho da Europa pode, depois de ter consultado os Estados contratantes da Convenção e de ter obtido o acordo unânime, convidar qualquer Estado não membro do Conselho e que não tenha participado na sua elaboração, a aderir à presente Convenção. A decisão é tomada pela maioria prevista no artigo 20º, alínea d), dos Estatutos do Conselho da Europa e por unanimidade dos representantes dos Estados contratantes com direito de voto no Comitê de Ministros (COUNCIL OF EUROPE, 2001a).

Até 15 de dezembro de 2017, 56 (cinquenta e seis) países ratificaram a convenção em comento[95].

A Federação Russa é o único Estado que integra o Conselho da Europa a não assinar nem ratificar a Convenção de Budapeste sobre o Cibercrime. Embora tenha externado interesse na Convenção, a Federação Russa discordou publicamente dos termos do artigo 32.b, por entender que contrariam normas internacionais de respeito à soberania e aos direitos humanos (CYBERCRIME CONVENTION COMMITTEE, 2008; CYBERCRIME CONVENTION COMMITTEE, 2007).

A atitude da Russia foi, em parte, motivada por uma investigação criminal conduzida por agentes do FBI, a partir dos Estados Unidos[96], contra dois cidadãos russos (*Alexey Ivanov* e *Vasily Gorshkov*), residentes na cidade Chelyabinsk/Rússia, pela prática de crimes cibernéticos contra empresas norte-americanas. As investigações foram procedidas pelo núcleo do FBI de Seattle, no final de 1999. Empresas norte-americanas, que realizavam transações financeiras e comerciais *on-line*, por meio de cartão de crédito, tiveram seus sistemas atacados e suas bases de dados comprometidas, com o acesso dos infratores a informações pessoais dos clientes, inclusive a números de cartões de crédito. No decorrer das investigações, os agentes do FBI utilizaram disfarces virtuais e conseguiram convencer os suspeitos a se deslocarem aos Estados Unidos, a fim de participar de uma entrevista de emprego numa empresa de segurança digital, que foi criada unicamente para ludibriar os investigados e fazê-los acreditar que o teste de penetração ao qual foram submetidos fazia parte do processo seletivo. De forma insidiosa, utilizando ferramentas que simulavam falhas de segurança em sistemas (*honeypot*) e permitiam a captura de teclas (*keylogger*), os agentes conseguiram as credenciais de acesso e devassaram remotamente os computadores que se encontravam instalados em território russo, copiando diversos arquivos (CLOUGH, 2015; ATTFIELD, 2006).

Em abril de 2017, o aludido país preparou uma minuta de uma nova convenção sobre o cibercrime e submeteu a especialistas das Nações Unidas. A intenção era substituir a Convenção de Budapeste sobre o Cibercrime, sob o

[95] https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185/signatures?p_auth=VMziopdi. Acesso em: 15 dez. 2017.
[96] COMPUTER CRIME RESEARCH CENTER. Putin defies Convention on Cybercrime. Mar., 2008. Disponível em: <http://www.crime-research.org/news/28.03.2008/3277/>. Acesso em 30 set. 2017.

argumento de que o artigo 32 constituía uma ameaça à soberania de Estados independentes.

O Brasil ainda não foi convidado a aderir à referida Convenção nem manifestou interesse[97].

6.4.4 Alterações em andamento

Em 08 de junho de 2017, durante o 17º encontro do Comitê da Convenção de Budapeste sobre o Cibercrime[98] (T-CY), realizado de 07 a 09 de junho, em Estrasburgo/França, foi revisado e aprovado o Termo de Referência (CYBERCRIME CONVENTION COMMITTEE, 2017) que orienta a elaboração do segundo protocolo adicional à Convenção de Budapeste sobre o Cibercrime, relativamente a medidas que otimizem o acesso a evidências criminais, armazenadas no ambiente de computação em nuvem.

6.5 Acordo entre os Governos dos Estados Membros da Organização para Cooperação de Xangai sobre a Cooperação no campo da Segurança da Informação Internacional

6.5.1 A Organização para Cooperação de Xangai

A Organização para Cooperação de Xangai (SCO)[99] é uma organização intergovernamental internacional, criada pelos líderes da República Cazaquistão, República Popular da China, República do Quirgustão, Federação Russa, República do Tajiquistão e República do Uzbequistão, em 15 de junho de 2001, com o objetivo de fomentar parceria nas áreas política, militar, econômica e cultural, primando pela não interferência nos assuntos internos e na soberania territorial dos Estados Membros (HESSBRUEGGE, 2004).

---

[97] Informação obtida por meio de resposta (em 15 nov. 2017) à consulta realizada ao *Bureau des Traités*, do Conselho da Europa, através do site: https://www.coe.int/en/web/conventions/contact.
[98] Livre tradução da autora para: *Cybercrime Convention Committee.*
[99] Refere-se a sigla em inglês para *Shanghai Cooperation Organization* (SCO).

Em 2015, por ocasião da 15ª Cúpula da Organização para Cooperação de Xangai, foi iniciado o processo de integração da Índia e do Paquistão (anteriormente membros observadores), como membros permanentes da Organização[100].

6.5.2 A estrutura normativa do Acordo

O Acordo entre os Estados Membros da Organização para Cooperação de Xangai sobre a Cooperação no Campo da Segurança da Informação Internacional foi realizado na cidade de Ecaterimburgo/Rússia, em 16 de junho de 2009, nos idiomas russo e chinês (SHANGHAI COOPERATION ORGANIZATION, 2009).

O Acordo foi estabelecido com o objetivo de criar um quadro jurídico e organizacional para nortear a cooperação entre as Partes, no sentido de limitar as ameaças cibernéticas, proteger os interesses das Partes e estabelecer um ambiente de informação internacional, caracterizado pela paz, a cooperação e a harmonia.

Os termos do Acordo estão dispostos em 12 (doze) artigos, iniciando com a definição da terminologia utilizada no texto.

O artigo 2º define as ameaças à segurança da informação internacional, quais sejam:

a) o desenvolvimento e aplicação de armas de informação, informação de capacitação e manutenção;
b) o terrorismo da informação;
c) informação da delinquência;
d) utilização de uma posição dominante no espaço de informação, em detrimento dos interesses e segurança de outros estados;
e) divulgação de informações prejudiciais ao ambiente sócio-político e socioeconômico, espiritual, moral, cultural e do meio ambiente de outros Estados;
f) ameaça à segurança, o funcionamento estável da infraestrutura de informações globais e nacionais.

---

[100] Putin: "Adesão de Índia e Paquistão marca nova etapa da SCO". 10 de julho de 2015. Disponível em: <https://www.terra.com.br/noticias/mundo/putin-adesao-de-india-e-paquistao-marca-nova-etapa-da-sco,6988829b23836478d29223e136f53f1clq00RCRD.html>. Acesso em 13 jun., 2017.

A cooperação entre as Partes é trazida pelos artigos 3º, 4º e 5º, e deve ser executada em observância a princípios e normas universalmente reconhecidos pelo direito internacional, incluindo os princípios de resolução pacífica dos conflitos, não uso da força, vedação à interferência nos assuntos internos, o respeito aos direitos e liberdades fundamentais do ser humano.

A proteção da informação é referida no artigo 6º.

Os dispositivos restantes referem-se à operacionalização do Acordo, como financiamento, relação com outros acordos internacionais, resolução de controvérsias, idioma de trabalho, depósito e disposições finais.

Por fim, não há qualquer referência à localização, preservação, produção, acesso, busca e apreensão dados armazenados em servidor de computação em nuvem, localizado em outro Estado.

6.6 A Convenção da Liga dos Estados Árabes sobre o Combate às Ofensas contra a Tecnologia da Informação

6.6.1 A Liga dos Estados Árabes

A Liga dos Estados Árabes (LEA) é uma organização internacional intergovernamental de caráter regional, fundada no Cairo, em 1945, com o objetivo de coordenar a ação política e realizar uma estreita colaboração entre os membros, a fim de salvaguardar sua independência e soberania (SEITENFUS, 2016).

O principal órgão decisório é o Conselho da Liga, no qual todos os Estados Membros estão representados. A Presidência do Conselho é ocupada em caráter de rodízio, por um período de seis meses. As Cúpulas da Liga ocorrem em frequência anual, geralmente no mês de março. Atualmente, reúne 22 (vinte e dois) países islâmicos.

6.6.2 Estrutura normativa da Convenção

A Convenção da Liga dos Estados Árabes sobre o Combate às Ofensas contra a Tecnologia da Informação (LEAGUE OF ARAB STATES, 2010) foi concluída em 21 de dezembro de 2010, na cidade do Cairo (Egito), sendo escrita em árabe e depositada na Secretaria-Geral da Liga dos Estados Árabes. Tem por objetivo reforçar

a cooperação e adotar uma política criminal comum entre as Partes, com vistas a proteger a sociedade árabe contra os delitos intensivos no emprego da tecnologia da informação e comunicação, que ameacem os interesses e a segurança dos Estados, das comunidades e dos indivíduos (LEAGUE OF ARAB STATES, 2010).

A Convenção está dividida em 05 (cinco) capítulos, por onde se distribuem 43 (quarenta e três) artigos.

O Capítulo I traz as disposições gerais, que incluem o propósito da Convenção (artigo 1), as definições para as terminologias empregadas ao longo do texto (artigo 2), as áreas de aplicação (artigo 3) e as salvaguardas acerca da soberania (artigo 4).

Nas salvaguardas relativas à soberania, a Convenção assegura o respeito aos princípios da igualdade soberana e da não interferência nos assuntos internos de outro Estado, asseverando a vedação ao exercício extraterritorial da jurisdição ou de outras funções que são inerentes às autoridades do outro Estado, em virtude do seu direito interno.

O Capítulo II abrange as disposições concernentes ao crime cibernético e a condutas relacionadas à tecnologia da informação e comunicação. São definidas pela Convenção as seguintes infrações: acesso ilícito (artigo 6), interceptação ilícita (artigo 7), ofensa contra a integridade dos dados (artigo 8), uso indevido da tecnologia da informação para diversos fins (artigo 9), falsificação (artigo 10), fraude (artigo 11), infrações relacionada à pornografia (artigos 12 e 13), violação à privacidade (artigo 14), ofensas relacionadas ao terrorismo cometidas por meio da tecnologia da informação (artigo 15), infrações relacionadas ao crime organizado, cometidas por meio da tecnologia da informação (artigo 16), infrações relacionadas à violação de direitos autorais e conexos (artigo 17), fraude no pagamento eletrônico (artigo 18). Nos termos do artigo 21, os crimes comuns, cometidos com o auxílio da tecnologia da informação e comunicação, devem ter a pena majorada ou agravada.

O Capítulo III apresenta as prescrições relacionadas ao direito processual, tais como: preservação expedita de dados armazenados (artigo 23), custódia expedita e divulgação parcial de dados de tráfego (artigo 24), ordem de produção de dados (artigo 25), inspeção de informação armazenada (artigo 26), apreensão de informação armazenada, mantendo a integridade (artigo 27), recolhimento de dados de tráfego em tempo real (artigo 28) e interceptação de dados de conteúdo (artigo 29).

O Capítulo IV contem as disposições relativas à cooperação entre as partes, trazendo regras de extradição (artigo 31), assistência judiciária mútua (artigos 32 a

34), confidencialidade (artigo 36), proteção dos dados armazenados (artigo 37), divulgação expedita de informações de rastreamento de usuários (artigo 38), cooperação e assistência bilateral em relação ao acesso a informações armazenadas (artigo 39), acesso transfronteiriço a dados armazenados (artigo 40), cooperação e assistência bilateral para recolhimento de dados de tráfego (artigo 41), cooperação e assistência bilateral para informações de conteúdo (artigo 42).

As regras para a cooperação preveem a possibilidade de, em caso de emergência, um Estado Parte poder enviar o pedido de forma expedita, por fax ou *e-mail*, desde que tal comunicação assegure um grau razoável de segurança (inclusive usando codificação) e confirmação de envio, conforme exigido pelo Estado requerido, o qual deve responder ao pedido o mais breve possível, podendo utilizar-se inclusive de meios de comunicação informais, embora céleres, como o *e-mail* (artigo 32.3).

Nos termos do artigo 33.1, um Estado Parte pode, sem requisição prévia, entregar a outro Estado Parte informações obtidas por meio de investigações próprias, se considerar que essa divulgação é relevante à investigação procedida pelo Estado receptor ou que poderá levar a um pedido de cooperação.

Os Estados Parte nomearão uma autoridade central responsável pelos pedidos de auxílio mútuo, bem como os encaminhamentos relativos aos pedidos de outro Estado Parte (artigo 34.2). Em caso de emergência, pedidos de assistência mútua podem ser enviados diretamente às autoridades judiciárias da Parte requerida, devendo as autoridades centrais dos Estados Parte envolvidos serem informadas (artigo 34.8).

Via de regra, quando um Estado Parte, durante um procedimento investigatório, necessita de dados que estão armazenados em servidores localizados em território de outro Estado Parte, pode requerer assistência judiciária para que a Parte requerida investigue, acesse, apreenda, preserve ou divulgue essas evidências criminais eletrônicas (artigo 39).

6.6.3 O acesso transfronteiriço a dados armazenados

O acesso transfronteiriço e direto às referidas evidências, sem prévia requisição de auxílio mútuo, está previsto no artigo 40, sendo possível nas mesmas circunstâncias trazidas pela Convenção de Budapeste sobre o Cibercrime, quais sejam:

a) quando os dados estão disponíveis para acesso público (fonte aberta), a exemplo das divulgações em sítios eletrônicos da internet, desde que não estejam protegidas por senhas ou códigos de acesso, ou quaisquer outros mecanismos de segurança;
b) quando o acesso ou recebimento de dados digitais armazenados no território de uma outra Parte ocorra mediante consentimento voluntário da pessoa com legitimidade jurídica para proceder à divulgação dos mesmos, por meio de um sistema informático localizado território do Estado Parte de origem.

Por fim, o Capítulo V traz as disposições finais, informando acerca dos procedimentos de ratificação, aceitação, depósito, vigência, dentre outros disciplinamentos.

6.7 Convenção da União Africana sobre Segurança Cibernética e Proteção de Dados Pessoais

6.7.1 A União Africana

A União Africana (UA), formada por 55 (cinquenta e cinco) países, é uma organização internacional intergovernamental de alcance regional, constituída na cidade de Lome (Tongo), em 11 de julho de 2000, durante a 36ª Sessão Ordinária da Assembeia de Chefes de Estado e Governo (AFRICAN UNION, 2000), sendo lançada pela Cúpula de Durban (África do Sul), em 2002, durante a 1ª Assembleia Ordinária dos Chefes de Estado da União Africana. A UA substituiu a antiga Organização de Unidade Africana (OUA)[101].

Os objetivos perseguidos pela nova organização se afastam das lutas históricas da OUA, que estavam centradas na luta contra a dominação branca e combate ao colonialismo, e enfatizam a necessidade do desenvolvimento econômico, da atração de investimentos estrangeiros e da promoção da democracia (SEITENFUS, 2016).

[101] https://au.int/en

6.7.2 A estrutura normativa da Convenção

A Convenção da União Africana sobre Segurança Cibernética e Proteção de Dados (AFRICA UNION, 2014) foi adotada durante a 23ª Sessão Ordinária da Assembleia da União Africana, realizada na cidade de Malabo (República da Guiné Equatorial), 27 de junho de 2014. A estrutura normativa da Convenção está resuminda na Figura 7.

O artigo 1 define as terminologias empregadas no texto.

O Capítulo I traz disposições que regulamentam o comércio eletrônico, as obrigações contratuais na prestação de serviços em meio digital e as medidas de segurança nas transações eletrônicas.

O Capítulo II dispõe sobre a proteção de dados pessoais.

O Capítulo III aborda a promoção da segurança cibernética e o combate ao cibercrime.

Relativamente à criminalidade cibernética, a Convenção impulsiona a harmonização regional das leis e regulamentos dos Estados Parte, bem como promove o respeito ao princípio da dupla incriminação. A cooperação judiciária e a cooperação administrativa também são incentivadas, com o intuito de promover o intercâmbio e o compartilhamento de informações. A Seção II do Capítulo III abrange as disposições relativas ao crime cibernético, ao crime comum praticado por meio da tecnologia da informação e comunicação, além de questões atinentes ao direito processual.

Article 1: Definitions
CHAPTER I: ELECTRONIC TRANSACTIONS
Section I: Electronic Commerce
Article 2: Scope of application of electronic commerce
Article 3: Contractual liability of the provider of goods and services by electronic means
Article 4: Advertising by electronic means
Section II: Contractual Obligations in Electronic Form
Article 5: Electronic contracts
Article 6: Writing in electronic form
Section III: Security of Electronic Transactions
Article 7: Ensuring the Security of Electronic Transactions
CHAPTER II: PERSONAL DATA PROTECTION.
Section I: Personal data protection
Article 8: Objective of this Convention with respect to personal data
Article 9: Scope of application of the Convention
Article 10: Preliminary personal data processing formalities
Section II: Institutional framework for the protection of personal data
Article 11: Status, composition and organization of National Personal Data Protection Authorities
Article 12: Duties and Powers of National Protection Authorities
Section III: Obligations relating to conditions governing personal data processing
Article 13: Basic principles governing the processing of personal data
Article 14: Specific principles for the processing of sensitive data
Article 15: Interconnection of personal data files
Section IV: The Data Subjects" Rights
Article 16: Right to information
Article 17: Right of access
Article 18: Right to object
Article 19: Right of rectification or erasure
Section V: Obligations of the Personal Data Controller
Article 20: Confidentiality obligations
Article 21: Security obligations
Article 22: Storage obligations
Article 23: Sustainability obligations
CHAPTER III – PROMOTING CYBER SECURITY AND COMBATING CYBERCRIME
Section I: Cyber Security Measures to be taken at National Level
Article 24: National cyber security framework
Article 25: Legal measures
Article 26: National cyber security system
Article 27: National cyber security monitoring structures
Article 28: International cooperation
Section II: Criminal Provisions
Article 29: Offences specific to Information and Communication Technologies
Article 30: Adapting certain offences to Information and Communication Technologies
Article 31: Adapting certain sanctions to Information and Communication Technologies
CHAPTER IV: FINAL PROVISIONS
Article 32: Measures to be taken at the level of the African Union
Article 33: Safeguard Provisions
Article 34: Settlement of Disputes
Article 35: Signature, Ratification or Accession
Article 36: Entry into Force
Article 37: Amendment
Article 38: Depository

Figura 7 - Estrutura normativa da Convenção da União Africana sobre Segurança Cibernética e Proteção de Dados Pessoais

São definidas pela Convenção as seguintes infrações: ataques a sistemas informáticos, violação de dados armazenados (alterar, apagar, divulgar) ou em trânsito (interceptação), ofensas relacionadas a conteúdo (pornografia infantil, xenofobismo, racismo, promover por meio de sistemas informáticos a negação ou justificação de atos de genocídio ou praticados por contra a humanidade) e outros crimes comuns cometidos por meio da tecnologia da informação e comunicação (fraude, roubo, abuso de confiança, extorsão).

Nos crimes de conteúdo, a Convenção recomenda garantir que as evidências eletrônicas a serem utilizadas no processo penal sejam coletadas corretamente, obedecendo procedimentos estabelecidos em lei, com a devida identificação de quem a produziu ou divulgou, os métodos utilizados na coleta, clareza na cadeia de custódia, para que, no momento da apresentação em juízo, não reste dúvidas quanto à integridade das evidências e à legalidade em sua obtenção.

Acerca do direito processual penal, a Convenção traz disposições que se aplicam a qualquer infração cometida por meio da tecnologia da informação e comunicação e que deixam vestígios em formato eletrônico. São alguns exemplos de poderes processuais estabelecidos: a interceptação de conteúdo; a coleta, produção e divulgação de evidências eletrônicas; a preservação da integridade de evidências eletrônicas armazenadas em sistemas informáticos, por um prazo máximo de 02 (dois) anos, quando houver suspeita de perda ou alteração, devendo o responsável pela custódia manter o sigilo em relação aos dados.

6.7.3 O acesso transfronteiriço a dados armazenados

Relativamente a possibilidade de acesso a evidências criminais, dispostas em servidores localizados em território de outro Estado Parte, dispõe o artigo 31.3.a):

> State Parties shall take the necessary legislative measures to ensure that where the data stored in a computer system or in medium where computerized data can be stored in the territory of a State Party, are useful in establishing the truth, the court applied to may carry out a search to access all or part of a computer system through another computer system, where the said data are accessible from or available to the initial system (AFRICA UNION, 2014).[102]

[102] Livre tradução da autora: "Os Estados Partes adotarão as medidas legislativas necessárias para assegurar que, quando os dados armazenados num sistema informático ou em outro meio de armazenamento, em território de um Estado Parte, são úteis para esclarecer a verdade, o tribunal requerido pode realizar uma busca para acessar todo ou parte de um sistema de computador através de outro sistema de computador, onde os dados são acessíveis ou disponíveis para o sistema inicial."

Por fim, o Capítulo IV apresenta as cláusulas finais, como o início da vigência, assinatura, ratificação ou adesão, emendas, depósito.

6.8 Acordo entre os Estados Unidos da América e a União Europeia sobre a Proteção dos Dados Pessoais no Âmbito da Prevenção, Investigação, Detecção e Repressão de Infrações Penais

Em 02 de dezembro de 2016, por meio da Decisão (EU) 2016/2220 (CONSELHO DA UNIÃO EUROPEIA, 2016), foi aprovado, em nome da União Europeia, o Acordo entre os Estados Unidos da América e a União Europeia sobre a proteção dos dados pessoais no âmbito da prevenção, investigação, detecção e repressão de infrações penais (EUROPEAN UNION; UNITED STATES OF AMERICA, 2016).

O referido Acordo foi assinado em 2 de junho de 2016, em Amsterdão/Holanda, sob reserva da sua celebração em data posterior, e tem por objetivo assegurar um elevado nível de proteção de dados pessoais e reforçar a cooperação entre os Estados Unidos e a União Europeia e os seus Estados-Membros, em matéria de prevenção, investigação, deteção ou repressão de infrações penais, incluindo o terrorismo (artigo 1º.1).

Desse modo, o referido Acordo estabelece o regime jurídico da proteção de dados pessoais, por ocasião da sua transferência entre os Estados Unidos, por um lado, e a União Europeia e os seus Estados-Membros, por outro (artigo 1º.2).

Embora não constituindo a base jurídica para a transferência de dados pessoais para os Estados Unidos (artigo 1º.3), o Acordo completa, quando necessário, as garantias em matéria de proteção de dados previstas nos acordos, existentes ou futuros, em matéria de transferência de dados ou nas disposições nacionais que autorizam tais transferências.

6.8.1 A estrutura normativa do Acordo

O Acordo está estruturado em 29 (vinte e nove) artigos que disciplinam diversas questões, dentre elas o âmbito de aplicação, a limitação das finalidades e da

utilização, a vedação a transferência ulterior dos dados sem consentimento prévio da autoridade que procedeu à transferência inicial (artigo 7º), manutenção da qualidade e da integridade dos dados (artigo 8º), segurança dos dados e notificações (artigos 9º e 10º), prazos para conservação dos dados (artigo 12º), salvaguardas especiais para o tratamento de dados pessoais que revelem a origem racial ou étnica, as opiniões políticas e as convicções religiosas, a filiação sindical ou informações pessoais relativas à saúde ou à vida sexual (artigo 13º), acesso e retificação de dados pessoais pelo indivíduo sobre o qual a informação se refere (artigos 16º a 19º), cooperação entre autoridades de supervisão (artigos 21 e 22) e outras disposições finais, como prazo de vigência e entrada em vigor.

Não há qualquer previsão relativamente à possibilidade de acesso direto, por parte de um Estado, a dados armazenados em servidores dispostos no território do outro Estado.

6.9 Organização das Nações Unidas

No âmbito das Nações Unidas, não há qualquer tratado internacional que, diretamente, cuide da prevenção ou repressão ao crime cibernético, conforme se constata verificando a *United Nations Treaty Series*, que é a coleção das Nações Unidas sobre tratados internacionais, atualmente composta por centenas de volumes[103]. No entanto, Broadhurst (2006) entende que a Convenção das Nações Unidas contra o Crime Organizado Trasnacional[104] é um importante instrumento jurídico internacional na luta contra a criminalidade organizada no espaço cibernético, e por isso, pode fundamentar a cooperação jurídica entre agências de investigação criminal.

Relativamente ao crime cibernético, o que existe é um amplo estudo, intitulado *Comprehensive Study on Cybercrime* (UNODC, 2013), apresentado em 2013 e elaborado por um grupo intergovernamental de especialistas na área do crime cibernético, o *Expert Group to Conduct a Comprehensive Study on Cybercrime (*doravante denominado Grupo de Especialistas da UNODC), constituído pela

[103] https:// treaties.un.org.

[104] Adotada em Nova York, em 15 de novembro de 2000; entrou em vigor internacional no ano de 2003; instrumento de ratificação depositado pelo Governo brasileiro junto à Secretaria-Geral da ONU, em 29 de janeiro de 2004; promulgada pelo Brasil, por meio do Decreto nº 5.015, de 12 de março de 2004 (BRASIL, 2004).

Comissão de Prevenção ao Crime e Justiça Penal, do Escritório das Nações Unidas sobre Drogas e Crime (UNODC), em atendimento à Resolução nº 65/230 da Assembleia Geral da ONU, na sua 65ª Sessão (ONU, 2010a).

A referida Resolução enfatiza o compromisso assumido pelas Nações Unidas, no campo da prevenção ao crime e da justiça criminal, constante no Parágrafo 42 do *Draft Salvador Declaration on Comprehensive Strategies for Global Challenges: Crime Prevention and Criminal Justice Systems and Their Development in a Changing World* (ONU, 2010b), doravante referido como Declaração de Salvador, que foi o documento final do 12º Congresso das Nações Unidas sobre Prevenção ao Crime e Justiça Criminal, realizado na cidade de Salvador/Bahia, no ano de 2010.

O estudo elaborado pelo grupo de especialistas traz abordagens relativas a legislações nacionais e internacionais, melhores práticas adotadas nos países, assistência técnica e cooperação internacional, coleta de evidências eletrônicas, dentre outras questões, concernentes ao crime cibernético.

A *Doha Declaration on Integrating Crime Prevention and Criminal Justice into the Wider United Nations Agenda to Address Social and Economic Challenges and to Promote the Rule of Law at the National and International Levels, and Public Participation* (ONU, 2015), referida adiante como Declaração de Doha, que foi o documento final do 13º Congresso das Nações Unidas sobre Prevenção ao Crime e Justiça Criminal, realizado em 2015, ressalta a importância de continuidade dos estudos conduzidos pelo Grupo de Especialistas da UNODC, recomendando inclusive alterações em legislações internas e internacionais.

Atendendo ao disposto na Declaração de Doha, a Terceira Sessão do Grupo de Especialistas da UNODC foi realizada em Viena/Áustria, de 10 a 13 de abril de 2017, com a participação de representantes de 90 (noventa) países e de organizações intergovernamentais (*Council of Europe, Economic Community of West African States, European Union, Organization for Security and Cooperation in Europe* (OSCE)), na qualidade de observadores[105], da qual resultou o relatório parcial dos trabalhos (UNODC, 2017), que concluiu pela continuidade do grupo de estudo, devendo os próximos encontros serem dedicados ao aprofundamento das discussões sobre os Capítulos 3 a 8 do citado estudo (sendo o Capítulo 6 relativo à evidência eletrônica e à justiça criminal), com vistas a examinar opções para fortalecer as respostas do

[105] http://www.unodc.org/documents/organized-crime/cybercrime/Cybercrime-April-2017/LoP_CBR.pdf. Acesso em: 06 dez. 2017.

Estado ao crime cibernético, bem como propor novas respostas legais ou de outra natureza.

Ainda durante o evento, foi relatado, por representantes de vários Estados, dificuldades relacionadas à preservação e à coleta de evidências criminais eletrônicas (parágrafo 32). Para reuniões futuras, a computação em nuvem e o acesso transfronteiriço a dados eletrônicos foram escolhidos como temas a serem aprofundados pelo Grupo de Especialistas da UNODC, e debatidos pelos demais participantes, nos termos do parágrafo 47 do Relatório (UNODC, 2017).

6.10 Contribuições à pesquisa

O estudo comparativo das normas internacionais, todas de alcance regional, que disciplinam questões legais sobre segurança da informação digital e combate à criminalidade informática levou à certeza da ausência de regramento jurídico de abrangência ampla internacional, acerca de diligências para a localização, preservação, acesso, produção, busca e apreensão de evidências criminais, armazenadas em servidor de computação em nuvem, em território de Estado estrangeiro, mesmo que se trate de Estado Parte.

As normas internacionais analisadas ao longo dessa seção estão sumarizadas na Tabela 5, que apresenta as características básicas. A Tabela 6 condensa os aspectos observados na análise do tratamento legal conferido a cada instrumento.

Conclui-se, a essa altura, que a regionalização das normas internacionais não favorece ao controle da criminalidade cibernética, que tem natureza transnacional, e não reconhece nem respeita fronteiras físicas de Estado soberano.

Tabela 5 - Características entre as normas internacionais analisadas

Norma	Ano aprovação	Estados membros	Nº artigos
Acordo de Cooperação entre os Estados Membros da Comunidade dos Estados Independentes para o Combate a Infrações Relacionadas à Informação Computacional	2001	9	17
Convenção de Budapeste sobre o Cibercrime	2001	56	48
Acordo entre os Governos dos Estados Membros da Organização para Cooperação de Xangai sobre a Cooperação no Campo da Segurança da Informação Internacional	2009	6	12
Convenção da Liga dos Estados Árabes sobre o Combate às Ofensas contra a Tecnologia da Informação	2010	-	43
Convenção da União Africana sobre Segurança Cibernética e Proteção de Dados Pessoais	2014	55	38

Tabela 6 - Comparação entre requisitos analisados nas normas internacionais

Norma	Acesso Extrater	Preservação	Busca Apreen	Pedido urgência	Requis Direta	Cooperaç autoridade judiciária
Acordo de Cooperação entre os Estados Membros da Comunidade dos Estados Independentes para o Combate a Infrações Relacionadas à Informação Computacional	-	-	-	Sim	-	Art. 4º, a cooperação ocorreráentre autoridades competentes autorizadas previamente
Convenção de Budapeste sobre o Cibercrime	Art. 32	Art. 29	Art. 19	Art. 25, art. 27	Art. 18 (Estado Parte)	Art. 27
Acordo entre os Governos dos Estados Membros da Organização para Cooperação de Xangai sobre a Cooperação no Campo da Segurança da Informação Internacional	-	-	-	-	-	Art. 3º (autoridade central)
Convenção da Liga dos Estados Árabes sobre o Combate às Ofensas contra a Tecnologia da Informação	Art. 40	Art. 23.2	Art. 27	Art. 32.3 Art. 34.8	Art. 28	Art. 34.8
Convenção da União Africana sobre Segurança Cibernética e Proteção de Dados Pessoais	Estado Parte	Art. 31.3.d	Art. 31.3.b	-	-	-

7 O ESTADO DA ARTE SOBRE A COLETA EXTRATERRITORIAL DE EVIDÊNCIAS CRIMINAIS ELETRÔNICAS

O mundo está se tornando cada vez mais globalmente interdependente (SCHULTHEIS, 2015) e a computação em nuvem tem a sua parcela de contribuição, a partir do momento em que viabiliza a implantação de estratégias para garantir aos clientes alta performance de processamento, alta disponibilidade de sistemas e de informações, mobilidade de dados, resiliência, tornando-se uma tendência de modelo a ser adotado por empresas, em diversas áreas.

Ao mesmo tempo, tem sido a computação em nuvem pública um ambiente onde criminosos têm deixado evidências de práticas delituosas, sobretudo na forma de *e-mail*s ou de arquivos armazenados.

Por estratégia técnica ou de negócio, grandes empresas provedoras de nuvem pública têm espalhado *data centers* pelo mundo, sob as mais diversas jurisdições, criando desafios de ordem legal à busca e apreensão de evidências criminais eletrônicas armazenadas nesses ambientes. Estudos destinados a apresentar propostas para enfrentar esses desafios têm se multiplicado.

Nos Estados Unidos, por exemplo, é comum aos acadêmicos sugerirem que a solução está em promover alterações no ECPA, seja para permitir que Estados soberanos requisitem dados diretamente a provedores norte-americanos, seja para criar a versão *on-line* do MLAT, dentre outras.

Na Europa, em nível do Conselho da Europa, foram criados dois grupos de trabalho, no âmbito do Comitê para a Convenção do Cibercrime, dedicados ao estudo dos impactos trazidos pela computação em nuvem para a justiça criminal. São os grupos de trabalho: *Ad-hoc sub-group of the T-CY on jurisdiction and transborder access to data and data flows* (*Transborder group)* e o *Cloud Evidence Group (CEG)*, instituídos em novembro de 2011 (CYBERCRIME CONVENTION COMMITTEE, 2011) e janeiro de 2015 (até dezembro de 2016) (CYBERCRIME CONVENTION COMMITTEE, 2014), respectivamente. Um termo de referência foi elaborado com vistas a orientar a escrita do Segundo Protocolo Adicional à Convenção de Budapeste

sobre o Cibercrime, que disciplinará o acesso a evidências criminais eletrônicas, no ambiente da computação em nuvem.

Nesse capítulo, são indicados os caminhos para onde estão seguindo as diversas propostas que vêm sendo apresentadas, com vistas a superar os desafios trazidos pela tecnologia da informação e comunicação, por ocasião da localização, preservação, produção, acesso, busca e apreensão extraterritorial de evidências criminais eletrônicas, no ambiente de computação em nuvem.

7.1 Os desafios para uma solução jurídica

Antes de iniciar a escrita de qualquer solução jurídica, relativamente à coleta extraterritorial de evidências criminais armazenadas em ambiente de computação em nuvem, Koops e Goodwin (2014) opinam pela observância preliminar de três condições, que precisam ser examinadas.

A primeira refere-se à importância de haver o reconhecimento, por parte da comunidade internacional, acerca dos desafios que a justiça criminal vem sendo obrigada a enfrentar, quando, no curso da persecução penal, é verificada a necessidade de acesso a evidências de crime, localizadas em ambiente de computação em nuvem, em Estado estrangeiro.

Em segundo lugar, os problemas precisam ser identificados e contextualizados, tendo em conta o espaço cibernético mais como "espaço" (uma área mais abstrata) do que como "lugar" (uma área física definida), de maneira a possibilitar às autoridades de justiça criminal o exercício da jurisdição também no espaço cibernético, ao invés de aplicar, exclusivamente, o princípio da territorialidade na determinação da competência para autorizar a produção, o acesso, a busca e apreensão extraterritorial de evidências criminais eletrônicas armazenadas em nuvem compitacional.

Finalmente, as comunidades acadêmicas e os operadores do direito precisam estabelecer uma compreensão mútua, relativamente aos problemas descritos, e, compartilhando a linguagem, os conceitos, os pressupostos inerentes ao assunto, contribuírem conjuntamente para a construção da solução jurídica e/ou técnica para o problema, que atenda aos anseios de todos os envolvidos.

7.2 A necessidade de elaboração de tratado internacional

Não há consenso entre os autores pesquisados acerca da necessidade ou não de edição de norma de direito internacional, com o objetivo de disciplinar a localização, preservação, produção, acesso, busca e apreensão extraterritorial de evidências criminais armazenadas em nuvem.

Sob o argumento de que a elaboração de novo tratado de direito internacional atinente ao tema seria procedimento indesejável e desnecessário, Woods (2016) defende que as regras de conflitos de leis existentes proporcionam mais flexibilidade e adaptabilidade do que um regime de tratados, comparativamente rígido e inflexível.

Por outro lado, Daskal e Woods (2015), Currie (2017), Jaycox e Tien (2015), ONU (UNODC, 2013) entendem que a solução do direito internacional para o problema seria encontrada por meio da edição de um tratado internacional multilateral, de caráter vinculativo.

Defendendo uma posição intermediária, Svantesson (2016a) acredita que a melhor opção seria alterar a Convenção de Budapeste sobre o Cibercrime, disciplinando a matéria. Esse entendimento vem sendo perseguido pelo Conselho da Europa que, em junho de 2017, aprovou Termo de Referência (CYBERCRIME CONVENTION COMMITTEE, 2017) para marcar o início dos trabalhos de elaboração do Segundo Protocolo Adicional à Convenção de Budapeste, relativamente à coleta de evidências criminais armazenadas em ambiente de computação em nuvem.

Existem ainda os autores, como Lin e Fidler (2017), Krishnamurthy (2016), woods (2016), Swire e Kennedy-Mayo (2016), que acreditam estar a solução para o problema na alteração da legislação vigente nos Estados Unidos (mais especificamente no ECPA), que é o país que concentra o maior número de grandes empresas provedoras de computação em nuvem.

As próximas subseções apresentam propostas para enfrentar os desafios descritos ao longo do trabalho.

7.3 A proposta do Segundo Protocolo Adicional à Convenção de Budapeste

A Assembleia Parlamentar do Conselho Europeu, por meio da Recomendação 2077/2015 (COUNCIL OF EUROPE, 2015), relativa à cooperação contra o terrorismo cibernético e outros ataques em larga escala na Internet,

reconheceu a necessidade de aditar a Convenção de Budapeste sobre o Cibercrime, com o objetivo de disciplinar o acesso a evidências criminais eletrônicas, armazenadas em ambiente de computação em nuvem. Esse posicionamento foi ratificado pelo Comitê de Ministros do Conselho da Europa, em 27 de abril de 2016 (COUNCIL OF EUROPE, 2016).

Em 08 de junho de 2017, durante o 17º encontro do Comitê da Convenção de Budapeste sobre o Cibercrime (T-CY), realizado de 07 a 09 de junho, em Estrasburgo/França, foi revisado e aprovado o Termo de Referência (CYBERCRIME CONVENTION COMMITTEE, 2017) que orienta a elaboração do Segundo Protocolo Adicional à Convenção de Budapeste sobre o Cibercrime, relativamente a medidas que otimizam o acesso e a coleta de evidências criminais, armazenadas em ambiente de computação em nuvem.

De acordo com o Termo de Referência, caberá ao T-CY elaborar a minuta do protocolo e o respectivo relatório explicativo, durante o período compreendido entre 01 de setembro de 2017 a 31 de dezembro de 2019, para posterior aprovação pelo Comitê de Ministros.

É esperado que as disposições trazidas pelo protocolo considerem as temáticas identificadas e sugeridas pelo CEG, no relatório *Criminal justice access to electronic evidence in the cloud* (CYBERCRIME CONVENTION COMMITTEE, 2016b), quais sejam:

a) assistência judiciária mútua mais efetiva, incluindo produção de evidências criminais, cooperação direta entre autoridades judiciárias, investigações conjuntas, solicitações na língua inglesa, recursos multimídia (áudio e vídeo) na audiência de vítimas, testemunhas e peritos, e definição de procedimentos para casos de emergência;
b) cooperação direta com provedores de serviço em outras jurisdições;
c) estrutura mais clara e garantias mais robustas nas atuais práticas relativas ao acesso extraterritorial a dados;
d) salvaguardas e requisitos de proteção de dados.

As subseções seguintes descreverão detalhes das temáticas aludidas acima.

7.3.1 Assistência judiciária mútua mais efetiva

No contexto da investigação criminal no espaço cibernético, o MLAT é o instrumento mais utilizado para um Estado a requisitar a outro Estado dados armazenados em servidores que estejam sob a jurisdição deste último.

Em relatório apresentado pelo T-CY, em dezembro de 2014, foi exposto que, embora os MLATs constituíssem importantes medidas de combate ao crime cibernético, na prática mostravam-se ineficientes, visto que disciplinavam procedimentos complexos, morosos e burocráticos. O elevado tempo de resposta, que poderia chegar a 24 (vinte e quatro) meses, motivou o abandono de muitas investigações (CYBERCRIME CONVENTION COMMITTEE, 2014).

Por conseguinte, foram apresentadas propostas de alterações nos procedimentos constantes nos MLATs, considerando, como ponto de partida, os três tipos de dados mais comumente procurados em investigação criminais no espaço cibernético, quais sejam:

a) sobre o usuário, que identificam o assinante do serviço de Internet;
b) sobre o tráfego de dados, que registram as atividades do usuário;
c) sobre o conteúdo das comunicações, como o texto de *e-mail*s, imagens, vídeos, documentos e outros arquivos.

Essa diferenciação é relevante, visto que pode indicar a autoridade competente para requisitar os dados, o procedimento a ser adotado, as situações que a autorizam, bem como o tipo de ordem a ser expedida. No Brasil, por exemplo, o Marco Civil da Internet considera essa distinção para estabelecer como deve ocorrer a quebra do sigilo dos dados armazenados. Assim, nos termos do § 2º do art. 10, o conteúdo das comunicações privadas somente poderá ser disponibilizado mediante ordem judicial. Por outro lado, o acesso a dados cadastrais que informem qualificação pessoal, filiação e endereço poderá ser requerido diretamente por autoridade administrativa (autoridade de polícia judiciária, por exemplo) que detenha competência legal para fazê-lo (§ 3º do art. 10).

A primeira mudança considerada na elaboração do protocolo adicional é a possibilidade de simplificar as regras para os pedidos de assistência judiciária mútua, relativas às informações de usuários investigados. A natureza desses dados é menos sensível às regras de proteção à privacidade do que os conteúdos de comunicações ou os registros de tráfego e os registros de atividade dos usuários. Ademais, os dados

relativos à identificação do investigado são os mais comumente requisitados na fase inicial de uma investigação criminal (CYBERCRIME CONVENTION COMMITTEE, 2016b).

A segunda proposta refere-se à possibilidade de adotar, no âmbito da investigação criminal no espaço cibernético, a Decisão Europeia de Investigação (DEI), que é um instrumento utilizado para orientar a coleta de evidências criminais em Estado estrangeiro, que foi instituído pela Diretiva 2014/41/EU, do Parlamento Europeu e do Conselho, de 3 de abril de 2014 (PARLAMENTO EUROPEU; CONSELHO DA UNIÃO EUROPEIA, 2014).

A terceira proposta refere-se à possibilidade de estabelecer cooperação direta entre autoridades judiciárias, seguindo o disposto no artigo 4º do Segundo Protocolo Adicional à Convenção Europeia de Auxílio Judiciário Mútuo em Matéria Penal do Conselho da Europa[106] (COUNCIL OF EUROPE, 2001c), e do artigo 6º da Convenção sobre Assistência Mútua em Matéria Penal entre os Estados-Membros da União Europeia[107] (COUNCIL OF EUROPE, 2000). A Convenção de Budapeste sobre o Cibercrime, no artigo 27.9.a, dispõe sobre a possibilidade excepcional, apenas em caso de urgência, de autoridades judiciárias da Parte requerente podem enviar diretamente às suas homólogas da Parte requerida os pedidos de auxílio mútuo ou as comunicações que lhes digam respeito, devendo também encaminhar uma cópia às autoridades centrais da Parte requerida, por intermédio da autoridade central da Parte requerente.

---

[106] Artigo 4º.1: Os pedidos de auxílio judiciário mútuo, bem como as informações espontâneas, serão enviados por escrito pelo Ministério da Justiça da Parte requerente ao Ministério da Justiça da Parte requerida e reenviados pelas mesmas vias. No entanto, podem ser enviados diretamente pela autoridade judiciária da Parte requerente à autoridade judiciária da Parte requerida e reenviados pela mesma via. Artigo 4º.3: Os pedidos de auxílio judiciário mútuo relativos aos processos previstos no nº3 do artigo 1º da presente Convenção podem igualmente ser enviados diretamente pela autoridade administrativa ou judiciária da Parte requerente à autoridade administrativa ou judiciária da Parte requerida, consoante o caso, e reenviados pela mesma via. Artigo 4º 5: Os pedidos previstos no nº 1 do artigo 13º da presente Convenção podem ser enviados diretamente pelas autoridades judiciárias em causa ao serviço competente da Parte requerida e as respostas podem ser enviadas diretamente por esse serviço. Os pedidos previstos no nº 2 do artigo 13º da presente Convenção serão enviados pelo Ministério da Justiça da Parte requerente ao Ministério da Justiça da Parte requerida.

[107] Artigo 6º.1: Os pedidos de auxílio judiciário mútuo e o intercâmbio espontâneo de informações a que se refere o artigo 7.º serão feitos por escrito, ou por quaisquer meios susceptíveis de dar origem a um registo escrito em condições que permitam ao Estado membro receptor determinar a sua autenticidade. Estes pedidos serão feitos diretamente entre autoridades judiciárias com competência territorial para os fazer e executar e a respectiva resposta será feita pela mesma via, salvo disposição em contrário do presente artigo. [...].

A quarta proposta refere-se à viabilidade de investigação conjunta, em caso de crimes cibernéticos transnacionais, seguindo o modelo constante no artigo 20 do Segundo Protocolo Adicional à Convenção Europeia de Auxílio Judiciário Mútuo em Matéria Penal do Conselho da Europa (COUNCIL OF EUROPE, 2001c), uma vez que a Convenção de Budapeste sobre o Cibercrime não dispõe sobre a questão.

A padronização do idioma inglês, no texto das requisições, constitui objeto da quinta proposta, que tem por finalidade otimizar o tempo de resposta. Assim, pelo menos as solicitações de preservação de evidências eletrônicas ou aquelas relativas à identificação do usuário, devem, preferencialmente, ser elaboradas no idioma inglês, de maneira a evitar imprecisões nas traduções, bem como custo e tempo adicionais na validação de possíveis inconsistências.

A sexta proposta é a previsão de videoconferência nas audiências de vítimas, testemunhas e peritos, a exemplo do constante nos artigos 9 e 10 do Segundo Protocolo Adicional à Convenção Europeia de Auxílio Judiciário Mútuo em Matéria Penal do Conselho da Europa (COUNCIL OF EUROPE, 2001c).

A possibilidade dos provedores de serviço Internet responderem diretamente a Estado estrangeiro requisições em casos de emergência é a sétima proposta. Com exceção de dois países (Japão e Estados Unidos), nenhum outro possui uma legislação que autorize um provedor de serviço Internet, sediado em seu território, divulgar dados à autoridade competente de Estado estrangeiro, em situações de emergência, sem a necessidade de formalizar assistência judiciária mútua (CYBERCRIME CONVENTION COMMITTEE, 2016a). No Brasil, não há previsão nesse sentido no Marco Civil da Internet ou em seu Regulamento (BRASIL, 2016).

7.3.2 Cooperação direta com provedores de serviço em outras jurisdições

A cooperação direta entre autoridades de persecução criminal e provedores de serviço de computação em nuvem é prevista apenas nas requisições por informações pessoais de usuários em caso de emergência, e para requerer a preservação de evidências de crimes.

O artigo 18.1 da Convenção de Budapeste sobre o Cibercrime convida as Partes a investir as suas autoridades competentes de poderes necessários para obrigar uma pessoa que se encontre em seu território a fornecer os dados

armazenados especificados (artigo 18.1.a), ou um fornecedor de serviços que ofereça os seus serviços no território a prestar informações relativamente aos usuários dos serviços (artigo 18.1.b).

A regra constante no artigo 18.1. b. foi utilizada no caso Reino da Bélgica *versus* Yahoo! Inc.[108], quando, em 1 de dezembro de 2015, o Tribunal de Cassação[109] do Reino da Bélgica entendeu que, em razão de o provedor oferecer serviços no território do país, adotando inclusive o domínio *yahoo.com.be*, usando o idioma local, apresentando publicidades locais, o direito interno seria suficiente para obrigar a empresa a fornecer os dados relativos a usuário (cidadão belga), investigado por prática de crime, sem que fosse necessário utilizar-se da cooperação internacional com os Estados Unidos para obtê-los, mesmo que a empresa não mantenha representação comercial no país. A Yahoo!.Inc foi multada, por se recusar a cooperar com a polícia belga e por se negar a entregar informações ao Ministério Público da cidade de Termonde/Bélgica. Ademais, entenderam as autoridades belgas que os

[108] A Yahoo!, Inc. está sediada na cidade de Sunnyvale, Califórnia, Estados Unidos.

[109] O sistema jurídico belga é um sistema de tradição civilista que engloba um conjunto de normas codificadas, aplicadas e interpretadas pelos juízes. A Bélgica está dividida em cinco grandes zonas judiciais, correspondentes às áreas de jurisdição territorial dos cinco tribunais de recurso (*cour d'appel/hof van beroep*): Bruxelas, Liège, Mons, Gante e Antuérpia. Estas áreas subdividem-se em comarcas (*arrondissements judiciaires/gerechtelijke arrondissementen*), cada uma das quais tem um tribunal de primeira instância (*tribunal de première instance/rechtbank van eerste aanleg*). Existem 12 (doze) comarcas no país. A comarca de Bruxelas tem dois tribunais de primeira instância, um neerlandófono e outro francófono. Cada comarca tem 9 tribunais de trabalho (*tribunaux du travail/arbeidsrechtbanken*) e 9 tribunais de comércio (*tribunaux de commerce/rechtbanken van koophandel*). As comarcas, por sua vez, dividem-se em cantões judiciais (*canton judiciaire/gerechtelijk kanton*), cada um dos quais com um julgado de paz (*justice de paix/vredegrerecht)*. Existem 187 cantões judiciais em todo o país**.** Cada uma das dez províncias, bem como a circunscrição administrativa de Bruxelas-Capital, dispõe de um tribunal penal (*cour d'assises/hof van assisen*). O tribunal penal não é um tribunal permanente. Constitui-se apenas quando lhe é presente um arguido para julgamento. A natureza e a gravidade da infração, ou a natureza do litígio, bem como a importância dos montantes em causa, determinam o tribunal competente para cada processo. Os tribunais estão organizados de acordo com uma estrutura hierarquizada. A estrutura dos tribunais é a seguinte: 4. Tribunal de Cassação; 3. Tribunais de recurso, Tribunais de trabalho, Tribunais de júri; 2. Tribunais de primeira instância, Tribunais de trabalho, Tribunais de comércio; 1. Julgados de Paz, Tribunais de polícia. Em instância de apelação, os juízes deliberam uma segunda e derradeira vez sobre a matéria de fundo, decidindo a causa a título definitivo. Às partes resta ainda, porém, a hipótese de apelar para o Tribunal de Cassação. O Tribunal de Cassação não constitui uma terceira instância ou um terceiro nível de jurisdição. O Tribunal de Cassação não examina os factos do processo que lhe é submetido, limitando-se a controlar o respeito pela legalidade. Para além dos tribunais supramencionados, existem na Bélgica dois outros órgãos jurisdicionais, com funções de controle: o Conselho de Estado e o Tribunal Constitucional. O Conselho de Estado é uma alta jurisdição administrativa encarregada de controlar a administração. É chamado a intervir quando algum cidadão considera que a administração desrespeitou a lei. Ao Tribunal Constitucional compete assegurar a constitucionalidade das leis, dos decretos e das ordenações e fiscalizar a repartição correta das competências entre os poderes públicos na Bélgica (EUROPEAN JUSTICE, 2017).

dados solicitados se referiam basicamente à identificação do usuário, cuja divulgação é permitida, nos termos da legislação norte-americana (*18 U.S.C Chapter 121* - §§ 2701 a 2712). Na argumentação, a empresa provedora de serviços Internet alegou ter entendido que a expressão "*any other personal details or information that might lead to the identification of the account user(s)"*[110], constante na requisição, poderia referir-se a dado de conteúdo (CURRIE, 2017; CYBERCRIME CONVENTION COMMITTEE, 2016a; VERGNOLLE, 2016; BELGIË, 2015).

A definição de um regime separado de acesso a informações de usuários, em consonância com o artigo 18, contribuiria de forma significativa para tornar mais eficiente o processo de MLAT, em relação à investigação de crime cibernético. Nesse sentido, o CEG sugere interpretação extensiva ao artigo 18.1.b para possibilitar a autoridade competente de uma Parte solicitar informações de usuários a provedor de Internet que ofereça serviço em seu território, independentemente de onde a informação seja armazenada ou de onde o provedor de serviço esteja sediado ou mantenha representação comercial (CYBERCRIME CONVENTION COMMITTEE, 2016b). Nesse sentido, de acordo com o Termo de Referência (CYBERCRIME CONVENTION COMMITTEE, 2017), espera-se que o Protocolo:

a) defina procedimentos e condições para permitir a cooperação direta com provedores de serviço de nuvem em outras jurisdições, para as requisições de informações sobre usuários, garantindo a admissibilidade dos dados recebidos nos processos criminais;
b) estabeleça base jurídica para os pedidos de preservação de evidências a provedores de serviço estrangeiros;
c) determine as condições de emergência que autorizam a cooperação direta com prestadores de serviços localizados em jurisdições estrangeiras.

7.3.3 Estruturas explícitas e garantias robustas para o acesso extraterritorial a evidências criminais em nuvem

Nessa questão, é esperado que sejam consideradas melhorias nas atuais práticas de coleta de evidências criminais armazenadas em nuvem, por meio da edição de normas internacionais, assegurando que sejam superados os desafios

[110] Livre tradução da autora: "qualquer outra informação ou detalhes que permitam a identificação da conta do usuário(s)".

inerentes ao conflito de leis vigentes em Estados soberanos distintos (CYBERCRIME CONVENTION COMMITTEE, 2016b).

Como exemplo dessa diversidade normativa, alguns aspectos concernentes à legislação europeia e norte-americana são conflitantes, o que dificulta a adoção das regras do artigo 18.1.b. A proteção de dados, a notificação do usuário, as requisições de emergência, dentre outras, são exemplos de questões que precisam ser harmonizadas.

7.3.4 Salvaguardas e requisitos de proteção de dados.

A elaboração do protocolo adicional à Convenção de Budapeste sobre o Cibercrime deverá considerar as normas vigentes na União Europeia, relativamente à proteção de dados pessoais (CYBERCRIME CONVENTION COMMITTEE, 2016b). Até setembro de 2017, encontravam-se em vigor os seguintes instrumentos:

a) Convenção do Conselho da Europa para a Proteção das Pessoas em Relação ao Processamento Automático de Dados[111] - ETS nº 108 (COUNCIL OF EUROPE, 1981);
b) Recomendação R (87)15 do Comitê de Ministros do Conselho da Europa, que regulamenta o uso de dados pessoais pela polícia[112] (COUNCIL OF EUROPE, 1987);
c) Diretiva da União Europeia 95/46/EC, sobre a proteção de pessoas singulares no que diz respeito ao tratamento de dados pessoais e a livre circulação desses dados[113] (PARLAMENTO EUROPEU; CONSELHO DA UNIÃO EUROPEIA, 1995);
d) Decisão-Quadro 2008/977/JAI, de 27 de novembro de 2008, relativa à proteção dos dados pessoais tratados no âmbito da cooperação policial e judiciária em matéria penal[114] (CONSELHO DA UNIÃO EUROPEIA, 2008);

---

[111] Livre tradução da autora para: *Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data* (ETS 108).
[112] *Council of Europe Recommendation "R(87)15 Regulating the use of personal data in the police sector*".
[113] *European Union Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data*. Será revogada pelo Regulamento de Proteção Geral de Dados da EU, a partir de 25 de maio de 2018.
[114] *European Union Framework Decision 2008/977/JHA of the European Union on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters*. Será revogado pela Diretiva (UE) 2016/680, do Parlamento Europeu e do Conselho, de 27 de abril de 2016, a partir de 6 de maio de 2018.

e) Diretiva 2002/58/CE, relativa ao tratamento dos dados pessoais e à tutela da vida privada no setor das comunicações eletrônicas[115] (PARLAMENTO EUROPEU; CONSELHO DA UNIÃO EUROPEIA, 2002).

Ainda devem ser considerados os novos instrumentos cujo início da vigência está previsto para maio de 2018. São eles:

a) Regulamento Geral sobre a Proteção de Dados da União Europeia[116], aprovado pelo Parlamento Europeu em 14 de abril de 2016 (PARLAMENTO EUROPEU; CONSELHO DA UNIÃO EUROPEIA, 2016b), devendo entrar em vigor em 25 de maio de 2018, e que revoga a Diretiva 95/46/CE;
b) Diretiva (UE) 2016/680, do Parlamento Europeu e do Conselho, de 27 de abril de 2016 (PARLAMENTO EUROPEU; CONSELHO DA UNIÃO EUROPEIA, 2016a), relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais pelas autoridades competentes para efeitos de prevenção, investigação, detecção ou repressão de infrações penais ou execução de sanções penais, e à livre circulação desses dados, e que revoga a Decisão-Quadro 2008/977/JAI do Conselho.

De acordo com o novo Regulamento Geral sobre a Proteção de Dados (PARLAMENTO EUROPEU; CONSELHO DA UNIÃO EUROPEIA, 2016b), as empresas de tratamento de dados que operam na União Europeia estarão sujeitas às normas de proteção de dados vigentes no âmbito da União Europeia (artigo 22º).

Nesse sentido, o Termo de Referência recomenda que o protocolo adicional à Convenção de Budapeste sobre o Cibercrime discipline as requisições aos provedores de serviço situados em terceiros países, observando as previsões contida no artigo 39 da Diretiva (UE) 2016/680, bem como as solicitações oriundas desses países, quando o provedor de serviço esteja situado em território europeu.

Por fim, outra questão que se espera ser tratada no protocolo adicional está relacionada à obrigatoriedade de notificar os usuários acerca dos pedidos legais por quebra de sigilo. De acordo com o CEG, a notificação do cliente não é um requisito constante nas normas europeias de proteção de dados, diferentemente do disposto

---

[115] *E-Privacy Directive* 2002/58/EC.

[116] *EU General Data Protection Regulation*. Regulamento (UE) 2016/679, do Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados).

no ECPA, dos Estados Unidos. Segundo o grupo, predomina o entendimento de que essa revelação pode comprometer a investigação, além de criar riscos aos policiais, a membros do Ministério Público ou a qualquer agente público ou terceira pessoa envolvida na persecução criminal (CYBERCRIME CONVENTION COMMITTEE, 2016b).

7.3.5 Outras medidas oriundas do Conselho da Europa

Ainda em 08 de junho de 2017, quando foi revisado e aprovado o Termo de Referência para a elaboração do Segundo Protocolo Adicional à Convenção de Budapeste sobre o Cibercrime, a Comissão Europeia apresentou aos Ministros da Justiça da Europa propostas de implementações práticas imediatas e alterações legislativas, com vistas a otimizar o processo de busca e apreensão de evidências criminais armazenadas em ambiente de computação em nuvem (EUROPEAN COMMISSION, 2017).

As medidas de ordem prática versam sobre o aperfeiçoamento da cooperação entre autoridades judiciárias e sobre as possíveis contribuições dos provedores de serviço Internet no combate ao crime cibernético, ao terrorismo ou a qualquer outra modalidade criminosa intensiva no uso da tecnologia da informação e comunicação. Um exemplo dessas medidas é a recomendação da Comissão para aprimorar a segurança das comunicações entre os agentes públicos.

Outra medida, sugerida no âmbito da relação entre a Europa e os Estados Unidos, é o patrocínio de treinamento de autoridades europeias em assuntos de interesse na legislação norte-americana.

Em relação aos provedores de serviço Internet, espera-se que a cooperação voluntária com as autoridades europeias seja o principal canal para a obtenção de dados não relacionados a conteúdo. Assim, as propostas caminham no sentido de:

a) definir pontos de contato únicos nos Estados-Membros, de forma a garantir correção nas requisições e criar relação de confiança com os provedores;
b) rever as políticas dos provedores relativas às divulgações de dados solicitados;
c) implantar programas de intercâmbio e treinamento profissional para policiais e autoridades judiciárias, com ênfase nas melhores práticas a serem implementadas na cooperação com provedores norte-americanos;

d) desenvolver um portal *on-line* no sítio eletrônico da União Europeia, com vistas a prestar suporte às investigações no espaço cibernético.

Para respaldar as medidas propostas, a Comissão Europeia sugere alterações normativas, cujas propostas encontram-se no Termo de Referência aludido acima, enfatizando os seguintes requisitos:

a) permitir que autoridades europeias possam requisitar informações diretamente a provedores de serviço de computação em nuvem, autorizando-os inclusive a responder solicitações de outros Estados Parte, independentemente de onde esteja sediada a empresa;
b) considerar a possibilidade de acesso direto à evidência eletrônica, respeitando as normas de proteção à privacidade e aos direitos fundamentais vigentes no âmbito da União Europeia, caso haja dificuldade ou até mesmo impossibilidade de contato com a empresa provedora de serviços Internet;
c) promover alterações na legislação em vigor no âmbito da União Europeia, que seriam suplementadas por meio da edição de novos tratados internacionais ou pela expansão de tratados multilaterais existentes, em particular a Convenção de Budapeste sobre Cibercrime.

7.4 Requisição de evidências criminais diretamente a provedor de computação em nuvem

Diferentes propostas vêm sendo apresentadas para enfrentar os desafios concernentes ao acesso a evidências criminais eletrônicas, quando armazenadas em servidor de computação em nuvem, localizado no território de terceiro Estado, não envolvido na prática do delito investigado.

O poder das autoridades investidas na persecução criminal de requisitarem a divulgação de qualquer dado digital (seja conteúdo das comunicações, sejam dados pessoais ou registros de atividades do usuário) diretamente a provedores de Internet, independentemente de onde estejam sediados ou de onde mantenham representação comercial, sem a necessidade de formalizar o pedido por meio de MLAT, é o objeto de estudo na presente subseção.

Para Daskal e Woods (2015) e Currie (2017), a escrita de um tratado internacional que normatize essa possibilidade deverá considerar os seguintes requisitos:

a) acesso célere e recíproco aos dados;

b) proteção aos direitos humanos;

c) transparência e responsabilização.

Segundo os autores, o rápido acesso aos dados poderá ser provido com alterações no *Electronic Communications Privacy Act,* dos Estados Unidos, no sentido de permitir que Governos estrangeiros possam requisitar diretamente a provedores de serviços Internet, baseados em território norte-americano. Nesse caso, o Estado requerente deverá provar que tem interesse legítimo sobre o fato criminal investigado, que os envolvidos (vítima e suspeito) não sejam cidadãos norte-americanos ou residentes legais nos Estados Unidos, bem como os envolvidos se encontrem fora da jurisdição daquele país.

Nesses termos, uma autoridade policial brasileira, por exemplo, que esteja investigando um crime grave, ocorrido em território nacional, praticado por brasileiro e contra brasileiro, residente ou domiciliado no Brasil, cujas evidências eletrônicas relevantes da prática delituosa, como *e-mail*s ou arquivos de imagens, encontram-se armazenadas em território norte-americano, poderá requisitá-las diretamente ao provedor de serviço de computação em nuvem sediado nos Estados Unidos, sem a necessidade de formalizar o pedido através de um MLAT. Em sentido inverso, a reciprocidade com o país deverá ser respeitada.

Outra questão a ser considerada é, se o Estado requisitante promove e respeita os direitos humanos. Nesse sentido, deverá ser observada a importância conferida pelo Estado, relativamente à inviolabilidade da intimidade, da vida privada, da honra e da imagem das pessoas, bem como a proteção à privacidade dos dados digitais, disposta em lei, além de outras disposições não relacionadas à privacidade, como a proibição à tortura, a tratamentos cruéis e desumanos, dentre outros.

Em termos gerais, a escrita de um tratado internacional relativamente ao acesso direto da autoridade de persecução criminal de país estrangeiro a provedores de serviço de computação em nuvem deverá considerar os seguintes requisitos:

a) a autorização para o acesso às evidências criminais eletrônicas deverá ser emitida por meio de mandado judicial ou ordem equivalente, demonstrada justa causa e gravidade do fato;

b) demonstrar que a informação requisitada é relevante à investigação criminal, por constituir forte indício de que o crime foi, está sendo ou será cometido;
c) o pedido deverá ser individualizado, constando especificamente informações sobre o indivíduo investigado, a conta ou o dispositivo a ser devassado, bem como o período e o escopo dos dados a serem pesquisados;
d) o fato investigado deve estar subsumido à norma penal vigente no Estado requisitante, devendo o pedido ao provedor de serviço de computação em nuvem incluir uma breve descrição da conduta, a tipificação penal correspondente no direito penal pátrio e a indicação da autoridade legal para o pedido;
e) a conduta investigada deve ser punível com, pelo menos, 01 (um) ano de encarceramento;
f) o Estado requisitante obriga-se a informar o investigado acerca da devassa em seus dados, a menos que esse aviso venha comprometer a investigação ou colocar em risco a vida e a integridade física de terceiro;
g) o pedido não pode ser usado com o intuito de limitar a livre manifestação do pensamento do investigado;
h) o Estado requisitante deverá estabelecer mecanismos para minimizar a coleta de dados, restringindo-a, unicamente, a dados relevantes à investigação e quando não seja possível a evidência ser obtida por outros meios menos invasivos;
i) a autorização judicial pode ser dispensada nos casos em que haja risco de morte ou de lesão corporal grave.

Por fim, devem ser estabelecidos mecanismos de auditoria e transparência, incluindo os respectivos relatórios, além das sanções adotadas, em caso de descumprimento às normas.

A fiscalização e a auditoria nos Estados requisitantes terão por objetivo principal zelar pela observância às exigências legais, por ocasião do pedido de acesso a evidências eletrônicas de crime, sem violar a soberania estatal.

Os relatórios de transparência deverão ser periódicos e apresentar o resumo das requisições realizadas, atendidas e não atendidas. Serão elaborados tanto pelo

Estado requisitante quanto pelas empresas provedoras de serviços de computação em nuvem.

Em caso de violação aos requisitos apresentados, o Estado requisitante pode perder o direito de solicitar diretamente ao provedor de serviço de computação em nuvem, em terceiro Estado. Caso a violação seja por parte da empresa, essa responderá perante as leis norte-americanas.

Recentemente, algumas das proposições acima, apresentadas por Daskal e Woods (2015) e ratificadas por Currie (2017), passaram a integrar os termos do Acordo entre os Estados Unidos da América e a União Europeia sobre a Proteção dos Dados Pessoais no Âmbito da Prevenção, Investigação, Detecção e Repressão de Infrações Penais (EUROPEAN UNION; UNITED STATES OF AMERICA, 2016), assinado em 02 de junho de 2016 e, atualmente, em vigor.

Jaycox e Tien (2015) criticaram o modelo proposto por Daskal e Woods (2015), afirmando que eventuais mudanças na legislação norte-americana poderiam comprometer o rigor conferido à proteção da privacidade dos dados armazenados nos Estados Unidos, sob o respaldo do ECPA. Ademais, estabelecer subjetivamente que países estariam autorizados a requerer diretamente a provedores norte-americanos, com base no nível de respeito aos direitos humanos, seria dividir o mundo entre os Estados “bons” e os Estados “maus”, na Internet.

Os autores propuseram que, antes de alterar a legislação norte-americana ou editar tratado internacional, primeiramente dever-se-ia adotar outras providências, como:

a) reformular o processo do MLAT;
b) promover maior cooperação entre as agências de investigação criminal instaladas em diversos países;
c) capacitar os agentes de investigação criminal;
d) uniformizar as causas prováveis que justifiquem a violação do sigilo dos dados dos usuários;
e) reestruturar o Departamento de Justiça dos Estados Unidos e capacitar seus os agentes, de forma a proporcionar celeridade às respostas.

Em última instância, caso tenha sido identificada a necessidade de promover alterações na legislação vigente nos Estados Unidos, bem como de editar novo regime jurídico em nível internacional, os autores recomendam considerar a proteção prevista pela Quarta Emenda à Constituição dos Estados Unidos e a possibilidade de aviso

prévio ao investigado, relativamente à violação do sigilo dos seus dados, por parte do Governo requisitante.

No mesmo sentido de Daskal e Woods (2015) e Currie (2017), acerca da possibilidade de contato direto entre as autoridades de persecução criminal e os provedores de serviço de computação em nuvem, Svantesson (2016a) apresenta um conjunto de medidas, agrupadas em 03 (três) etapas, para subsidiar a elaboração de um documento internacional, seja um código de conduta policial ou um tratado de caráter vinculante, salvaguardando os direitos e os interesses dos indivíduos, dos provedores de computação em nuvem e dos Estados envolvidos. As etapas aludidas são:

a) etapa 1: envolvimento de diversos atores (*stakholders*);
b) etapa 2: restrições fundamentais;
c) etapa 3: restrições não fundamentais.

De acordo com a etapa 1, para ser bem sucedida, a estrutura normativa precisa ser elaborada conjuntamente pelos diversos atores (*stakholders*) interessados na questão, quais sejam: Governos, agências de investigação criminal, provedores de serviço de computação em nuvem, organizações internacionais (por exemplo, o Conselho da Europa, a ONU), estudiosos do Direito e da Ciência da Computação.

A etapa 2 trata das restrições fundamentais que devem ser consideradas na edição do novo documento, com vistas a facilitar o acesso das autoridades de persecução criminal à evidência criminal, armazenada em ambiente de computação em nuvem, por meio de contato direto com os provedores de serviço. São elas:

a) os provedores têm o dever de auxiliar as ações legais desenvolvidas pelas agências de investigação criminal;
b) os provedores têm o dever de respeitar os direitos fundamentais (como o direito à privacidade) de seus clientes;
c) os provedores têm o dever de respeitar os direitos fundamentais (como a privacidade, a honra, a imagem) dos indivíduos que não são seus clientes;
d) os provedores não podem cumprir ordens conflitantes;
e) a soberania territorial absoluta é incompatível com a Internet e a computação em nuvem;
f) em relação à jurisdição, as medidas de persecução criminal não podem ser tratadas sob as regras estritas concernentes à jurisdição de execução;

g) as normas devem regulamentar o acesso aos dados, considerando o quão sensível é esse dado no contexto da privacidade;
h) é necessária a distinção entre dados armazenados e dados em trânsito;
i) deve ser considerado o direito vigente no Estado com o qual o provedor mantém forte relação (como o Estado que sedia a empresa provedora), na avaliação do cumprimento dos deveres que lhe cabem, bem como por ocasião de conflito de leis entre o Estado requisitado e o Estado requisitante;
j) evidências criminais eletrônicas armazenadas em Estado estrangeiro frequentemente são relevantes a investigações de crimes domésticos;
k) a inviolabilidade absoluta do anonimato prejudica a localização do sujeito ativo do crime e a determinação de sua nacionalidade;
l) os provedores devem manter relatórios periódicos de transparência, com informações relativas à quantidade de requisições realizadas e atendidas, origem dessas requisições, objeto requerido etc;
m) os provedores devem ser transparentes quanto à forma de cooperação com as agências de investigação criminal, explicitando-a nos termos de privacidade;
n) os provedores devem informar ao usuário investigado acerca da violação da privacidade de seus dados, exceto quando houver motivo justificável para não o fazer;
o) a urgência para o acesso aos dados depende da análise do caso em concreto;
p) indivíduos têm interesse na privacidade de seus dados;
q) indivíduos têm interesse na prevenção, na investigação e na repressão ao crime;
r) as vítimas de crime têm particular interesse na prevenção, na investigação e na repressão ao crime;
s) os Estados têm o dever de auxiliar as ações legais de agências de investigação criminal de outros países;
t) os Estados têm o dever de controlar as ações criminosas dentro de sua jurisdição, de forma a prevenir que seus efeitos sejam sentidos internamente ou em Estado estrangeiro;
u) os Estados têm o dever de respeitar os direitos humanos;

v) nem sempre é possível precisar a localização física do servidor onde os dados se encontram armazenados;
w) no contexto da computação em nuvem, os dados são frequentemente distribuídos por mais de um servidor, seja como cópia de segurança (*backup*) ou como partes de uma divisão programada;
x) devem ser estabelecidas salvaguardas processuais que assegurem a legitimidade da requisição de dados;
y) a eficácia de qualquer norma internacional que discipline o acesso às evidências criminais eletrônicas, por meio de contato direto com os provedores, depende da adesão dos países.

A etapa 3 alude às restrições que, embora não sejam fundamentais, devem ser consideradas na elaboração do documento. São elas:

a) é preferível alterar os instrumentos existentes (como a Convenção de Budapeste sobre o Cibercrime) a elaborar um novo;
b) o consenso é mais facilmente conseguido em grupos de Estados com abordagens legislativas semelhantes e entre os quais existe um certo grau de confiança na cooperação (ex: União Europeia);
c) as regras para as agências de investigação criminal não devem ser as mesmas aplicadas aos serviços de inteligência;
d) a balcanização implica em custo, inclusive para intermediários, e perda de eficiência para os usuários;
e) a iniciativa unilateral de agências de investigação criminal para obter acesso direto aos dados é inadequada, como estratégia de longo prazo;
f) a eficiência da cooperação entre as agências de investigação criminal e terceiros vai depender, em parte, da promoção de uma cultura de cooperação;
g) investir na coordenação entre leis processuais, visto que a harmonização do direito substantivo é um processo mais demorado;
h) definir os tipos penais graves que permitiriam a requisição de evidências criminais eletrônicas diretamente ao provedor de serviço de computação em nuvem;
i) o procedimento de coleta de evidências criminais eletrônicas pode influenciar na valoração das mesmas nos tribunais.

Em concordância com Daskal (2016b), conclui o autor que é importante fomentar uma solução equilibrada para o problema, uma vez que a privacidade absoluta e o acesso irrestrito aos dados pelas agências de investigação criminal são dois extremos não desejados por qualquer dos envolvidos. Outrossim, caso uma solução não seja definida, é provável que as agências de investigação criminal, cada vez mais, invistam em ações unilaterais que autorizem o acesso às evidências criminais armazenadas no ambiente de computação em nuvem, sob o amparo de tribunais superiores, como demonstrado nos casos Microsoft Corporation *versus* Estados Unidos, Reino da Bélgica *versus* Yahoo!. Inc, dentre outros. Essas ações unilaterais são inadequadas como estratégia de longo prazo.

No mesmo sentido que os autores acima, Krishnamurthy (2016) propõe alterações no ECPA para permitir que os provedores de nuvem norte-americanos respondessem diretamente a Governos estrangeiros que solicitassem evidências criminais, armazenadas em território norte-americano. Reciprocamente, o Governo norte-americano pode requisitar diretamente ao provedor de serviço de nuvem, localizado no território do Estado requisitante.

De acordo com a estrutura apresentada por Krishnamurthy (2016), os provedores de computação em nuvem, sediados nos Estados Unidos, poderiam responder diretamente aos Governos estrangeiros, sem a necessidade de obedecer ao rito determinado pelo MLAT, caso o Governo dos Estados Unidos tenha reconhecido o Governo requisitante como respeitante de direitos, e que a requisição dos dados seja realizada em conformidade com a lei, obedecendo aos seguintes requisitos:

a) a autorização para o fornecimento dos dados armazenados seja emitida por magistrado competente ou por autoridade com poderes legais, do Estado requisitante;
b) a garantia, pelo Estado requisitante, de que o investigado não é cidadão norte-americano nem residente nos Estados Unidos;
c) demonstrar que a informação a ser obtida é relevante para a investigação de crime grave;
d) a notificação, pelo Estado requisitante, do usuário investigado acerca da violação do sigilo de seus dados;

e) limitação do escopo das requisições em relação a contas, dispositivos e indivíduos, com restrição adicional ao volume de dados solicitados numa determinada requisição.

Ainda assim, a estrutura proposta apresenta desafios operacionais, do tipo:

a) como garantir que o investigado não é um nacional ou residente do país requerido?
b) como garantir que os Estados Unidos não investigarão cidadãos estrangeiros ou residentes em outros países se, com a quantidade expressiva de servidores alocados em seu território, certamente possuem mais informações sobre os estrangeiros do que o país de origem dos mesmos? Essa assimetria é mais favorável ao Governo norte-americano do que aos estrangeiros;
c) ademais, no início de uma investigação, dificilmente as autoridades de investigação criminal dispõem da identificação do investigado; aliás, a violação de sigilo, muitas vezes, decorre da necessidade de identificar o investigado;
d) dificilmente, países como a China e a Rússia, que possuem *data centers* de empresas norte-americanas, atenderão aos requisitos mínimos de respeito aos direitos humanos exigidos pela estrutura proposta.

Em sentido análogo aos autores acima, Woods (2016), que é contrário à edição de norma internacional sobre o tema, sugeriu também que sejam operadas mudanças no ECPA, de forma autorizar os provedores de computação em nuvem sediados nos Estados Unidos, a atenderem diretamente requisições de Estados estrangeiros para violar o sigilo de pessoa investigada, desde que observados os seguintes requisitos:

a) os dados não se refiram a cidadão norte-americano ou residente dos Estados Unidos;
b) que tenha sido solicitado para instruir processo criminal ou investigação contra o terrorismo;
c) aprovação do pedido por um terceiro, com competência legal para autorizar o ato (um magistrado, por exemplo);
d) observância ao devido processo legal e respeito aos direitos humanos.

Também é referida a possibilidade de os Estados Unidos adotarem uma abordagem descentralizada (Estado-por-Estado), semelhante ao modelo do *Visa Waiver Program*[117], que será abordado na próxima subseção.

Enquanto não se processam as alterações no ECPA, o autor propôs estabelecer critérios para a interpretação, relativamente à localização dos dados, considerando aspectos mais amplos, como a localização do servidor, o local a partir de onde o usuário acessou o dado pela última vez, o lugar onde ocorreu a criação da conta, dentre outros.

A requisição de evidências criminais eletrônicas diretamente ao provedor de serviço de computação em nuvem, sem interferência do Estado onde esteja sediado, é também uma das alternativas que vem sendo estudada na elaboração da minuta do Segundo Protocolo Adicional à Convenção de Budapeste, para casos específicos.

7.5 A reformulação do MLAT

A reformulação dos procedimentos alusivos ao MLAT foi a proposta que prevaleceu entre os autores pesquisados, diferindo a natureza da mudança e a forma de implementação.

Swire e Kennedy-Mayo (2016) analisaram 03 (três) opções de reforma para o MLAT. Primeiramente, os autores propuseram manter o estado atual do MLAT, aplicando as regras do caso *Microsoft Ireland*, ou seja, nos Estados Unidos, continuariam as limitações ao acesso de Estado estrangeiro a evidências criminais eletrônicas impostas pela Quarta Emenda à Constituição dos Estados Unidos e pelo ECPA, devendo as mesmas limitações serem aplicadas ao país, quando necessitarem coletar dados digitais armazenados em território alheio.

A segunda opção seria a prevalência da aplicação do princípio da extraterritorialidade, permitindo a Estados solicitarem diretamente a provedores de serviço de computação em nuvem, independentemente de onde a evidência criminal estivesse armazenada. Nesse modelo, há sérios riscos que comprometem direitos fundamentais dos usuários, especialmente a privacidade.

---

[117] Livre tradução da autora: Programa de Isenção de Visto. Trata-se de um programa do governo dos Estados Unidos que permite a cidadãos de 38 (trinta e oito) países ingressar no país para viagens a turismo ou negócios, de até noventa dias, sem a necessidade de obtenção prévia de visto (SWIRE; HEMMINGS; VERGNOLLE, 2017).

E por fim, a aplicação de um modelo inspirado no *Visa Waiver Program*, segundo o qual os países negociariam acordos, com o objetivo de facilitar o acesso simplificado aos dados, desde que respeitados os direitos fundamentais dos usuários.

Swire e Hemmings (2016) propõem reformas nos acordos bilaterais de assistência judiciária em matéria penal, com vistas a otimizar o processo de resposta às requisições por evidências criminais armazenadas em ambiente de computação em nuvem. Partindo de uma analogia com o *Visa Waiver Program*, os autores propõem que os tradicionais MLATs sejam substituídos por "estatutos de assistência judiciária", inspirados nos fundamentos para a concessão de benefícios do referido programa. Esses estatutos disciplinam as regras para o reconhecimento de Estados parceiros, facilitando a validação de requisições e promovendo celeridade ao atendimento e resposta.

A reforma proposta possibilita, por exemplo, que um país parceiro requisite dados diretamente a provedores de serviço de computação em nuvem sediados nos Estados Unidos, sem a necessidade de formalizar o pedido por meio de MLAT, reduzindo, assim, o tempo de processamento de uma requisição. O modelo, portanto, ensejaria mudanças no ECPA.

De acordo com os autores, todos os envolvidos numa transação MLAT têm interesse nas mudanças (SWIRE; HEMMINGS, 2015).

O Governo dos Estados Unidos tem interesse em apoiar as investigações estrangeiras, permitindo às autoridades de persecução criminal o acesso às evidências eletrônicas de que necessitem.

Os Governos estrangeiros têm interesse em garantir a soberania absoluta sobre os delitos internos, de interesse exclusivo desse Estado[118]. Para esses Governos, a obrigatoriedade de formalizar acordo de cooperação jurídica com os Estados Unidos para obter acesso às evidências eletrônicas de crime doméstico parece uma restrição ao exercício pleno de sua soberania.

As empresas provedoras de serviços de computação em nuvem, independentemente de onde estejam sediadas, têm interesse em cumprir os pedidos legais, desde que não violem direitos fundamentais de seus clientes, como a

[118] Exemplo: um homicídio na cidade de recife, praticado contra brasileiro por um suspeito brasileiro. O planejamento do crime encontra-se descrito no corpo de *e-mail* enviado pelo suspeito ao cúmplice. Embora o provedor do *e-mail* mantenha filial no Brasil e adote o domínio .br, os dados de conteúdo encontram-se localizados fisicamente em *data center* da empresa, nos Estados Unidos.

privacidade. Ademais, importa evitar o crescimento das regulamentações domésticas, dispondo sobre a localização dos dados, como instituiram, mesmo que implicitamente, a Federação Russa e o Brasil.

Por fim, é interesse da sociedade civil organizada manter a Internet livre e aberta, protegendo os direitos humanos e o direito à privacidade, inerentes a todas os usuários.

Ainda, os autores propõem otimizar as respostas dos Estados Unidos às requisições do MLAT, por meio de ações administrativas, como aumentando o orçamento do Departamento de Justiça norte-americano; reduzindo as etapas de processamento das requisições externas, bem como o tempo entre elas; melhorando a transparência; promovendo o uso do MLAT global e desenvolvendo ferramentas *on-line* para o MLAT.

A versão *on-line* do MLAT otimizaria as respostas, vez que seria dispensada a entrega física (em papel ou em mídia digital) das evidências, além de serem estabelecidos mecanismos de acompanhamento da requisição, tanto para as autoridades do Estado requisitado quanto para os agentes de investigação criminal do Estado requisitante.

Além de Swire e Hemmings (2016), Woods (2016) também propõe a reformulação e a padronização do MLAT, por meio do desenvolvimento de um aplicativo *on-line*, que possibilita ser o pedido realizado, acompanhado e respondido pela Internet, através de formulários pré-definidos. Essa é uma das propostas constantes no projeto de lei que tramita em ambas as Casas do Congresso norte-americano, intitulado *International Communications Privacy Act*, estudado na seção 4.

Ainda acerca do MLAT, é oportuno ressaltar a medida administrativa adotada pelo Governo da França para otimizar o atendimento às requisições do país. Como em muitas ocasiões a demora no processamento de uma requisição MLAT decorre de diferenças nos ordenamentos jurídicos dos países envolvidos, o Governo francês mantém “magistrados de ligação”, nos países onde são registrados os maiores volumes de requisições e que apresentam um sistema judiciário com diferenças consideráveis. Os “magistrados de ligação” funcionam como apoio aos magistrados de investigação, a quem estes podem se reportar diretamente para solicitar acompanhamento junto às autoridades do Estado requisitado, visando prover celeridade às respostas esperadas. A França mantém “magistrado de ligação” em

diversos países europeus, bem como no Brasil e nos Estados Unidos (VERGNOLLE, 2016).

7.6 Proposta do Departamento de Justiça dos Estados Unidos para o acesso extraterritorial a evidências de crimes graves, inclusive o terrorismo

Em 15 de julho de 2016, o Departamento de Justiça dos Estados Unidos encaminhou proposta legislativa à Casa do Senado, no Congresso norte-americano, com o objetivo de alterar o *Electronic Communication Privacy Act* (ECPA), de modo a permitir que Estado estrangeiro requisite diretamente a provedor de serviço Internet baseado nos Estados Unidos, a interceptação de comunicações e a divulgação de dados armazenados em território norte-americano.

O Departamento de Justiça reconhece as dificuldades enfrentadas por Estados estrangeiros no curso de investigação domésticas de crimes graves[119] e de terrorismo, quando relevantes evidências se encontram armazenadas fisicamente em servidores nos Estados Unidos.

Existe a expectativa de que a proposta apresentada, quando aprovada, evite que os Estados editem leis que obriguem as empresas provedoras de serviço Internet a armazenar, dentro do seu território, todos os dados relativos aos seus usuários nacionais (*data localization*), sejam os conteúdos das comunicações ou os metadados (UNITED STATES, 2016b), bem como obstem medidas que desautorizem o provimento de serviços Internet e que imponham às empresas provedoras a obrigação de decidirem, mesmo diante de um conflito de leis (LIN; FIDLER, 2017).

A proposta se afasta do sistema baseado em tratados que atualmente está subjacente ao processo de assistência judiciária mútua, cujo procedimento de tramitação nos Estados Unidos é apresentado pela Figura 8.

Em vez disso, a nova legislação exigiria acordos bilaterais entre os Estados Unidos e os países participantes. Uma vez aprovados para esses acordos bilaterais, a legislação permitiria que fossem enviadas solicitações de divulgação de dados diretamente aos provedores de serviços eletrônicos dos Estados Unidos, considerando o Direito vigente no âmbito do país requisitante (Figura 9). O Reino Unido seria o primeiro país aprovado a fazer pedidos ao abrigo desta nova legislação,

[119] A proposta não define "*serious crime*" ou crimes graves; alude, porém, a crime violento, exploração infantil, fraude financeira significativa, crime organizado transnacional e crimes contra a segurança nacional (terrorismo).

sendo possível, igualmente, estabelecer acordos bilaterais com outros países (LIN; FIDLER, 2017; SWIRE; KENNEDY-MAYO, 2016).

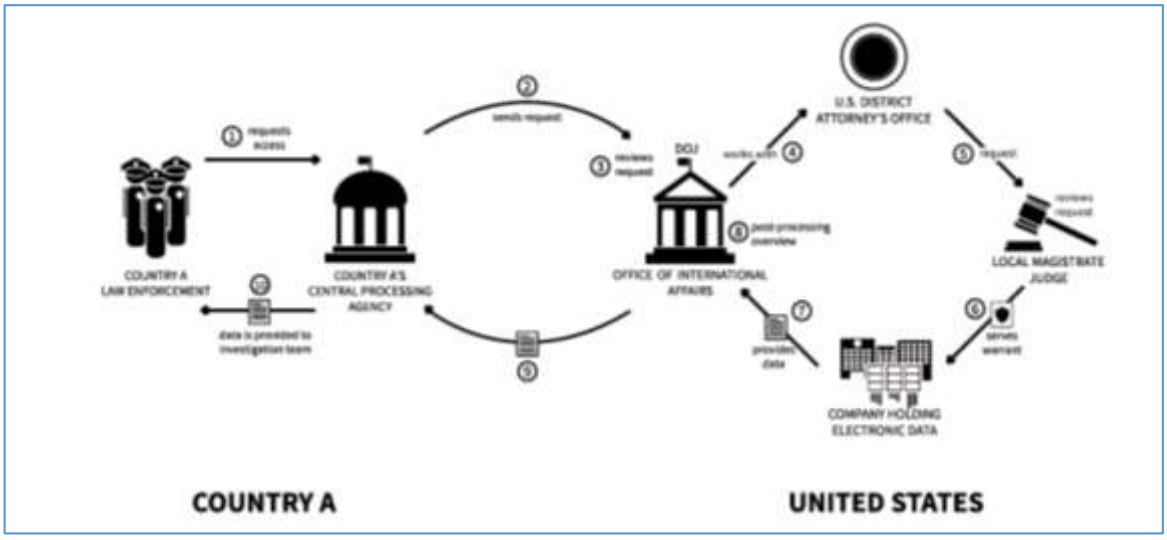

Figura 8 - Processo de tramitação, nos Estados Unidos, de uma requisição realizada nos termos de Acordo de Assistência Judiciária em Matéria Penal - MLAT.
Fonte: (LIN; FIDLER, 2017, p. 3).

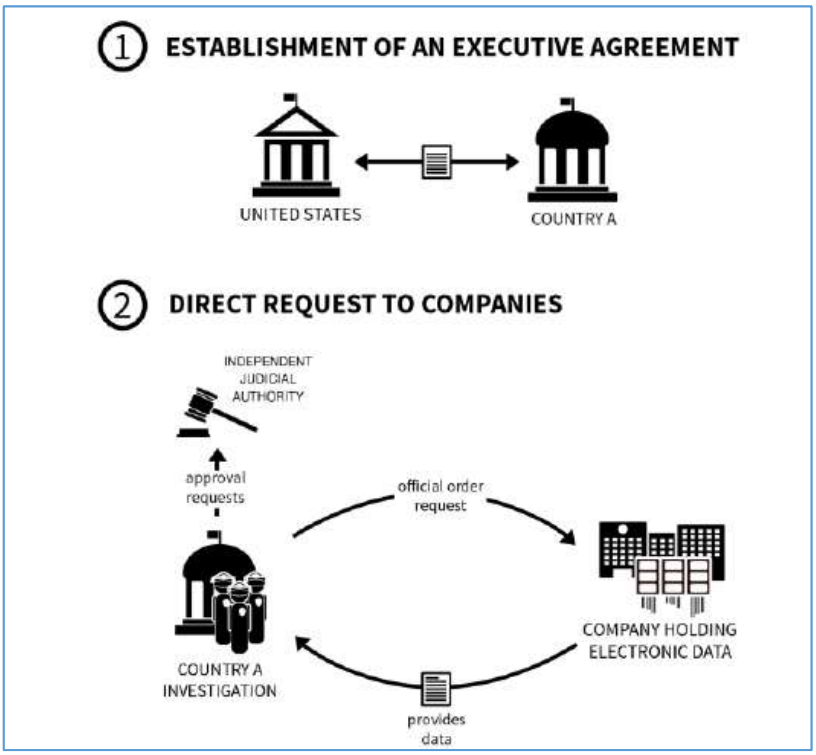

Figura 9 - Diagrama da proposta do Departamento de Justiça dos Estados Unidos.
Fonte: (LIN; FIDLER, 2017, p. 6).

As condições exigidas pelos Estados Unidos para que um Estado estrangeiro ocupe a posição no outro polo do acordo bilateral, bem como as restrições

concernentes às requisições que serão realizadas diretamente a empresa norte-americana, estão descritas na *Section 4 - Executive Agreements on Access to Data by Foreign Governments* do projeto de lei (UNITED STATES, 2016b).

Suscintamente, as condições a serem atendidas pelos Estados estrangeiros para a celebração do referido acordo bilateral com os Estados Unidos são as seguintes:

a) o ordenamento jurídico do Estado estrangeiro deve garantir proteção à privacidade e às liberdades civis, inclusive durante a coleta de evidências criminais eletrônicas;
b) o ordenamento jurídico do Estado estrangeiro deve dispor de leis substantivas e processuais relativamente ao crime cibernético e à coleta de evidências criminais eletrônicas, respectivamente;
c) a comprovação do respeito ao princípio da não discriminação e aos direitos humanos;
d) a demonstração de procedimentos e supervisão efetiva por ocasião da coleta, retenção, uso e compartilhamento de dados pelas autoridades;
e) a adoção de mecanismos de responsabilização e transparência para a coleta e uso dos dados;
f) a adoção de mecanismos para prestação de contas e transparência na coleta de dados;
g) o compromisso de promover e proteger a livre circulação dos dados e a Internet aberta (ou seja, o compromisso de não “localizar os dados”).

Uma vez estabelecido o acordo bilateral com os Estados Unidos, o Estado estrangeiro poderá solicitar dados diretamente ao provedor de serviço Internet, obedecendo as seguintes restrições, relativamente à requisição:

a) não poderá ter por objetivo restringir a liberdade de expressão da pessoa investigada;
b) deve ser revisada e fiscalizada por um tribunal, juiz, magistrado ou outra autoridade independente no país emissor;
c) deve estar argumentada em justificativa razoável, fundada em fatos verossímeis;
d) deve ser emitida em conformidade com a legislação do Estado requisitante, e a obrigação de o provedor divulgar os dados estará vinculada à legislação interna desse país;

e) não podem se referir a cidadão norte-americano ou residente nos Estados Unidos, nem tampouco a qualquer indivíduo através do qual, intencionalmente, almeje-se violar dados relativos a cidadão norte-americano ou a residente nos Estados Unidos;
f) deve subsidiar a prevenção, detecção, investigação e persecução de crimes graves (crime violento, exploração infantil, fraude financeira significativa, crime organizado transnacional) e crimes contra a segurança nacional (terrorismo);
g) deve particularizar a busca, por meio de informações que facilitem a identificação da pessoa investigada, como nome, conta de usuário, dispositivo pessoal, dentre outros;
h) deve estar baseada em fatos verossímeis, considerados crimes graves no ordenamento jurídico interno, e ter previsão legal;
i) as interceptações de comunicação eletrônicas devem ser realizadas por um período fixo, previamente estabelecido, sendo autorizadas apenas nos casos em que a informação não possa ser obtida por outro método menos invasivo.

Outras medidas procedimentais são esperadas dos Estados estrangeiros, como:

a) inutilizar os dados que não interessem à prova;
b) não divulgar a autoridades norte-americanas informações de um nacional dos Estados Unidos, a menos que esteja relacionado a danos ou ameaças significativas contra nacional dos Estados Unidos ou se refira a crimes contra a segurança nacional, terrorismo, crimes violentos, exploração infantil ou fraude financeira significativa;
c) garantir reciprocidade ao Governo dos Estados Unidos;
d) concordar com revisões periódicas, inclusive com o direito de rescindir o acordo;
e) as empresas provedoras de serviço Internet não estariam obrigadas a responder às requisições, embora estejam sujeitas a enfrentar outras imposições, por parte do Estado requisitante.

Esses novos acordos bilaterais não substituiriam, mas complementariam o sistema MLAT. Os governos estrangeiros ainda podem usar o processo MLAT para solicitações que ficam fora dos parâmetros do referido acordo, ou para as situações

em que o Estado estrangeiro mantenha com os Estados Unidos apenas o MLAT (LIN; FIDLER, 2017).

Em resposta, a sociedade civil posicionou-se cautelosamente otimista, ressaltando que a proposta não poderá olvidar proteger os direitos fundamentais e as liberdades civis dos usuários. Para Daskal (2016a), a proposta será uma oportunidade para pacificar as tensões em torno do tema, definir tendências relacionadas à localização dos dados e contribuir na definição de um padrão de privacidade para todos.

7.7 Um modelo de investigação criminal para as autoridades policiais

Em estudo sobre os procedimentos policiais para a coleta extraterritorial de evidências criminais armazenadas em ambiente de computação em nuvem, Svantesson (2016b) analisa quatro propostas:

a) proposta 1: o acesso extraterritorial ao dado deve ser entendido como um procedimento atinente à "jurisdição investigativa", que deve estar desvinculada do princípio da territorialidade e do conceito de jurisdição executiva;
b) proposta 2: elaborar um teste multifatorial para definir a jurisdição relativamente ao acesso extraterritorial à evidência digital;
c) proposta 3: afastar a territorialidade como o cerne da jurisdição;
d) proposta 4: no silêncio do direito internacional, um Estado somente exercerá sua jurisdição em situação previamente estabelecida.

7.7.1 A Jurisdição investigativa

Svantesson (2016b) propõe que seja instituída, e reconhecida pela comunidade internacional, a “jurisdição investigativa”, destinada exclusivamente à coleta extraterritorial de evidências criminais armazenadas em ambiente de computação em nuvem.

Então, além da jurisdição legislativa, da jurisdição executiva, e da jurisdição adjudicatória, a jurisdição investigativa otimizaria o processo de busca e apreensão de evidências criminais no ambiente de computação em nuvem, uma vez que a autoridade policial estaria desobrigada de cumprir requisitos legais atinentes à

jurisdição executiva, como a celebração de MLATs, para a obtenção de evidências criminais.

7.7.2 Teste multifatorial

Via de regra, as leis processuais penais são informadas pelo princípio da territorialidade absoluta, conforme abordado na seção 5.

Ocorre que, nos casos em que é identificada a necessidade de coleta a evidências criminais armazenadas em servidor de computação em nuvem, localizado em terceiro país, outras questões devem ser consideradas.

Para Svantesson (2016b), a jurisdição, nesses casos, pode ser determinada pela combinação de múltiplos fatores, ao invés de critérios únicos e isolados, tais como: localização do dado, localização do suspeito, localização da vítima, nacionalidade do suspeito, nacionalidade da vítima, residência habitual do suspeito, residência habitual da vítima, sede da empresa provedora do *data center*, sede da empresa subsidiária de suporte a *data center*, presença da empresa no Estado.

Segundo o autor, o critério de determinação da jurisdição baseado, apenas e sempre, na localização física da evidência criminal eletrônica não parece ser adequado, pois, em geral, dificilmente uma autoridade policial é capaz de precisá-la, principalmente no início da investigação.

7.7.3 Afastar a territorialidade

A terceira proposta apresentada por Svantesson (2016b) é a de afastar a territorialidade como o núcleo do princípio da jurisdição, nos casos em que o acesso extraterritorial a evidências criminais eletrônicas se faz necessário.

Enquanto a territorialidade enfatiza a importância da localização dos dados, o argumento de afastar o princípio da territorialidade como fundamento da jurisdição não implica em afirmar que a localização dos dados é irrelevante. O fato de um *data center* encontrar-se instalado no território de um Estado, não o autoriza a destruí-lo, embora a possibilidade exista. Por essas e outras razões, a localização do dado é relevante, mas não significa que seja motivo determinante nas reinvindicações jurisdicionais.

Outrossim, problemas relacionados à territorialidade como fundamento da jurisdição não é uma questão apenas relativa à Internet. Outras áreas também enfrentam dilemas semelhantes, como o direito ambiental, o direito de pesca, os direitos humanos, o direito espacial e aéreo. Nesse sentido, o esforço despendido na área da computação em nuvem poderá contribuir para formar um conceito mais abrangente sobre jurisdição.

7.7.4 Uma nova estrutura para definir a jurisdição

A última proposta apresentada por Svantesson (2016b) refere-se a uma nova estrutura para aplicação dos princípios da jurisdição, com vistas a delinear os procedimentos relativos ao acesso extraterritorial a evidências criminais, armazenadas em ambiente de computação em nuvem.

Nos termos da proposta, em caso de ausência de normas de direito internacional, o Estado só poderá exercer a jurisdição quando:

a) existir uma conexão substancial entre a questão e o Estado interessado em exercer sua jurisdição;
b) o Estado que busca exercer sua jurisdição tem interesse legítimo na questão;
c) o exercício da jurisdição é razoável, considerando o equilíbrio entre os interesses envolvidos.

Embora o esquema acima não tenha sido adotado formalmente, é possível observá-lo em pesquisas concernentes ao acesso extraterritorial a evidências eletrônicas de crime.

7.8 A solução é harmonizar o direito substantivo

Hooper, Martini e Choo (2013) acreditam que a viabilidade da coleta de evidências criminais armazenadas em servidor de ambiente de computação em nuvem, localizado em Estado estrangeiro, passa pela harmonização das legislações vigentes nas jurisdições envolvidas, bem como na adoção de medidas processuais mais céleres, garantidas na assistência mútua entre as agências de investigação criminal.

Nesse sentido, os autores propõem harmonizar o direito penal material e incentivar maior cooperação entre as agências de persecução criminal, permitindo assim que as investigações possam ocorrer em nível internacional, procurando sempre o equilíbrio entre o direito fundamental à privacidade e os procedimentos necessários à elucidação de fatos criminosos.

7.9 Enunciado no Direito Brasileiro

Os desafios inerentes à busca e apreensão de evidências criminais eletrônicas em ambiente de computação em nuvem foram reconhecidos pela Justiça Federal brasileira, por ocasião do curso “Investigação e prova nos crimes cibernéticos. Dificuldades técnicas e jurídicas – Questões práticas”, promovido pela Escola de Magistrados da Justiça Federal da 3ª Região, no ano de 2016.

A primeira dificuldade identificada pelos magistrados é referente à necessidade de indicação, no respectivo mandado, da forma mais precisa possível, do local onde deveria ser realizada a diligência de busca e apreensão de evidências eletrônicas.

Entendem os magistrados que o local onde se encontram armazenados os documentos digitais de pessoa investigada, acessível por meio de seus equipamentos de informática, ou mediante uso de códigos de acesso, deve ser considerado uma extensão de sua casa, estando tais documentos, portanto, sujeitos à apreensão mediante imagem. Contudo, para que tal procedimento seja validamente realizado, é necessário que conste do mandado de busca e apreensão a possibilidade de que a diligência seja efetuada em documentos digitais, remotamente armazenados.

Assim, de acordo com o Enunciado 4 - Busca e apreensão: conteúdo armazenado remotamente,

> Enunciado 4 - Busca e apreensão: conteúdo armazenado remotamente
> Recomenda-se que, no mandado de busca e apreensão de equipamentos de informática, conste expressa autorização para que seja vasculhado conteúdo remotamente armazenado, se localizados meios de acesso. Considerando, porém, que a busca e apreensão de material indiciário pode se dar fora dos equipamentos diligenciados, mas com base em meios de acesso neles encontrados (como o sistema de armazenamento na “nuvem”), em discussão sobre a extensão da ordem judicial, concluiu-se pela recomendação de expressa autorização em mandado. (BRASIL, 2017, p. 346).

Entendem os magistrados que,

> constando do mandado a possibilidade de busca em conteúdo armazenado remotamente, e se o acesso é protegido por senha, nada impede a diligência, se esta puder ser obtida mediante busca nos arquivos localmente armazenados, ou mesmo mediante quebra por meio de programas específicos (BRASIL, 2017, p. 208).

Observa-se que não há qualquer ressalva quanto à possibilidade de localização dos dados, em Estado estrangeiro. De acordo com o entendimento, é bastante encontrar, no dispositivo informático da pessoa investigada, qualquer registro (senha, por exemplo) que possibilite a exploração de conteúdo armazenado remotamente, sendo lícita a diligência de busca e apreensão de evidências criminais eletrônicas, mesmo que localizadas, fisicamente, em servidores sob jurisdição de Estado estrangeiro, desde que expressamente autorizado em mandado judicial.

7.10 Mecanismos alternativos de cooperação internacional

Os Estados têm procurado alternativas formais ou informais de cooperação, com vistas a otimizar o processo de investigação de delitos intensivos em tecnologia da informação e comunicação, sem comprometer a soberania de terceiro Estado, quando envolve a busca e apreensão extraterritorial de evidências criminais eletrônicas. Osula (2015a) apresenta algumas dessas alternativas que, segundo a autora, já se encontram implantadas ou estão sendo objeto de discussão.

A primeira é a cooperação formal ou informal entre Estados, possibilitando que agências de investigação criminal de dois ou mais países estabeleçam relação direta ou compartilhem informações disponíveis em sistemas integrados de comunicação.

Organizações internacionais, como a Interpol, auxiliam na cooperação entre agências de investigação criminais de todo o mundo. Outras instituições, também de caráter internacional, apoiam os Estados na luta contra a criminalidade. Na Europa, por exemplo, destacam-se a *Europol* e a *Eurojust.*

O compartilhamento de informações pode ocorrer tanto por meio de bases de dados multinacionais ou através da troca de informações entre agências. Na Europa, por exemplo, o Sistema de Informações de *Schengen* permite o acesso a informações variadas sobre objetos e pessoas, bem como de pessoas procuradas por prática de crime ou pessoas desaparecidas.

A segunda forma sugerida pela autora é por intermédio da cooperação formal ou informal entre os Estados e terceiros, que pode ocorrer tanto pelo do contato direto com provedores de serviço, quanto por meio do acesso extraterritorial e direto aos dados, quando autorizado na forma da lei.

No caso do contato direto com o provedor, a resposta dependerá de vários fatores, dentre eles os compromissos assumidos pela empresa com o país onde aloca seus equipamentos, bem como os termos contratuais pactuados com os usuários do serviço. Alguns provedores de serviço, como o Facebook[120] e o eBay[121], dispõem de sistemas de informações *on-line* que facilitam o intercâmbio com os agentes da persecução criminal.

O acesso direto a evidências criminais eletrônicas apenas é permitido nos termos do artigo 32 da Convenção de Budapeste sobre o Cibercrime, conforme descrito na seção 6.

Por fim, os Estados podem, após revisão crítica dos modelos vigentes, implementar reformas nos procedimentos do MLAT, com o objetivo de otimizar as respostas às requisições por evidências criminais eletrônicas. Podem, por exemplo, instituir reforço operacional às autoridades centrais, uniformizar as solicitações, reforçar a cooperação e a comunicação entre entidades nacionais relevantes.

7.11 Uma nova abordagem para avaliar a jurisdição dos mandados expedidos nos termos do SCA

No caso *Microsoft Ireland*, a Microsoft empreendeu uma fervorosa defesa em favor da inviolabilidade da privacidade de seus clientes, suscitando inclusive relevantes questões quanto à aplicação extraterritorial do direito processual norte-americano.

No entanto, com a expansão cada vez mais intensa da computação em nuvem, favorecendo a distribuição do processamento e do armazenamento dos dados por jurisdições distintas ao redor do mundo, o trabalho dos agentes públicos encarregados pela aplicação da lei tem se tornado cada vez mais desafiador, vez que uma parcela considerável de criminosos tem deixado evidências de seus delitos em ambiente de computação em nuvem pública.

---

[120] Facebook: https://www.facebook.com/records/x/login/
[121] eBay: https://lers.corp.ebay.com/AIP/portal/home.do

No âmbito dos Estados Unidos, Pecoraro (2017) propõe uma nova abordagem para avaliar a jurisdição dos mandados expedidos nos termos do SCA, com fundamento em dois critérios, quais sejam:

a) a identidade ou nacionalidade do investigado;

b) a localização do provedor de serviços.

De acordo com o autor, a posição predominante entre os doutrinadores norte-americanos é a de que devem prevalecer a nacionalidade e a localização do investigado para determinar a jurisdição competente que expedirá a ordem judicial que autorizará a divulgação dos dados. Esse é o entendimento, inclusive, que está presente no projeto de lei que tramita nas duas Casas do Congresso norte-americano, intitulado *International Communications Privacy Act* (ICPA). De acordo com o projeto de lei, a autoridade policial deve instruir o pedido de mandado de busca e apreensão com informações acerca da nacionalidade e da localização do investigado, informando inclusive as diligências efetuadas para obtê-las, desde que mantenha com os Estados Unidos *Law Enforcement Cooperation Agreement.*

Na prática, a exigência de precisar a localização do investigado parece não ser uma tarefa trivial. A identificação do endereço IP utilizado pelo investigado é um recurso relevante para auxiliar na sua localização. No entanto, existem também diversos aplicativos que mascaram o endereço IP, ocultando assim a real localização do infrator.

Sob o enfoque da localização do servidor, uma empresa provedora de serviço, sediada em território norte-americano, deve cumprir mandado judicial que lhe obrigue a produzir dados que estejam sob sua posse ou responsabilidade, independentemente de onde estejam fisicamente armazenados. Mas essa também não é uma questão trivial. Segundo o autor, no caso *Microsoft Ireland*, em momento algum foi interposta, pelo Governo da República da Irlanda ou por qualquer *amicus curiae*, posição contrária a trazer de volta os dados solicitados para os Estados Unidos nem tampouco que essa prática contrariaria lei irlandesa de proteção de dados. Questiona-se qual o real interesse da República da Irlanda em proteger esses dados, uma vez que, aparentemente, o investigado não era cidadão irlandês, bem como inexistiam disposições no direito interno irlandês contrárias à remoção dos dados dos servidores situados no país.

No entanto, nesse contexto, não é suficiente que a empresa esteja sediada nos Estados Unidos, mas a informação buscada deve ter relação forte com atividades

criminosas praticadas em território norte-americano. O autor cita o caso *Zheng versus Yahoo*! Inc., no qual um tribunal distrital dos Estados Unidos rejeitou o argumento de que o SCA poderia ser aplicado para recuperar dados armazenados em *data center* da empresa na China, por funcionários chineses e dentro das instalações chinesas.

Por fim, o autor espera que sejam encontradas soluções legislativas no direito interno norte-americano que permitam a realização de buscas extraterritoriais por evidências criminais eletrônicas, com prevalência do respeito à privacidade e à soberania internacional, além do compromisso das empresas provedoras com a compreensão evidente da responsabilidade que possuem nesse cenário.

7.12 Uma analogia interpretativa com o direito de perseguição

O acesso extraterritorial a evidências criminais armazenadas em servidores de computação em nuvem, localizados em terceiro Estado, foi objeto de analogia interpretativa com o direito de perseguição (*hot pursuit*), presente na Convenção das Nações Unidas sobre o Direito do Mar[122].

Vargas-Leon (2016) analisou as consequências da aplicação do direito de perseguição[123], na busca de evidências criminais no espaço cibernético, adotando o caso *Microsoft Ireland* como cenário para o estudo.

---

[122] No Brasil, foi declarada a entrada em vigor da Convenção das Nações Unidas sobre o Direito do Mar, por meio do Decreto nº 1.530, de 22 de junho de 1988 (BRASIL, 1988b). Promulgada a Convenção, por meio do Decreto nº 99.165, de 12 de março de 1990 (BRASIL, 1990).

[123] Artigo 111. Direito de perseguição. 1. A perseguição de um navio estrangeiro pode ser empreendida quando as autoridades competentes do Estado costeiro tiverem motivos fundados para acreditar que o navio infringiu as suas leis e regulamentos. A perseguição deve iniciar-se quando o navio estrangeiro ou uma das suas embarcações se encontrar nas águas interiores, nas águas arquipelágicas, no mar territorial ou na zona contígua do Estado perseguidor, e só pode continuar fora do mar territorial ou da zona contígua se a perseguição não tiver sido interrompida. Não é necessário que o navio que dá a ordem de parar a um navio estrangeiro que navega pelo mar territorial ou pela zona contígua se encontre também no mar territorial ou na zona contígua no momento em que o navio estrangeiro recebe a referida ordem. Se o navio estrangeiro se encontrar na zona contígua, como definida no artigo 33, a perseguição só pode ser iniciada se tiver havido violação dos direitos para cuja proteção a referida zona foi criada. 2. O direito de perseguição aplica-se, *mutatis mutandis*, às infrações às leis e regulamentos do Estado costeiro aplicáveis, de conformidade com a presente Convenção, na zona econômica exclusiva ou na plataforma continental, incluindo as zonas de segurança em volta das instalações situadas na plataforma continental, quando tais infrações tiverem sido cometidas nas zonas mencionadas. 3. O direito de perseguição cessa no momento em que o navio perseguido entre no mar territorial do seu próprio Estado ou no mar territorial de um terceiro Estado. 4 A perseguição não se considera iniciada até que o navio perseguidor se tenha certificado, pelos meios práticos de que disponha, de que o navio perseguido ou uma das suas lanchas ou outras embarcações que trabalhem em equipe e utilizando o navio perseguido como navio mãe, se encontram dentro dos limites do mar territorial ou, se for o caso, na zona contígua, na zona econômica exclusiva ou na plataforma continental. Só pode dar-se início à perseguição depois de ter sido emitido sinal de parar, visual ou auditivo, a uma distância que permita ao navio estrangeiro vê-lo ou ouvi-lo. 5. O direito de perseguição

No Direito do Mar, o direito de perseguição permite que um Estado costeiro aplique suas leis e regulamentos contra navio estrangeiro que, violando direito interno, escapa para o alto mar, onde os Estados não têm jurisdição. E uma vez iniciada, a perseguição cessa no momento em que o navio perseguido entre no mar territorial do seu próprio Estado ou no mar territorial de um terceiro Estado (BRASIL,1990).

A perseguição ocorre com o fim de garantir o exercício do direito de punir, negando ao navio ofensivo a oportunidade de fugir ao reclamar o direito de livre navegação inerente aos navios inocentes.

No espaço cibernético, os Estados costumam agir, tentando ampliar sua soberania, acessando dados armazenados além das fronteiras de seu território, ou tentando manter os dados dentro de suas fronteiras territoriais.

Na análise do caso *Microsoft Ireland*, Vargas-Leon (2016) observou que a primeira condição para aplicar o princípio da perseguição, que é a suspeita de atividade criminosa praticada dentro do território de um Estado, foi atendida. No entanto, as evidências eletrônicas relevantes à elucidação do crime encontravam-se armazenadas em território de outro país, a República da Irlanda. O acesso aos dados não exigiria o deslocamento de equipe técnica até a Irlanda, vez que poderiam ser coletados remotamente, por estarem sob controle da Microsoft. Ademais, também de acordo com a teoria do princípio da perseguição, não importa que tipo de atividade criminosa esteja sob investigação, a busca deve cessar quando envolve a soberania de um Estado diferente (além daquele onde o ato criminoso foi cometido).

Assim, em analogia com o princípio *hot pursuit*, os Estados Unidos, ou qualquer outro país, está impedido de acessar diretamente evidências criminais

---

só pode ser exercido por navios de guerra ou aeronaves militares, ou por outros navios ou aeronaves que possuam sinais claros e sejam identificáveis como navios e aeronaves ao serviço de um governo e estejam para tanto autorizados. 6. Quando a perseguição for efetuada por uma aeronave: a) aplicam-se, mutatis mutandis, as disposições dos parágrafos 1º e 4º; b) a aeronave que tenha dado a ordem de parar deve continuar ativamente a perseguição do navio até que um navio ou uma outra aeronave do Estado costeiro, alertado pela primeira aeronave, chegue ao local e continue a perseguição, a não ser que a aeronave possa por si só apresar o navio. Para justificar o apresamento de um navio fora do mar territorial, não basta que a aeronave o tenha descoberto a cometer uma infração, ou que seja suspeito de a ter cometido, é também necessário que lhe tenha sido dada ordem para parar e que tenha sido empreendida a perseguição sem interrupção pela própria aeronave ou por outras aeronaves ou navios. 7. Quando um navio for apresado num lugar submetido à jurisdição de um Estado escoltado até um porto desse Estado para investigação pelas autoridades competentes, não se pode pretender que seja posto em liberdade pelo simples fato de o navio e a sua escolta terem atravessado parte de uma zona econômica exclusiva ou do alto mar, se as circunstâncias a isso obrigarem. 8. Quando um navio for parado ou apresado fora do mar territorial em circunstâncias que não justifiquem o exercício do direito de perseguição, deve ser indenizado por qualquer perda ou dano que possa ter sofrido em consequência disso.

armazenadas em servidores dispostos em território estrangeiro, podendo solicitá-las por meio de instrumentos tradicionais de assistência judiciária mútua, como o MLAT.

Essa conclusão vem corroborar com a posição dos acadêmicos e doutrinadores que defendem a soberania territorial sobre o espaço cibernético, considerando a localização física da infraestrutura da rede para determinar a jurisdição competente para o exercício do direito processual penal.

7.13 Contribuições à pesquisa

Essa subseção deixa contribuições relevantes à proposta apresentada nessa Tesa, principalmente os relatórios do Conselho da Europa, que subsidiam os trabalhos (em andamento) de elaboração do Segundo Protocolo Adicional à Convenção de Budapeste sobre o Cibercrime, e as propostas apresentadas no âmbito dos Estados Unidos.

Vários critérios foram sugeridos com o objetivo determinar a jurisdição competente para requisitar dados digitais de interesse à investigação criminal. São exemplos, a nacionalidade da vítima, do acusado, o local onde o crime foi praticado ou onde os seus efeitos foram sentidos.

Outros aspectos também são analisados, como a possibilidade de autoridades de investigação criminal solicitarem diretamente ao provedor de computação em nuvem os dados digitais ou informações atinentes à pessoa investigada.

8 COOPERAÇÃO DIRETA ENTRE ESTADO E PROVEDOR DE COMPUTAÇÃO EM NUVEM EM OUTRA JURISDIÇÃO

Esta seção apresenta os requisitos para compor os termos de um tratado internacional, multilateral e vinculante, com o objetivo de viabilizar a colaboração direta entre Estado soberano e empresa provedora de serviço Internet que implementa computação em nuvem, para permitir que autoridades de persecução criminal possam interagir diretamente com provedor de serviço, sediado em território de outro Estado Parte, sem a obrigatoriedade de formalizar acordo bilateral de assistência judiciária em matéria penal entre os Estados envolvidos, para fins de localização, preservação, acesso, produção, busca e apreensão de evidências eletrônicas, relativas a prática de crimes graves.

8.1 Discussões preliminares

O espaço cibernético, no direito internacional, para fins de regulamentação, é interpretado tanto como espaço apartado do mundo real, merecedor de novos princípios e tratamento jurídico diferenciado (Escola dos excepcionalistas), quanto como uma extensão do mundo físico, porque é oriundo da conexão entre vários dispositivos físicos, e utilizado por indivíduos de um mundo real (Escola dos não-excepcionalistas). Defendem a primeira Escola autores como Hard (1994), Post (1995), Johnson e Post (1996). Lessig (1999) e Goldsmith (1999) pertencem a segunda Escola, que também vem sendo a visão que prevalecente entre os governantes, que legislam acerca da parte da Internet que consideram sob sua esfera de poder, fundamentados na localização física dos dispositivos informáticos ou dos equipamentos de comunicação e processamento de dados (KOOPS; GOODWIN, 2014), contrariando a natureza transnacional da grande rede.

Do estudo da seção 6, que analisou 05 (cinco) tratados internacionais, multilaterais, todos de alcance regional e de caráter vinculante, ficou evidente que as normas internacionais em vigor, concernentes à segurança da informação e à criminalidade cibernética, carecem de regramento acerca das diligências para a localização, preservação, acesso, produção, busca e apreensão de evidências criminais, armazenadas em servidor de computação em nuvem, em território de Estado estrangeiro, mesmo que se trate de Estado Parte.

A Convenção de Budapeste sobre o Cibercrime (COUNCIL OF EUROPE, 2001a) e a Convenção da Liga dos Estados Árabes sobre o Combate às Ofensas contra a Tecnologia da Informação (LEAGUE OF ARAB STATES, 2010) aludem às mesmas possibilidades, relativamente ao acesso transfronteiriço a dados eletrônicos. Também tratam, de forma semelhante, a busca e apreensão de evidências eletrônicas, limitada sua aplicação ao âmbito interno.

A Convenção da União Africana sobre Segurança Cibernética e Proteção de Dados (AFRICA UNION, 2014) dispõe sobre a possibilidade de acesso a dados, localizados em sistemas informáticos instalados em outro Estado Parte.

Ao que parece, a regionalização das normas internacionais, concernentes ao tema em estudo, constitui um contrassenso à natureza transnacional dos crimes intensivos no uso da tecnologia da informação e comunicação, seja porque seus efeitos podem ser sentidos além das fronteiras do Estado onde foram perpetradas as condutas, seja porque as evidências eletrônicas de sua prática estejam em servidor de computação em nuvem, localizado em outro Estado.

Diante do exposto, acredita-se que o disciplinamento das requisições para localização, preservação, acesso, produção, busca e apreensão de evidências criminais, armazenadas em servidor de computação em nuvem, disposto em território de Estado estrangeiro, deve ser amplamente discutido em processo de negociação conduzido por organismo internacional de abrangência universal, como as Nações Unidas, sendo, ao final, as normas positivadas em instrumento jurídico cujos requisitos para adesão e ratificação não estejam vinculados à anuência prévia e unânime dos Estados Parte ou de qualquer outro Estado.

O caso *Microsoft Ireland*, referente à disputa judicial travada entre a *Microsoft Corporation* e o Governo dos Estados Unidos, ressaltou os desafios à persecução criminal, trazidos pela computação em nuvem, que implementa o estado da arte da mobilidade dos dados. A Corte Suprema dos Estados Unidos irá decidir se provedor

de serviço de *e-mail*, localizado nos Estados Unidos, é obrigado a cumprir mandado (*Warrant*), expedido com base em causa provável, nos termos do 18 USC § 2703 do SCA, para violar sigilo de comunicações eletrônicas sob o controle do provedor, mesmo que esse provedor tenha decidido por armazenar os dados em território estrangeiro (UNITED STATES, 2017a). A deliberação a ser prolatada reveste-se da expectativa de referencial importante, na medida em que esse país concentra número considerável de provedores mundiais de Internet pública.

A seção 7 apresentou várias proposições para enfrentar os problemas relacionados à preservação, acesso, coleta, produção, busca e apreensão de evidências criminais eletrônicas, quando armazenadas em servidores de ambiente de computação em nuvem, localizados em território de país distinto daquele que realiza a investigação criminal. Foi possível identificar cinco tendências predominantes, não excludentes entre si, relativamente ao direcionamento das proposições. São elas:

a) no sentido de alterar a legislação norte-americana, defendidas por Currie (2017), Pecoraro (2017), Woods (2016), Swire e Hemmings (2016), Krishnamurthy (2016), Daskal e Woods (2015);
b) direcionadas a alterar os procedimentos comumente adotados nos acordos de cooperação judiciária em matéria penal – MLATs, conforme Swire e Kennedy-Mayo (2016), Swire e Hemmings (2016), Woods (2016), Osula (2015a), Jaycox e Tien (2015);
c) voltadas a estabelecer procedimentos administrativos a serem seguidos pelas agências de persecução criminal, segundo Svantessen (2016b);
d) no sentido de estabelecer contato direto do Estado com o provedor de serviço, segundo Lin e Fidler (2017), Woods (2016), Krishnamurthy (2016), Svantessen (2016a), Swire e Kennedy-Mayo (2016), United States (2016b), Daskal e Woods (2015) e Currie (2017);
e) tendentes a instituir ou alterar tratados multilaterais existentes.

As propostas que defendem alterações na legislação norte-americana são relevantes, pois se trata do país que concentra o maior número servidores (*hosts*), *data centers* de empresas provedoras de serviços de computação em nuvem pública.

No entanto, alterar a legislação interna do país, unicamente, não parece solucionar o problema, uma vez que existem diversos *data centers* espalhados por países de vários continentes, mesmo que subsidiários de empresas norte-americanas ou pertencentes a outras empresas provedoras de computação em nuvem.

Assim, mesmo que sejam procedidas alterações no ECPA, de maneira a permitir que provedores norte-americanos possam responder diretamente a Estados estrangeiros que requisitam evidências criminais armazenadas em ambiente de computação em nuvem, sem a necessidade de estabelecer assistência judiciária internacional formal (MLAT, por exemplo), ainda assim permanecem as restrições e impasses nos casos em que a evidência esteja armazenada fora dos Estados Unidos.

Ainda no sentido de promover alterações na legislação norte-americana, a proposta de instituir um programa semelhante ao *Visa Waiver Program* (defendidas por Woods (2016), Swire e Kennedy-Mayo (2016), Swire e Hemmings (2016)) significaria dividir o mundo em Estados "confiáveis" e Estados "não confiáveis", do ponto de vista unicamente dos Estados Unidos. O Brasil, hoje, estaria entre os Estados "não confiáveis", tomando por referência a situação atual no *Visa Waiver Program.*

A segunda tendência identificada nas propostas apresentadas está relacionada à promoção de mudanças nos atuais procedimentos adotados nos acordos de cooperação judiciária em matéria penal (MLATs). Por serem tratados bilaterais, as alterações sugeridas até poderiam contribuir para diminuir o tempo de resposta e proporcionar o acompanhamento das requisições. No entanto, estariam limitadas a atender unicamente os interesses dos Estados envolvidos.

Ademais, é louvável a proposta de criação de uma versão automatizada para orientar a operacionalização do MLAT que vem sendo defendida no projeto de lei norte-americano *International Communications Privacy Act,* referido na seção 4, e por Woods (2016), Swire e Hemmings (2016). Por meio de uma ferramenta *on-line*, disponível no sítio eletrônico do Departamento de Justiça dos Estados Unidos, representantes de Estados estrangeiros poderiam formalizar as requisições por busca e apreensão de dados armazenados em servidores dentro do território norte-americano, bem como seria possível acompanhar os encaminhamentos das providências adotadas para a elaboração da resposta. Ocorre que a aludida ferramenta estaria disponível apenas aos Estados com os quais existissem formalizados tratados bilaterais de assistência judiciária, em matéria penal. Mesmo procedendo as alterações sugeridas, o MLAT continuaria burocrático, moroso e ineficiente.

A terceira tendência das propostas pode ser agrupada no conjunto de ideias que visa estabelecer procedimentos administrativos a serem seguidos pelas agências

de persecução criminal. Svantessen (2016b) apresenta recomendações, sem, no entanto, referir à necessidade de formalização no Direito Internacional.

A quarta tendência identificada agrupa as propostas no sentido de estabelecer contato direto entre as autoridades de persecução criminal e os provedores de serviço que implementam a computação em nuvem, de forma a viabilizar a solicitação direta de evidências criminais eletrônicas, sem a necessidade de estabelecer acordo bilateral de assistência judiciária em matéria penal. O Comitê para a Convenção do Cibercrime, por meio de Termo de Referência para a elaboração do Segundo Protocolo Adicional à Convenção (CYBERCRIME CONVENTION COMMITTEE, 2017), defende que, em determinadas situações (como emergência, risco de morte), seja admitida a requisição diretamente ao provedor de serviço. Essa possibilidade é também defendida pelo Departamento de Justiça dos Estados Unidos (UNITED STATES, 2016b) e por outros autores, como Lin e Fidler (2017), Woods (2016), Krishnamurthy (2016), Svantessen (2016a), Swire e Kennedy-Mayo (2016). A proposta apresentada nessa Tese segue essa tendência, embora apresente características próprias, não identificadas nas referências pesquisadas.

A última tendência identificada refere-se às propostas voltadas a instituir novos tratados internacionais, ou suplementar Convenções existentes, com a finalidade de normatizar os procedimentos de busca e apreensão de evidências criminais eletrônicas, quando armazenadas em servidores de computação em nuvem, dispostos em Estado distinto do que procede a investigação criminal. Durante a Terceira Sessão de trabalho do Grupo de Especialistas da UNODC, alguns Estados, por meio de seus representantes, mostraram-se favoráveis a edição de um novo instrumento jurídico internacional, para dar uma resposta mundial mais eficaz contra a delinquência cibernética. Outros Estados, no entanto, entenderam que iniciar uma discussão nesse sentido colocaria em risco os esforços em curso para melhorar as legislações existentes. Demais Estados, ainda, opinaram pela melhoria dos mecanismos existentes, aperfeiçoando a cooperação policial e judicial, além das atividades de assistência técnica e criação de capacidade (UNODC, 2017).

A esse respeito, existem vantagens e desvantagens associadas a cada uma das opções: instituir um novo tratado ou suplementar a Convenção de Budapeste sobre o Cibercrime, que é considerada o tratado internacional mais proeminente sobre o crime cibernético.

A vantagem de formalizar um novo tratado internacional concernente ao acesso a evidências criminais eletrônicas armazenadas em ambiente de computação em nuvem é a possibilidade de instituir um amplo processo participativo de negociação, envolvendo representantes de diversas áreas implicadas e interessadas no problema. Poderia ser também uma oportunidade para fazer reunir os Estados signatários dos tratados internacionais relativos à criminalidade cibernética, vistos na seção 6, de maneira a unificar esforços na busca de uma solução com o mesmo alcance que possui a Internet, ou seja, uma solução global. Por outro lado, o tempo de elaboração de um novo instrumento e o processo de adesão dos Estados são desvantagens a essa opção.

A vantagem de suplementar a Convenção de Budapeste sobre o Cibercrime, que vem sendo o objeto do grupo de trabalho instituído pelo Conselho da Europa, por meio de Termo de Referência (CYBERCRIME CONVENTION COMMITTEE, 2017), está associada à maturidade e ao nível de conhecimento internacional em relação à norma.

Se o Segundo Protocolo Adicional à Convenção de Budapeste sobre o Cibercrime for adotado por número suficiente de Estados-Membros, tornar-se-á o complemento mais importante desde 2001, visto que possui o potencial de facilitar o intercâmbio de dados para os processos criminais.

A redação do aludido Protocolo será um grande esforço que poderá impactar na forma como os Estados percebem a soberania e a jurisdição no espaço cibernético. Pode expandir as jurisdições dos Estados em relação às investigações de crimes cibernéticos e, portanto, levar a uma cooperação mais efetiva e ao objetivo final de um espaço cibernético mais seguro e aberto para todos que integram o conjunto dos Estados Membros.

Por outro lado, a Convenção de Budapeste sobre o Cibercrime é um documento regional, cuja elaboração foi negociada também em nível regional. E procedimentos idênticos serão adotados nas negociações para a elaboração do Segundo Protocolo Adicional, o que pode ser entendido como uma desvantagem, pela carência de um amplo debate, de abrangência universal.

Outro inconveniente é que, embora seja admitida a participação de Estados não membros do Conselho da Europa, o processo de adesão desses Estados exige convite do Comitê de Ministros do Conselho da Europa, emitido após aquiescência unânime dos Estados contratantes, nos termos do artigo 37.1 da referida Convenção

(COUNCIL OF EUROPE, 2001a). Essa exigência procedimental também foi percebida com inquietude por representantes de Governos, durante a Terceira Sessão do Grupo de Especialistas da UNODC, ligada à Comissão de Prevenção ao Crime e Justiça Penal, da UNODC, realizada no mês de abril de 2017 (UNODC, 2017). Segundo os representantes, essa regra limita a liberdade dos Estados para expressar seu intuito de participar da Convenção. O Brasil, por exemplo, como citado na seção 6, ainda não foi convidado a aderir à Convenção, embora se sobressaia, no cenário mundial, como local de destaque na prática de crimes cibernéticos (EUROPOL, 2015).

8.2 Delineamento da proposta

Diante do exposto nas seções anteriores, que evidenciaram os desafios à localização, preservação, acesso, produção, busca e apreensão extraterritorial de evidências criminais eletrônicas, em ambiente de computação em nuvem, advindos sobretudo da universalização da mobilidade dos dados, é razoável propor a negociação de um instrumento jurídico internacional que viabilize a cooperação direta entre Estado soberano e empresa provedora de serviço de computação em nuvem pública, para permitir que autoridades de persecução criminal possam requisitar evidências eletrônicas, relativas a pessoas investigadas por prática de crimes graves, diretamente a provedor de serviço sediado em território de outro Estado Parte, sem a obrigatoriedade de formalizar acordo bilateral de assistência judiciária em matéria penal, simplificando os procedimentos persecutórios, de forma que não se inviabilizem pela burocracia e morosidade contraproducente à apuração das infrações penais. Por outro lado, a medida também autoriza o provedor de serviço a responder diretamente ao Estado requisitante.

8.3 Premissas que orientam a proposta

Norteiam a proposta apresentada nesta Tese as seguintes premissas:

a) a Internet é uma rede mundial de computadores, democrática, livre, aberta, transnacional, que não respeita fronteiras territoriais, não é propriedade de qualquer empresa ou Estado, nem mantém com este qualquer vínculo formal;
b) o espaço cibernético é mais um “espaço” do que um “lugar”;
c) a computação em nuvem é o estado da arte da mobilidade dos dados;
d) no mundo hiperconectado, com o crescimento da Internet das coisas e da computação em nuvem, dificilmente um crime não deixará evidências eletrônicas na nuvem (UNODC, 2013);
e) a soberania territorial absoluta é incompatível com a Internet e com a computação em nuvem (SVANTESSON, 2016a);
f) o acesso célere às evidências criminais eletrônicas é importante à investigação criminal;
g) o crime cibernético frequentemente apresenta dimensões transnacionais (UNODC, 2017; GUILLOT, 2014; UNODC, 2013; ITU, 2009; ITU, 2012; COSTA, 2011; KOOPS, 2010; FERREIRA, 2007; FERREIRA, 2005);
h) a localização física do dado é de difícil precisão, tendo em conta o fenômeno da “perda da localização”;
i) a “localização dos dados”, por meio de normatizações domésticas, contraria a natureza transnacional da Internet;
j) a distinção entre metadados, dados armazenados e dados em trânsito é relevante ao Direito;
k) o direito de punir as infrações penais é expressão de soberania dos Estados;
l) a igualdade soberana deve ser respeitada;
m) a solução para a localização, preservação, acesso, produção, busca e apreensão de evidências criminais eletrônicas, armazenadas em servidor de computação em nuvem, localizado em Estado estrangeiro, está no Direito Internacional Público.

8.4 Descrição dos requisitos da proposta

A descrição detalhada da proposta é realizada com base nas seguintes etapas:

a) recomendar o mecanismo jurídico a ser utilizado;
b) definir os tipos de evidências eletrônicas de crime suscetíveis de serem requisitadas;
c) estabelecer os crimes graves;
d) determinar os requisitos para um Estado aderir ao tratado internacional;
e) assentar o compromisso principal dos Estados Parte;
f) precisar as condições que autorizam a requisição direta ao provedor de nuvem;
g) determinar as exigências legais por tipo de dados;
h) definir as restrições;
i) estabelecer mecanismos de auditoria e transparência;
j) estabelecer os requisitos de proteção de dados e de respeito à privacidade
k) definir os requisitos de proteção à soberania;
l) estabelecer penalidades.

Nas próximas subseções, as etapas citadas acima estão detalhadas.

8.4.1 O mecanismo jurídico a ser utilizado

A Internet é uma rede mundial de computadores que, por fundamento de sua origem e existência, não respeita fronteiras territoriais. Os dados, que são fragmentados em pacotes, trafegam livremente através da vasta e complexa malha de meios físicos de comunicação, que estão presentes em quase todos os recantos do mundo.

Pela sua natureza transnacional, é conveniente acreditar que a solução para o problema da coleta extraterritorial de evidências criminais deve ser buscada no Direito Internacional Público, por meio da edição de um tratado internacional multilateral, que vincule os Estados participantes a adotarem medidas, no seu Direito

Interno, de forma a possibilitar a superação das adversidades relativas aos problemas descritos no presente trabalho.

Tratado, de acordo com Resek (2014), é um termo genérico para designar todo acordo formal concluído por escrito entre pessoas jurídicas de Direito Internacional Público, e destinado a produzir efeitos jurídicos. Não há regra formal que estabeleça uma tipologia associada aos tratados internacionais. Na prática convencional, os tratados recebem denominações, em função do assunto por eles tratados, de sua finalidade, da qualidade das partes, do número de participantes, dentre outros aspectos (MAZZUOLI, 2015).

Diante das várias terminologias apresentadas, a natureza desta proposta sugere que o tratado a ser celebrado entre os Estados poderia ser formalizado por meio de uma Convenção, um Acordo ou um Protocolo.

A adoção de uma Convenção seria uma alternativa, pois espera-se que sua formalização seja precedida de amplo debate entre os diversos atores interessados na solução do problema, como representantes do Governo dos Estados, a sociedade civil organizada, os doutrinadores e operadores do Direito, autoridades de investigação criminal, os profissionais da tecnologia da informação e comunicação. Grupos de trabalho poderiam ser constituídos e os resultados discutidos em conferências internacionais, sendo, o documento final, a expressão da vontade paralela e uniforme das Partes.

Similarmente, seria possível estabelecer um *Acordo* que, em geral, é o termo empregado para designar tratados bilaterais ou multilaterais que dispõem sobre segurança recíproca, projetos de desarmamento, questões sobre fronteiras, questões de ordem política, dentre outras. Tendo o tratado a ser proposto como objetivo principal deliberar sobre a localização, preservação, acesso, produção, busca e apreensão extraterritorial de evidências eletrônicas de crimes graves, também seria cabível o emprego do termo Acordo.

Um Protocolo, termo geralmente usado para designar acordos menos formais que os tratados ou complementares a acordos pré-existentes, seria conveniente no caso de suplementar a Convenção de Budapeste sobre o Cibercrime, como está sendo proposto pelo Conselho da Europa, ou a Convenção das Nações Unidas contra o Crime Organizado Trasnacional, em concordância com Broadhurst (2006), que a considera um importante instrumento jurídico internacional na luta contra a criminalidade organizada no espaço cibernético.

Independentemente da terminologia adotada ou da estratégia escolhida, são os tratados internacionais o meio que têm os Estados e as organizações intergovernamentais de, a um só tempo, acomodar seus interesses contrastantes e cooperar entre si para a satisfação de suas necessidades comuns (MAZZUOLI, 2015). Portanto, a terminologia escolhida não influencia nos resultados esperados.

8.4.2 Os tipos de evidências criminais eletrônicas suscetíveis de serem requisitadas

São objeto de violação de sigilo para prova em investigação criminal e em instrução processual penal os seguintes tipos de dados:

a) pessoais, relacionados à pessoa natural identificada ou identificável, inclusive números identificativos, dados locacionais ou identificadores eletrônicos, quando estes estiverem relacionados a uma pessoa (BRASIL, 2014). São exemplos os dados cadastrais (nome, prenome, estado civil, profissão do usuário, sexo, data de nascimento, naturalidade, filiação, endereço físico, endereço eletrônico), o número de telefone, as informações de cobrança, o número IP associado a dispositivo utilizado pelo usuário, lista de contatos, dentre outros;
b) de conteúdo, que estão no corpo das comunicações, como o texto de *e-mail*s, arquivos armazenados, dentre outros. Os dados de conteúdo podem estar armazenados em servidores ou em trânsito;
c) registro de conexão, que é o conjunto de informações referentes à data e hora de início e término de uma conexão à internet, sua duração e o endereço IP utilizado pelo terminal para o envio e recebimento de pacotes de dados (BRASIL, 2014);
d) registro de acesso a aplicações de internet, que é o conjunto de informações referentes à data e hora de uso de uma determinada aplicação de internet a partir de um certo endereço IP (BRASIL, 2014).

Essa distinção é relevante para determinar a competência para autorizar a divulgação de dados sob proteção de sigilo.

8.4.3 Os crimes graves

Importa ao contexto da norma internacional a ser editada a investigação e a persecução de crimes graves, considerados como tais aqueles descritos conforme os critérios a seguir:

a) os crimes de competência do Tribunal Penal Internacional, nos termos do artigo 5º do Estatuto de Roma do Tribunal Penal Internacional[124] (crime de genocídio, crimes contra a humanidade, crimes de guerra, crimes de agressão);
b) os crimes definidos em tratados internacionais, tais como os descritos na Tabela 7 (rol meramente exemplificativo);
c) os crimes puníveis, pelo Direito do Estado Parte requisitante, com pena privativa de liberdade, cujo máximo não seja inferior a quatro anos ou com pena superior;
d) os crimes praticados exclusivamente por meio da tecnologia da informação e comunicação e contra recursos da tecnologia da informação e comunicação, desde que a pena prevista seja privativa de liberdade.

[124] Promulgado pelo Brasil através do Decreto nº 4.388, de 25 de Setembro de 2002 (BRASIL, 2002).

Tabela 7 - Infrações penais em tratados internacionais

Conduta criminosa	Tratado internacional	Início vigência
Tráfico de órgãos humanos	Convenção do Conselho da Europa contra o tráfico de órgãos humanos, Santiago de Compostela, 25 de março de 2015.	Depende de adesão de Estados.
Tráfico de armas	Protocolo contra a Fabricação e o Tráfico Ilícito de Armas de Fogo, suas Peças, Componentes e Munições, complementando a Convenção das Nações Unidas contra o Crime Organizado Transnacional, adotado em Nova York, em 31 de maio de 2001.	2005
Corrupção	Convenção das Nações Unidas contra a Corrupção, adotada pela Assembléia-Geral das Nações Unidas, em 31 de outubro de 2003[125]	2005
Organização criminosa Lavagem de produto de crime Lavagem de dinheiro Corrupção	Convenção das Nações Unidas contra o Crime Organizado Transnacional, adotada em Nova York, em 15 de novembro de 2000.	2003
Tráfico de seres humanos	Protocolo Adicional à Convenção das Nações Unidas contra o Crime Organizado Transnacional Relativo à Prevenção, Repressão e Punição do Tráfico de Pessoas, em Especial Mulheres e Crianças, adotado em Nova York em 15 de novembro de 2000. E outras Convenções da ONU.	2003
Terrorismo	Convenção Interamericana Contra o Terrorismo, Bridgetown/Barbados, em 03 de junho de 2002 (OEA, 2002).	2003
Venda de criança, prostituição infantil e pornografia infantil.	Protocolo Facultativo à Convenção sobre os Direitos da Criança referente à venda de crianças, à prostituição infantil e à pornografia infantil, adotado em Nova York em 25 de maio de 2000.	2002
Financiamento ao terrorismo	Convenção Internacional para Supressão do Financiamento do Terrorismo.	2002
Acesso ilegítimo Interceptação ilegítima Interferência em dados Interferência em sistemas Uso abusivo de dispositivos Falsidade informática Burla informática Violação de direitos autorais	Convenção de Budapeste sobre o cibercrime e outros tratados regionais.	2001
Infrações relacionadas ao tráfico de drogas	Convenção contra o Tráfico Ilícito de Entorpecentes e Substâncias Psicotrópicas, concluída em Viena, a 20 de dezembro de 1988.	1990
Tortura	Convenção das Nações Unidas Contra a Tortura e Outros Tratamentos ou Penas Cruéis, Desumanos ou Degradantes[126].	1987
Genocídio	Convenção das Nações Unidas para a Prevenção e a Repressão do Crime de Genocídio, concluída em Paris, a 11 de dezembro de 1948, por ocasião da III Sessão da Assembléia Geral das Nações Unidas[127].	1951

Fonte: direta

[125] Promulgada pelo Brasil por meio do Decreto nº 5.687, de 31 de janeiro de 2006 (BRASIL, 2006).
[126] Promulgada pelo Brasil por meio do Decreto Nº 40, de 15 de fevereiro de 1991 (BRASIL, 1991).
[127] Promulgada pelo Brasil por meio do Decreto nº 30.822, de 06 de maio de 1952 (BRASIL, 1952b).

8.4.4 Os requisitos para um Estado aderir ao tratado internacional

Considerando que deve prevalecer a legislação interna do Estado Parte requerente para disciplinar a requisição de evidências criminais, armazenadas em servidor de nuvem, situado em outro Estado Parte, são requisitos a serem atendidos pelos Estados para aderir ao tratado internacional:

d) existência, no ordenamento jurídico interno, de leis substantivas e processuais, relativamente ao crime cibernético e à coleta de evidências criminais eletrônicas, respectivamente;
e) regulamentação, no direito interno, das causas prováveis que justifiquem a quebra de sigilo, definindo as respectivas autoridades públicas com competência ou atribuição para determinar o ato, considerando a natureza dos dados e o potencial de invasão à privacidade;
f) comprovar a adoção de mecanismos de controle e supervisão, por parte do Estado, das atividades de coleta, retenção, uso e compartilhamento de dados;
g) assumir o compromisso de promover e proteger a livre circulação dos dados e a Internet aberta (ou seja, o compromisso de não legislar sobre a "localização os dados");
h) assumir o compromisso de adotar medidas legislativas e outras que se revelem necessárias para estabelecer mecanismos para minimizar a coleta de dados, restringindo-a unicamente a dados relevantes à investigação criminal;
i) cada Estado Parte enviará ao Secretário Geral da Organização das Nações Unidas a catalogação das leis internas e regulamentos referidos acima, bem como uma cópia de qualquer alteração ulteriormente introduzida a essas leis e regulamentos ou uma descrição dessas leis, regulamentos e alterações ulteriores;
j) um Estado Parte poderá recusar a cooperação que lhe é solicitada, caso a infração a que se refere o pedido não seja abrangida pela Convenção.

8.4.5 O principal compromisso dos Estados Parte

Cada Estado Parte se compromete a adotar medidas legislativas e outras que se revelem necessárias para permitir que provedores de serviço de computação em nuvem respondam diretamente a requisições de localização, preservação, acesso, produção, busca e apreensão de evidências criminais, relativas a pessoas investigadas pela prática de crimes graves, emitidas por autoridades de persecução criminal de qualquer Estado Parte, independentemente de formalização de Acordo de Assistência Judiciária em Matéria Penal.

8.4.6 As condições que autorizam a requisição direta ao provedor de nuvem

São condições que autorizam um Estado Parte a requisitar a divulgação de dados, diretamente a provedor de serviço de computação em nuvem, situado no território de outro Estado Parte:

a) que a conduta investigada constitua crime grave (conforme parâmetros na subseção 8.4.3), no direito interno do Estado Parte requisitante;
b) que exista procedimento investigatório formalmente instaurado para apurar crime grave, fundada em fatos verossímeis, devendo constar em apenso à requisição a descrição da conduta e a correspondente tipificação penal, ressaltando o *quantum* previsto para a pena máxima;
c) que o crime tenha sido praticado dentro das fronteiras territoriais do Estado Parte requisitante, considerando o local do crime como aquele onde a conduta foi praticada, orientado o princípio da ubiquidade;
d) que o crime tenha sido praticado por nacional do Estado Parte requisitante, contra outro nacional desse mesmo Estado Parte, ou contra qualquer pessoa aí residente;
e) que o bem jurídico violado interesse unicamente ao Estado parte requisitante;
f) que a requisição para a localização, preservação, acesso, produção, busca e apreensão de evidências criminais eletrônicas seja autorizada por tribunal, magistrado ou autoridade competente do Estado Parte requisitante, na forma prevista em lei doméstica, demonstrada justa causa e gravidade do fato;

g) que a requisição para a localização, preservação, acesso, produção, busca e apreensão de evidências criminais eletrônicas seja acompanhada e fiscalizada por tribunal, magistrado ou outra autoridade competente do Estado Parte requisitante, nos termos de lei interna;
h) que a informação requerida seja relevante à elucidação do fato criminoso investigado, não sendo possível ser obtida por outros meios, devendo os dados que não interessarem à prova serem inutilizados;
i) que o Estado Parte requisitante se comprometa a não divulgar a autoridade de outro Estado informações sobre o indivíduo investigado, a menos que estejam relacionadas a danos ou ameaças significativas contra nacional desse país ou se refira a crimes contra a segurança nacional, terrorismo, crimes violentos, exploração infantil, fraude financeira significativa;

Autorizam um Estado Parte a requisitar a interceptação de dados de conteúdo em trânsito, diretamente a provedor de serviço de computação em nuvem, situado no território de outro Estado Parte, as seguintes condições, além das citadas acima:

a) quando houver indícios razoáveis da autoria ou participação em infração penal grave;
b) quando a prova não puder ser feita por outros meios disponíveis menos invasivos.

8.4.7 As exigências legais por tipo de dados

O tipo de dado a ser acessado, recuperado, produzido determinará os procedimentos a serem adotados e a autoridade competente para requerer ou determinar o cumprimento da quebra do sigilo.

Assim, relativamente a dados pessoais armazenados, a requisição pode ser realizada por autoridade policial ou membro da Procuradoria de Justiça, legalmente investido da responsabilidade pela persecução criminal. Aliás, no início de uma investigação criminal, dificilmente as autoridades dispõem da identificação do investigado (KRISHNAMURTHY, 2016). A quebra de sigilo, muitas vezes, decorre da necessidade de identificar a pessoa que supostamente cometeu a infração penal.

Quando a informação requerida se tratar de conteúdo de comunicação privada, de arquivo armazenado em conta pessoal protegida por senha, de registro

de conexão e de registro de acesso a aplicações de internet, a divulgação somente poderá ser efetuada mediante ordem judicial, expedida por magistrado ou tribunal competente para o ato, na forma que a lei do Estado Parte estabelecer.

A interceptação de comunicações em trânsito deve ser realizada unicamente mediante ordem judicial, devendo o pedido demonstrar que a sua realização é imprescindível à apuração de infração penal, não podendo exceder o prazo de 15 (quinze) dias, renovável por igual período, uma vez comprovada a indispensabilidade do meio de prova.

Obrigatoriamente, o processo de interceptação das comunicações em trânsito deverá ser fiscalizado por terceira autoridade pública, com competência legal para o ato. Os dados coletados que não interessem à prova serão inutilizados, por meio de procedimentos previstos em lei interna.

8.4.8 As restrições

Não são admitidas as requisições:

a) que tenham por finalidade a investigação de crimes políticos ou de opinião;
b) para subsidiar ações de inteligência, mesmo que sejam voltadas à prevenção da violência criminal;
c) para subsidiar ações que possam significar restrição à liberdade de manifestação do pensamento, de expressão, de comunicação, de atividades intelectuais, artísticas, científicas ou de comunicação;
d) para subsidiar investigação criminal procedida contra cidadão estrangeiro;
e) que intencionalmente a investigação almeje obter informações sobre cidadão estrangeiro, coletada transversalmente por meio de violação de sigilo de um cidadão nacional.

Além das hipóteses acima, será vedado o compartilhamento com outro Estado dos dados obtidos mediante violação legal do sigilo de pessoa investigada, exceto nos casos estabelecidos no tratado.

8.4.9 Os mecanismos de auditoria e transparência

O texto do tratado internacional deve conter disposições atinentes a mecanismos de auditoria e transparência.

Os relatórios de transparência devem ser elaborados periodicamente pelos Estados Parte, devendo apresentar o resumo das requisições realizadas, destacando, pelo menos, as seguintes informações, sob a forma de estatísticas:

a) a origem das requisições;
b) a natureza do objeto pleiteado (se metadados, conteúdo de comunicação, registros de conexão, registros de acesso a aplicações);
c) os pedidos deferidos e indeferidos pelos provedores de serviço;
d) os provedores de serviço aos quais os dados foram requeridos;
e) o número de usuários atingidos por tais solicitações.

É importante também que os provedores mantenham relatórios periódicos de transparência, divulgando, além das informações acima, as remoções realizadas por força de ordem judicial, as solicitações governamentais de remoção de conteúdo. A divulgação dessas informações contribui para a compreensão de como as ações de Governos e empresas afetam a privacidade, a segurança e o acesso à informação.

8.4.10 A proteção de dados e respeito à privacidade

Na elaboração do tratado internacional, a proteção dos dados e o respeito à inviolabilidade do direito fundamental à intimidade e à vida privada dos usuários devem ser considerados, sob dois aspectos.

Primeiramente, sob a ótica da normatização abrangente do direito em vigor nos Estados Parte. Nesse sentido, é relevante avaliar as proteções conferidas aos dados, bem como em que nível a privacidade dos usuários está protegida. No Brasil, por exemplo, a proteção dos dados pessoais é um dos princípios trazidos pelo Marco Civil da Internet (BRASIL, 2014). No tocante à privacidade, a Constituição Federal brasileira (BRASIL, 1988a) confere que são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito à indenização pelo dano material ou moral decorrente de sua violação (artigo 5º, inciso X).

Em segundo lugar, devem ser consideradas as garantias protecionistas conferidas aos cidadãos, relativamente à busca e apreensão de evidências criminais, seja no mundo físico seja no ambiente de computação em nuvem. No direito norte-americano, é oportuno citar a Quarta Emenda à Constituição dos Estados Unidos. No direito brasileiro, a casa é asilo inviolável do indivíduo, ninguém nela podendo penetrar

sem consentimento do morador, salvo em caso de flagrante delito ou desastre, ou para prestar socorro, ou, durante o dia, por determinação judicial (artigo 5º, inc. XI).

Esses aspectos serão relevantes na definição dos critérios autorizadores da participação do Estado como Parte do tratado.

Além de considerar a legislação interna dos Estados, como pré-requisito para que um Estado se torne Parte do tratado, é fundamental definir a base jurídica do próprio tratado, concernente a questões de proteção de dados e respeito à privacidade, que subsidiará os procedimentos de busca e apreensão de evidências criminais eletrônicas, armazenadas em servidor de ambiente de computação em nuvem, situado em território de outro Estado Parte.

Dessa forma, devem ser consideradas normatizações que estejam em vigor em países com expressiva participação no processamento e na distribuição da computação em nuvem, como os Estados Unidos, além de Diretivas, Recomendações e Regulamento Geral vigentes no âmbito do continente europeu, conforme abordado na seção 7.

Ademais, outras questões devem ser consideradas na elaboração do documento, como a divulgação dos dados a Estados que não integram o tratado, o compartilhamento de dados com outros Estados Parte e a notificação prévia do usuário investigado.

Assim, relativamente ao atendimento de requisição de divulgação de dados armazenados, oriunda de um Estado que não aderiu ao tratado, é recomendável que sejam definidos procedimentos.

Outra questão refere-se à entrega de evidências criminais eletrônicas a outro Estado Parte. Via de regra, essa hipótese deve ser vedada, de maneira a evitar possível violação transversal intencional do sigilo de dados. Por outro lado, se as informações coletadas se referirem a danos ou ameaças significativas contra nacional ou bem jurídico protegido pelo Direito de outro Estado Parte, ou se refira a crimes contra a segurança nacional, terrorismo, crimes violentos, exploração infantil, fraude financeira significativa, podem ser repassadas ao Estado Parte diretamente interessado no controle criminal.

Em relação à notificação do usuário ou cliente acerca da divulgação legal de seus dados à instituição governamental, é recomendável estabelecer, como regra geral, a obrigatoriedade de informar previamente o investigado sobre o procedimento, a exemplo do direito norte-americano, conforme disposto no 18 U.S.C §§ 2703

(b)(1)(B)(i) e (b)(2) - *Stored Communications Act* (UNITED STATES, 1986). Como exceções à regra, estão os casos em que a notificação ao usuário pode comprometer a investigação ou oferecer risco às autoridades ou a terceiros (testemunhas, por exemplo) envolvidos no processo. Caberá ao provedor de serviço de computação em nuvem informar ao usuário acerca da divulgação de seus dados, quando não exigido o sigilo pela autoridade pública.

Via de regra, os usuários desconhecem que o sigilo de seus dados eventualmente foi violado, mesmo que exista, no direito norte-americano, a previsão de notificação prévia, quando não há risco às pessoas envolvidas na investigação criminal. Pugh (2017) propõe alterações no ECPA para permitir ao provedor de serviço a defesa, em juízo, dos direitos e interesses relacionados à privacidade dos seus clientes, nas situações em que estes desconhecem a devassa em seus dados.

A promoção e a proteção interna aos direitos fundamentais, principalmente em relação à privacidade e às liberdades civis, também devem ser aspectos analisados, em relação ao Estado que pleiteia a ratificação. Assim, deve ser considerada a existência de normas, no ordenamento jurídico interno do Estado requerente, dispondo acerca da proteção à privacidade e às liberdades civis, inclusive durante a busca e apreensão de evidências criminais eletrônicas, a exemplo da proteção trazida pela Quarta Emenda à Constituição dos Estados Unidos e de vários dispositivos presentes na Carta Magna brasileira, como os constantes no seu artigo 5º (BRASIL, 1988a).

Pela breve análise que foi realizada nos termos da política de privacidade de grandes empresas provedoras de serviço que implementam a tecnologia de computação em nuvem pública, como *Facebook Inc*., a *Google LLC*, *Microsoft Corporation*, foi possível observar que não há clareza sobre a política de localização e controle dos dados dos usuários. A última proposta se insere nessa lacuna e tem por objetivo promover ações que incentivem a prática da transparência relativamente à política de localização e controle dos dados, por parte das empresas provedoras de computação em nuvem, fazendo-as divulgar aos usuários, sempre que possível, a localização dos seus dados, inclusive referindo a eventuais mudanças, decorrentes de características intrínsecas à tecnologia aqui discutida. A criação de uma conta de serviço poderia indicar o momento ideal para informar o usuário, inclusive de angariar a sua anuência.

8.4.11 Proteção da soberania

Os Estados Partes cumprirão as suas obrigações decorrentes do tratado a ser firmado, no respeito pelos princípios da igualdade soberana e da integridade territorial dos Estados Parte, bem como da não-ingerência nos assuntos internos de outros Estados, não autorizando qualquer Estado Parte a exercer, em território de outro Estado, jurisdição ou funções não acordadas ou que o direito interno desse Estado reserve exclusivamente às suas autoridades.

8.4.12 Penalidades

Em caso de violação aos requisitos apresentados, o Estado Parte infrator ficará impedido de requisitar evidências criminais eletrônicas diretamente a provedor de serviço de computação em nuvem, situado no território de outro Estado Parte, até que cesse a situação que motivou o impedimento. Caso a violação seja por parte da empresa, essa responderá perante as leis do Estado Parte onde está sediada ou mantém representação comercial, sem, no entanto, isentá-la de obrigação penal ou civil perante o Estado Parte requisitante.

8.5 Processo participativo para a elaboração do tratado internacional

Preliminarmente, é imprescindível que haja o reconhecimento e a sensibilização mundial, no tocante às dificuldades enfrentadas pelas autoridades de investigação criminal quando se deparam com a necessidade de coletar evidências eletrônicas de crimes, em servidores de ambiente de computação em nuvem, localizados em Estado estrangeiro.

Em nível regional, o Conselho da Europa reconheceu a necessidade de suplementar a Convenção de Budapeste sobre o Cibercrime para dispor acerca das hipóteses autorizadoras ao acesso a evidências criminais eletrônicas armazenadas em ambiente de computação em nuvem (COUNCIL OF EUROPE, 2015), delineando, inclusive, os trabalhos a serem realizados, por meio de Termo de Referência, aprovado em junho de 2017 (COUNCIL OF EUROPE, 2017).

Relativamente aos demais Acordos e Convenções regionais analisados na seção 6, não foi possível identificar iniciativa semelhante a adotada pelo Conselho da

Europa, na elaboração do Segundo Protocolo Adicional à Convenção de Budapeste sobre o Cibercrime.

Diante do exposto, acredita-se que as Nações Unidas sejam o foro legítimo para as negociações de um marco jurídico mundial, um instrumento multilateral, que discipline a localização, preservação, produção, acesso, busca e apreensão extraterritorial de evidências criminais eletrônicas, armazenadas em servidores de computação em nuvem, localizados em terceiro Estado, sem a necessidade de formalização de acordo de assistência judiciária e sem prejuízo dos instrumentos regionais existentes. Além do mais, a ONU é uma organização internacional, de relevância e abrangência mundial.

No âmbito das Nações Unidas, o Escritório sobre Drogas e Crime – UNODC, reúne os requisitos necessários para assumir o protagonismo do processo de elaboração do instrumento proposto nesta Tese.

Atualmente, o UNODC implementa medidas que refletem as três convenções internacionais de controle de drogas e as convenções contra o crime organizado transnacional e contra a corrupção. O trabalho do UNODC está baseado em três grandes áreas: saúde, justiça e segurança pública. Dessa base tripla, desdobram-se temas como drogas, crime organizado, tráfico de seres humanos, corrupção, lavagem de dinheiro e terrorismo, além de desenvolvimento alternativo e de prevenção ao HIV entre usuários de drogas e pessoas em privação de liberdade[128].

Como protagonista, caberia a UNODC coordenar as atividades de negociação de um novo instrumento jurídico internacional, com o propósito de normatizar a localização, preservação, produção, acesso, busca e apreensão de evidências eletrônicas de crimes graves, quando armazenadas em servidores de ambiente de computações em nuvem, dispostos fisicamente em território de Estado estrangeiro.

As atividades de elaboração do tratado devem observar as regras gerais referentes aos tratados firmados entre Estados, constante na Convenção Viena sobre o Direito dos Tratados, concluída em maio de 1969, que regula o desenvolvimento progressivo daquelas matérias ainda não consolidadas em nível internacional. A referida Convenção regula desde questões pré-negociais (capacidade para concluir tratados e plenos poderes), até o processo de formação dos tratados (adoção, assinatura, ratificação, adesão, reservas etc), sua entrada em vigor, aplicação

[128] https://www.unodc.org/lpo-brazil/pt/sobre-unodc/index.html.

provisória, observância e interpretação, bem como a nulidade, extinção e suspensão de sua execução.

O processo de negociação ocorreria por meio de processo participativo, envolvendo vários atores (*stakholders*), como representantes de Governos, acadêmicos do direito e da ciência da computação, operadores do direito, representantes de empresas provedoras de serviço de computação em nuvem, sociedade civil organizada.

Entende-se que já foi iniciado um processo de construção de conhecimento, amplo e abrangente, acerca do crime cibernético, com abordagens relativas a legislações nacionais e internacionais, melhores práticas adotadas nos países, assistências técnica e cooperação internacional, coleta de evidências eletrônicas, dentre outras, com a elaboração e apresentação, em 2013, do *Comprehensive Study on Cybercrime* (UNODC, 2013), pelo Grupo de Especialistas da UNODC para o crime cibernético. E os trabalhos do grupo continuam (nos termos da Declaração de Doha), podendo inclusive subsidiar a elaboração da Convenção.

É importante também a realização de conferências internacionais e regionais, com vistas a coletar posicionamentos dos vários setores da sociedade, em todos os continentes.

São fatores críticos de sucesso a participação, na coordenação das atividades, de representantes de países que concentram número expressivo de empresas e *data centers* de computação em nuvem (Estados Unidos, por exemplo), bem como de representantes de países ou instituições que adotam tradicionalmente modelos legais de proteção de dados e respeito à privacidade (países da Europa, Conselho da Europa, por exemplo).

8.6 Comparação entre o modelo proposto a os pesquisados

Nesse momento, cabe ressaltar as diferenças entre o modelo proposto nesta Tese e os modelos analisados na seção 7.

A Tabela 8 apresenta as características gerais das normas analisadas, comparando-as com a proposta final da Tese. A Tabela 9 compara os tipos de dados, ofensividade e diligências propostas.

Tabela 8 - Características gerais das propostas analisadas, em comparação ao modelo apresentado

Aspecto	Proposta da Tese	Conselho da Europa (*)	DoJ Estados Unidos	Daskal;Woods (2015) e Currie (2017)	Woods (2016)
Tipo da norma	Tratado internacional	Protocolo adicional à Convenção de Budapeste	Acordo	Acordo	Interna (Estados Unidos).
Alcance da norma	Universal	Regional	-	-	-
Natureza do tratado	Multilateral	Multilateral	Bilateral (Estados Unidos X outro país)	Bilateral (Estados Unidos X outro país)	Bilateral (Estados Unidos X outro país)
Origem	Negociações internacionais, coordenadas pela ONU	Estudo do Conselho da Europa	Estados Unidos (Projeto de Lei DOJ)	Estados Unidos	Estados Unidos
Coordenação	ONU	Conselho da Europa	Estados Unidos	Estados Unidos	Estados Unidos
MLAT	Não há necessidade.	Complementa o MLAT.	Complementa o MLAT.	Não há necessidade.	-
Auditoria e transparência	Pelo Estado e pelas empresas provedoras de serviço.	Pelo Estado e pelas empresas provedoras de serviço.	Pelo Estado e pelas empresas provedoras de serviço.	Pelo Estado e pelas empresas provedoras de serviço.	-
Política de localização e controle dos provedores	Informar ao usuário a localização dos seus dados.	-	-	-	-

(*) considerando os requisitos que norteiam o Termo de Referência para a elaboração da proposta do Segundo Protocolo Adicional à Convenção de Budapeste sobre o Cibercrime.

Tabela 9 - Comparação entre os tipos de dados, ofensividade e diligências propostas

Aspecto	Proposta apresentada	Conselho da Europa (*)	DoJ Estados Unidos	Daskal;Woods (2015) e Currie (2017)	Woods (2016)
Tipos de dados	Dados pessoais; dados de conteúdo; dados em trânsito; registro de conexão; registro de acesso.	Dados pessoais.	Dados pessoais; dados em trânsito; Metadados; outros tipos de dados.	-	-
Exigências legais por tipo de dados	Dados pessoais podem ser requisitados por autoridade policial. Os demais e a interceptação, via ordem judicial.	Autoridade judicial.	Autoridade judicial.	Autoridade judicial.	Autoridade judicial.
Diligências	Localização, preservação, produção, acesso e busca e apreensão de evidências criminais eletrônicas armazenadas; Interceptação de dados em trânsito.	-	Acesso e divulgação de dados armazenados; Interceptação de dados em trânsito.	Requisição de dados armazenados.	-
Notificação prévia do usuário	Via de regra, o usuário deverá ser informado, pelo provedor, exceto quando comprometa a investigação.	Não dispõe. Entende que essa revelação pode comprometer a investigação.	-	Cabe ao Estado requisitante.	-
Ofensividade da conduta	Crimes graves, conforme subseção 8.4.3.	-	Crimes graves (crime violento, exploração infantil, fraude financeira significativa, crime organizado transnacional) e crimes contra a segurança nacional (terrorismo).	Punível com pelo menos 01 (um) ano de encarceramento.	Terrorismo.

(*) considerando os requisitos que norteiam o Termo de Referência para a elaboração da proposta do Segundo Protocolo Adicional à Convenção de Budapeste sobre o Cibercrime.

Os requisitos para adesão dos Estados Parte ao tratado internacional estão na Tabela 10. As restrições que vedam a requisição de dados para constituir evidências de crime são apresentadas na Tabela 11. As exigências para requisitar diretamente ao provedor de computação em nuvem, situado no território de outro Estado Parte encontra-se na Tabela 12.

Tabela 10 - Comparação entre os requisitos de adesão ao tratado

Aspecto	Proposta apresentada	Conselho da Europa (*)	DoJ Estados Unidos	Daskal;Woods (2015) e Currie (2017)	Woods (2016)
Promoção e respeito aos direitos humanos.	Exige.	-	Exige.	Exige.	Exige.
Reciprocidade.	Exige.	Exige.	Exige.	Exige.	-
Direito interno sobre o cibercrime e coletas de evidências.	Exige.	-	Exige.	-	
Regulamento interno sobre quebra de sigilo.	Exige	-	-	-	-
Mecanismos de controle e supervisão	Exige.	-	-		
Promover internamente a livre circulação dos dados	Exige.	-	Exige.	-	-
Catalogação de leis internas	Cada Estado deve enviar à ONU catálogo de leis e regulamentos.	-	-	-	-

(*) considerando os requisitos que norteiam o Termo de Referência para a elaboração da proposta do Segundo Protocolo Adicional à Convenção de Budapeste sobre o Cibercrime.

Tabela 11 - Restrições na requisição de dados digitais

Aspecto	Proposta apresentada	Conselho da Europa (*)	DoJ Estados Unidos	Daskal;Woods (2015) e Currie (2017)	Woods (2016)
Investigação de crimes políticos ou de opinião	Não admite.	-	-	-	-
Restrição de liberdade expressão/ pensamento	Não admite.	-	Não admite.	Não admite.	
Subsidiar ações de inteligência	Não admite.	-	-	-	-
Investigação contra estrangeiro	Não admite.	-	-	-	-
Investigação contra cidadão ou residente dos Estados Unidos	-	-	Não admite.	Não admite.Os envolvidos devem estar fora da jurisdição dos Estados Unidos.	Não admite.
Compartilhar dados com outro Estado	Não admite.	-	Não admite.	Não admite.	Não admite.

(*) considerando os requisitos que norteiam o Termo de Referência para a elaboração da proposta do Segundo Protocolo Adicional à Convenção de Budapeste sobre o Cibercrime.

Tabela 12 - Exigências para requisitar diretamente ao provedor de computação em nuvem

Aspecto	Proposta apresentada	Conselho da Europa (*)	DoJ Estados Unidos	Daskal;Woods (2015) e Currie (2017)	Woods (2016)
Norma penal considerada	Do Estado requisitante	-	Do Estado requisitante.	Do Estado requisitante.	-
Alteração de legislação interna	Estado parte altera legislação interna, permitindo que Estado Parte estrangeiro requisite diretamente a provedor que tem sede ou armazena dados em seu território.	Inerente às normas do Conselho da Europa.	Alterar ECPA para permitir que provedores norte-americanos respondam diretamente a requisições realizadas por Estados estrangeiros (autorizados) para obter dados em solo norte-americano.	Alterar ECPA para permitir que provedores norte-americanos respondam diretamente a requisições estrangeiras.	Alterar ECPA para permitir que provedores norte-americanos respondam diretamente a requisições realizadas por Estados estrangeiros (autorizados) para obter dados em solo norte-americano.
Demonstrar justa causa e gravidade do fato	Exige.	-	Exige.	Exige.	-
Exista processo investigatório formalmente instaurado	Exige.	-	-	-	-
Crime praticado dentro do território do requisitante	Exige.	-	-	-	-
Crime praticado por nacional do requisitante	Exige.		Exige.	-	-
Vítima é nacional do Estado requisitante	Exige.		Exige.		
Bem jurídico violado interesse unicamente ao Estado requisitante	Exige.	-	-	-	-
Requisições acompanhadas e fiscalizadas por terceira autoridade do Estado requisitante	Exige.	-	-	-	-
Não é possível obter a informação por outra via.	Exige.	-	Exige.	Exige.	-
Pedido individualizado	Informações sobre o indivíduo investigado, conta ou dispositivo a ser devassado.	-	Informações sobre o indivíduo investigado, conta ou dispositivo a ser devassado.	Informações sobre o indivíduo investigado, conta ou dispositivo a ser devassado.	

(*) considerando os requisitos que norteiam o Termo de Referência para a elaboração da proposta do Segundo Protocolo Adicional à Convenção de Budapeste sobre o Cibercrime.

9 CONSIDERAÇÕES FINAIS

Esta última seção resulta do encerramento das atividades da pesquisa encetada, colimando a elaboração da Tese, cujo tema, por sua complexidade, globalidade e constante evolução nos parâmetros do direito internacional e da ciência da computação, constitui desafio de múltiplas possibilidades a transcender os limites de um Doutorado, malgrado o esforço de exaurir o essencial do universo enfocado.

Primeiramente, foram apresentados os principais obstáculos relacionados ao acesso extraterritorial a evidências criminais eletrônicas, armazenadas em servidor de computação em nuvem, sobre território de Estado estrangeiro. Em seguida, o espaço cibernético no direito internacional foi estudado, com o objetivo de trazer à tona as acepções relacionadas à virtualidade desse espaço e sua relação com o Direito. Da análise dos tratados internacionais que tratam do controle da criminalidade cibernética, objeto de estudo da seção 6, foi possível constatar a inexistência de norma internacional universal sobre o crime cibernético, merecendo destaque a Convenção do Conselho da Europa sobre o Cibercrime, que é o documento mais importante na área, cujo teor deixou *in albis*[129] a disciplina da questão aqui explorada.

Outra importante referência ao tema foi o *Microsoft Ireland Case*, que revelou ao mundo um processo judicial, envolvendo a empresa norte-americana *Microsoft Corporation* e o Governo dos Estados Unidos, relativamente ao cumprimento de mandado de busca e apreensão de evidências criminais eletrônicas, armazenadas em ambiente de computação em nuvem, sobre o território da República da Irlanda. A importância do tema foi tamanha que motivou a Suprema Corte dos Estados Unidos a conhecer do *writ of certiorari,* impetrado pelo Departamento de Justiça dos Estados Unidos, em 2017, para análise e deliberação acerca da seguinte questão: se provedor de serviço de *e-mail*, localizado nos Estados Unidos, é obrigado a cumprir mandado (*Warrant*), expedido com base em causa provável, nos termos do 18 USC § 2703 do SCA, para violar sigilo de comunicações eletrônicas sob o controle do provedor, mesmo que esse provedor tenha decidido por armazenar os dados em território estrangeiro. A decisão final é aguardada.

[129] Livre tradução da autora do latim: “em branco”.

Por fim, a contribuição principal dessa Tese é apresentada na seção 8, por meio de proposta de edição de tratado internacional, multilateral e vinculante, que regule a cooperação direta entre Estado soberano e empresa provedora de serviço de computação em nuvem pública, para permitir que autoridades de persecução criminal possam requisitar evidências eletrônicas, relativas a pessoas investigadas por prática de crimes graves, diretamente a provedor de serviço sediado em território de outro Estado Parte, sem a obrigatoriedade de formalizar acordo bilateral de assistência judiciária em matéria penal.

9.1 Respostas às perguntas de pesquisa

Questionou-se, desde o início das atividades de pesquisa, onde estaria a solução para o complexo problema identificado e descrito ao longo dessa Tese. A busca por uma solução, na tecnologia da informação, foi uma constante, justificada pela natureza do programa ao qual está submetido esse trabalho, embora numa linha de pesquisa multidisciplinar (Análise Multidisciplinar do Cibercrime).

Ocorre que, como o objeto de estudo constitui-se primordialmente em dados digitais ou ambientes virtuais, chancelados com a restrição de sigilo, é difícil idealizar uma ferramenta tecnológica que os explore, devasse em busca de evidências de crime, sem violar a soberania de estado estrangeiro, considerando a multijuridicidade característica da nuvem computacional.

Aplicativos inteligentes, que monitoram o ambiente de computação em nuvem a procura de indícios de prática de crimes, são válidos quando se trata de área aberta à livre circulação e navegação de todos os usuários, indistintamente. Mas não se aplicam ao espaço virtual restrito, protegido por senhas e cifras, que guardam segredos legítimos de seus proprietários, invioláveis até que o Direito disponha em contrário. Aliás, se tecnicamente é possível vasculhar a intimidade dos usuários no referido ambiente, juridicamente pode se constituir em conduta criminosa.

Da análise realizada na seção 6, foi possível verificar que os tratados internacionais vigentes, em matéria de segurança da informação e criminalidade cibernética, são todos de alcance regional e não regulam a localização, preservação, acesso, produção, busca e apreensão extraterritorial de evidências criminais, armazenadas em servidor de computação em nuvem, sobre território estrangeiro.

A Convenção de Budapeste sobre o Cibercrime e a Convenção da Liga dos Estados Árabes sobre o Combate às Ofensas contra a Tecnologia da Informação aludem ao acesso extraterritorial a dados localizados em Estado estrangeiro, desde que abertos e disponíveis para acesso irrestrito. No entanto, os dados protegidos por sigilo são imprestáveis à prova no processo penal, se recolhidos sem observância às exigências prevista em lei. A busca e apreensão de evidências são diligências também referidas pelas Convenções, permitidas apenas no âmbito interno de cada Estado Parte.

Por fim, é recomendado a negociação de um novo tratado internacional que regule a cooperação direta entre Estado soberano e empresa provedora de serviço de computação em nuvem pública, para permitir que autoridades de persecução criminal possam requisitar evidências eletrônicas, relativas a pessoas investigadas por prática de crimes graves, diretamente a provedor de serviço sediado em território de outro Estado Parte, sem a necessidade de formalizar acordo bilateral de assistência judiciária em matéria penal. A medida também autoriza que o provedor de computação em nuvem responda diretamente ao Estado requisitante. Devem orientar a sua elaboração os requisitos descritos na proposta final apresentada.

9.2 Recomendações para trabalhos futuros

O tema aqui estudado não se exaure na abordagem apresentada. Recomenda-se, então, pesquisas sobre vários temas, como:

a) a investigação criminal na *Dark Web* e a legalidade das técnicas de infiltração e *hacking,* na obtenção de evidências eletrônicas para instruir processo penal;
b) a localização, preservação, acesso, produção, busca e apreensão extraterritorial de evidências eletrônicas armazenadas em nuvem, no processo civil;
c) detalhamento da metodologia para negociação de tratado internacional que regule a cooperação direta entre Estado soberano e empresa provedora de serviço de computação em nuvem pública, para fins de produção de prova no processo penal;

d) a proteção de dados no resguardo ao direito fundamental da privacidade e sua proporcionalidade com a proteção da segurança pública, que pertine à paz e à tranquilidade social.

9.3 Conclusão final

O tema da Tese é indissociável de ampla abordagem jurídica, em particular no que concerne à apuração de certos crimes e de sua autoria, sem divórcio ou indiferença à computação em nuvem, no tocante aos princípios, à ética, aos meandros de sua concretude dentro da virtualidade.

O objeto do presente estudo é complexo, transcende aos limites estritos do Direito (Direito Internacional, Direito Penal, Direito Processual Penal) e da ciência da computação. Não há compartimentação estanque, isolacionista de ambos, dado que são enfocados como se num estado de existência imbricado, amalgamado, um em função do outro. A prova do crime como necessidade indeclinável do direito para esclarecer o delito e fundamentar-lhe a punição. A mesma prova da materialidade do fato que não pode ser, quando contida em nuvem, acessada a olho nú, coligida para os autos do processo sem a interveniência da tecnologia, do computador, da Internet, que a tornem visível na sua inconcretude aparente da virtualidade.

O armazenamento de dados em nuvem não põe esses dados fora da incidência jurídica, mormente quando os mesmos constituem prova da criminalidade e da autoria de uma conduta. Tornar inacessíveis, indevassáveis, os dados armazenados em nuvem, fora do Estado em que uma infração penal foi perpetrada e da qual eles são prova, alegando-se ser preciso preservar-lhes o sigilo, seria o mesmo que admitir-se a impunidade em nome dessa preservação, colocando-a acima dos direitos fundamentais das pessoas ofendidas.

O valor da tecnologia e de seus fundamentos não pode ignorar o valor jurídico que permeia as interrelações sociais, e muito menos sobrepor-se a ele como se a virtualidade da nuvem fosse um valor em si mesmo, indisciplinável, de imperatividade absoluta, maior que a do Direito.

Tratou-se, pois, da virtualidade, não como ciência da informática, mas como fenômeno resultante da tecnologia da informação e comunicação em suas implicações correlacionadas ao Direito, na medida em que se pressupõe a ilicitude penal de comportamentos que deixam rastros, indícios, vestígios, provas

armazenadas em nuvem que, se não forem acessíveis à persecução penal, tornarão os crimes impuníveis, estimulando a criminalidade.

O crescimento da criminalidade, instrumentalizada em sua propagação pela Internet, criou uma necessidade coletiva, de natureza pública e transnacional, de proteção, de segurança, de prevenção à ofensividade, frequentemente massiva desses delitos, tornando imperativo o estabelecimento urgente de normas que lastreiem o esforço de apurar e punir essas infrações penais, o que certamente fica inviável se não houver a colaboração mútua dos Estados soberanos na persecução penal.

Em nome de quaisquer princípios ou argumentos, obstar o esclarecimento dos crimes e a punição dos criminosos por estarem os vestígios da autoria e da materialidade dos delitos em nuvem, sobre território estrangeiro, seria como transformar um termo de expectativa feliz, esperança de chuvas nas regiões de sol e aridez inclementes, em prenúncio de devastação social e tempestade.

Normas internacionais regulam a conduta de Estados soberanos, pertinente aos diversos tipos de espaços territoriais, mas o espaço virtual, por suas intrínsecas qualidades a torná-lo discutível no tocante à sua localização e constituição, mesmo espacial, até hoje, malgrado a necessidade evidente de disciplinar a relação estatal com o mesmo, permanece a lacuna que desampara a sociedade, exposta à ganância de criminosos que permanecem impunes, pela falta de rastro e de rosto.

É desafiante tentar condicionar o poder soberano de alguns países, que muitas vezes afrontam o bom senso e até os direitos fundamentais da humanidade, mas a evolução da história do mundo seria impossível se não fosse permeada de sonhos, em busca de transformações da realidade. Foi assim na abolição da escravatura, na emancipação da mulher, na conquista da liberdade e da igualdade entre as pessoas. Será assim também, no empenho por uma Internet livre da criminalidade, a serviço exclusivamente do bem, onde a união de todos construa paz, segurança, inofensividade, uso exclusivo na estruturação de um convívio global novo, escoimado de vícios que, atualmente, provocam medo, causam prejuízos, comprometem a tranquilidade da sociedade.

REFERÊNCIAS

AFRICA UNION. **African Union Convention on Cyber Security and Personal Data Protection**. Adotada pela 23 Seção Ordinária da Assembleia da União Africana, Malabo, 27 de junho de 2014. Disponível em: <https://ccdcoe.org/sites/default/files/documents/AU-270614-CSConvention.pdf>. Acesso em: 20 jun. 2016.

_____. Constitutive Act of The African Union. **Constitutive Act of The African Union Adopted by the Thirty-Sixth Ordinary Session of the Assembly of Heads of State and Government**. Lome, Togo. 11 JUL 2000. Disponível em: <https://au.int/sites/default/files/pages/32020-file-constitutiveact_en.pdf>. Acesso em: 11 set. 2017.

ARMBRUST, Michael; FOX, Armando; GRIFFITH, Rean; JOSEPH, Anthony D.; KATZ, Randy; KONWINSKI, Andy; LEE, Gunho; PATTERSON, David; RABKIN, Ariel; STOICA, ion; ZAHARIA, Matei. A View of Cloud Computing. Clearing the clouds away from the true potential and obstacles posed by this computing capability. **Communications of the Acm**, New York, NY, USA, V. 53, Issue 4, p. 50-58, abr. 2010. Disponível em: <http://delivery.acm.org/10.1145/1730000/1721672/p50-armbrust.pdf?ip=187.58.106.135&id=1721672&acc=OPEN&key=4D4702B0C3E38B35%2E4D4702B0C3E38B35%2E4D4702B0C3E38B35%2E6D218144511F3437&CFID=843544713&CFTOKEN=96499656&__acm__=1474893820_bade16e4938ee4b63a8ef92ef5fa0981>. Acesso em: 26 set. 2016.

ATTFIELD, Philip. United States *v.* Gorshkov: Detailed Forensics and Case Study; Expert Witness Perspective. In: First International Workshop on Systematic Approaches to Digital Forensic Engineering (SADFE'05), 2005, Taipei, Taiwan. **IEEE Xplore**, fev. 2006. Disponível em: <http://ieeexplore.ieee.org/document/1592518/?part=1>. Acesso em: 30 set. 2017.

BANCO MUNDIAL. **Relatório sobre o Desenvolvimento Mundial de 2016**: Dividendos Digitais. 2016. Disponível em: <http://www-wds.worldbank.org/external/default/WDSContentServer/WDSP/IB/2016/01/13/090224b08405bbbe/1_0/Rendered/PDF/Relat0rio0sobr0digitais0vis0o0geral.pdf>. Acesso em: 25 abr. 2016.

BAUTISTA, Christian Brazil. 47 percent of American adults were hacked in the last year. **Digital Trends**. United States of America, 28 mai. de 2014. Disponível em: <https://www.digitaltrends.com/mobile/research-almost-half-of-american-adults-hacked/#!SAXd2>. Acesso em: 25 set. 2017.

BECHARA, Fabio Ramazzini. **Cooperação Jurídica Internacional em Matéria Penal**. A eficácia da prova produzida no exterior. São Paulo: Saraiva, 2011.

BECHTEL, Calistha. **Cloud Computing and Forensic Accounting**: Friends or Foes? February, 15, 2013. Disponível em: https://ssrn.com/abstract=2218697>. Acesso em: 30 mar. 2017.

BELGIË. Hof van Cassatie van België. Arrest. Nr. P.13.2082.N. 1 dez 2015. Disponível em: <http://jure.juridat.just.fgov.be/pdfapp/download_blob?idpdf=N-20151201-1>. Acesso em: 16 set. 2017.

BITENCOURT, Cezar Roberto. **Tratado de Direito Penal**. 14 ed. São Paulo: Saraiva, 2009.

BLAKESLEY, C.L.; STIGALL, Dan. Wings For Talons: The Case for Extraterritorial Jurisdiction Over Sexual Exploitation of Children Through Cyberspace. University of Nevada, Las Vegas, 2004. Disponível em: <http://scholars.law.unlv.edu/cgi/viewcontent.cgi?article=1317&context=facpub>. Acesso em: 10 out. 2017.

BOLT BERENEK AND NEWMAN Inc. A History of the Arpanet. The first decade. **Report nº 4799**. Prepared for DARPA by Bolt Berenek and Newman, Inc. Arlington, Virginia/ United States of America, April, 1981. Disponível em: <http://oai.dtic.mil/oai/oai?verb=getRecord&metadataPrefix=html&identifier=ADA115440 >. Acesso em: 15 jul. 2016

BRANDÃO, Claudio. **Curso de Direito Penal**. Parte Geral. Rio de Janeiro: Forense, 2008.

BRASIL. **Constituição da República Federativa do Brasil de 1988**. Disponível em: < http://www.planalto.gov.br/ccivil_03/Constituicao/Constituicao.htm>. Acesso em: 10 set. 2016. a

_____. **Decreto n° 5.687, de 31 de janeiro e 2006**. Promulga a Convenção das Nações Unidas contra a Corrupção, adotada pela Assembléia-Geral das Nações Unidas em 31 de outubro de 2003 e assinada pelo Brasil em 9 de dezembro de 2003. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2004-2006/2006/decreto/d5687.htm>. Acesso em: 01 jul. 2017.

_____. **Decreto nº 1.530, de 22 de junho de 1988**. Declara a entrada em vigor da Convenção das Nações Unidas sobre o Direito do Mar, concluída em Montego Bay, Jamaica, em 10 de dezembro de 1982. Disponível em: < http://www.planalto.gov.br/ccivil_03/decreto/1995/D1530.htm>. Acesso em: 15 set. 2016. b

_____. **Decreto nº 1.570, de 13 de abril de 1937.** Promulga as Convenções sobre direitos e deveres dos Estados e sobre Asilo político, assinadas em Montevidéo a 26 de dezembro de 1933, por ocasião da Sétima Conferência internacional americana. Disponível em: <http://www.planalto.gov.br/ccivil_03/decreto/1930-1949/D1570.htm>. Acesso em: 25 mai. 2017.

_____. **Decreto nº 19.841, de 22 de outubro de 1945**. Promulga a Carta das Nações Unidas, da qual faz parte integrante o anexo Estatuto da Corte Internacional de Justiça, assinada em São Francisco, a 26 de junho de 1945, por ocasião da Conferência de Organização Internacional das Nações Unidas. Disponível em: < http://www.planalto.gov.br/ccivil_03/decreto/1930-1949/d19841.htm>. Acesso em: 25 set. 2017.

_____. **Decreto nº 3.810, de 02 de maio de 2001**. Promulga o Acordo de Assistência Judiciária em Matéria Penal entre o Governo da República Federativa do Brasil e o Governo dos Estados Unidos da América, celebrado em Brasília, em 14 de outubro de 1997, corrigido em sua versão em português, por troca de Notas, em 15 de fevereiro de 2001. Disponível em: <http://www.planalto.gov.br/ccivil_03/decreto/2001 /D3810.htm>. Acesso em: 24 mai. 2016.

_____. **Decreto nº 30.544, de 14 de fevereiro de 1952**. Promulga a Carta da Organização dos Estados Americanos, firmada em Bogotá, a 30 de abril de 1948. Disponível em: <http://www2.camara.leg.br/legin/fed/decret/1950-1959/decreto-30544-14-fevereiro-1952-340000-publicacaooriginal-1-pe.html>. Acesso em: 10 set. 2016. a

_____. **Decreto nº 30.822, de 06 de maio de 1952**. Promulga a Convenção para a Prevenção e a Repressão do Crime de Genocídio, concluída em Paris, a 11 de dezembro de 1948, por ocasião da III Sessão da Assembléia Geral das Nações Unidas. Disponível em: <http://www2.camara.leg.br/legin/fed/decret/1950-1959/decreto-30822-6-maio-1952-339476-publicacaooriginal-1-pe.html>. Acesso em: 08 set. 2017.b

_____. **Decreto nº 40, de 15 de fevereiro de 1991**. Promulga a Convenção Contra a Tortura e Outros Tratamentos ou Penas Cruéis, Desumanos ou Degradantes. Disponível em: <http://www.planalto.gov.br/ccivil_03/decreto/1990-1994/D0040.htm>. Acesso em: 25 set. 2017.

_____. **Decreto nº 4.388, de 25 de setembro de 2002**. Promulga o Estatuto de Roma do Tribunal Penal Internacional. Disponível em: <http://www.planalto.gov.br/ccivil_03/decreto/2002/D4388.htm>. Acesso em: 25 set. 2017.

_____. **Decreto Nº 5.015, de 12 de março de 2004**. Promulga a Convenção das Nações Unidas contra o Crime Organizado Transnacional. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2004-2006/2004/decreto/d5015.htm>. Acesso em: 30 set. 2016.

_____. **Decreto nº 56.435, de 8 de junho de 1965**. Promulga a Convenção de Viena sôbre Relações Diplomáticas. Disponível em: <http://www.planalto.gov.br/ccivil_03/decreto/Antigos/D56435.htm>. Acesso em: 10 set. 2016.

_____. **Decreto nº 592, de 6 de julho de 1992**. Atos Internacionais. Pacto Internacional sobre Direitos Civis e Políticos. Promulgação. Disponível em: < http:// www.planalto.gov.br/ccivil_03/decreto/1990-1994/d0592.htm>. Acesso em: 30 mai. 2016.

_____. **Decreto nº 61.078, de 26 de julho de 1967**. Promulga a Convenção de Viena sôbre Relações Consulares. Disponível em: <http://www.planalto.gov.br/ccivil_03/decreto/d61078.htm>. Acesso em: 10 jun. 2017.

_____. **Decreto nº 64.362, de 17 de abril de 1969**. Promulga o Tratado sôbre Exploração e Uso do Espaço Cósmico. Disponível em: <http://legis.senado.gov.br/legislacao/ListaPublicacoes.action?id=118828>. Acesso em: 10 set. 2016. a

_____. **Decreto nº 7.030, de 14 de dezembro de 2009**. Promulga a Convenção de Viena sobre o Direito dos Tratados, concluída em 23 de maio de 1969, com reserva aos Artigos 25 e 66. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2007-2010/2009/decreto/d7030.htm>. Acesso em: 25 mai. 2017.

_____. **Decreto nº 75.963, de 11 de julho de 1975**. Promulga o Tratado da Antártida. Disponível em: <http://www.planalto.gov.br/ccivil_03/decreto/1970-1979/D75963.htm>. Acesso em: 10 out. 2017.

_____. **Decreto nº 8.771, de 11 de maio de 2016**. Regulamenta a Lei no 12.965, de 23 de abril de 2014, para tratar das hipóteses admitidas de discriminação de pacotes de dados na internet e de degradação de tráfego, indicar procedimentos para guarda e proteção de dados por provedores de conexão e de aplicações, apontar medidas de transparência na requisição de dados cadastrais pela administração pública e estabelecer parâmetros para fiscalização e apuração de infrações. Disponível em: < http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2016/Decreto/D8771.htm>. Acesso em: 25 set. 2017.

_____. **Decreto nº 99.165, de 12 de março de 1990**. Promulga a Convenção das Nações Unidas sobre o Direito do Mar. Disponível em: <http://www2.camara.leg.br/legin/fed/decret/1990/decreto-99165-12-marco-1990-328535-publicacaooriginal-1-pe.html>. Acesso em: 16 set 2017.

_____. **Decreto-lei nº 1.001, de 21 de outubro de 1969**. Código Penal Militar. Disponível em: <http://www.planalto.gov.br/ccivil_03/decreto-lei/Del1001.htm>. Acesso em: 10 set. 2016. b

_____. **Decreto-lei nº 2.848, de 7 de dezembro de 1940**. Código Penal. Disponível em: <http://www.planalto.gov.br/ccivil_03/decreto-lei/Del2848compilado.htm>. Acesso em: 10 set. 2016.

_____. **Decreto-lei nº 3.689, de 3 de outubro de 1941.** Código de Processo Penal. Disponível em: <http://www.planalto.gov.br/ccivil_03/decreto-lei/Del3689.htm>. Acesso em: 10 set. 2016.

_____. **Lei nº 12.965, de 23 de abril de 2014**. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm>. Acesso em: 30 mai. 2017.

_____. **Lei nº 13.441, de 08 de maio de 2017**. Altera a Lei nº 8.069, de 13 de julho de 1990 (Estatuto da Criança e do Adolescente), para prever a infiltração de agentes de polícia na internet com o fim de investigar crimes contra a dignidade sexual de criança e de adolescente. Disponível em: < http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2017/Lei/L13441.htm>. Acesso em: 20 dez. 2017.

_____. Tribunal Regional Federal da 3ª Região. Escola de Magistrados. **Investigação e prova nos crimes cibernéticos**. São Paulo: EMAG, 2017. Disponível em: <http://www.trf3.jus.br/documentos/emag/Midias_e_publicacoes/Cadernos_de_Estudos_Crimes_Ciberneticos/Cadernos_de_Estudos_n_1_Crimes_Ciberneticos.pdf > Acesso em: 04 dez. 2017.

_____. Tribunal Regional Federal da 4ª Região. Quebra de sigilo em mensagens eletrônicas: TRF4 ordena que Google forneça conteúdo de mensagens enviadas e recebidas por usuário do Gmail investigado em representação criminal. Mandado de Segurança Nº 2009.04.00.011335-1/PR. Relator: Juiz Federal José Paulo Baltazar Junior. Rel. Acórdão: Juíza Federal Salise Monteiro Sanchotene. Impetrante: Google Brasil Internet Ltda. 11 jun 2013. **Boletim Jurídico**, n. 136, Justiça Federal, Tribunal Regional Federal da 4ª Região, Emagis – Escola da Magistratura do TRF da 4ª Região. 2013. Disponível em: <http://www.conteudojuridico.com.br/pdf/cj044538.pdf>. Acesso em: 4 jun. 2017.

BRENNAN CENTER FOR JUSTICE et al. United States District Court Southern District of New York. In the Matter of a Warrant to Search a Certain E-Mail Account Controlled and Maintained by Microsoft Corporation. Microsoft v. United States. **Brief for Amici Curiae Brennan Center for Justice at NYU School of Law, American Civil Liberties Union, The Constitution Project, And Electronic Frontier Foundation in Support of Appellant.** New York, New York, Case 13-MAG-2814, 15 dec., 2014. Disponível em: <https://www.eff.org/document/eff-brennan-center-aclu-constitution-project-second-circuit-amicus-brief-support-microsoft>. Acesso em: 25 set. 2017.

BROADHURST, Roderic. Developments in the Global Law Enforcement of Cyber-Crime. **Policing**: an International Journal of Police Strategies and Management, v. 29(3), 2006. p. 408-433. Disponível em: <https://ssrn.com/abstract=2089650>. Acesso em: 30 mar. 2017.

BROWNLEE, Laura Richardson. Extraterritorial Jurisdiction in the United States: American Attitudes and Practices in the Prosecution of Charles “Chuckie” Taylor Jr.. **Washington University Global Studies Law Review**, Washington, D.C, USA, v. 9, n. 2, 2010. Disponível em: <http://openscholarship.wustl.edu/cgi/viewcontent.cgi?article=1048&context=law_globalstudies>. Acesso em: 10 out. 2017.

BUTLER, Jadzia. The Microsoft Ireland Case: A Clear Answer, An Uncertain Future. **Center for Democracy & Technology**, publicado em 18 jul. 2016. Disponível em: <https://cdt.org/blog/the-microsoft-ireland-case-a-clear-answer-an-uncertain-future/>. Acesso em: 30 abr. 2017.

CARNEIRO, Athos Gusmão. **Jurisdição e competência**. 14 ed. São Paulo: Saraiva, 2005.

CARVALHO, Marcelo Sávio Meneses de. **A trajetória da Internet no Brasil**: do surgimento das redes de computadores à instituição dos mecanismos de governança. Dissertação do curso de pós-graduação de engenharia da Universidade Federal do Rio de Janeiro. Mestrado em ciências da engenharia de sistemas e computação. Rio de Janeiro, setembro, 2006. Disponível em: <http://www.slideshare.net/msavio/a-trajetoria-da-internet-no-brasil-2362034?from=share_email_logout2>. Acesso em: 01 jun. 2016.

CASEY, Eoghan. **Digital Evidence and Computer Crime**. Forensic Science, Computers and The Internet. 3ed. United States of Amercia: Academic Press, 2011.

CLOUGH, Jonathan. **A world of difference**: the Budapest Convention on Cybercrime and the challenges of harmonisation. Ago., 2015. Disponível em: <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2615789>. Acesso em: 25 set. 2017.

_____. **Principles of cybercrime**. New York: Cambridge University Press, 2011.

COMMONWEALTH OF INDEPENDENT STATES. **Agreement on cooperation among the States members of the Commonwealth of Independent States in combating offences relating to computer information**. Minsk, jun, 2001. Disponível em: <https://cms.unov.org/llsulinkbase/contenttree.aspx?nodeID=5958>. Acesso em: 20 jun. 2016.

CONGRESS (United States of America). **H.R.387**: Email Privacy Act. Apresentado ao 115th Congress, em 09 jan., 2017. Disponível em: <https://www.govtrack.us/congress/bills/115/hr387>. Acesso em: 16 set. 2017. a

_____. **S.1671**: International Communications Privacy Act. Apresentado ao 115th Congress, 1st Session, em 27 jul., 2017. Disponível em: <https://www.govtrack.us/congress/bills/115/s1671>. Acesso em: 20 out. 2017. b

_____. **S.512**: Law Enforcement Access to Data Stored Abroad Act. Apresentado ao 114th Congress, 1st session, em 12 fev 2015. Disponível em: <https://www.congress.gov/bill/114th-congress/senate-bill/512/text>. Acesso em: 20 set. 2017.

CONSELHO DA UNIÃO EUROPEIA. Decisão (UE) 2016/2220 do Conselho, de 02 de dezembro de 2016, relativa à celebração, em nome da União Europeia, de um acordo entre os Estados Unidos da América e a União Europeia sobre a proteção dos dados pessoais no âmbito da prevenção, investigação, deteção e repressão de infrações penais. **Jornal Oficial da União Europeia**, 10 dez., 2016, Acordos Internacionais, L336/1. Disponível em: <http://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX :32016D2220&from=PT>. Acesso em: 23 ago. 2017.

_____. Decisão-Quadro 2008/977/JAI, de 27 de novembro de 2008, relativa à protecção dos dados pessoais tratados no âmbito da cooperação policial e judiciária em matéria penal. **Jornal Oficial da União Europeia**, 30 dez. 2008, L350/60. Disponível em: <http://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32008F0977&from=EN>. Acesso em: 25 ago. 2017.

COSTA, Fernando José. ***Locus delicti* nos crimes informáticos**. 2011. 355 f. Tese (Doutorado em Direito) – Faculdade de Direito da Universidade de São Paulo. São Paulo, 2011.

COUNCIL OF EUROPE. Committee of Ministers. **Recommendation nº R (87) 15, regulating the use of personal data in the police sector**. Adopted by the Committee of Ministers on 17 September 1987 at the 410th meeting of the Ministers' Deputies. Disponível em: <http://www.coe.int/T/DG1/LegalCooperation/Economiccrime/organisedcrime/Rec_1987_15.pdf>. Acesso em: 25 ago. 2017.

_____. Committee of Ministers. **Recommendation nº R (89) 9 on Computer-related Crime and Final Report of European Committee on Crime Problems**. Strasbourg, 1990. Disponível em: < http://www.oas.org/juridico/english/89-9&final%20report.pdf. Acesso em: 26 ago. 2016.

_____. Committee of Ministers. **Recommendation nº R (95) 13 Concerning Problems of Criminal Procedural Law connected with Information Technology**. September, 1995. Disponível em: <https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016804f6e76>. Acesso em: 26 ago. 2016.

_____. Committee of Ministers. **Reply of the Committee of Ministers. Increasing co-operation against cyberterrorism and other large-scale attacks on the Internet**. Parliamentary Assembly Recommendation 2077 (2015). 1254 th meeting of the Ministers' Deputies, 27 abr 2016. Disponível em: <https://search.coe.int/cm/Pages/result_details.aspx?ObjectID=090000168064951d>. Acesso em: 25 ago., 2017.

_____. **Convenção Relativa ao Auxílio Judiciário Mútuo em Matéria Penal entre os Estados Membros da União Europeia**. Bruxelas, 29 maio 2000. Disponível em: < http://www.gddc.pt/siii/im.asp?id=88 >. Acesso em: 05 set. 2017.

_____. **Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data** (ETS nº 108). Strasbourg, 28, jan.,1981. Disponível em: <http://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/108>. Acesso em: 25 ago., 2017.

_____. **Convention on Cybercrime**. Série de Tratados Europeus n.º 185. Budapeste, 2001. Disponível em:< http://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185>. Acesso em: 22 mai. 2016. a

_____. Economic Crime Division Directorate General of Human Rights and Legal Affairs. **Cloud Computing and cybercrime investigations: Territoriality vs. the power of disposal?**. Discussion paper. Strasbourg, France, Version 31, August, 2010. Disponível em: <https://rm.coe.int/16802fa3df>. Acesso em: 31 ago. 2017.

_____. **Explanatory Report to the Convention on Cybercrime. European Treaty Series nº 185**. Budapeste, 23 de novembro de 2001. Disponível em: <https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016800cce5b>. Acesso em: 26 ago., 2016. b

_____. **Protocolo Adicional à Convenção sobre o Cibercrime Relativo à Incriminação de Atos de Natureza Racista e Xenófoba Praticados através de Sistemas Informáticos.** Série de Tratados Europeus n.º 189. Aberto à assinatura em Estrasburgo a 28 de janeiro de 2003. Entrada em vigor na ordem internacional em 1 de março de 2006. Disponível em: <http://direitoshumanos.gddc.pt/3_2/IIIPAG3_2_5A.htm>. Acesso em: 22 ago., 2017.

_____. **Recommendation 2077 (2015).** Increasing co-operation against cyberterrorism and other large-scale attacks on the Internet. Parliamentary Assembly. Assembly debate, em 26 jun 2015 (27th sessão). Disponível em: <http://assembly.coe.int/nw/xml/XRef/Xref-XML2HTML-en.asp?fileid=21976&lang=en. Acesso em: 25 ago. 2017.

_____. **Segundo Protocolo Adicional à Convenção Europeia de Auxílio Judiciário Mútuo em Matéria Penal**. Estrasburgo, 08 nov 2001. Disponível em: <http://www.gddc.pt/siii/im.asp?id=1816>. Acesso em: 05 set. 2017. c

CURRIE, Robert J.. Cross-Border Evidence Gathering in Transnational Criminal Investigation: Is the Microsoft Ireland Case the 'Next Frontier'?. **Canadian Yearbook of International Law**. v. 54, March 15, 2017. Disponível em: <https://ssrn.com/abstract=2933511>. Acesso em: 30 mar., 2017.

CYBERCRIME CONVENTION COMMITTEE. Council of Europe. Ad-hoc sub-group of the T-CY on jurisdiction and transborder access to data and data flows. Adopted by the 12th Plenary of the T-CY, Strasbourg, 24 nov., 2011. Disponível em: < https://rm.coe.int/16802e703b>. Acesso em: 15 ago., 2017.

_____. Council of Europe. Compilation of Responses to Questionnaire for the Parties Concerning the Practical Implementation of the Convention on Cybercrime. Strasbourg, mar., 2008. Disponível em: <https://www.coe.int/t/dg1/legalcooperation/economiccrime/cybercrime/T-CY/T-CY_2008_01_questionnaire_en.PDF>. Acesso em: 10 out. 2017.

_____. Council of Europe**. Criminal Justice Access to Data in the Cloud**: Cooperation with “Foreign” Service Providers. 03 mai., 2016. Disponível em: <https://publicintelligence.net/eu-cloud-access/>. Acesso em: 15 ago. 2017. a

_____. Council of Europe. **Criminal justice access to data in the cloud**: challenges. Strasbourg, France, 26 mai., 2015. Disponível em: <http://www.statewatch.org/news/2015/jun/coe-crim-just-data-in-cloud.pdf>. Acesso em: 15 ago., 2017.

_____. Council of Europe. **Criminal justice access to electronic evidence in the cloud**: Recommendations for consideration by the T-CY. Final report of the T-CY Cloud Evidence Group. Strasbourg, set., 2016. Disponível em: <https://rm.coe.int/16806a495e>. Acesso em: 15 ago., 2017. b

_____. Council of Europe. **Report on the 2nd multilateral consultation of the parties**. Strasbourg, jun., 2007. Disponível em: <https://search.coe.int/cm/Pages/result_details.aspx?ObjectID=09000016805d52a1>. Acesso em: 30 set. 2017.

_____. Council of Europe. **Terms of Reference for the Preparation of a Draft 2nd Additional Protocol to the Budapest Convention on Cybercrime**. Approved by the 17th Plenary of the T-CY on 8 June 2017. Strasbourg, jun, 2017. Disponível em: <https://rm.coe.int/terms-of-reference-for-the-preparation-of-a-draft-2nd-additional-proto/168072362b>. Acesso em: 15 ago. 2017.

_____. Council of Europe. **Transborder access to data and jurisdiction**: Options for further action by the T-CY. Report prepared by the Ad-hoc Subgroup on Transborder Access and Jurisdiction. Adopted by the 12th Plenary of the T-CY, Strasbourg, 2 e 3 December 2014. Disponível em: <https://rm.coe.int/16802e726e>. Acesso em: 15 ago. 2017.

DASKAL, Jennifer C.. The Un-Territoriality of Data. **125 Yale Law Journal,** American University, WCL Research Paper No. 2015-5, 2015. Disponível em: <https://ssrn.com/abstract=2578229>. Acesso em: 30 mar. 2017.

_____. A Microsoft Ireland Fix: Time to Act is Now! **Just Security**, New York University School of Law, publicado em 14 abr. 2017. Disponível em: <https://www.justsecurity.org/39959/microsoft-ireland-fix-time-act-now/>. Acesso em: 30 abr. 2017. a

_____. A New UK-US Data Sharing Agreement: A Tremendous Opportunity, If Done Right. **Just Security**, New York University School of Law, publicado em 8 fev. 2016. Disponível em: < https://www.justsecurity.org/29203/british-searches-america-tremendous-opportunity/>. Acesso em: 30 abr. 2017. a

_____. Law Enforcement Access to Data Across Borders: The Evolving Security and Rights Issues. **Journal of National Security Law & Policy**. Publicado em 6 set. 2016. Disponível em: <http://jnslp.com/wp-content/uploads/2016/11/Law_Enforcement_Access_to_Data_Across_Borders_2.pdf>. Acesso em: 30 abr 2017. b

DASKAL, Jennifer; WOODS, Andrew K.. **Cross-Border Data Requests**: A Proposed Framework. Publicado em 24 de novembro de 2015. Disponível em: <https://www.justsecurity.org/27857/cross-border-data-requests-proposed-framework/>. Acesso 15 ago., 2017.

DE-LA-TORRE-UGARTE-GUANILO, Mônica Cecilia; TAKAHASHI, Renata Ferreira; BERTOLOZZI, Maria Rita. Revisão sistemática: noções gerais. **Revista da Escola de Enfermagem da USP**, São Paulo, v. 45, n.5, oct, 2011. Disponível em: <http://www.scielo.br/scielo.php?script=sci_arttext&pid=S0080-62342011000500033>. Acesso em: 10 dez., 2016.

DELGADO, Vladimir Chaves. **Cooperação Internacional em Matéria Penal na Convenção Sobre o Cibercrime**. Dissertação. (Mestrado) - Programa de Mestrado em Direito das Relações Internacionais do Centro Universitário de Brasília. Brasilia, 2007. Disponível em: < http://repositorio.uniceub.br/bitstream/123456789/3562/3/vladimir.pdf>. Acesso em: 26 ago. 2016.

DELLA VECCHIA, Evandro; WEBER, Daniel, ZORZO, Avelino. Antiforense Digital: conceitos, técnicas, ferramentas e estudos de caso. In: **XIII Simpósio Brasileiro de Segurança da Informação e de Sistemas Computacionais** - SBSeg 2013, 11 a 14 nov., Manaus/AM. Disponível em: http://sbseg2013.icomp.ufam.edu.br/images/Minicurso_SBSeg_2013.pdf. Acesso em: 03 fev. 2018.

DEPARTMENT OF JUSTICE. United States. In the matter of a warrant to search a certain e–mail account controlled and maintained by microsoft Corporation. **On Petition for a Writ of Certiorari to the United States Court of Appeals for the Second Circuit**. Case 13-Mag-2814. Set. 2017. Disponível em: <https://arstechnica.com/wp-content/uploads/2017/09/scotusmsftgoogyahoo.pdf>. Acesso em: 10 out. 2017.

_____. United States. Office of Justice Programs, Bureau of Justice Assistance. **Electronic Communications Privacy Act of 1986 (ECPA), 18 U.S.C. § 2510-22**. Last date revised: 30 de julho de 2013. Disponível em: < https://it.ojp.gov/privacyliberty/authorities/statutes/1285>. Acesso em: 15 ago. 2016.

_____. United States. **Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations**. 2009. Disponível em: <https://www.justice.gov/sites/default/files/criminal-ccips/legacy/2015/01/14/ssmanual2009.pdf>. Acesso em: 25 ago. 2016.

DFRWS Technical Report. **A Road Map for Digital Forensic Research**. Report From the First Digital Forensic Research Workshop (DFRWS). August 7-8, 2001, Utica, New York. Disponível em: <http://dfrws.org/sites/default/files/session-files/a_road_map_for_digital_forensic_research.pdf>. Acesso em: 03 fev. 2018.

DIDONÉ, Dener. **Computação em nuvem**: desafios e oportunidade para a forense computacional. Dissertação. (Mestrado) - Programa de Pós-Graduação em Ciência da Computação da Universidade Federal de Pernambuco. Recife, 2011.

DYKSTRA, Josiah; SHERMAN, Alan. Acquiring Forensic Evidence from Infrastructure-as-a-Service Cloud Computing., 2012. In: **The Digital Forensic Research Conference** - DFRWS 2012, Aug 6th - 8th, Washington DC, USA. Disponível em: <https://www.dfrws.org/sites/default/files/session-files/paper-acquiring_forensic_evidence_from_infrastructure-as-a-service_cloud_computing.pdf>. Acesso em: 03 fev. 2018.

ELECTRONIC FRONTIER FOUNDATION. United States District Court Southern District of New York. In the Matter of a Warrant to Search a Certain E-Mail Account Controlled and Maintained by Microsoft Corporation. Microsoft v. United States. **Brief Amicus Curiae of Electronic Frontier Foundation in support of Microsoft Corporation.** New York, New York, Case 13-MAG-2814, 12 jun., 2014. Disponível em: < https://www.eff.org/document/eff-amicus-brief-support-microsoft>. Acesso em: 25 set. 2017.

ELEUTÉRIO, Pedro M. da S.; MACHADO, Marcio P.. **Desvendando a computação forense**. São Paulo: Novatec, 2010.

ELLINGSEN, Nora. The Microsoft Ireland Case: A Brief Summary. Lawfare, Hard National Security Choices, July 15, 2016. Disponível em: < https://www.lawfareblog.com/microsoft-ireland-case-brief-summary>. Acesso em: 25 de jul. de 2016.

EUROPEAN COMMISSION. **How can we improve cross-border access to e-evidence?**. Migration and Home Affairs. Publicado em 12 jun 2017. Disponível em: <https://ec.europa.eu/home-affairs/news/how-can-we-improve-cross-border-access-e-evidence_en>. Acesso em: 30 ago. 2017.

EUROPEAN JUSTICE. **Sistemas judiciais nos Estados-Membros** – Bélgica. Organização da justiça – sistema judicial. Última atualização: 03/08/2017. Disponível em: <https://e-justice.europa.eu/content_judicial_systems_in_member_states-16-be-pt.do?member=1>. Acesso em: 16 set. 2017.

EUROPEAN UNION; UNITED STATES OF AMERICA. Acordo entre os Estados Unidos da América e a União Europeia sobre a proteção dos dados pessoais no âmbito da prevenção, investigação, deteção e repressão de infrações penais. Assinado em 02 jun 2016, em Amsterdam; publicado em 20 dez 2016. **Official Journal of the European Union**, L 336/3. Tradução oficial para o português disponível em: <http://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:22016A1210(01)&from=EN>. Acesso em: 15 ago. 2017.

EUROPOL. European Union Agency for Law Enforcement Cooperation. **European Union Serious and Organised Crime Threat Assessment 2017**. Crime in the age of technology. Disponível em: <https://www.europol.europa.eu/activities-services/main-reports/european-union-serious-and-organised-crime-threat-assessment-2017>. Acesso em:25 set. 2017.b

_____. European Union Agency for Law Enforcement Cooperation. **The Internet Organised Crime Threat Assessment (IOCTA) 2017**. Disponível em: <https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2017>. Acesso em: 15 dez. 2017.a

_____. European Union Agency for Law Enforcement Cooperation. **The Internet Organised Crime Threat Assessment (IOCTA) 2015**. Disponível em: < https://www.europol.europa.eu/iocta/2015/>. Acesso em: 20 jul. 2016.

_____. European Union Agency for Law Enforcement Cooperation. **The Internet Organised Crime Threat Assessment (IOCTA) 2016**. Disponível em: < https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2016>. Acesso em: 26 jul. 2017.

FERREIRA, Érica Lourenço de Lima. **Internet**: Macrocriminalidade e Jurisdição Internacional. Curitiba: Juruá, 2007.

FERREIRA, Ivette Senise. A criminalidade informática. In: DE LUCCA, Newton; SIMÃO FILHO, Adalberto (coord). **Direito & Internet**. 2 ed. São Paulo: Quartier Latin, 2005.

FINKLEA, Kristin M.; THEOHARY, Catherine A.. **Cybercrime**: Conceptual Issues for Congress an U.S. Law Enforcement. R42547. Washington, DC: Congressional Research Service. Jan., 2015. Disponível em: <https://archive.org/details/R42547CybercrimeConceptualIssuesforCongressandUSLawEnforcement-crs>. Acesso em: 10 jun. 2016.

FLEURY, Maria Tereza Leme; OLIVEIRA JR, Moacir de Miranda. **Gestão estratégica do conhecimento**. Integrando aprendizagem, conhecimento e competências. São Paulo: Atlas, 2001.

FONTE II, Hamilton J. S.; SIMPLICIO JR., Marcos A. Dizang: Uma solução para coleta de evidências forenses de ataques de injeção na nuvem. In: **XVII Simpósio Brasileiro de Segurança da Informação e de Sistemas Computacionais** - SBSeg 2017, 06 a 09 nov., Brasília/DF. Disponível em: <https://sbseg2017.redes.unb.br/wp-content/uploads/2017/04/20171109_ANAIS_SBSEG_2017_FINAL_E-BOOK.pdf>. Acesso em: 03 fev. 2018.

GHAPPOUR, Ahmed. Searching Places Unknown: Law Enforcement Jurisdiction on the Dark Web. **Stanford Law Review**, v. 69, April 2017; UC Hastings Research Paper No. 170. Disponível em: <https://ssrn.com/abstract=2742706> Acesso em: 30 mar 2017.

GOLDSMITH, Jack L. Against Cyberanarchy. **University of Chicago Law School Occasional Papers**, n. 40, Law School Publications, 1999. Disponível em: <http://chicagounbound.uchicago.edu/cgi/viewcontent.cgi?article=1001&context=occasional_papers>. Acesso em: 30 mai. 2017.

GOODMAN, Marc. **Future Crimes**. Tudo está conectado, todos somos vulneráveis e o que podemos fazer sobre isso. São Paulo: HSM, 2015.

GRAY, Andrew R.. 'Cloud' Atlas — A Map to Amending Metadata Privacy Law in the Modern Era. **Gonzaga Law Review**, Spokane, Washington, USA, 2016. Disponível em: https://ssrn.com/abstract=2818751>. Acesso em: 30 mar 2017.

GREENBERG, Andy. Hacker Lexicon: What Is the Dark Web?. **Wired**, 19 nov. 2014. Security. Disponível em: <https://www.wired.com/2014/11/hacker-lexicon-whats-dark-web/>. Acesso em: 25 set. 2017.

GREWLICH, Klaus W.. **Governance in "Cyberspace":** Access and Public Interest in Global Communications. Hague: Kluwer Law International, 1999.

GUERRA, Sidney. **Curso de Direito Internacional Público**. 11 ed. São Paulo: Saraiva, 2017.

GUILLOT, Philippe Ch.-A.. Propos Introductifs: De La Repression des Infractions Cybernétiques à La Protection des Droits des Internautes. In: COLLOQUE DE ROUEN. **Internet et de droit international**. Paris: Pedone, 2014. p.325-338.

HARDY, I. Trotter. The Proper Legal Regime for 'Cyberspace'. Faculty Publications. William & Mary Law School, Paper 656, 1994. Disponível em: <http://scholarship.law.wm.edu/cgi/viewcontent.cgi?article=1536&context=facpubs>. Acesso em: 25 mai. 2017.

HARRIS, Ryan. Arriving at an Anti-forensics Consensus: Examining How to Define and Control the Anti-forensics Problem. In: **Digital Forensic Research Conference** – DFRWS 2006, Aug 14 a 16, Lafayette, IN, USA. Disponível em: < https://www.dfrws.org/sites/default/files/session-files/paper-arriving_at_an_anti-forensics_consensus_-_examining_how_to_define_and_control_the_anti-forensics_problem.pdf>. Acesso em: 03 fev. 2018.

HARVARD LAW REVIEW. **In re Warrant to Search a Certain Email Account Controlled & Maintained by Microsoft Corp**. District Court Holds that SCA Warrant Obligates U.S. Provider to Produce Emails Stored on Foreign Servers. Recent Case : 15 F. Supp. 3d 466 (S.D.N.Y. 2014). v. 128, n. 3, p. 1019-1026, Jan. 2015. Disponível em: <http://harvardlawreview.org/2015/01/in-re-warrant-to-search-a-certain-email-account-controlled-maintained-by-microsoft-corp/>. Acesso em: 25 jul. 2016.

HERZOG, Stephen. Revisiting the Estonian Cyber Attacks: Digital Threats and Multinational Responses. **Journal of Strategic Security**, v. 4, n. 2, 2011. p: 49-60. Disponível em: <http://scholarcommons.usf.edu/jss/vol4/iss2/4>. Acesso em: 16 nov., 2017.

HESSBRUEGGE, Jan Arno. The Shanghai Cooperation Organization: A Holy Alliance For Central Asia?. **The Fletcher School Online Journal for issues related to Southwest Asia and Islamic Civilization**, 2004. Disponível em: <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2409073>. Acesso em: 15 nov., 2017.

HOOPER, Christopher; MARTINI, Ben; CHOO, Kim-Kwang Raymond. Cloud Computing and Its Implications for Cybercrime Investigations in Australia. **Computer Law and Security Review**, v. 29, n. 2, p. 152-163, abril 2013. Disponível em: https://ssrn.com/abstract=2340805>. Acesso em: 30 mar. 2017.

HUNTER, Dan. Cyberspace as Place and the Tragedy of the Digital Anticommons. **California Law Review**, California/USA, v.91, n.2, artigo 4, mar. 2003. Disponível em: <http://scholarship.law.berkeley.edu/cgi/viewcontent.cgi?article=1380&context=californialawreview>. Acesso em: 20 mai. 2017.

IGLESIAS, Rebecca; NICHOLLS, Rob; TRAVIS, Anisha. Private Clouds with No Silver Lining: Legal Risk in Private Cloud Services. **Digiworld Economic Journal**, no. 85, 1, Q. 2012, p. 125 - 140. Disponível em: <http://citeseerx.ist.psu.edu/viewdoc/download;jsessionid=8569424566FA79AD19071A7A08815DB7?doi=10.1.1.466.9704&rep=rep1&type=pdf>. Acesso em: 25 set. 2017.

INTERNATIONAL COURT OF JUSTICE. **Corfu Channel Case (Merits)**. Judgment of 9 April 1949. Summaries of Judgments, Advisory Opinions and Orders of the International Court of Justice. Disponível em: <http://www.icj-cij.org/files/case-related/1/1647.pdf>. Acesso em: 10 jun. 2017.

IRELAND. United States District Court Southern District of New York. In the Matter of a Warrant to Search a Certain E-Mail Account Controlled and Maintained by Microsoft Corporation. Microsoft v. United States. **Brief for Amicus Curiae Ireland.** New York, New York, Case 13-MAG-2814, 23 dez., 2014. Disponível em: < https://blogs.microsoft.com/datalaw/wp-content/uploads/sites/149/2014/09/Ireland-AmicusBrief.pdf>. Acesso em: 25 set. 2017.

ITU. **Understanding Cybercrime**: A Guide of Developing Countries. Draft, Abril, 2009. Disponível em: <https://www.itu.int/ITU-D/cyb/cybersecurity/docs/itu-understanding-cybercrime-guide.pdf>. Acesso em: 22 mai. 2016.

_____. **Understanding cybercrime**: Phenomena, challenges and legal response. 2012. Disponível em:<http://www.itu.int/ITU-/cyb/cybersecurity/docs/Cybercrime%20legislation%20EV6.pdf>. Acesso em: 22 mai. 2016.

JAYCOX, Mark; TIEN, Lee. Reforms Abound for Cross-Border Data Requests. **Electronic Frontier Foundation**, dez., 2015. Disponível em: <https://www.eff.org/pt-br/deeplinks/2015/12/reforms-abound-cross-border-data-requests>. Acesso em: 20 jun. 2017.

JOHNSON, David R.; POST, David G.. Law And Borders: The Rise of Law in Cyberspace. **Stanford Law Review**, v. 48, p. 1367, 1996. Disponível em: <https://ssrn.com/abstract=535> or <http://dx.doi.org/10.2139/ssrn.535>. Acesso em: 25 mai. 2017.

KAHN, Robert E.; CERF, Vinton Gray. **What Is The Internet** (And What Makes It Work). December, 1999. Disponível em: <https://www.cnri.reston.va.us/what_is_internet. html>. Acesso em: 10 jul. 2016.

KATZ, Jonathan; LINDELL, Yehuda. Introduction to Modern Cryptography. CRC Press, 2007.

KAUFMAN, Lori M.. Data Security in the World of Cloud Computing. **IEEE Security & Privacy**, v. 7, Issue: 4, July-Aug. 2009.

KENT, Karen; CHEVALIER, Suzanne; GRANCE, Tim; DANG, Hung. Guide to Integrating Forensic Techniques into Incident Response. **Recommendations of the National Institute of Standards and Technology**. Computer Security Division. Information Technology Laboratory. NIST. US Department of Commerce. Gaithersburg, Maryland, United States. August, 2006. Disponível em: <https://ws680.nist.gov/publication/get_pdf.cfm?pub_id=50875>. Acesso em: 03 fev. 2018.

KERR, Orion S.. A User's Guide to the Stored Communications Act, and a Legislator's Guide to Amending it. George Washington Law Review 1208, volume 72, 2004. Disponível em SSRN: <http://ssrn.com/abstract=421860> or <http://dx.doi.org/10.2139/ssrn.421860>. Acesso em: 16 ago. 2016. Acesso em: 16 ago. 2016.

KONTOROVICH, Eugene. The inefficiency of universal jurisdiction. **University of Illinois Law Review**, Illinois, United States, 2008. pp. 389 - 418. Disponível em: <https://www.illinoislawreview.org/wp-content/ilr-content/articles/2008/1/Kontorovich.pdf>. Acesso em: 10 out. 2017.

KOOPS, Bert-Jaap. The Internet and its Opportunities for Cybercrime. In: HERZOG-EVANS; M.. **Transnational Criminology Manual**. Nijmegen: WLP, 2010. v.1, p. 735-754.

KOOPS, Bert-Jaap; GOODWIN, Morag. Cyberspace, the Cloud, and Cross-Border Criminal Investigation. The Limits and Possibilities of International Law. Tilburg Institute for Law, Technology, and Society CTLD – Center for Transboundary Legal Development, December 2014; Tilburg Law School Research Paper No. 5/2016. Disponível em: <https://ssrn.com/abstract=2698263>. Acesso em: 30 mar 2017.

KRISHNAMURTHY, Vivek. Cloud with a Conflict of laws. **Berkman Center Research Publication No. 2016-3**, Cambridge, Massachusetts, USA: Berkman Center for Internet & Society, Harvard University, 22 Feb 2016. Disponível em: < http://papers.ssrn.com/sol3/ papers.cfm?abstract_id=2733350>. Acesso em: 13 abr. 2016.

KUROSE, James F.; ROSS, Keith W. **Redes de Computadores e a Internet**: Uma abordagem top-down. 5 ed. São Paulo: Person Education do Brasil, 2010.

LAURITS, Eneli; KASPER, Agnes. Challenges in Collecting Digital Evidence: A Legal Perspective. In: KERIKMÄE, Tanel; RULL, Addi . **The Future of Law and eTechnologies**. Switzerland: Springer International Publishing, 2016. p. 195-233.

LEAGUE OF ARAB STATES. **Arab Convention on Combating Information Technology Offences**. Cairo, 21 dez 2010. Disponível em: < https://dig.watch/actors/arab-league >. Acesso em: 10 jun., 2016.

LEINER, Barry M.; CERF, Vinton G.; CLARK, David D.; KAHN, Robert E.; KLEINROCK, Leonard; LYNCH, Daniel C.; POSTEL, Jon; ROBERTS, Larry G.; WOLFF, Stephen. **Brief History of the Internet**. Internet Society. 15 de outubro de 2012. Disponível em:< http://www.internetsociety.org/sites/default/files/Brief_History_of_the_Internet.pdf>. Acesso em: 15 jul. 2016.

LESSIG, Lawrence. The Zones of Cyberspace. **Stanford Law Review**, v. 48, n. 5, pp. 1403-1411, maio, 1996.

LIMA, Renato Brasileiro de. **Manual de Processo Penal**. Niterói: Impetus, 2011.

LIN, Tiffany; FIDLER, Mailyn. Cross-Border Access Reform: A primer on the proposed US-UK Agreement. **Berkman Klein Center for Internet & Society at Harvard University**, Research Publication n. 2017-7, set, 2017. Disponível em: https://cyber.harvard.edu/research/cybersecurity. Acesso em: 08 out., 2017.

LOPES, M.; GABRIEL, M. M.; BARETA, G. M. S. Cadeia de custódia: Uma abordagem preliminar. **Revista Visão Acadêmica**, v.7, n.1, 2006. UFPR: Curitiba. Disponível em: <https://revistas.ufpr.br/academica/article/view/9022>. Acesso em: 03 fev. 2018.

MARTINI, Ben; CHOO, Kim-Kwang Raymond. Remote Programmatic vCloud Forensics. July 21, 2014. In: **13th IEEE International Conference on Trust, Security and Privacy in Computing and Communications** – TrustCom-2014, September 2014, Beijing, China. Disponível em: https://ssrn.com/abstract=2469605>. Acesso em: 30 mar. 2017.

MARTINI, Ben; QUICK, Darren; CHOO, Kim-Kwang Raymond. Cloud Computing and Digital Forensics. In: KIM, I-S (edi). **Information Society and Cybercrime**: Challenges for Criminology and Criminal Justice. Research Report Series 13-B-01. Korean Institute of Criminology, December 9, 2013. p. 111–125. Disponível em: https://ssrn.com/abstract=2365631>. Acesso em: 30 mar. 2017.

MAUÉS, Marcelo B.; HOELZ, Werneck P.. Modelagem de ameaças antiforenses aplicada ao processo forense digital. In: **XVI Simpósio Brasileiro de Segurança da Informação e de Sistemas Computacionais** – SBSeg 2016, 07 a 10 nov., Niterói/DF.

MAZZUOLI, Valério de Oliveira. **Curso de Direito Internacional Público**. 9 ed.. São Paulo: Revista dos Tribunais, 2015.

McKEMMISH, Rodney. What is Forensic Computing?. In: **Trends & Issues in crime and criminal justice**. Australian Institute of Criminology. June, 1999. Disponível em: < https://aic.gov.au/publications/tandi/tandi118>. Acesso em: 03 fev. 2018.

MEDVEDEV, Sergey. Data protection in Russian Federation: overview. **Thomson Reuters. Practical Law**. 01 mai., 2016. Disponível em: <https://uk.practicallaw.thomsonreuters.com/2-502-2227?transitionType=Default&contextData=(sc.Default)&firstPage=true&bhcp=1>. Acesso em: 25 set. 2017.

MELL, Peter; GRANCE, Timothy. The NIST Definition of Cloud Computing. Recommendations of the National Institute of Standards and Technology. National Institute of Standards and Technology. **NIST Special Publication 800-145**, 2011. Disponível em: <http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf>. Acesso em: 22 mai. 2016.

MESQUITA, Frederico Imbroisi; HOELZ, Bruno W.P; RALHA, Célia G.. Raciocínio baseado em casos aplicado em análise *live*. In: **Proceeding of the sixth International Conference on Forensic Computer Science** – ICoFCS, 2011. Brasília, DF, 2011. p. 68 – 77.

MICROSOFT CORPORATION. United States District Court Southern District of New York. In the Matter of a Warrant to Search a Certain E-Mail Account Controlled and Maintained by Microsoft Corporation. Microsoft v. United States. **Reply Memorandum in Support of Microsoft´s Motion to Vacate in Part na SCA Warrant Seeking Customer Information located Outside the United States.** Case 13-Mag-2814. New York, New York, 14 mar., 2014. Disponível em: <https://www.justsecurity.org/wp-content/uploads/2014/05/Reply-Memorandum-in-Support-of-Motion-to-Vacate-doc-98.pdf>. Acesso em: 26 jul. 2016. a

_____. United States District Court Southern District of New York. In the Matter of a Warrant to Search a Certain E-Mail Account Controlled and Maintained by Microsoft Corporation. Microsoft v. United States**. Memorandum in Support of Microsoft´s Motion to Vacate in Part na SCA Warrant Customer Information located Outside the United States.** Case 13-Mag-2814. New York, New York, 18 dez., 2013. Disponível em: <https://www.justsecurity.org/wp-content/uploads/2014/05/Memorandum-in-Support-of-Microsofts-Motion-to-Vacate-doc-94-1.pdf>. Acesso em: 30 jul. 2016.

_____. United States District Court Southern District of New York. In the Matter of a Warrant to Search a Certain E-Mail Account Controlled and Maintained by Microsoft Corporation. Microsoft v. United States. **Microsoft's Objections to the Magistrate's Order Denying Microsoft's Motion to Vacate In Part a Search Warrant Seeking Customer Information Located Outside the United States**. New York, New York, Case nº 13-MAG-2814. 06 jun., 2014. Disponível em: <https://pt.scribd.com/document/229268932/Microsoft-fights-warrant-for-overseas-data>. Acesso em: 20 ago. 2016. b

MORAIS NETO, Arnaldo Sobrinho de. **Cibercrime e Cooperação Penal Internacional:** um Enfoque à Luz da Convenção de Budapeste. Dissertação. (Mestrado) - Programa de PósGraduação em Ciências Jurídicas da Universidade Federal da Paraíba, na área de concentração em Direito Econômico. Paraíba, 2009. Disponível em: <http://www.egov.ufsc.br/portal/conteudo/cibercrime-e-coopera%C3%A7%C3%A3o-penal-internacional-um-enfoque-%C3%A0-luz-da-conven%C3%A7%C3%A3o-de-budapeste. Acesso em: 26 ago. 2016.

NASH, Nathaniel. Holding Compuserve Responsible. **The New York Times**. January 15, 1996, page D00004 of the National edition. Disponível em: <http://www.nytimes.com/1996/01/15/business/holding-compuserve-responsible.html?_r=0>. Acesso em: 15 set. 2016.

NETANEL, Neil Weinstock. Cyberspace Self-Governance: A Skeptical View from Democratic Theory. **California Law Review**, v. 88, mar. 2000. Disponível em: <https://ssrn.com/abstract=175828> or <http://dx.doi.org/10.2139/ssrn.175828>. Acesso em: 30 mai. 2017.

NOLAN, Richard; O´SULLIVAN, Colin; BRANSON, Jake; WAITS, Cal. **First Responders Guide to Computer Forensics**. CERT Training and Education. March, 2005. Disponível em: <https://resources.sei.cmu.edu/asset_files/Handbook/2005_002_001_14429.pdf> . Acesso em: 03 fev. 2018.

OEA. Carta da Organização dos Estados Americanos. **IX Conferência Internacional Americana**, Bogotá, abr., 1948. Disponível em: <http://www.oas.org/es/sla/ddi/docs/tratados_multilaterales_interamericanos_A-41_carta_OEA.pdf>. Acesso em: 25 set. 2017.

_____. **Convenção Interamericana Contra o Terrorismo**. Assinada em Bridgetown/Barbados, em 03 de junho de 2002. Disponível em: <http://www.oas.org/juridico/portuguese/treaties/A-66.htm>. Acesso em: 20 jun., 2017.

ONU. Carta das Nações Unidas. Concluída e assinada, pelos Plenipotenciários, em São Francisco/Estados Unidos, a 26 de junho de 1945. Disponível em: <http://www.un.org/en/charter-united-nations/index.html>. Acesso em: 25 set. 2017.

_____. Declaration on Principles of International Law concerning Friendly Relations and Co-operation among States in accordance with the Charter of the United Nations. A/Res/25/2625, 24 out, 1970. Disponível em: <http://www.un-documents.net/a25r2625.htm>. Acesso em: 25 mai. 2017.

_____. Doha Declaration on Integrating Crime Prevention and Criminal Justice into the Wider United Nations Agenda to Address Social and Economic Challenges and to Promote the Rule of Law at the National and International Levels, and Public Participation. In: **Thirteenth United Nations Congress on Crime Prevention and**

Criminal Justice, Doha, 12-19 April 2015. Disponível em: <<https://www.unodc.org/documents/congress//Declaration/V1504151_English.pdf >. Acesso em: 25 set. 2017.

_____. **Resolution adopted by the General Assembly on 21 December 2010**. On the report of the Third Committee (A/65/457). 65ª Sessão, 21 dez., 2010. Disponível em: <https://documents-dds-ny.un.org/doc/UNDOC/GEN/N10/526/34/PDF/N1052634.pdf?OpenElement>. Acesso em: 25 set. 2017. a

_____. Salvador Declaration on Comprehensive Strategies for Global Challenges: Crime Prevention and Criminal Justice Systems and Their Development in a Changing World**.** In: **Twelfth United Nations Congress on Crime Prevention and Criminal Justice**. Salvador, Brazil, 12-19 ab 2010. Disponível em: <https://documents-dds-ny.un.org/doc/UNDOC/LTD/V10/529/03/PDF/V1052903.pdf?OpenElement>. Acesso em: 25 set. 2017. b

ORTON, Ivan; ALVA, Aaron; ENDICOTT-POPOVSKY, Barbara. Legal Process and Requirements for Cloud Forensic Investigations. In: RUAN, Keyun (editor). **Cybercrime and Cloud Forensics**: Applications for Investigation Processes. IGI Global, 2012, p. 186-229. Disponível em: https://ssrn.com/abstract=2197978>. Acesso em: 30 mar. 2017.

OSULA, Anna-Maria. **Accessing Extraterritorially Located Data**: Options for States. NATO Cooperative Cyber Defence Centre of Excellence, Tallinn, 2015. Disponível em: <https://ccdcoe.org/sites/default/files/multimedia/pdf/Accessing%20extraterritorially%20located%20data%20options%20for%20States_Anna-Maria_Osula.pdf>. Acesso em: 25 jul., 2016. a

_____. Mutual Legal Assistance & Other Mechanisms for Accessing Extraterritorially Located Data. **Masaryk University Journal of Law and Technology**, v.9, n.1, 2015. Disponível em: <https://journals.muni.cz/mujlt/article/view/2981>. Acesso em: 30 abr., 2017. b

_____. **Remote search and seizure of extraterritorial data**. Dissertation (Doctor of Philosophy (PhD) in law) - School of Law, University of Tartu, Estonia, 2017. Disponível em: <http://dspace.ut.ee/bitstream/handle/10062/55683/osula_anna_maria.pdf?sequence=1&isAllowed=y>. Acesso em: 30 abr., 2017.

OTTIS, R.. Analysis of the 2007 Cyber Attacks against Estonia from the Information Warfare Perspective. Proceedings of the **7th European Conference on Information Warfare and Security**, Plymouth, 2008. pp 163-168.

PARLAMENTO EUROPEU; CONSELHO DA UNIÃO EUROPEIA. Diretiva (UE) 2016/680, de 27 de abril de 2016, relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais pelas autoridades competentes para efeitos de prevenção, investigação, deteção ou repressão de infrações penais ou execução de sanções penais, e à livre circulação desses dados, e que revoga a Decisão-Quadro 2008/977/JAI do Conselho. **Jornal Oficial da União Europeia**, 04 mai 2016, L119/89. Disponível em: <http://eur-lex.europa.eu/legal-content/PT/TXT/?uri=uriserv:OJ.L_.2016.119.01.0089.01.POR&toc=OJ:L:2016:119:TOC>. Acesso em: 25 ago. 2017. a

_____. Diretiva 2002/58/CE, de 12 de julho de 2002, relativa ao tratamento de dados pessoais e à protecção da privacidade no sector das comunicações electrónicas (Directiva relativa à privacidade e às comunicações electrónicas). **Jornal Oficial da União Europeia**, 31 jul 2002, L201, p.0037-0047. Disponível em: <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32002L0058:pt:HTML>. Acesso em: 25 ago. 2017.

_____. Diretiva 2014/41/UE do Parlamento Europeu e do Conselho, de 3 de abril de 2014, relativa à decisão europeia de investigação em matéria penal. **Jornal Oficial da União Europeia**, 01 mai., 2014, L130/1. Disponível em: <http://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:32014L0041&from=PT>. Acesso em: 25 ago. 2017.

_____. Diretiva 95/46/CE de 24 de outubro de 1995, relativa à protecção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados. **Jornal Oficial da União Europeia**, 23 nov 1995, L281/31. Disponível em: <http://ec.europa.eu/justice/policies/privacy/docs/95-46-ce/dir1995-46_part1_pt.pdf>. Acesso em: 25 ago. 2017.

_____. Regulamento (UE) 2016/679, do Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados). Bruxelas. **Jornal Oficial da União Europeia**, 04 maio 2016, L119/1. Disponível em: <http://eur-lex.europa.eu/legal-content/PT/TXT/?uri=uriserv:OJ.L_.2016.119.01.0001.01.POR&toc=OJ:L:2016:119:TOC>. Acesso em: 25 ago. 2017. b

PECORARO, Andrew J.. Drawing Lines in the Cloud: Implications of Extraterritorial Limits to the Stored Communications Act. **51 Creighton Law Review**, 2017. Disponível em: <https://ssrn.com/abstract=2928839>. Acesso em: 30 mar 2017.

PESQUISA NACIONAL POR AMOSTRA DE DOMICÍLIO CONTÍNUA. Características gerais dos domicílios 2016. Rio de Janeiro: IBGE, 2017. Disponível em: < https://biblioteca.ibge.gov.br/visualizacao/livros/liv101379.pdf>. Acesso em: 15 dez. 2017.

POST, David G.. Anarchy State and the Internet. **Journal of Online Law**, Article 3, 1995. Disponível em:<https://ssrn.com/abstract=943456>. Acesso em: 25 mai. 2017.

PUGH, Sarah. Cloudy with a Chance of Abused Privacy Rights: Modifying Third-Party Fourth Amendment Standing Doctrine Post-Spokeo. **American University Law Review**, Washington, D.C, USA, v. 66, n. 3, 2017. Disponível em: <https://ssrn.com/abstract=2926473>. Acesso em: 30 mar. 2017.

QUICK, Darren; CHOO, Kim-Kwang Raymond. Google Drive: Forensic Analysis of Cloud Storage Data Remnants. **Journal of Network and Computer Applications**. v. 40, abril, 2014. Disponível em: <https://ssrn.com/abstract=2340234>. Acesso em: 23 jul. 2016.

RANGEL, Vicente Marotta. A Corte Internacional de Justiça e o Direito do Mar. **Aula inaugural do ano letivo de 1976**, Faculdade de Direito da Universidade de São Paulo. Disponível em: <https://www.revistas.usp.br/rfdusp/article/download/66781/69391>. Acesso em: 10 jun. 2017.

REED, Chris. **Making laws for cyberspace**. Oxford, UK: Oxford University Press, 2012.

REZEK, Francisco. **Direito Internacional Público**. Curso elementar. 15 ed. São Paulo: Saraiva, 2014.

ROBISON, William Jeremy. Free at What Cost? Cloud Computing Privacy Under the Stored Communications Act. **Georgetown Law Journal**, v. 98, n. 4, 2010. Disponível em: <https://ssrn.com/abstract=1596975>. Acesso em: 30 mar. 2017.

RUAN, Keyun; CARTHY, Joe; KECHADI, Tahar; CROSBIE, Mark. Cloud forensics: An overview. In: **Advances in Digital Forensics VII**, 7th IFIP WG 11.9 International Conference on Digital Forensics, Orlando, FL, USA, January 31 - February 2, 2011. Disponível em: <https://www.researchgate.net/publication/229021339_Cloud_forensics_An_overview>. Acesso em: 03 fev. 2018.

SANG, Ting. A Log-based Approach to Make Digital Forensics Easier on Cloud Computing. In: **Third International Conference on Intelligent System Design and Engineering Applications**, 2013. Disponível em: <https://www.academia.edu/7826089/A_Log-based_Approach_to_Make_Digital_Forensics_Easier_on_Cloud_Computing>. Acesso em: 03 fev. 2018.

SCASSA, Teresa; CURRIE, Robert J.. New First Principles? Assessing the Internet's Challenges to Jurisdiction. **Georgetown Journal of International Law**, v. 42, 2011. Disponível em: <https://ssrn.com/abstract=2116364>. Acesso em: 30 mar. 2017.

SCHIMITT, Michael N. (Editor). **Tallinn Manual on the International Law Applicable to Cyber Warfare**. United Kingdom: Cambridge University Press, 2013.

SCHJOLBERG, Stein. **The History of Global Harmonization on Cybercrime Legislation** - The Road to Geneva. December, 2008. Disponível em: < http://www.cybercrimelaw.net/documents/cybercrime_history.pdf>. Acesso em: 26 ago. 2016.

SCHRIJVER, Steven De; DAENENS, Thomas. The Yahoo! Case: The End of International Legal Assistance In Criminal Matters. **Who's Who Legal**, set., 2013. Telecommunications Media & Technology. Disponível em: <http://whoswholegal.com/news/features/article/30840/the-yahoo-case-end-international-legal-assistance-criminal-matters>. Acesso em: 20 jun. 2016.

SCHULTHEIS, Ned. Warrants in the Clouds: How Extraterritorial Application of the Stored Communications Act Threatens the United States Cloud Storage Industry. **9 Brooklyn Journal of Corporate, Financial & Commercial Law**, 2015. Disponível em: <https://ssrn.com/abstract=2738705> . Acesso em: 30 mar 2017.

SEITENFUS, Ricardo. **Organizações Internacionais**. 6 ed.. Porto Alegra: Livraria do Advogado, 2016.

SHANGHAI COOPERATION ORGANIZATION. Agreement between the Governments of Member States of the Shanghai Cooperation Organization in the Field of International Information Security. Ecaterimburgo, em 16 de junho de 2009. Disponível em: <https://ccdcoe.org/sites/default/files/documents/SCO-090616-IISAgreementRussian.pdf>. Acesso em: 23 set. 2016.

SIBIYA, George; VENTER, Hein S.; FOGWILL, Thomas. Digital Forensic Framework for a Cloud Environment. In: **IIMC International Information Management Corporation**, 2012, Africa. Disponível em: <http://researchspace.csir.co.za/dspace/bitstream/handle/10204/5890/Sibiya_2012.pdf;sequence=1>. Acesso em: 03 fev. 2018.

SLAY, Jill; LIN, Yi-Chi; TURNBULL, Benjamin; BECKETT, Jason; LIN, Paul. Towards a formalization of digital forensics. In: **Advances in Digital Forensics** V: Fifth IFIP WG 11.9 International Conference on Digital Forensics, Orlando, Florida, USA, January 26-28, 2009. Revised Selected Papers. pp.37-47. Disponível em: <https://www.researchgate.net/publication/221352737_Towards_a_Formalization_of_Digital_Forensics>. Acesso em: 03 fev. 2018.

STEPHENSON, Peter. **Investigation Computer-related crime**. United States: CRC, 1999.

STJ. Inquérito nº 784/DF. Questão de Ordem. Acórdão. Relatora: Ministra Laurita Vaz. Data do julgamento: 17 de abril de 2013. Disponível em: <https://ww2.stj.jus.br/processo/revista/documento/mediado/?componente=ITA&sequencial=1226618&num_registro=201201075060&data=20130828&formato=PDF>. Acesso em: 14 jun. 2017.

_____. Recurso Especial nº 1.359.976-PB (2012/0270732-1). Relator: Ministro Paulo de Tarso Sanseverino. Recorrente: TNL PCS S/A. Recorrido: Germana Pereira Fernandes. Brasília, data julgamento: 25 de novembro de 2014. https://ww2.stj.jus.br/processo/revista/documento/mediado/?componente=ITA&sequencial=1370794&num_registro=201202707321&data=20141202&formato=PDF

SVANTESSON, Dan Jerker B.. Law Enforcement Access to Evidence via Direct Contact with Cloud Providers: Identifying the Contours of a Solution. **Computer Law & Security Review**, vol. 32, Issue 5, Pages 671-682, ago, 2016. Disponível em: <http://c.ymcdn.com/sites/www.iisfa.net/resource/resmgr/Slide_seminari/Convegno_Milano/LEAccessSVANTESSON20160418SU.pdf>. Acesso em: 30 mar., 2017. a

_____, Dan Jerker B.. **Law Enforcement Cross-Border Access to Data**: Preliminary Report. 22 nov, 2016. Disponível em: https://ssrn.com/abstract=2874238>. Acesso em: 30 mar 2017. b

SWIRE, Peter; HEMMINGS, Justin D.. Mutual Legal Assistance in an Era of Globalized Communications: The Analogy to the Visa Waiver Program. **Georgia Tech Scheller College of Business,** Research Paper No. WP 38., Atlanta, Georgia, USA, 11 jan 2016. Disponível em: <https://ssrn.com/abstract=2728478>. Acesso em: 30 mar 2017.

_____. Stakeholders in Reform of the Global System for Mutual Legal Assistance. **Georgia Tech Scheller College of Business,** Research Paper No. 32., Atlanta, Georgia, USA, 08 nov 2015. Disponível em: <https://ssrn.com/abstract=2696163 or http://dx.doi.org/10.2139/ssrn.2696163 >. Acesso em: 26 set 2017.

SWIRE, Peter; HEMMINGS, Justin D.; VERGNOLLE, Suzanne. A Mutual Legal Assistance Case Study: The United States and France. **Georgia Tech Scheller College of Business Research** Paper No. 2017-54, Atlanta, Georgia, USA, january 19, 2017. Disponível em: https://ssrn.com/abstract=2921289>. Acesso em: 30 mar 2017.

SWIRE, Peter; KENNEDY-MAYO, DeBrae. How Both the EU and the U.S. Are 'Stricter' Than Each Other for the Privacy of Government Requests for Information. **Emory Law Journal**, Atlanta, GA, v. 66, 2016; Georgia Tech Scheller College of Business Research Paper No. 2017-53. Disponível em: <https://ssrn.com/abstract=2920748>. Acesso em: 30 mar. 2017.

TANENBAUM, Andrew S.; J. WETHERALL, David. **Rede de computadores**. 5ed. São Paulo: Pearson, 2011.

TÁVORA, Nestor; ALENCAR, Rosmar Rodrigues. **Curso de Direito Processual Penal**. 3 ed. Salvador: Jus Podium, 2009.

TOURINHO FILHO, Fernando da Costa. **Manual de Processo Penal**. 9 ed. São Paulo: Saraiva, 2007.

_____. **Processo Penal**. 34 ed. São Paulo: Saraiva, 2012.

UNCTAD. Information Economy Report 2017: Digitalization, Trade and Development. **United Nations Conference on Trade and Development**. 23 Octuber 2017. New York oe Genebra: United Nations, 2017. Disponível em: <http://unctad.org/en/PublicationsLibrary/ier2017_en.pdf>. acesso em: 01 nov. 2017.

UNITED STATES FEDERAL NETWORKING COUNCIL. Definition of "Internet". RESOLUTION, October 24, 1995. Disponível em: < https://www.nitrd.gov/fnc/Internet_res.aspx>. Acesso em: 20 jul. 2016.

UNITED STATES. **Constitution of the United States.** Escrita em 1787, ratificada em 1788, e vigente desde 1789. Disponível em: < http://www.senate.gov/civics/constitution_item/constitution.htm>. Acesso em: 20 ago. 2016.

_____. Court of Appeals for the Second Circuit. In the matter of a warrant to search a certain e–mail account controlled and maintained by microsoft Corporation. **On Appeal from the United States District Court for the Southern District of New York**. Reply Brief for Appellant. Appellant: Microsoft Corporation. Appellee: United States. Case 14-2985, New York, New York, 08 abr., 2015. Disponível em: <http://mscorp.blob.core.windows.net/mscorpmedia/2015/04/Microsoft-Reply-Brief.pdf>. Acesso em: 26 jul., 2016. a

_____. Court of Appeals for the Second Circuit. In the matter of a warrant to search a certain e–mail account controlled and maintained by microsoft Corporation. **On Appeal from the United States District Court for the Southern District of New York**. Brief for Appellant. Preet Bharara, *US Attorney for Southern District of New York*. Appellant: Microsoft Corporation. Appellee: United States. Case 14-2985, New York, New York, 09 mar., 2015. Disponível em: <https://blogs.microsoft.com/datalaw/wp-content/uploads/sites/149/2014/09/GovtBrief-2ndCircuit.pdf>. Acesso em: 26 jul., 2016. b

_____. Court of Appeals for the Second Circuit. In the matter of a warrant to search a certain e–mail account controlled and maintained by microsoft Corporation. **On Appeal from the United States District Court for the Southern District of New York**. Brief for Appellant. Appellant: Microsoft Corporation. Appellee: United States. Case 14-2985, New York, New York, 08 dez., 2014. Disponível em: <https://blogs.microsoft.com/datalaw/wp-content/uploads/sites/149/2014/09/Microsoft-Opening-Brief-12082014.pdf >. Acesso em: 26 jul., 2016. a

_____. Court of Appeals for the Second Circuit. In the Matter of a Warrant to Search a Certain E-Mail Account Controlled and Maintained by Microsoft Corporation. Microsoft v. United States, Case 14-2985, Document 286-1, 14 jul., 2016, 1815361, Appellant: Microsoft Corporation, Appellee: United States of America. Argued: September 9, 2015, Decided: July 14, 2016. Disponível em: < https://www.justsecurity.org/wp-content/uploads/2016/07/Microsoft-Ireland-2d-Cir-Opinion-20160714.pdf>. Acesso em: 26 ago., 2016. a

_____. Department of Justice. **Legislation to Permit the Secure and Privacy-Protective Exchange of Electronic Data for the Purposes of Combating Serious Crime Including Terrorism**. Proposta legislativa de alteração do Electronic Communications Privacy Act (ECPA), encaminhada pelo Departamento de Justiça dos Estados Unidos ao Presidente do Senado, em 15 de julho de 2016. Disponível em: <https://www.aclu.org/sites/default/files/field_document/doj_legislative_proposal.pdf>. Acesso em: 08 out., 2017. b

_____. District Court SD Texas. In re Warrant to Search a Target Computer at Premises Unknown. **Case No. H–13–234M**. 22 apr. 2013. Disponível em: <http://md.fd.org/cja2014/nov2014/riley/In_re_warrant_to_search_a_ target_computer_at_premises_unknown.pdf>. Acesso em: 25 set. 2017.

_____. District Court Southern District of New York. In the matter of a warrant to search a certain e–mail account controlled and maintained by microsoft Corporation. **Memorandum of law in Support of Motion by Apple Inc. and Cisco System Inc. to Participate as *amicus curiae* and Microsoft Inc.´s Motion to Vacate Search Warrant.** Apple Inc. and Cisco System Inc.. Case 13-Mag-2814, New York, New York, 13 jun., 2014. Disponível em: <https://blogs.microsoft.com/datalaw/wp-content/uploads/sites/149/2014/09/ATT-AmicusBrief.pdf>. Acesso em: 26 jul., 2016. b

_____. District Court Southern District of New York. In the matter of a warrant to search a certain e–mail account controlled and maintained by microsoft Corporation. **Memorandum of law in Support of Verizon Communications Inc.´s Motion to Participate as *amicus curiae* and Microsoft Inc.´s Motion to Vacate Search Warrant.** Verizon Communications Inc. Case 13-Mag-2814, New York, New York, 10 jun., 2014. Disponível em: <https://blogs.microsoft.com/datalaw/wp-content/uploads/sites/149/2014/09/Verizon-AmicusBrief.pdf>. Acesso em: 26 jul. 2016. c

_____. District Court Southern District of New York. In the matter of a warrant to search a certain e–mail account controlled and maintained by microsoft Corporation. **Memorandum and Order**. Magistrate Judge James C. Francis IV. Case 13-Mag-2814, New York, New York, 25 abr., 2014. Disponível em: <http://www.nysd.uscourts.gov/cases/show.php?db=special&id=398>. Acesso em: 26 jul. 2016. d

_____. District Court Southern District of New York. In the matter of a warrant to search a certain e–mail account controlled and maintained by microsoft Corporation. **Memorandum and Order**. Chief Magistrate Loretta A. Preska. Case 13-Mag-2814, New York, New York, 29 ago., de 2014. Disponível em: < http://online.wsj.com/public/resources/documents/microsoftstay.pdf>. Acesso em: 20 ago. 2016. e

_____. District Court Southern District of New York. In the matter of a warrant to search a certain e–mail account controlled and maintained by Microsoft Corporation. **Governments' Memorandum of Law in Opposition to Microsoft´s Motion to Vacate Email Account Warrant**. Case 13-Mag-2814, New York, New York, 14 feb., 2014. Disponível em: <https://www.justsecurity.org/wp-content/uploads/2014/05/Governments-Memorandum-of-Law-in-Opposition-to-Motion-to-Vacate-doc-97....pdf>. Acesso em: 26 jul. 2016. f

_____. District Court Southern District of New York. In the matter of a warrant to search a certain e–mail account controlled and maintained by Microsoft Corporation. **Government's Brief in Support of The Magistrate Judge's Decision to Uphold a Warrant Ordering Microsoft to Disclose Records Within Its Custody and Control**. Preet Bharara, US Attorney for Southern District of New York. Case 13-Mag-2814, New York, New York, 09 jul., 2014. Disponível em: <https://cdn.arstechnica.net/wp-content/uploads/2014/07/federalbrief-microsoftcase.pdf>. Acesso em: 26 jul. 2016. g

_____. **Federal Rules of Criminal Procedure**. The original Federal Rules of Criminal Procedure were adopted by order of the Supreme Court on Dec. 26, 1944, transmitted to Congress by the Attorney General on Jan. 3, 1945, and became effective on Mar. 21, 1946. Disponível em: <https://www.law.cornell.edu/rules/frcrmp>. Acesso em: 09 nov., 2017.

_____. Supreme Court of the United States. In the matter of a warrant to search a certain e–mail account controlled and maintained by microsoft Corporation. **On Petition for a Writ of Certiorari to The United States Court of Appeals for the Second Circuit.** Petition for a Writ of Certiorari. Petitioner: United States of America. Respondent: Microsoft Corporation. Case nº 17-2, 23 jun., 2017. Disponível em: <https://www.justice.gov/sites/default/files/briefs/2017/06/28/17-2_microsoft_corp_petiton.pdf >. Acesso em: 26 out., 2017. a

_____. Supreme Court of the United States. In the matter of a warrant to search a certain e–mail account controlled and maintained by microsoft Corporation. **On Petition for a Writ of Certiorari to The United States Court of Appeals for the Second Circuit**. Brief for the States of Vermont, Alabama, Arizona, Arkansas, Connecticut, Delaware, Hawaii, Idaho, Illinois, Indiana, Iowa, Kansas, Kentucky, Louisiana, Maine, Maryland, MassachuSetts, Michigan, Montana, Nebraska, New Hampshire, New Mexico, New York, North Carolina, Ohio, Oregon, Pennsylvania, South Carolina, South Dakota, Texas, Utah, Virginia, Wyoming and the Commonwealth of Puerto Rico as Amici Curiae in Support of Petitioner. Petitioner: United States of America. Respondent: Microsoft Corporation. Case nº 17-2, 27 jul., 2017. Disponível em: <http://www.scotusblog.com/wp-content/uploads/2017/08/17-2-tsac-states-of-vermont.pdf. Acesso em: 30 out. 2017. b

_____. Supreme Court of the United States. Morrison et al v. National Australia Bank LTD et al. **Certiorari to the United States Court of Appeal for the Second Circuit**. Case No. 08–1191. Argued March, 29, 2010. Decided June, 24,2010. Disponível em: < https://www.supremecourt.gov/opinions/09pdf/08-1191.pdf>. Acesso em: 20 ago., 2016.

_____. United States Code Title 18. Crimes and Criminal Procedure. Part I – Crimes. Chapter 121: **Stored Wire and Electronic Communications and Transactional Records Access**. 1986. Disponível em: <https://www.law.cornell.edu/uscode/text/18/part-I/chapter-121>. Acesso em: 24 mai. 2016.

_____. United States Code Title 50: War and National Defense. Chapter 36: **Foreign Intelligence Surveillance**. 1978. Disponível em: < https://www.law.cornell.edu/uscode/text/50/chapter-36>. Acesso em: 24 mai. 2016.

_____. **Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism** - Usa Patriot Act. 107th Congress Public Law 56, approved October 26, 2001. Legislative History--H.R. 3162. Disponível em: <https://www.gpo.gov/fdsys/pkg/PLAW-107publ56/html/PLAW-107publ56.htm>. Acesso em: 20 ago. 2016.

UNODC. United Nations. **Comprehensive Study on Cybercrime**. Draft Februar y 2013. Vienna. New York: United Nations, 2013. Disponível em: <https://www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf>. Acesso em: 25 set. 2017.

_____. United Nations. **Report on the meeting of the Expert Group to Conduct a Comprehensive Study on Cybercrime**. Vienna, 10 a 13 de abr., 2017. Disponível em: <http://www.unodc.org/documents/organized-crime/cybercrime/Cybercrime-April-2017/Cybercrime_report_2017/Report_Cyber_E.pdf>. Acesso em: 22 out. 2017.

US-CERT. **Computer Forensics**. Produzido e atualizado em 2008. Disponível em: <https://www.us-cert.gov/sites/default/files/publications/forensics.pdf>. Acesso em: 03 fev. 2018.

VAILE, David; KALINICH, Kevin P.; FAIR, Patrick V.; LAWRENCE, Adrian. Data Sovereignty and the Cloud: A Board and Executive Officer's Guide. **UNSW Law Research,** Sidney, Australia, paper nº. 2013-84, december 16, 2013. Disponível em: <https://ssrn.com/abstract=2369660>. Acesso em: 30 mar. 2017.

VAN HOBOKEN, Joris; ARNBAK, Axel; VAN EIJK, N.A.N.M., Obscured by Clouds or How to Address Governmental Access to Cloud Data from Abroad. In: **The 6th Privacy Law Scholars Conference**, 2013, **Berkeley Center for Law & Technology,** Berkeley, CA. Disponível em: <https://ssrn.com/abstract=2276103>. Acesso em: 30 mar., 2017.

VARGAS-LEON, Patricia Adriana. Implications of the Application of the 'Hot Pursuit' Principle in the Cyberspace: An Analysis of the Case 'Microsoft v. United States of America'. **GigaNet: Global Internet Governance Academic Network**, Annual Symposium, December 1, 2016. Disponível em: <https://ssrn.com/abstract=2909894>. Acesso em: 30 mar. 2017.

VERAS, Manoel. **Computação em Nuvem**: Nova arquitetura de TI. Rio de Janeiro: Brasport, 2015.

VERGNOLLE, Suzanne. Understanding the French Criminal Justice System as a Tool for Reforming International Legal Cooperation and Cross-Border Data Requests. February 21, 2017. In: BRÄUTIGAM, Tobias; MIETTINEN, Samuli (toim.). **Data Protection, Privacy and European Regulation in the Digital Age**, 2016; Georgia Tech Scheller College of Business Research Paper No. 2017-55. Disponível em: <https://ssrn.com/abstract=2921364>. Acesso em: 30 mar. 2017.

VIDIGAL, Erick. A Lex mercatoria como fonte do direito do comércio internacional e a sua aplicação no Brasil. **Revista de informação legislativa**, Brasília, v. 47, n. 186, p. 171-193, abr./jun. 2010. Disponível em: <https://www2.senado.leg.br/bdsf/bitstream/handle/id/198681/000888826.pdf?sequence=1>. Acesso em: 25 mai. 2017.

WALDEN, Ian. Accessing Data in the Cloud: The Long Arm of the Law Enforcement Agent. **Queen Mary School of Law Legal Studies Research** Paper No. 74, London, England, nov. 14, 2011. Disponível em: https://ssrn.com/abstract=1781067>. Acesso em: 30 mar 2017.

WEBER, Patrícia Nuñez. **A cooperação jurídica internacional em medidas processuais penais**. Porto Alegre: Verbo Jurídico, 2011.

WENDT, Emerson; BARRETO, Alessandro Gonçalves. **Inteligência Digital**. Foco nas fontes abertas como ferramentas para produção de provas e conhecimentos de inteligência policial. Rio de Janeiro: Brasport, 2013.

WENDT, Emerson; JORGE, Higor Vinicius Nogueira. **Crimes Cibernéticos**: ameaças e procedimentos de investigação. Rio de Janeiro: Brasport, 2012.

WESTMORELAND, Kate; KENT, Gail. **International Law Enforcement Access to User Data**: A Survival Guide and Call for Action. January 8, 2015. Disponível em: <https://ssrn.com/abstract=2547289>. Acesso em: 30 mar. 2017.

WOODS, Andrew Keane. ECPA Reform: A Primer. **Just Security**, New York University School of Law, publicado em 16 set. 2015. Disponível em: <https://www.justsecurity.org/26120/ecpa-reform-primer/>. Acesso em: 30 abr. 2017.

_____. Against Data Exceptionalism (March 8, 2016). **Stanford Law Review**, v. 68, n. 729, mar., 2016. Disponível em: <https://ssm.com/abstract=2745038>. Acesso em: 10 jul. 2017.

ZACON, R. Hobbes' Internet Timeline. **Request for Comments 2235**. Category: Informational. November, 1997. Disponível em: <https://www.rfc-editor.org/rfc/rfc2235.txt>. Acesso em: 20 jul. 2016.

GLOSSÁRIO

Amicus curiae	Consiste numa pessoa ou entidade que é chamada ou se voluntaria a contribuir em determinado processo judicial em que não é parte, com o objetivo de apresentar a sua opinião sobre o assunto debatido em Tribunal.
Autoridade de persecução criminal	Expressão genérica utilizada para referir às autoridades públicas legalmente autorizadas a requisitar informações, expedir ordem de busca e apreensão, determina a produção de dados, em qualquer fase da persecução criminal. No Brasil, por exemplo, durante o inquérito policial, o Delegado de Polícia pode requisitar diretamente ao provedor de serviço dados cadastrais que informem qualificação pessoal, filiação e endereço (artigo 10 §3º do Marco Civil da Internet). Por outro lado, conteúdo de comunicações, registros de conexão e de acesso a aplicações de Internet serão fornecidas apenas mediante ordem judicial (artigo 10 §§ 1º e 2º do Marco Civil da Internet). Outro exemplo vem da Justiça francesa, que está dividida em dois ramos independentes: a Justiça Administrativa e a Justiça Judiciária. Para julgar os conflitos de jurisdição entre estas mesmas, há o Tribunal de Conflitos, formado por oito juízes, com mandato de três anos. Compete à Justiça Administrativa assessorar na redação de projetos de leis, ordenanças e decretos do Conselho de Estado e interpretação dos textos administrativos; e julgar as causas em que a Administração é parte (contencioso administrativo) etc. O outro ramo é a Justiça Judiciária, que é composta pelo magistrado de instrução ou de investigação (*juge d´instruction*) e o magistrado de julgamento (*magistrat*), que exercem as funções de investigação e julgamento, respectivamente. Os magistrados de investigação atuam na apuração de delitos graves e complexos. Compete-lhes a busca da verdade dos fatos, reunindo evidências que possam incriminar ou exonerar o investigado da prática do delito. Caso haja proposta de ação penal, os autos serão encaminhados ao *magistrat* (VERGNOLLE, 2016).
Bitcoin	É uma tecnologia digital que permite reproduzir em pagamentos eletrônicos a eficiência dos pagamentos convencionais. Pagamentos com bitcoins podem ser feitos para qualquer pessoa, que esteja em qualquer lugar do planeta, sem limite mínimo ou máximo de valor (https://www.bitcoinbrasil.com.br/o-que-e-bitcoin/).
Cadeia de custódia	É um processo usado para manter e documentar a história cronológica da evidência, para garantir a idoneidade e o rastreamento das evidências utilizadas em processos judiciais (LOPES; GABRIEL; BARETA, 2006).

Dado	É um sinal ou um sinal sem significado (FLEURY; OLIVEIRA JR, 2001).
Domain Name System	É o serviço da Internet cuja função é mapear os endereços IP em nomes, tecnicamente chamados de domínio, e vice-versa (KUROSE; ROSS, 2010).
Evidências digitais ou eletrônicas	São informações de valor probatório que estão armazenadas ou são transmitidas em formato digital, sendo relevantes tanto ao processo penal quanto na solução de litígios cíveis.
Hacking	Técnica de coleta de dados, baseada no envio de *malwares* a computadores remotos (GHAPPOUR, 2017).
Honeypot	Ferramenta que simula falhas de segurança em sistemas.
Hosts	Denominação atribuída a computadores que executam as aplicações dos usuários, numa rede geograficamente distribuída (TANENBAUM; WETHERALL, 2011).
Informação	É um sinal cujo significado pode ser procurado no sistema em que está incorporado, seja um sistema de informação, seja um sistema de prática coerente (FLEURY; OLIVEIRA JR, 2001).
Interpol	Instituição internacional que tem por objetivo patrocinar a cooperação entre autoridades policiais de 192 países membros, proporcionando inclusive apoio técnico e operacional nas ações, de forma a contribuir no combate à criminalidade internacional (https://www.interpol.int/About-INTERPOL/Overview).
Keylogger	É o termo oriundo da língua inglesa que significa registrador do teclado, ou seja, realiza a monitoração das informações digitadas pelo usuário do computador (WENDT; JORGE, 2012).
Malware	Programa ou *Software* malicioso, como vírus, worms ou Trojans (CLOUGH, 2011).
Metadado	Os metadados referentes ao *e-mail* são os nomes e endereços eletrônicos do destinatário e do remetente, os endereços IP associados, o dia e a hora em que o *e-mail* foi enviado, as informações de cobrança e outros que facilitam a identificação do usuário (KERR, 2004).
MLAT	Mutual legal assistance (MLA) is the formal government-to-government process for sharing information in criminal matters (WESTMORELAND; KENT, 2015).
Persecução penal	Ocorre para a apuração de infrações penais e sua respectiva autoria. No Brasil, apresenta dois momentos: o inquérito policial e a fase processual. A primeira é a fase inquisitiva, preliminar, preparatória para a ação penal. A segunda consiste no pedido

	de julgamento da pretensão punitiva (TÁVORA; ALENCAR, 2009).
Pesquisa Nacional por Amostra de Domicílios - PNAD	Investiga anualmente, de forma permanente, características gerais da população, de educação, trabalho, rendimento e habitação e outras, com periodicidade variável, de acordo com as necessidades de informação para o País, como as características sobre migração, fecundidade, nupcialidade, saúde, segurança alimentar, entre outros temas.
Provedor de serviço Internet	Significa: (i) Qualquer entidade pública ou privada que faculte aos utilizadores dos seus serviços a possibilidade de comunicar por meio de um sistema informático e (ii) Qualquer outra entidade que processe ou armazene dados informáticos em nome do referido serviço de comunicação ou dos utilizadores desse serviço (COUNCIL OF EUROPE, 2001a).
Ramsonware	Ransomware é um tipo de código malicioso que torna inacessíveis os dados armazenados em um equipamento, geralmente usando criptografia, e que exige pagamento de resgate (ransom) para restabelecer o acesso ao usuário (https://cartilha.cert.br/ransomware/).
Violação de dados pessoais	uma violação da segurança que provoca, de modo acidental ou ilícito, a destruição, a perda, a alteração, a divulgação não autorizada de dados pessoais transmitidos, conservados ou tratados de outro modo, ou o acesso não autorizado a esses dados;
Webmail	Aplicativo de correio eletrônico diretamente em site internet.
Writ of certiorari	No direito da *common law*, o termo *certiorari* significa um *writ* (ordem judicial) original, ao determinar que juízes de uma corte inferior ou oficiais certifiquem e transfiram o registro dos procedimentos da corte inferior no caso em exame para uma corte superior. No vocabulário da Suprema Corte, o sentido originário do termo foi expandido. Certiorari refere-se, genericamente, ao processo de revisão discricionária pela Suprema Corte de uma decisão de corte inferior. Essa revisão é buscada por meio de uma petição que requer *writ of certiorari*. Cada juiz, depois de analisar essa petição, faz o seu juízo sobre a propriedade ou não da revisão plenária pela corte inteira. Tal revisão é admitida se ao menos quatro juízes votam pela admissibilidade da petição, prática conhecida como *rule of four*.

APÊNDICE A – PROTOCOLO DE REVISÃO SISTEMÁTICA

1. Sobre a revisão sistemática de literatura

Revisão sistemática é uma metodologia rigorosa proposta para identificar os estudos sobre um tema em questão, aplicando métodos explícitos e sistematizados de busca, bem como para avaliar a qualidade e validade desses estudos e sua aplicabilidade, selecionando, ao final, aqueles que fornecerão as informações de interesse.

Diferencia-se da revisão tradicional, também conhecida como revisão narrativa da literatura, pois responde a uma pergunta mais pontual. Para superar possíveis tendências em cada etapa, exige-se o planejamento de um protocolo rigoroso sobre busca e seleção dos estudos, avaliação da validade e aplicabilidade desses estudos e síntese e interpretação dos dados coletados (DE-LA-TORRE-UGARTE-GUANILO; TAKAHASHI; BERTOLOZZI, 2011).

Conserando que não é o objetivo principal desta Tese apresentar uma rigorosa revisão sistemática de literatura sobre a coleta extraterritorial de evidências criminais eletrônicas em ambiente de nuvem, mas reconhecendo as facilidades e os benefícios trazidos pela metodologia na coordenação das operações de busca e seleção dos estudos de interesse, foi elaborado o presente Protocolo, que registra os critérios de pesquisa e seleção, sem no entanto apresentar discussões acerca da validade, aplicabilidade, síntese e interpretação dos dados coletados.

Este protocolo de revisão sistemática apresenta o modelo de busca e seleção de pesquisas científicas e de pareceres estatais, relativamente à coleta extraterritorial de evidências criminais eletrônicas armazenadas em ambiente de computação em nuvem, com o propósito de identificar as seguintes questões:

a) que pesquisas abordam diretamente questões legais alusivas à busca e apreensão extraterritorial de evidências criminais eletrônicas armazenadas em nuvem;
b) que pesquisas potencialmente podem contribuir com a proposta a ser apresentada, embora não estejam diretamente relacionadas ao tema (por exemplo: caso Microsoft Ireland, princípio da extraterritorialidade);
c) que propostas estão sendo apresentadas;
d) quais os fundamentos jurídicos utilizados.

As publicações selecionadas pelo processo sistemático descrito nesse Apêndice embasaram, principalmente, a escrita de duas seções, quais sejam: OS DESAFIOS AO ACESSO EXTRATERRITORIAL A EVIDÊNCIAS CRIMINAIS EM NUVEM COMPUTACIONAL (seção 2) e O ESTADO DA ARTE SOBRE A COLETA EXTRATERRITORIAL DE EVIDÊNCIAS CRIMINAIS ELETRÔNICAS (seção 7). Eventualmente, podeM fundamentar as argumentações presentes em outras seções da Tese.

2. O processo de busca das publicações

A pesquisa e a recuperação da literatura científica foram realizadas por meio de buscas automáticas e manuais. As pesquisas automáticas foram efetuadas com o emprego de engenhos de busca constantes em bibliotecas digitais, criadas para permitir acesso às publicações, seja em repositório próprio ou por meio de indexação de diversas bases de dados.

A consulta manual foi procedida no repositório de informações do Comitê para a Convenção do Cybercrime do Conselho da Europa.

Ademais, referências a novos artigos, que atendiam aos critérios da revisão, foram recuperadas a partir da leitura das publicações pesquisadas.

2.1 Definição das bibliotecas digitais

Foram selecionadas as bibliotecas digitais nomeadas na Tabela 13, que reuniam publicações das áreas das ciências sociais, onde se subsume o Direito, e da ciência da computação. Ademais, bases de dados de teses e dissertações nacionais e de abrangência mundial também foram consideradas neste processo de busca.

2.2 Definição das palavras-chaves

As palavras-chaves utilizadas na composição da expressão de busca, e os termos correspondentes, são apresentados na Tabela 14.

Os descritores foram combinados na forma de expressões lógicas, cuja sintaxe foi diversificada de acordo com os motores de busca utilizados. Por conseguinte, mais adiante, serão apresentadas as variadas expressões booleanas empregadas em cada ambiente de pesquisa.

Tabela 13 - Bibliotecas digitais utilizadas na busca por trabalhos científicos

Biblioteca digital	Área do conhecimento
Social Science Research Network (SSRN)[130];	Trata-se de uma rede mundial de colaborativa, dedicada a rápida disseminação de pesquisas em diversas áreas do conhecimento, predominantemente nas Ciências sociais. Nesse ambiente, os autores são encorajados a disponibilizar gratuitamente suas publicações, sejam no formato de resumo ou texto completo. Foi fundada em 1994 e, em 2016, foi adquirida por *Social Science Electronic Publishing Inc. by Elsevier*.
IEEE Xplore Digital Library[131];	Ferramenta de busca e acesso a publicações técnicas e científicas nas áreas da engenharia elétrica, ciência da computação e eletrônica, disponibilizadas pelo *Institute of Electrical and Electronics Engineers* (IEEE) e entidades parceiras.
Springer[132];	Publicações científicas, técnicas e da área médica, tem a finalidade de atender a pesquisadores da academia e profissionais relacionados ao desenvolvimento tecnológico empresarial.
Cyber Security Publication Library from Nato Cooperative Cyber Defense Centre of Excellence[133];	Direito Internacional de Guerra. Reúne livros, artigos, relatórios e outras publicações do *Nato Cooperative Cyber Defense Centre of Excellence* (CCDCOE), Centro de Excelência em Defesa Cibernética Cooperativa da Otan.
Banco de Teses e Dissertações da Coordenação de Aperfeiçoamento de Pessoal de Nível Superior - Capes[134];	A Capes, fundação do Ministério da Educação (MEC), dedica-se à expansão e consolidação da pós-graduação *stricto sensu* (mestrado e doutorado), em todos os Estados da Federação. O banco de dados mantido pela instituição disponibiliza acesso a teses e dissertações defendidas em programas de pós-graduação do Brasil.
Biblioteca Digital Brasileira de Teses e Dissertações (BDTD) do Instituto Brasileiro de Informação em Ciência e Tecnologia (IBICT)[135];	Teses e dissertações. Indexa, em um único portal, os sistemas de informação de teses e dissertações existentes no país.
Open Access Theses and Dissertations[136];	Teses e dissertações. Ferramenta de pesquisa desenvolvida e mantida por Thomas Dowling, que viabiliza o acesso a teses e dissertações defendidas e publicadas por mais de 1.100 (hum mil e cem) universidades, faculdades e instituições de pesquisa em todo o mundo. Em abril de 2017, constam mais de 3 milhões de trabalhos indexados.
Public version of WorldCat[137].	Acrônimo para "*World Catalog*", trata-se de um sistema web mantido pela *On-line Computer Library Center* (OCLC), que indexa acervos disponíveis em mais de 10.000 bibliotecas, distribuídas por cerca de 170 países. É considerada a maior rede mundial de conteúdos e serviços de bibliotecas.

Fonte: direta

[130] SSRN. Frequently Asked Questions. Atualizado em fev. 2017. Disponível em: <https://www.ssrn.com/en/index.cfm/ssrn-faq/>. Acesso em: 30 abr. 2017

[131] IEEE. About IEEE *Xplore*® Digital Library. Disponível em: <http://ieeexplore.ieee.org/xpl/aboutUs.jsp>. Acesso em: 30 mar. 2017.

[132] SPRINGER. About Springer. Diponível em: <http://www.springer.com/br/about-springer>. Acesso em: 30 mar. 2017.

[133] https://ccdcoe.org/publication-library.html

[134] CAPES. Competências. Publicado em 11 de maio de 2016. Disponível em: <http://www.capes.gov.br/acessoainformacao/80-conteudo-estatico/acesso-a-informacao/5418-competencias>. Acesso em: 30 mar. 2017

[135] IBICT. Sobre a BDTD. 2012. Disponível em: <http://www.ibict.br/informacao-para-ciencia-tecnologia-e-inovacao%20/biblioteca-digital-Brasileira-de-teses-e-dissertacoes-bdtd>. Acesso em: 30 mar. 2017.

[136] OATD. About OATD – The FAQ. 2017. Disponível em: <https://oatd.org/faq.html>. Acesso em: 30 mar. 2017.

[137] WORLDCAT. What is WorldCat? Disponível em: <http://www.worldcat.org/whatis/default.jsp>. Acesso em: 15 abr. 2017

Tabela 14 - Palavras-chaves utilizadas para compor a expressão de busca

Palavras-chaves	Termos correspondentes
Electronic evidence	Digital evidence; computer evidence; prova digital; prova eletrônica; prova informática; evidência digital; evidência eletrônica; evidência informática.
Extraterritorial	Extraterritoriality; trans-border; cross-border; overseas; extraterritorialidade;
Criminal	Penal; crime; cybercrime.
Cloud	Nuvem; computação em nuvem.
Microsoft Ireland Case	

Fonte: direta

2.3 Limitação temporal

O processo de busca considerou o período compreendido entre os anos 2006 a 2017, e foi realizado durante os meses de março e abril de 2017.

Embora, na literatura, não esteja claro quando o termo “computação em nuvem” foi utilizado pela primeira vez (MARTINI; QUICK; CHOO, 2013), o ano de 2006 foi escolhido como marco inicial da pesquisa porque, comercialmente, esse parece ter sido a primeira referência encontrada, quando, em março de 2006, a empresa Amazon.com Inc. lançou a Amazon Web Services (AWS), plataforma de serviços em nuvem que oferece processamento computacional, armazenamento de banco de dados, distribuição de conteúdo e outras funcionalidades[138]. Na academia, um dos registros mais remotos para o termo foi trazido pelo professor de sistemas de informação, Ramnath Chellappa[139], no ano de 1997.

3. Critérios de inclusão e exclusão das publicações

Os critérios de busca utilizados nas pesquisas retornaram um conjunto de publicações que, em parte, não abordavam temas diretamente relacionados ao presente estudo ou não permitiam o acesso gratuito ou apresentavam apenas o resumo, dentre outros aspectos restritivos à pesquisa.

Sendo assim, a escolha das publicações a serem consideradas nessa revisão foi orientada pelos seguintes critérios:

[138] https://aws.amazon.com/pt/what-is-aws/
[139] http://www.dell.com/learn/br/pt/brbsdt1/sb360/social_cloud

a) as que apresentavam aspectos legais ou técnicos, relacionados à coleta extraterritorial de evidências eletrônicas de crime;

b) as relacionadas diretamente com as discussões travadas sobre assuntos de interesse à pesquisa, mas que não constituem seu objeto (ex: sobre o caso *Microsoft Ireland*, sobre o *Stored Communications Act*, sobre temas de direito internacional);

c) disponíveis na forma completa;

d) escritas em inglês, português ou espanhol;

e) gratuidade de acesso para a pesquisadora.

Estudos foram excluídos quando:

a) o tema investigado não estava relacionado à busca extraterritorial de evidências eletrônicas de crime nem foi considerado relevante à proposta;

b) disponibilizavam unicamente o resumo do trabalho;

c) apresentavam apenas proposta de pesquisa;

d) foram publicados fora do limite temporal estabelecido.

Para classificar as publicações selecionadas de acordo com os critérios acima, foram utilizados os seguintes padrões:

a) FR, para referir as publicações fortemente relacionadas ao tema investigado;

b) RL, para indicar as publicações relacionadas a temas de interesse à pesquisa, mas que não constituem seu objeto principal. Exemplos: o caso Microsoft Ireland, sistemas de investigação criminal, cooperação internacional, dentre outros;

4. Estratégia de pesquisa e seleção das publicações

Durante o processo de busca das publicações, optou-se, sempre que possível, pela alternativa de busca avançada e, nesta, pela construção livre da expressão booleana de pesquisa, partindo, em todo o caso, de uma expressão abrangente para uma expressão mais restritiva, utilizando as palavras-chaves definidas.

Ao longo das pesquisas nas 09 (nove) bases de dados escolhidas, foi possível perceber que não há uniformidade na sintaxe usada para a construção das expressões booleanas. O engenho de busca da Springer, por exemplo, aceita que o pesquisador insira uma longa expressão booleana. Por sua vez, o IEEE Xplore Digital Library limita a expressão a 15 (quinze) termos de busca. E a biblioteca da Nato/Otan não aceita expressões booleanas, sendo as pesquisas realizadas apenas por meio de palavras-chaves ou variáveis (*tags*) pré-definidas.

Em razão dessa diversidade, o detalhamento sobre os procedimentos de consulta será apresentado por ocasião da abordagem particularizada acerca de cada biblioteca digital consultada.

A expressão mínima empregada na consulta foi "*electronic evidence OR digital evidence OR computer evidence*", pois o termo *evidence* isoladamente remeteu a uma infinidade de publicações em diversas áreas, como medicina, sociologia, psicologia.

Por sua vez, essa evidência eletrônica, digital ou de computador necessariamente deveria relacionar-se a prática de crime, o que motivou o arranjo seguinte, que incluía palavras-chaves "*crime OR criminal OR penal*". Posteriormente, decidiu-se por incluir o termo "*forensic*", em razão de constar em muitos resultados retornados a partir da primeira interação.

Os termos "*extraterritorial OR cross-border OR trans-border OR overseas*" também são considerados imprescindíveis ao contexto pesquisado, compondo assim a expressão de busca.

Por outro lado, o termo "*cloud*" foi tido como complementar à busca, uma vez que foi interesse da pesquisadora analisar também estudos acerca da coleta extraterritorial de evidências criminais em ambientes computacionais diversos do conceito de *cloud computing*. Não obstante, o termo foi considerado, mas sem restringir o resultado.

Por fim, foi considerada a expressão "*microsoft ireland case*", tendo em conta a significação do aludido caso às discussões sobre o tema ora estudado.

Todas as pesquisas foram repetidas e revisadas, de forma a garantir precisão nos resultados.

As publicações de interesse ao estudo foram escolhidas com base na leitura dos respectivos resumo, introdução e conclusão.

A seguir, serão detalhados procedimentos de busca e os resultados obtidos, em cada biblioteca consultada.

4.1 *Social Science Research Network* - SSRN

A primeira ressalva a ser apresentada quanto às consultas realizadas a fonte de dados SSRN refere-se a escolha do limite temporal. Dentre as opções estabelecidas pela ferramenta de busca (*all dates*; *last week*; *last month*; *last 3 months*; *last 6 months*; *last year*; *last 2 years*; *last 3 years*), foi eleita a mais abrangente, ou seja, "*all dates*". No entanto, foram considerados tão somente os estudos publicados a partir do ano de 2006.

Optou-se também pela pesquisa em *Title, Abstract, Keywords & Full Text.*

O motor de busca opera com refinamento de pesquisas. Sendo assim, iniciou-se a pesquisa com a expressão "*electronic evidence*", da qual retornaram 460 (quatrocentos e

sessenta) publicações. Dessas, aplicando-se o filtro com o termo "*extraterritorial*", resultaram 07 (sete), sendo as publicações de interesse ao tema apresentas na Tabela 15.

Tabela 15 - Resultados para as expressões "*electronic evidence*" e filtro "*extraterritorial*"

Ano	Título	Autor (es)	Propósito	CIs
2017	Cross-Border Evidence Gathering in Transnational Criminal Investigation: Is the Microsoft Ireland Case the 'Next Frontier'?	CURRIE, Robert J.	"The author here contends that the problems involved are best understood—and potentially resolved—via examination through the lens of the public international law of jurisdiction, and specifically the prohibition of extraterritorial enforcement jurisdiction".	FR
2017	Drawing Lines in the Cloud: Implications of Extraterritorial Limits to the Stored Communications Act	PECORARO, Andrew J. .	"The paper highlights two conclusions that may impact these other doctrines: First, the conclusion that a provider accessing data on one of its servers constitutes a search under the Fourth Amendment; and second, that the location of the data is a determinative factor in deciding jurisdiction over that data." "it proposes a new test for the validity of SCA warrants, positing that such warrants should be quashed upon a prima facie showing that either the target of the investigation is not a U.S. national or acting in the United States, or that retrieving the data would violate the laws of the country in which the data is being stored. Such a proposal allows law enforcement the flexibility to investigate as needed, but respects both the international sovereignty of other nations and the privacy interests of the owners of the data."	RL
2016	Searching Places Unknown: Law Enforcement Jurisdiction on the Dark Web	GHAPPOUR, Ahmed.	"This Article outlines a regulatory framework that reallocates decision-making to the institutional ac- tors who are best suited to determine U.S. foreign policy without sacrificing law enforcement's ability to identify and locate criminal suspects that have taken cover on the dark web".	RL
2015	The Un-Territoriality of Data	DASKAL, Jennifer C.	"the Article warns against the kind of unilateral, extraterritorial law enforcement that electronic data encourages — in which nations	FR

			compel the production of data located anywhere around the globe, without regard to the sovereign interests of other nations".	
2015	Warrants in the Clouds: How Extraterritorial Application of the Stored Communications Act Threatens the United States Cloud Storage Industry	SCHULTHEIS, Ned.	"[…] the extraterritorial application of the SCA places pressure on international relations, particularly between the United States and the European Union (the E.U.), over data protection law, which only further constrains the U.S. technology and cloud data industry […].This Note recommends certain amendments to the SCA to improve its relevancy to modern technology, based on the newly introduced Senate bill entitled the Law Enforcement Access to Data Stored Abroad Act (the LEADS Act).	RL
2011	New First Principles? Assessing the Internet's Challenges to Jurisdiction	SCASSA, Teresa; CURRIE, Robert J.	"The article examines how states exercise their authority with respect to Internet activities by addressing governance issues, by engaging in normative ordering for the Internet, and by extending the reach of their domestic laws to capture Internet-based activities. Lastly, the article concludes by offering a set of "first principles," in the form of policy precepts, to guide the evolution of public international law norms and to address problems particular to the context of the global Internet".	RL

Fonte: direta

Das publicações selecionadas acima, 02 (duas) abordam especificamente o ambiente de computação em nuvem.

Ocorre que, utilizando o filtro "*cloud*" sobre o universo da primeira pesquisa, obteve-se 29 (vinte e nove) publicações, sendo de interesse as constantes na Tabela 16, incluindo as duas citadas anteriormente.

Tabela 16 - Resultados de interesse ao estudo, para as expressões "*electronic evidence*" e filtro "*cloud*"

Ano	Título	Autor(es)	Propósito	CIs
2017	A Mutual Legal Assistance Case Study: The United States and France	SWIRE, Peter; HEMMINGS, Justin D.; VERGNOLLE, Suzanne.	"We conclude that the France/US relationship is a good case study for MLA reform, given the large differences in criminal procedure and substantive standards for access to evidence".	RL
2017	Cloudy with a Chance of Abused Privacy Rights: Modifying Third-Party Fourth Amendment Standing Doctrine Post-Spokeo	PUGH, Sarah.	"Microsoft is bringing a Fourth Amendment challenge to sections 2703 and 2705 of the SCA, which—when used in combination—permit the government to use "no-notice warrants" and secrecy orders to access a cloud user's communications and data from the electronic communications provider without the cloud user's knowledge."	RL
2016	Mutual Legal Assistance in an Era of Globalized Communications: The Analogy to the Visa Waiver Program	SWIRE, Peter; HEMMINGS, Justin D.	"[…] proposes an alternative way to improve MLA requests, what we call a Mutual Legal Assistance Statute (MLAS). Fortunately, there is a statutory precedent for addressing the higher volume of cross-border activity that arises with globalization – the Visa Waiver Program (VWP). Due to the analogous globalization of cross-border evidence, the idea is that eligible countries, with high-quality procedures for seeking evidence, would face a streamlined process for gaining evidence in the U.S".	RL
2016	'Cloud' Atlas — A Map to Amending Metadata Privacy Law in the Modern Era	GRAY, Andrew R..	"I propose practical changes to current data and metadata laws. I borrow from a proposal by Professor Andrew K. Woods, but give significant consideration to the issue of metadata. Properly amending these laws can increase law enforcement efficiency, while protecting personal privacy"	RL
2016	Law Enforcement Cross-Border Access to Data: Preliminary Report	SVANTESSON, Dan.	Propõe um novo framework para aplicação dos princípios da jurisdição no acesso transfronteiriço a evidências criminais eletrônicas, com base no afastamento da territorialidade do cerne da jurisdição.	FR

2016	Law Enforcement Access to Evidence via Direct Contact with Cloud Providers – Identifying the Contours of a Solution	SVANTESSON, Dan.	“My aim is to map out the interests and considerations that need to be taken into account in the pursuit of a framework (whatever form it may take) for facilitating appropriate LEA access to evidence via direct contact with cloud providers while still safeguarding the rights and interest of individuals, as well as the rights and interest of the cloud provider, and those of other states.”	FR
2015	Stakeholders in Reform of the Global System for Mutual Legal Assistance	SWIRE, Peter; HEMMINGS, Justin D.	Os atores envolvidos numa transação MLAT são agrupados conforme o interesse e o contexto das reformas a serem empreendidas. São eles: Governo norte-americano, Governo estrangeiro; provedores de Internet; sociedade civil organizada.	RL
2014	Cyberspace, the Cloud, and Cross-Border Criminal Investigation. The Limits and Possibilities of International Law	KOOPS, Bert-Jaap; GOODWIN, Morag.	“We argue that solutions require substantial preliminary work to create a shared basis of common understanding. First, cyber-investigations challenges need to be formally recognised at the international level by state representatives. Second, problems need to be conceptualised carefully, using appropriate metaphors. […].Third, the cyber-investigation and international law communities must familiarise themselves with each other’s language, concepts, and assumptions. […]. Long-term efforts should seek to develop a new international or widely shared multilateral legal instrument that allows narrowly defined and strongly safeguarded forms of cross-border cyber-investigations. […]. Meanwhile, in the shorter term, some states — early adopters — could start creating and enhancing the legitimacy of unilateral actions that are narrowly defined, transparently conducted, and strongly safeguarded, by advancing an alternative account of sovereignty in cyberspace.”	FR
2014	Remote Programmatic vCloud Forensics	MARTINI, Ben; CHOO, Kim-Kwang Raymond.	“We then propose a six-step process for the remote programmatic collection of evidential data to ensure as few changes as possible are made as part of evidence collection and that no potential evidence is missed”.	RL

2013	Obscured by Clouds or How to Address Governmental Access to Cloud Data from Abroad	HOBOKEN, Joris van; ARNBAK, Axel; VAN EIJK, N.A.N.M..	Este *paper* analisa questões legais dos Estados Unidos, bem como os impactos ante as leis de proteção de dados vigentes no continente europeu, concernente ao acesso extraterritorial a dados armazenados em nuvem, no exercício de operações de vigilância de inteligência pelo Governo norte-americano.	RL
2013	Cloud Computing and Forensic Accounting: Friends or Foes?	BECHTEL, Calistha.	"This paper explores challenges posed by cloud computing focusing on issues associated with the acquisition of evidence in virtualised environments. Since its advent, there has been a profound shift regarding the nature of digital evidence and throughout this paper we explore how cloud computing will impact the current tools, frameworks and procedures used or followed in forensic investigation."	RL
2013	Cloud Computing and Its Implications for Cybercrime Investigations in Australia	HOOPER, Christopher; MARTINI, Ben; CHOO, Kim-Kwang Raymond.	"It concludes that effective law enforcement operations in this area require harmonious laws across jurisdictions and streamlines procedures for granting assistance between law enforcement agencies."	FR
2013	Cloud Computing and Digital Forensics	MARTINI, Ben; QUICK, Darren; CHOO, Kim-Kwang Raymond.	"In this essay, we outline our cloud forensic framework that can be used to guide digital forensic investigations involving cloud computing services."	RL
2013	Data Sovereignty and the Cloud: A Board and Executive Officer's Guide	VAILE, David; KALINICH, Kevin P. ; FAIR, Patrick V.; LAWRENCE, Adrian.	Analisa vários aspectos relacionados à soberania dos dados na nuvem. Recomenda a empresas estabelecerem e seguirem política de localização e controle dos dados.	RL
2012	Legal Process and Requirements for Cloud Forensic Investigations	ORTON, Ivan; ALVA, Aaron; ENDICOTT-POPOVSKY, Barbara	"The authors will detail the process in criminal cloud forensic investigations for commanding production from cloud providers including constitutional and statutory limitations, and the civil and criminal admissibility processes."	RL
2011	Accessing Data in the Cloud: The Long Arm of the Law Enforcement Agent	WALDEN, Ian.	"This article examines how and when those boundaries apply, and what mechanisms have been adopted, or are proposed, to address the needs of LEAs in a cloud environment. This article focuses on European Union and	FR

			international legal rules, particularly the Council of Europe Cybercrime Convention (2001), on obtaining data for investigative and subsequent prosecutorial purposes, and how such rules interact and potentially conflict with foreign laws and rules".	
2010	Free at What Cost? Cloud Computing Privacy Under the Stored Communications Act	ROBISON, William Jeremy.	A principal contribuição é em relação ao SCA e a política dos provedores de computação em nuvem.	RL

Fonte: direta

Ainda sobre o primeiro conjunto, foi aplicado o filtro com o termo "*cross-border*", que resultou em 10 (dez) publicações, das quais 02 (duas) não são referidas nas consultas anteriores, conforme Tabela 17.

Tabela 17 - Resultados relevantes ao estudo, para as expressões "*electronic evidence*" e filtro "*cross-border*"

Ano	Título	Autor(es)	Propósito	CIs
2016	Understanding the French Criminal Justice System as a Tool for Reforming International Legal Cooperation and Cross-Border Data Requests	VERGNOLLE, Suzanne.	"MLATs have become an area of international dispute, with states becoming increasingly frustrated with the length and complication of the process for requesting electronic evidence".	RL
2006	Developments in the Global Law Enforcement of Cyber-Crime	BROADHURST, Roderic.	"In response to the threat of cyber-crime there is an urgent need to reform methods of mutual legal assistance and to develop trans-national policing capability. The international response is briefly outlined in the context of the United Nations Transnational Organised Crime Convention (in force from September 2003) and the Council of Europe's innovative Cybercrime Convention (in force from July 2004)"	RL

Fonte: direta

O termo “*overseas*” não trouxe resultados diferentes dos apresentados acima.

Para “*digital evidence*” e “*cloud*”, resultaram 21 (vinte e uma) publicações. Para “*digital evidence*” e “*crime*”, 56 (cinquenta e seis) publicações. Em ambas as consultas, interessa ao estudo e que não foi listada anteriormente, a publicação constante naTabela 18.

Para os termos “*extraterritorial*”, “*overseas*”, “*cross-border*” não houve resultado.

A expressão “*Microsoft ireland case*” retornou 13 publicações, das quais 08 (oito) relevantes ao presente estudo. Dessas, 04 (quatro) estão listadas nas Tabelas acima, restando as descritas na Tabela 19.

Tabela 18 - Resultados para as expressões “*digital evidence*” + “*cloud*” e “*digital evidence*” + “*crime*”, não listados anteriormente.

Ano	Título	Autor(es)	Propósito	CIs
2016	Against Data Exceptionalism	WOODS, Andrew Keane.	Como um Estado pode aplicar a legislação interna para apurar delitos ocorridos em seu território, envolvendo apenas seus nacionais ou residentes, sem que os efeitos alcancem Estado estrangeiro, quando evidências criminais eletrônicas relevantes à elucidação do caso encontram-se armazenadas nuvem global.	FR

Fonte: direta

Tabela 19 - Resultados relevantes ao estudo, para a expressão “*Microsoft ireland case”*.

Ano	Título	Autor (es)	Propósito	CIs
2016	Cloudy with a Conflict of Laws	KRISHNAMURTHY, Vivek	“What I hope this paper will contribute is a fuller description of why the MLAT system and cloud computing as we know them are fundamentally irreconcilable, and what are the minimum requirements of an alternative regime that can prevent the splintering of these services along national geographic lines”.	FR
2016	Implications of the Application of the 'Hot Pursuit' Principle in the Cyberspace: An Analysis of the Case 'Microsoft v. United States of America'	VARGAS-LEON, Patricia Adriana.	“Taking the ‘Microsoft Ireland’ case as a case study, this paper will: a) provide an overview of how the hot pursuit mechanism has been understood by the international court of justice (ICJ) and the International Tribunal of the Law of the Sea (ITLOS), b) analyze the arguments and allegations of the parties involved in the Microsoft case about why one nation-state’s	RL

			sovereignty should be applicable or not beyond the borders of its own territory, and c) analyze the possible repercussions of applying the hot pursuit, a mechanism used in the past by nation-states when they were trying to regulate a space beyond their national jurisdiction and apply their sovereignty into the cyberspace (an electronic medium that cannot be govern by any nation-state)".	
2016	How Both the EU and the U.S. Are 'Stricter' Than Each Other for the Privacy of Government Requests for Information	SWIRE, Peter; KENNEDY-MAYO, DeBrae.	"The discussion next turns to three models for the future of MLA, especially in the wake of the 2016 Second Circuit decision in Microsoft Ireland, which set important new limits on U.S. government access to emails held in overseas servers. We call the three models: (1) MLA status quo; (2) extraterritoriality; and (3) Visa Waiver Program (VWP). We assess the ability of each model both to protect privacy and civil liberties, and to fulfill legitimate law enforcement requests. We conclude that a well-designed VWP is the best available approach".	RL
2015	International Law Enforcement Access to User Data: A Survival Guide and Call for Action	WESTMORELAND, Kate; KENT, Gail.	"This paper provides an overview of the current system for foreign governments seeking user data from U.S.-based internet companies. After describing the way in which the system currently operates, it identifies problems with the system, and outlines the reform efforts that are beginning to emerge".	RL

Fonte: direta

Outras consultas foram realizadas, todavia, sem resultados diferentes dos apresentados anteriormente.

4.2 IEEE Xplore Digital Library

As pesquisas foram realizadas na opção Avançada (*advanced search*), utilizando a expressão lógica de busca constante na Figura 10, que resultou em 66 (sessenta e seis)

publicações, embora apenas as listadas na Tabela 20 são de interesse ao presente estudo. Não houve retorno para a expressão "*Microsoft Ireland case*".

É oportuno ressaltar que a ferramenta de busca limita a consulta booleana a, no máximo, 15 (quinze) termos.

("electronic evidence" OR "digital evidence" OR "computer evidence") AND (crime OR penal) AND (extraterritorial OR cross-border OR trans-border OR overseas).

Figura 10 - Expressão booleana com as palavras-chaves de interesse, sobre a IEEE Xplore
Fonte: direta

Tabela 20 - Resultados de interesse para a expressão da Figura 10

Ano	Título	Autor(es)	Propósito	CIs
2016	Forensic model for cloud computing: An overview	ALEX, M.Edington; KISHORE, R. .	"For mitigating dependence on CSP we come up with a new model for collecting forensic evidences outside cloud environment."	RL
2016	Microsoft v. USA: Location of Data and the Law of the Horse	TENE, Omer.	"For centuries, private international law, the branch of law concerning conflicts of law across international borders and jurisdictions, established rules based on the location of people, organizations, and activities"	RL
2015	Cloud Forensics: A Review of Challenges, Solutions and Open Problems	ALQAHTANY, Saad; CLARKE, Nathan ; FURNELL, Steven; REICH, Christoph	"There are plenty of issues that need to be resolved in order to perform a proper digital investigation in the cloud environment. This paper examines the challenges in cloud forensics that are identified in the current research literature."	RL

Fonte: direta

4.3 *Springer*

As pesquisas foram realizadas na opção Avançada (*advanced search*), utilizando as expressões lógicas de busca constantes na Tabela 21, que retornaram as quantidades respectivas. As publicações de interesse, disponíveis gratuitamente ou enviadas gentilmente pelos autores, estão listadas na Tabela 22.

Tabela 21 - Expressões lógicas de busca com as palavras-chaves de interesse, sobre a biblioteca digital *Springer*

Expressão de busca	Quantidade Publicações
("electronic evidence" OR "digital evidence" OR "computer evidence") AND (criminal OR penal OR crime OR cybercrime OR threat OR forensic) AND (extraterritorial OR excepcionalism OR cross-border OR trans-border OR overseas)	98
("electronic evidence" OR "digital evidence" OR "computer evidence") AND (criminal OR penal OR crime OR cybercrime OR threat OR forensic) AND (extraterritorial OR excepcionalism OR cross-border OR trans-border OR overseas) AND cloud	30
“Microsoft Ireland case”	01

Fonte: direta

Tabela 22 - Publicações disponíveis e de interesse ao estudo, retornadas pelo uso das expressões lógicas da Tabela 21

Ano	Título	Autor(es)	Propósito	CIs
2016	Challenges in Collecting Digital Evidence: A Legal Perspective	LAURITS, Eneli; KASPER, Agnes.	“This article discusses issues relating to collection of digital evidence in criminal proceedings, civil cases, arbitration and other legal purposes in order to identify areas where private sector actions can inform law enforcement efforts and vice versa while outlining a model for legal requirements of digital forensic readiness”.	RL

Fonte: direta

4.4 *Cyber Security Publication Library from Nato Cooperative Cyber Defense Centre of Excellence*

São disponibilizadas duas formas de pesquisa: por meio de palavras-chaves e através de variáveis (*tags*) pré-definidas. Em ambos os casos, o engenho de busca não admite operadores booleanos. Por conseguinte, foram utilizadas as seguintes palavras-chaves, em pesquisas individualizadas: *cross-border*, *extraterritorial*, *overseas*, *evidence*, *digital*, *electronic*, *computer*, *cloud*, *criminal, Microsoft.*

As palavras-chaves *cloud*, *microsoft* e *computer* não retornaram publicações. As demais, retornaram 07 (sete), sendo que apenas 02 (duas) de interesse à pesquisa e apenas 01 (uma) disponível (Tabela 23).

Tabela 23 - Publicação retornada, e disponível, pelo uso das palavras-chaves *transborder*, *cross-border*, *extraterritorial*, *evidence*, *digital*, *electronic*, *criminal*, relevantes ao processo de revisão.

Ano	Título	Autor(es)	Propósito	CIs
2015	Accessing Extraterritorially Located Data: Options for States	OSULA, Anna-Maria	"This analysis gives a brief overview on the role of criminal procedure and law enforcement entities in investigating cyber incidents, and then moves on to the options for States to access extraterritorially located data".	FR

Fonte: direta

4.5 Banco de Teses e Dissertações da Capes

Foram realizadas consultas, utilizando-se as expressões lógicas constantes na Tabela 24, que retornaram as quantidades respectivas, sendo apenas uma publicação de interesse ao presente estudos, conforme Tabela 25.

É oportuno ressaltar que, por razões não compreensíveis, o montante de trabalhos retornados com as referidas expressões inclui, em sua grande maioria, resultados não desejados. Após o emprego de vários filtros de pesquisa, os trabalhos foram analisados individualmente e selecionados pela pesquisadora, chegando à Tabela 25.

Especificamente sobre o tema pesquisado, não foi encontrada qualquer Tese ou Dissertação, sendo selecionadas apenas as que analisavam temas relevantes à escrita deste trabalho.

Tabela 24 - Expressões lógicas de busca com as palavras-chaves de interesse, sobre o Banco de Teses e Dissertações da Capes

Expressões de busca	Quantidade Publicações	Publicações de interesse
"electronic evidence" OR "digital evidence" OR "computer evidence"	04	0
("evidência digital" OR "evidência eletrônica" OR "evidência informática") AND (criminal OR penal OR crime)*	92	02
("prova digital" OR "prova eletrônica" OR "prova informática") AND (criminal OR penal OR crime)*	258	02
Extraterritorial	43	00
microsoft AND cloud	07	0

(*) nas áreas de conhecimento das ciências sociais e da ciência da computação
Fonte: direta

Tabela 25 - Publicação de interesse ao estudo, retornada pelo uso das expressões lógicas da Tabela 24.

Ano	Título	Autor(es)	Propósito	CIs
2007	Cooperação internacional em matéria Penal na Convenção sobre o Cibercrime.	DELGADO, Vladimir Chaves	Analisar as disposições relativas ao auxílio mútuo em matéria penal, contidas na Convenção sobre o Cibercrime, adotada pelo Conselho da Europa, em Budapeste, a 23 de novembro de 2001.	RL

Fonte: direta

4.6 Biblioteca Digital Brasileira de Teses e Dissertações do IBICT

Foram realizadas consultas, utilizando-se as expressões lógicas constantes na Tabela 26, que retornaram as quantidades respectivas, embora não tenha retornado qualquer pesquisa relacionada ao tema.

Tabela 26 - Expressões lógicas de busca com as palavras-chaves de interesse, sobre o BDTD/IBICT

Expressões de busca	Quantidade Publicações	Publicações de interesse
"electronic evidence" OR "digital evidence" OR "computer evidence"	11	0
"evidência digital" OR "evidência eletrônica" OR “evidência informática”	01	0
"prova digital" OR "prova eletrônica" OR “prova informática”	03	01
Extraterritorial	26	01
microsoft AND cloud	08	0

Fonte: autora

4.7 *Open Access Theses and Dissertations* (OATD)

Foram realizadas consultas, utilizando-se as expressões lógicas constantes na Tabela 27, que retornaram as quantidades respectivas, sendo de interesse à pesquisa a listada na Tabela 28.

Tabela 27 - Expressões lógicas de busca com as palavras-chaves de interesse, sobre o OATD

Expressões de busca	Quantidade Publicações	Publicações de interesse
(("computer evidence") OR ("digital evidence") OR ("electronic evidence")) AND (crime)	37	0
(computer OR digital OR electronic) AND evidence AND criminal AND cross-border	05	01
“micrososft Ireland case”	0	0

Fonte: direta

Tabela 28 - Publicações de interesse ao estudo, retornadas pelo uso das expressões lógicas da Tabela 27.

Ano	Título	Autor(es)	Propósito	Cls
2017	Remote search and seizure of extraterritorial data	OSULA, Anna-Maria.	“The dissertation draws attention to the lack of clarity of the current Estonian regulation of remote search and seizure, and proposes elements that should be kept in mind while reviewing the Code of Criminal Procedure in order to guarantee both the effectiveness of criminal procedure as well as being in line with domestic and international norms”.	FR

Fonte: direta

4.8 *Public Version of WorldCat*

A consulta para a expressão “*Microsoft ireland case*” resultou em 20 (vinte) publicações, das quais 12 (doze) apresentam relação direta com o tema estudado. A maior parte dessas publicações, que estão listadas na Tabela 29, são opiniões de autores em *blogs* e periódicos da Internet, que, embora não sejam trabalhos científicos, foram considerados relevantes à compreensão do cerne desta pesquisa.

Tabela 29 - Publicações de interesse ao estudo, retornadas pelo uso expressão “Microsoft ireland case”, na *Public Version of WorldCat*

Ano	Título	Autor(es)	Propósito	CIs
2017	A Microsoft Ireland Fix: Time to Act is Now!	DASKAL, Jennifer.	“Here I suggest three possible options, designed to address the relevant security, privacy, and economic interests at stake”	RL
2016	The "Microsoft Ireland" Case (Amicus Brief)	BRENNAN Center for Justice	“The Brennan Center, in conjunction with […], filed an amicus brief in support of Microsoft Corporation, which cautions the Second Circuit against repeating two significant errors in the lower court’s reasoning. Both errors could have a powerful impact on the future of digital privacy, and therefore merit close consideration.”	RL
2016	The Microsoft Ireland Case: A Clear Answer, An Uncertain Future	BUTLER, Jadzia.	“Unfortunately, the future of cross-border law enforcement data requests is still messy, convoluted, and extremely uncertain.”	RL
2015	ECPA Reform: A Primer	WOODS, Andrew K.	“ECPA should be reformed to allow US firms to voluntarily comply with foreign government demands for US-stored electronic content if […]”	RL

Fonte: direta

5. Busca manual às publicações do Comitê para a Convenção do Cybercrime, do Conselho da Europa

Foi realizada busca por publicações de interesse, no sítio eletrônico do Comitê para a Convenção de Budapeste sobre o Cibercrime, da qual resultou as publicações constantes na Tabela 30.

Tabela 30 - Publicações do Comitê para a Convenção do Cibercrime, do Conselho da Europa

Ano	Título	CIs
2017	Terms of Reference for the Preparation of a Draft 2nd Additional Protocol to the Budapest Convention on Cybercrime	FR
2016	Criminal justice access to electronic evidence in the cloud: Recommendations for consideration by the T-CY. Final report of the T-CY Cloud Evidence Group	FR
2016	Criminal justice access to electronic evidence in the cloud - Informal summary of issues and options under consideration by the Cloud Evidence Group	FR
2016	Criminal justice access to data in the cloud: cooperation with "foreign" service providers	FR
2015	Criminal justice access to data in the cloud: challenges	FR
2014	Transborder access to data and jurisdiction: Options for further action by the T-CY	FR
2013	Guidance Note #3: Transborder access to data (Article 32)	RL

Fonte: direta

6. Considerações finais

O presente protocolo de revisão sistemática foi de grande valia para orientar a pesquisa, subsidiando uma ampla revisão de literatura sobre o tema estudado, principalmente na identificação da problemática alusiva à busca extraterritorial a evidências criminais eletrônicas armazenadas em servidor de computação em nuvem, localizado em território estrangeiro, bem como na árdua procura por soluções adequadas.

A partir da sistematização do processo de busca de publicações, bem como da padronização dos critérios de escolha, foi possível selecionar apenas as publicações relevantes ao estudo, facilitando assim o processo de escrita dos capítulos de revisão.

ANEXO A - OCORRÊNCIAS REGISTRADAS NA DELEGACIA DE POLÍCIA DE REPRESSÃO AO CRIME CIBERNÉTICO DE PERNAMBUCO, DE JANEIRO/2014 A OUTUBRO/2017

SECRETARIA DE DEFESA SOCIAL Pernambuco

ESTADO DE PERNAMBUCO
SECRETARIA DE DEFESA SOCIAL
GERÊNCIA DE ANÁLISE CRIMINAL E ESTATÍSTICA

C.I. nº 300/2017-GACE/SDS Recife, 27 de novembro de 2017.

Ao Ilmo° Senhor
MANOEL CAETANO CYSNEIROS DE ALBUQUERQUE NETO
Ouvidor da Secretaria de Defesa Social

ASSUNTO: Solicitação de Dados Estatísticos

Senhor Ouvidor,

Cumprimentando-o cordialmente, venho por meio desta, em resposta à CI nº 413/2017 OUV/SDS, referente ao pedido de informação solicitado pela Sra. **DANIELLE NOVAES DE S. VALVERDE**, a qual requer o número de ocorrências registradas na delegacia de polícia de repressão ao crime cibernético no Estado de Pernambuco, no período de janeiro de 2014 a outubro de 2017, encaminhar relatório nº 949/2017/GACE/SDS, contendo os dados estatísticos solicitados.

Sem mais para o momento, agradeço antecipadamente, e renovo meus protestos de elevada estima e consideração.

Atenciosamente,

JONAS SOBRAL MORENO – Maj PM
Gerente da GACE

Hayanna

Rua São Geraldo, N° 111 – Santo Amaro – Recife – PE.
CEP: 50040-020 Fone/Fax: 3183-5063 / e-mail: secretaria.gace@gmail.com

AMPLIAR AS AÇÕES DE PREVENÇÃO E DE REPRESSÃO QUALIFICADAS DA VIOLÊNCIA E DE RESSOCIALIZAÇÃO, COM FOCO NA REDUÇÃO DA CRIMINALIDADE.

PACTO PELA VIDA

NÚMEROS DE OCORRÊNCIAS REGISTRADAS NA DELEGACIA DE POLÍCIA DE REPRESSÃO AO CRIME CIBERNÉTICO NO ESTADO DE PERNAMBUCO, NO PERÍODO DE JANEIRO DE 2014 A OUTUBRO DE 2017.

Relatório nº 949/2017/GACE/SDS

DOCUMENTO DE REFERÊNCIA: CI OUV Nº 413/2017

SOLICITANTE: Danielle Novaes de S. Valverde

ÁREA DE ANÁLISE: Estado de Pernambuco

SISTEMA UTILIZADO: INFOPOL/SDS.

DATA DE DISTRIBUIÇÃO: 24/11/2017

METODOLOGIA UTILIZADA NA PESQUISA

Como procedimento metodológico adotado, em função dos objetivos, este Relatório foi concebido buscando essencialmente a enumeração e a ordenação de dados, sem o objetivo de comprovar ou refutar hipóteses exploratórias, abrindo espaço para uma nova pesquisa explicativa, fundamentada nas informações decorrentes do curso do processo ou das investigações.

Com a finalidade de atender a demanda do solicitante, foram coletados da base de dados criminais do Sistema INFOPOL – os números de ocorrências registradas na Delegacia de Polícia de Repressão ao Crime Cibernético no Estado de Pernambuco, no período de janeiro de 2014 a outubro de 2017.

Nota: As ocorrências registradas na Delegacia de Repressão ao Crime Cibernético incluem todos os tipos de natureza, não só crimes cibernéticos.

TABULAÇÃO DOS DADOS CRIMINAIS

Tabela 01. Números de ocorrências registradas na Delegacia de Repressão ao Crime Cibernético no Estado de Pernambuco, no período de janeiro a dezembro de 2014.

NATUREZA	JAN	FEV	MAR	ABR	MAI	JUN	JUL	AGO	SET	OUT	NOV	DEZ	TOTAL
ESTELIONATO / FRAUDE	6	14	10	15	23	18	24	22	12	11	14	13	**182**
DIFAMAÇÃO	2	7	12	15	28	19	17	26	16	15	12	13	**182**
INVASÃO DE DISPOSITIVO INFORMÁTICO	3	4	11	4	10	6	3	9	11	5	8	6	**80**
FALSA IDENTIDADE / FALSIDADE IDEOLÓGICA	3	4	1	8	11	7	5	6	7	1	1	2	**56**
AMEAÇA	1	1	3	8	7	4	4	6	8	2	3	2	**49**
INJÚRIA	1	3	5	2	4	2	2	0	1	1	0	2	**23**
CALÚNIA	0	2	1	0	0	1	1	1	1	0	0	4	**11**
OUTRAS OCORRÊNCIAS CONTRA PESSOA	3	1	0	0	0	1	0	1	3	2	0	0	**11**
OUTRAS OCORRÊNCIAS NÃO CRIMINAIS	1	0	1	3	0	2	0	1	0	0	1	0	**9**
OUTRAS OCORRÊNCIAS ILÍCITOS PENAIS	0	0	2	0	1	3	2	1	0	0	0	0	**9**
PORNOGRAFIA INFANTIL	0	0	0	1	2	2	0	0	1	1	1	0	**8**
EXTORSÃO	1	0	2	1	1	0	3	0	0	0	0	0	**8**
OUTROS FURTOS	0	1	0	0	1	2	1	0	0	0	1	1	**7**
ROUBO A TRANSEUNTE	0	0	0	0	0	0	1	2	0	0	0	0	**3**
FURTO A OUTRAS INSTITUIÇÕES FINANCEIRAS	0	0	0	0	0	0	0	0	0	0	1	0	**1**
OUTRAS OCORRÊNCIAS DE TRÂNSITO	0	1	0	0	0	0	0	0	0	0	0	0	**1**
FURTO EM ESTABELECIMENTO COMERCIAL OU DE SERVIÇOS	0	0	0	0	0	0	0	0	0	1	0	0	**1**
OUTRAS OCORRÊNCIAS CONTRA PATRIMÔNIO	0	0	0	0	0	0	0	0	0	0	0	1	**1**
TOTAL GERAL	**21**	**38**	**48**	**57**	**88**	**67**	**63**	**75**	**60**	**39**	**42**	**44**	**642**

Fonte: INFOPOL/GACE/SDS

Tabela 02. Números de ocorrências registradas na Delegacia de Repressão ao Crime Cibernético no Estado de Pernambuco, no período de janeiro a dezembro de 2015.

NATUREZA	JAN	FEV	MAR	ABR	MAI	JUN	JUL	AGO	SET	OUT	NOV	DEZ	TOTAL
DIFAMAÇÃO	19	13	19	14	14	18	9	10	13	11	9	5	**154**
ESTELIONATO / FRAUDE	7	7	5	6	5	7	8	9	5	16	7	9	**91**
INVASÃO DE DISPOSITIVO INFORMÁTICO	6	7	2	4	5	2	4	6	7	5	7	1	**56**
FALSA IDENTIDADE / FALSIDADE IDEOLÓGICA	6	3	5	2	3	4	4	2	5	6	1	2	**43**
AMEAÇA	0	2	2	5	4	0	4	4	2	1	1	3	**28**
INJÚRIA	2	0	0	4	3	1	2	1	3	2	2	3	**23**
CALÚNIA	1	0	1	2	2	1	0	2	6	1	3	1	**20**
OUTRAS OCORRÊNCIAS NÃO CRIMINAIS	0	0	0	0	5	1	0	2	0	0	0	0	**8**
OUTRAS OCORRÊNCIAS ILÍCITOS PENAIS	0	0	0	0	1	2	2	1	0	1	1	0	**8**
EXTORSÃO	0	0	0	1	0	0	1	0	1	0	1	0	**4**
PORNOGRAFIA INFANTIL	1	0	0	1	1	0	0	1	0	0	0	0	**4**
OUTROS FURTOS	2	0	0	0	1	0	1	2	0	0	0	0	**6**
ROUBO A TRANSEUNTE	0	0	0	0	0	0	0	0	0	0	1	1	**2**
OUTRAS OCORRÊNCIAS CONTRA PESSOA	1	0	0	0	1	0	0	0	0	0	0	0	**2**
DIFAMAÇÃO POR VIOLÊNCIA DOMÉSTICA/FAMILIAR	0	0	0	0	0	0	2	0	0	0	0	0	**2**
CRIMES CONTRA A ORDEM ECONÔMICA	0	0	0	0	0	0	0	0	0	0	1	0	**1**
CUMPRIMENTO DE MANDADO DE BUSCA E APREENSÃO DE OBJETOS	0	0	0	0	0	0	0	0	0	0	0	1	**1**
OUTROS CRIMES CONTRA O CONSUMIDOR	0	0	0	0	0	1	0	0	0	0	0	0	**1**
INJURIA QUALIFICADA RACIAL	0	0	0	0	0	0	0	0	1	0	0	0	**1**
PERTURBAÇÃO DO SOSSEGO / TRANQUILIDADE PÚBLICA	0	1	0	0	0	0	0	0	0	0	0	0	**1**
FURTO (SAÍDA DE BANCO/INSTITUIÇÃO FINANCEIRA)	0	0	0	0	0	0	0	0	1	0	0	0	**1**
OUTROS CRIMES CONTRA A DIGNIDADE SEXUAL	0	0	0	0	0	0	0	0	1	0	0	0	**1**
ASSÉDIO SEXUAL	0	0	0	0	0	0	1	0	0	0	0	0	**1**
TOTAL GERAL	**45**	**33**	**34**	**39**	**45**	**37**	**38**	**40**	**45**	**43**	**34**	**26**	**459**

Fonte: INFOPOL/GACE/SDS

Tabela 03. Números de ocorrências registradas na Delegacia de Repressão ao Crime Cibernético no Estado de Pernambuco, no período de janeiro a dezembro de 2016.

NATUREZA	JAN	FEV	MAR	ABR	MAI	JUN	JUL	AGO	SET	OUT	NOV	DEZ	TOTAL
ESTELIONATO / FRAUDE	14	6	7	12	10	11	13	12	15	10	18	18	**146**
DIFAMAÇÃO	18	6	17	10	12	10	10	8	11	11	14	13	**140**
INVASÃO DE DISPOSITIVO INFORMÁTICO	7	5	7	5	4	7	7	7	8	7	5	9	**78**
INJÚRIA	4	1	3	6	8	10	10	10	0	6	5	9	**72**
FALSA IDENTIDADE / FALSIDADE IDEOLÓGICA	1	4	3	3	5	9	5	3	3	6	4	9	**55**
AMEAÇA	4	2	2	2	3	3	2	4	4	4	5	1	**36**
CALÚNIA	1	1	1	0	2	4	1	0	3	2	1	1	**17**
EXTORSÃO	0	1	1	3	1	2	1	0	1	3	2	2	**17**
OUTROS FURTOS	2	0	0	0	1	1	0	0	0	1	3	1	**9**
OUTRAS OCORRÊNCIAS NÃO CRIMINAIS	2	2	0	1	0	0	1	1	0	0	0	0	**7**
PORNOGRAFIA INFANTIL	1	0	1	0	0	0	1	1	0	1	1	1	**7**
INJURIA QUALIFICADA RACIAL	0	0	0	0	0	1	0	0	1	1	0	1	**4**
OUTRAS OCORRÊNCIAS CONTRA PESSOA	0	0	0	0	0	0	1	1	2	0	0	0	**4**
OUTRAS OCORRÊNCIAS ILÍCITOS PENAIS	2	1	0	0	0	1	0	0	0	0	0	0	**4**
ACIDENTE DE TRÂNSITO SEM VÍTIMA	0	0	0	0	0	1	0	0	1	0	1	0	**3**
EXTORSÃO/RESTRIÇÃO LIBERDADE DA VÍTIMA (SEQUESTRO RELÂMPAGO)	0	0	0	0	0	0	0	0	1	0	2	0	**3**
ROUBO A TRANSEUNTE	0	0	1	1	1	0	0	0	0	0	0	0	**3**
PERTURBAÇÃO DO SOSSEGO / TRANQUILIDADE PÚBLICA	0	0	0	0	0	1	0	0	0	1	0	0	**2**
CORRUPÇÃO DE MENORES	0	0	0	0	1	0	0	0	0	0	0	0	**1**
INJÚRIA POR VIOLÊNCIA DOMÉSTICA/FAMILIAR	0	0	0	0	0	0	0	0	0	0	0	1	**1**
POSSE ILEGAL DE ARMA	0	0	0	0	0	0	0	0	0	1	0	0	**1**
PROSTITUIÇÃO/EXPLORAÇÃO SEXUAL DE VULNERÁVEL	0	0	0	0	0	0	1	0	0	0	0	0	**1**
RACISMO/PRECONCEITO/DISCRIMINAÇÃO	0	0	0	0	1	0	0	0	0	0	0	0	**1**
TOTAL GERAL	**56**	**29**	**43**	**43**	**49**	**61**	**53**	**47**	**50**	**54**	**61**	**66**	**612**

Fonte: INFOPOL/GACE/SDS

Tabela 04. Números de ocorrências registradas na Delegacia de Repressão ao Crime Cibernético no Estado de Pernambuco, no período de janeiro a outubro de 2017.

NATUREZA	JAN	FEV	MAR	ABR	MAI	JUN	JUL	AGO	SET	OUT	TOTAL
ESTELIONATO / FRAUDE	27	16	24	26	21	39	30	38	45	34	**300**
INVASÃO DE DISPOSITIVO INFORMÁTICO	9	10	13	13	13	1	7	10	3	6	**85**
DIFAMAÇÃO	13	9	2	2	0	0	0	2	7	6	**41**
FALSA IDENTIDADE / FALSIDADE IDEOLÓGICA	6	4	1	2	1	2	0	0	0	0	**16**
OUTROS FURTOS	2	4	3	1	0	1	2	1	2	0	**16**
AMEAÇA	5	2	0	0	1	0	2	0	0	2	**12**
EXTORSÃO	0	1	3	2	0	3	1	0	0	0	**10**
PORNOGRAFIA INFANTIL	3	1	1	0	0	0	3	1	0	0	**9**
INJÚRIA	6	0	0	0	1	0	0	0	0	1	**8**
OUTRAS OCORRÊNCIAS ILÍCITOS PENAIS	1	1	0	0	0	0	3	1	2	0	**8**
INJURIA QUALIFICADA RACIAL	1	3	0	0	0	0	0	0	0	0	**4**
OUTRAS OCORRÊNCIAS CONTRA PESSOA	1	1	0	0	1	0	1	0	0	0	**4**
CALÚNIA	1	0	0	0	0	0	0	0	0	1	**2**
RACISMO/PRECONCEITO/DISCRIMINAÇÃO	0	0	0	0	0	0	0	0	0	2	**2**
CORRUPÇÃO DE MENORES	0	0	1	0	0	0	0	0	0	0	**1**
DIFAMAÇÃO POR VIOLÊNCIA DOMÉSTICA/FAMILIAR	1	0	0	0	0	0	0	0	0	0	**1**
HOMICÍDIO	1	0	0	0	0	0	0	0	0	0	**1**
TOTAL GERAL	**77**	**52**	**48**	**46**	**38**	**46**	**49**	**53**	**59**	**52**	**520**

Fonte: INFOPOL/GACE/SDS

Recife, 24 de Novembro de 2017.

PRISCILA BAUMGARTNER
ANALISTA GACE SDS
MAT 108.916-7

Responsável pelas informações:
Priscila Baumgartner
Analista Criminal da Uniai/GACE

Responsável pela validação:
Cleyton Pimentel
Chefe da UNIAI/GACE

Cleyton Pimentel
Chefe - UNIAI/GACE-SDS
Mat. 106.287-5