DENISE PROVASI VAZ

PROVAS DIGITAIS NO PROCESSO PENAL:

*Formulação do conceito, definição das características e
sistematização do procedimento probatório*

TESE DE DOUTORADO

ORIENTADOR PROFESSOR TITULAR ANTONIO SCARANCE FERNANDES

FACULDADE DE DIREITO DA UNIVERSIDADE DE SÃO PAULO

São Paulo, 2012

DENISE PROVASI VAZ

PROVAS DIGITAIS NO PROCESSO PENAL:
Formulação do conceito, definição das características e
sistematização do procedimento probatório

Tese apresentada à Faculdade de Direito da Universidade de São Paulo, como exigência parcial para a obtenção do título de Doutor em Direito Processual, sob a orientação do Professor Titular Antonio Scarance Fernandes.

FACULDADE DE DIREITO DA UNIVERSIDADE DE SÃO PAULO

SÃO PAULO, 2012

Banca examinadora

Agradeço a Deus pelas oportunidades que me concedeu e pela possibilidade de concluir este trabalho, que dedico:

A Sérgio Marcos de Moraes Pitombo (*in memoriam*), meu primeiro mestre de Direito Processual Penal, a quem devo o amor pela matéria, a busca pelo rigor técnico e o espírito de defesa da liberdade humana.

A Antonio Scarance Fernandes, constante Professor, com quem aprendi técnica, métodos, equilíbrio em tudo e lições de vida.

À minha família, pela paciência e apoio, indispensáveis para que eu pudesse realizar este trabalho, em especial à minha mãe Mercia e às minhas irmãs Heloisa e Liliana.

A meus amigos a Gabriela Campos Sales, Mariângela Lopes e João Fábio Azeredo, que me auxiliaram com as revisões e discussões tão importantes à conclusão do estudo.

Às minhas queridas amigas Denise Banci, Cristina Jabardo, Daniela Antoniassi e Érika Pires de Campos, por todo o incentivo e por mais de uma década de amizade e de apoio. Ao amigo Daniel Campos de Carvalho, por dividir as mesmas angústias desse longo trabalho.

Aos todos os meus amigos de trabalho, pelo companheirismo e motivação diários, em especial Antonio Sergio Pitombo, Luciana Louzado, Flávia Lotfi de Queiroz, Rodrigo Teixeira Silva, Beatriz Ferraro e Julia Mariz.

RESUMO

O desenvolvimento de novas tecnologias e a formação da sociedade da informação, a partir do Século XX, acarretaram novos hábitos pessoais e sociais e transformações no processamento e arquivamento das informações.

O tratamento e o registro de fatos e ideias passaram a ser feitos de maneira digital, com o uso de dispositivos eletrônicos que operam no sistema binário.

Esse novo panorama trouxe diversos reflexos para o processo penal, principalmente relacionados à prova. Entretanto, a legislação e a jurisprudência não acompanharam o avanço tecnológico, abrindo-se um vazio normativo em matéria de procedimento probatório.

Por essa razão, faz-se imprescindível a análise dos aspectos técnicos e sociais em face da teoria da prova, para se buscar conceituar o resultado do desenvolvimento tecnológico, ou seja, a prova digital, com a verificação de sua natureza jurídica e do procedimento probatório adequado para sua utilização no processo penal brasileiro.

Assim, o objetivo desta tese é aferir o conceito e a natureza jurídica da prova digital e demonstrar que ela constitui espécie própria de fonte de prova, que, embora assemelhada ao documento, apresenta características peculiares, que demandam regulamentação específica de seu procedimento probatório.

A partir do delineamento do conceito, da classificação e da caracterização da prova digital, examinam-se os meios de obtenção de prova e meios de prova adequados a essa fonte *sui generis*, observando a suficiência e a propriedade das normas existentes no ordenamento atual. Ao final, destacam-se os principais aspectos que carecem de regulação, propondo-se estrutura ainda rudimentar de normas para a matéria.

ABSTRACT

The development of new technologies and the consequent rise of the Information Society, starting in the twentieth century, led to new personal and social habits and a revolution in the processing and storage of information.

In this context, treatment and record of facts and ideas turned to be made digitally with the use of electronic devices operating in the binary system.

This new situation has brought several consequences for the criminal proceedings, notably with respect to the evidence. However, legislation and case law have not kept up with the pace of technological change, opening up a normative vacuum in the field of evidence.

For this reason, it is essential to analyze the technical and social aspects of this new scenario state of evidence theory in the wake of these changes, so as to conceptualize and establish a proper legal and evidentiary procedure for the verification of digital evidence in the criminal justice process.

In assessing the concept and the legal nature of digital evidence, this thesis demonstrates that digital evidence is fundamentally a distinct kind of evidence, which, while similar to the document, nevertheless presents unique characteristics that require specific regulation of its evidentiary procedure.

From the definition of the concept, classification and characterization of digital evidence, this thesis examines the proper methods of obtaining and producing digital evidence in a manner consistent with its unique nature, while at the same time questioning the sufficiency and adequacy of the rules in the current law regarding such methods. Finally, this thesis proposes a rudimentary framework of rules for this field.

RÉSUMÉ

Le développement de nouvelles technologies et la formation de la société de l'information, à partir du siècle XX, ont engendré de nouvelles habitudes personnelles et sociales, autant que de transformations dans le traitement et l'archivage d'informations.

Le traitement et le registre d'événements et d'idées passent à se faire par la voie digitale, avec des dispositifs électroniques qui opèrent dans le système binaire.

Ce nouveau panorama a des conséquences pour la procédure pénale, voire la preuve. Toutefois, ni les lois ni la jurisprudence ont suivi ce progrès technologique, ce qui engendre un vide normatif pour la procédure probatoire.

De ce fait, l'analyse des aspects techniques et sociaux face à la théorie de la preuve est indispensable pour permettre la recherche d'un concept pour le résultat du développement technologique, soit, la preuve digitale, avec la vérification de sa nature juridique et de la procédure probatoire adéquate à l'utilisation dans la procédure pénale brésilienne.

Ceci dit, le but de cette thèse est de retrouver le concept et la nature juridique de la preuve digitale, aussi bien que de démontrer qu'il s'agit en effet d'une espèce propre de source de preuve laquelle, quoique semblable au document, a des caractéristiques péculiaires et requiert donc une réglementation spécifique pour la procédure probatoire.

Les moyens d'obtention de la preuve et les moyens de preuve adéquats à cette source *sui generis* sont examinés à partir de l'ébauche du concept, de la classification et de la caractérisation de la preuve digitale, en tenant compte de la suffisance et de la pertinence des normes existantes dans l'ordre juridique actuel. Dernièrement, nous identifions les aspects clés qui manquent de réglementation et proposons des normes, bien que rudimentaire, sur la matière.

SUMÁRIO

INTRODUÇÃO.....	10
 CAPÍTULO 1 – PREMISSAS SOBRE A TECNOLOGIA DA INFORMAÇÃO E SUA INFLUÊNCIA PARA AS PROVAS	13
1.1 Relevância e atualidade do tema.....	13
1.2 Desenvolvimento tecnológico e sociedade da informação	17
1.3 Noções fundamentais sobre dispositivos eletrônicos e sistemas informáticos	21
Informática e computadores	21
Dados e seu processamento.....	24
Internet e transmissão da informação.....	26
1.4 Alteração do processamento e do arquivo da informação e sua influência na produção de provas.....	29
1.5 Crimes informáticos, delitos tradicionais e a prova.....	31
 CAPÍTULO 2 – NOÇÕES SOBRE A TEORIA DA PROVA	36
2.1 Premissas relativas às provas e ao processo	36
2.2 Direito à prova e seus limites.....	39
2.3 Conceitos de prova.....	43
2.4 Momentos do procedimento probatório e espécies de provas	48
2.5 Tipicidade da prova e distinção com provas nominadas, anômalas e irrituais	52
 CAPÍTULO 3 – PROVAS DIGITAIS: CONCEITO, CARACTERÍSTICAS E NATUREZA JURÍDICA	61
3.1 Prova digital: conceito	61
3.2 Características da prova digital	66
Imaterialidade.....	67
Volatilidade	68
Suscetibilidade de clonagem.....	69
Necessidade de intermediação	69

3.3 Comparação entre prova digital e documento. Análise da natureza jurídica da prova digital.....	70
3.4 Necessidade de normas próprias para a prova digital	77

CAPÍTULO 4 - MEIOS DE OBTENÇÃO E DE PRODUÇÃO DA PROVA DIGITAL

.....	80
4.1 Busca e apreensão	84
4.2 Apreensão remota de dados e infiltração	94
4.3 Interceptação telemática	100
4.4 Produção da prova digital pelo meio documental.....	107
4.5 Produção da prova digital pelo meio pericial	115

CAPÍTULO 5 – QUESTÕES RELEVANTES SOBRE A PROVA DIGITAL E

PROPOSIÇÕES.....	120
5.1 A inviolabilidade dos dados e a validade de sua captação	120
5.2 Os limites à obtenção e à utilização da prova digital	128
5.3 A busca pelo equilíbrio entre eficiência e garantismo nas provas digitais.....	132
5.4 Proposição de regras para regulamentação da prova digital	138

CONCLUSÃO.....	146
-----------------------	------------

BIBLIOGRAFIA REFERIDA.....	152
-----------------------------------	------------

INTRODUÇÃO

INTRODUÇÃO

A revolução tecnológica, iniciada no século XX e ainda em curso, promoveu profundas modificações na sociedade e em seu modo de se relacionar, bem como projetou importantes reflexos na área jurídica.

Ainda recentes, tais modificações suscitam grandes debates nas diversas áreas.

No Direito Penal, discute-se a necessidade da tipificação de novas condutas perpetradas por meios informáticos e os bens jurídicos a serem tutelados.

No campo das relações comerciais e consumeristas, discute-se a contratação no ambiente virtual e suas consequências.

Ainda, é de se destacar a discussão sobre a validade e utilização do documento eletrônico para o Direito Civil e o Processo Civil.

Pouco explorada, mas não menos relevante, é a influência do desenvolvimento tecnológico sobre as provas no Processo Penal. Embora sejam frequentes interceptações telemáticas, buscas e apreensões de computadores e requisições de dados cadastrais de usuários da internet, as provas obtidas ou produzidas por esses meios carecem de regulamentação.

As principais consequências dessa situação são a insegurança jurídica e a fragilidade da proteção dos direitos fundamentais. Não obstante o emprego de provas originadas do desenvolvimento tecnológico, não se encontram definidos os limites de sua utilização, a forma de sua introdução no processo e os critérios para aferição de sua validade e de seu valor probatório.

A exemplo do que se inicia em outros países, mostra-se necessário organizar e aprofundar os estudos sobre a matéria, assim como construir regras processuais apropriadas.

Nesse contexto, o presente trabalho desenvolve a tese de que as provas digitais constituem fonte de prova diferenciada, embora assemelhada aos documentos. Esta premissa conduz à conclusão de que, para garantia dos direitos fundamentais, do devido

processo legal e da eficiência do processo penal, a forma de obtenção e produção dessa prova depende de normas específicas, que contemplem suas peculiaridades.

Ademais, demonstra-se que o procedimento probatório respectivo deve se pautar pelos objetivos de preservação da integridade e da autenticidade da prova, com a mínima intervenção na esfera individual, com vistas a assegurar a eficiência do procedimento em um processo garantista.

Para tanto, o estudo busca delinear o conceito de provas digitais e definir sua natureza jurídica, a partir da análise de suas principais características, de modo a indicar o procedimento probatório a ser aplicado, enfocando, então, a comparação entre as provas digitais e as provas documentais e concluindo pelo enquadramento das provas digitais em uma categoria própria.

Examinam-se, a seguir, os meios de obtenção de referida prova e as normas aplicáveis para sua produção, destacando as peculiaridades que acarretam questões relacionadas à validade e legitimidade da prova, bem como à garantia dos direitos fundamentais.

Encerra-se tratando das questões mais relevantes advindas desse novo cenário, assim como das possíveis respostas normativas.

Assim, no Capítulo 1, traçam-se as premissas essenciais para a compreensão e o debate do tema, em especial a conformação da sociedade da informação e as mudanças promovidas pelo desenvolvimento tecnológico. São indicados os principais conceitos atinentes à tecnologia, delineando-se, também, a relação entre provas e tecnologia. Ademais, analisa-se a pertinência do tema à linha de pesquisa seguida.

No Capítulo 2, são tratados os principais temas atinentes à teoria da prova penal, com destaque para a definição dos sentidos do termo “prova”, para o procedimento probatório e para a questão das provas típicas e atípicas.

O Capítulo 3 enfoca a análise das provas digitais, em seus contornos essenciais. Verificam-se seus conceitos, natureza, objeto e características, ensejando a discussão sobre as normas aplicáveis para a obtenção e produção de tais provas.

O Capítulo 4 dedica-se ao estudo dos meios de obtenção e produção de provas digitais, quais sejam, a busca e apreensão dos suportes eletrônicos e dos dados digitais, infiltração, interceptação telemática, e os meios de prova documental e pericial.

No Capítulo 5, condensam-se as questões relacionadas à prova digital, em especial considerando o cotejo com os direitos e garantias fundamentais, em busca de delineamentos gerais e proposições normativas sobre o tema.

Ao final, são reunidos os principais pontos levantados ao longo do estudo, apresentando-se as considerações finais sobre o tema.

CAPÍTULO 1 – PREMISSAS SOBRE A TECNOLOGIA DA INFORMAÇÃO E SUA INFLUÊNCIA PARA AS PROVAS

1.1 Relevância e atualidade do tema

O mundo atual é marcado pelo constante uso da tecnologia nos mais diversos âmbitos da atividade humana, na maior parte das nações. Desde a criação dos computadores em meados do século XX, o desenvolvimento de equipamentos dotados de tecnologia digital proliferou-se, vindo a alcançar o cotidiano de expressiva quantidade de pessoas.

No Brasil, a venda de computadores iniciou-se no final da década de 70 do século passado, sendo que, em edição de 10 de junho de 1981, a revista *Veja* noticiava que existiam no país cerca de 22 mil computadores.¹ De sua parte, a internet passou a estar disponível, de maneira comercial no país, a partir de 1995, ano em que foi criado o Comitê Gestor da Internet.²

Os números cresceram vertiginosamente, de modo que os Resultados Preliminares da Amostra do Censo Demográfico 2010, realizado pelo Instituto Brasileiro de Geografia e Estatística (IBGE), indicaram a existência do computador em 38,3% das residências brasileiras, o triplo do que havia em 2000. Isto representa cerca de 22 milhões de lares, dos quais 80% contavam com acesso à internet. No Distrito Federal e no Sudeste, esse número é ainda superior: 63% no DF, 53% em São Paulo e 49% no Rio de Janeiro³ Ainda, reportagem divulgada recentemente apontou que foram vendidos 3.860 milhões de computadores no Brasil, apenas no segundo trimestre de 2011.⁴

¹ Disponível em: http://veja.abril.com.br/arquivo_veja/capa_10061981.shtml. Acesso em 10.11.2011.

² Conforme <http://www.cg.org.br/sobre-cg/historia.htm>. Acesso em 10.11.2011.

³ Disponível em:

http://www.ibge.gov.br/home/estatistica/populacao/censo2010/resultados_preliminares_amostra/default_resu ltados_preliminares_amostra.shtm e <http://www1.folha.uol.com.br/mercado/1007350-triplica-numero-de-casas-com-computador-diz-ibge.shtml>. Acesso em 28.12.2011.

⁴ Disponível em: <http://video.globo.com/Videos/Player/Noticias/0,,GIM1598561-7823-BRASIL+ULTRAPASSA+O+JAPAO+NO+NUMERO+DE+COMPUTADORES+VENDIDOS,00.html>. Acesso em 10.11.2011.

O computador é utilizado na indústria, no comércio, nas comunicações, nas atividades de lazer, etc.

As inovações nos hábitos pessoais e profissionais provocaram reflexos nas atividades policiais. Tornou-se corriqueira a procura por dados digitais para subsidiar investigações criminais, com a realização de buscas e apreensões e interceptações de dados.

Nesse contexto, é de se notar a popularização das megaoperações policiais na última década, principalmente a partir de 2003, quando a Polícia Federal deflagrou a denominada Operação Anaconda. A ela se seguiram, no âmbito federal, Operação Vampiro, Operação Farol da Colina, Operação Chacal, Operação Capela, Operação Monte Éden, Operação Narciso, Operação Sanguessuga, Operação 14 Bis, Operação Tigre, Operação Dilúvio, Operação Kaspar, Operação Navalha, Operação Persona, Operação Furacão, Operação João-de-Barro, Operação Satiagraha, Operação Vulcano, Operação Castelo de Areia, Operação Caixa de Pandora, Operação Voucher, dentre inúmeras outras.⁵ É comum que a deflagração das operações inclua o cumprimento de inúmeros mandados de busca e apreensão, além de prisões e sequestro de bens, e ainda que seja precedida de interceptações telefônicas e telemáticas.⁶

Com isso, muitas investigações policiais resultam na apreensão de grande volume de suportes eletrônicos e de dados digitais, ensejando diversos questionamentos sobre os limites das apreensões, sobre a devolução dos equipamentos apreendidos, sobre o acesso e uso das informações captadas, bem como sobre a validade e autenticidade das provas.

Timidamente, os tribunais começam a discutir as questões suscitadas, nem sempre mantendo uma lógica e um padrão decisórios. A ilustrar a afirmação, veja-se que o Tribunal Regional Federal da 1ª Região, nos anos de 2007, 2008 e 2009, por meio da Terceira e da Quarta Turmas, apresentou decisões opostas com relação à restituição de

⁵ De acordo com informações divulgadas pela Polícia Federal, as operações policiais ultrapassam a soma de 1400, desde o ano de 2003. Disponível em: <http://www7.pf.gov.br/DCS/operacoes/indexop.html>. Acesso em 10.11.2011.

⁶ Segundo notícia divulgada pelo Conselho Nacional de Justiça, em 10 de janeiro de 2012, a Justiça autorizou a interceptação de, ao menos, 18.050 linhas telefônicas e o monitoramento de “204 endereços eletrônicos (e-mail) e 673 linhas telefônicas que utilizam a internet para a transmissão de voz, sistema conhecido como voz sobre protocolo de internet (VOIP)”, em outubro de 2011. Disponível em: <http://www.cnj.jus.br/noticias/cnj/17795-justica-autoriza-grampo-em-195-mil-telefones-em-2011>. Acesso em 14.01.2012.

computadores apreendidos. Enquanto a Terceira Turma entendeu que o disco rígido poderia ser restituído, mediante a realização de cópia⁷, a Quarta Turma denegou a restituição, sob o argumento da necessidade de conservação em razão de interesse para o processo (art. 118, CPP)⁸.

No mesmo passo, questões relevantes deixam de ser analisadas profundamente, não contando com uma interpretação legal e constitucional adequada. Como exemplo, nota-se que a discussão levantada pelos impetrantes do Habeas Corpus nº 33.682 acerca do sigilo das informações colhidas em diligência de busca e apreensão e da necessidade de contraditório para o acesso aos dados computacionais foi afastada pelo

⁷ PROCESSO PENAL. BUSCA E APREENSÃO. DISCO RÍGIDO DE COMPUTADOR E DINHEIRO. COMPROVAÇÃO DA PROPRIEDADE. RESTITUIÇÃO. 1. Bem apreendido, consistente em disco rígido de computador (HD), pode ser restituído, mediante realização de cópia (back up), caso ainda não tenha sido efetivada a perícia técnica, mormente quando já fora apreendido há mais de 2 (dois) anos.

2. Documentos indicativos da profissão de autônomo (revendedor de produtos de vestuário e calçados) e contracheques, contemporâneos aos fatos, demonstrando que o apelante trabalhava para o Governo do Distrito Federal, são indicativos de capacidade econômica e atividade lícita que justificam a posse do valor apreendido nos autos, devendo ser restituído.

ACR 2006.36.00.014589-7/MT, Desemb. Federal Tourinho Neto, Terceira Turma, e-DJF1 p.191 de 03/10/2008.

⁸ PENAL. PROCESSUAL PENAL. RESTITUIÇÃO DE COMPUTADOR/NOTEBOOK. INTERESSE AO PROCESSO. DEMONSTRAÇÃO. MANUTENÇÃO DA DECISÃO QUE INDEFERIU A RESTITUIÇÃO. REFORMA DA DECISÃO QUE INDEFERIU PEDIDO DE RESTITUIÇÃO DE VEÍCULO. TERMÔ DE COMPROMISSO DE FIEL DEPOSITÁRIO ATÉ O ENCERRAMENTO DA AÇÃO. ASSINALAÇÃO DE PRAZO À PERÍCIA. INCONSISTÊNCIA.

1. Interessando a apreensão dos bens para o processo (art. 118 do CPP), a manutenção da decisão que indeferiu pedido de restituição é medida que se impõe.

2. Inacolhível o pedido de assinatura de prazo à perícia, porque, objeto de decisão em primeiro grau, que não foi atacada mediante embargos de declaração, visando sua definição temporal.

3. Recurso improvido.

ACR 2005.39.00.010077-7/PA, Desemb. Federal Hilton Queiroz, Quarta Turma, DJ p.36 de 23/03/2007.

PROCESSUAL PENAL. RESTITUIÇÃO DE BENS E VALORES APREENDIDOS. ORIGEM LÍCITA NÃO DEMONSTRADA. IMÓVEL SOB RESTRIÇÃO JUDICIAL. AQUISIÇÃO ANTERIOR AOS FATOS SUPOSTAMENTE DELITUOSOS. APELAÇÃO PARCIALMENTE PROVIDA.

1. Não se vislumbra juridicamente admissível, no atual momento processual, a restituição definitiva do automóvel e dos valores em depósito bancário, pois somente a partir da cognição integral da questão, a ser levada a efeito quando do julgamento da ação penal, é que se poderá definir se os bens em referência possuem, ou não, origem lícita.

2. A Quarta Turma deste Tribunal Regional Federal, ao analisar questões que se vislumbra como semelhantes à presente hipótese, firmou posicionamento no sentido de se manter o bloqueio acautelatório durante a fase da instrução criminal, em face da ausência inequívoca da demonstração da origem lícita dos valores bloqueados.

3. Quanto aos equipamentos de informática requeridos pela apelante (02 CPU's de computador, 01 scanner de mesa, 01 impressora), afigura-se incabível a sua restituição no atual momento processual, nos termos do art. 118, do Código de Processo Penal. Com efeito, tais bens podem vir a auxiliar durante a instrução criminal, servindo como meio de prova à elucidação dos fatos reputados como delituosos e suas circunstâncias, razão pela qual a sua apreensão deve ser mantida.

4. Na forma da manifestação do d. Ministério Público Federal, afigura-se procedente o pedido da apelante quanto ao bem imóvel cuja restituição se requer.

5. Apelação criminal parcialmente provida.

ACR 2007.41.00.001619-9/RO, Desemb. Federal I'talo Fioravanti Sabo Mendes, Quarta Turma, e-DJF1 p.77 de 31/07/2009.

Superior Tribunal de Justiça, mediante a simples afirmação de que a busca e apreensão fora determinada por autoridade competente e de que o parágrafo único do artigo 1º da Lei 9.296/96 autoriza a interceptação do fluxo de comunicações em sistema de informática e telemática.⁹ Como se percebe, a resposta fornecida não se relaciona com o questionamento feito.

No campo legislativo, não se vislumbra a proposição de normas que possam conferir solução jurídica aos problemas surgidos com as provas digitais, no que se relaciona à classificação das provas, seu procedimento, seu valor probatório, os limites de sua utilização, dentre outros. O Marco Civil da Internet, Projeto de Lei nº 2.126/2011, disciplina o uso da internet e prevê os direitos dos usuários. Com referência a provas, porém, somente dispõe sobre a requisição judicial de registros de conexão e registros de acesso. A questão do registro e preservação dos dados também é objeto do Projeto de Lei nº 5.403/2001, que aguarda votação na Câmara dos Deputados.

Tramita ainda na Câmara dos Deputados o Projeto de Lei nº 84/99, de relatoria do Senador Eduardo Azeredo, que tipifica os denominados crimes eletrônicos. Do mesmo modo, em relação às provas, o projeto apenas trata da preservação de dados de acesso pelos provedores de internet.

Por seu turno, o projeto de novo Código de Processo Penal não contempla normas específicas sobre a obtenção e a produção de provas digitais. Há apenas previsão, como medida cautelar pessoal, de bloqueio de endereço eletrônico na internet (art. 533, XV). Ao se detalhar tal medida, relacionada aos crimes praticados por meio da internet, é prevista a preservação de provas, por meio da gravação, em meio magnético, das informações, dados e conteúdos do endereço eletrônico desabilitado (art. 605, §2º). Não se encontram, porém, as regras de procedimento para tanto.

De outro lado, cuidando de novo meio de investigação, encontra-se em trâmite o Projeto de Lei nº 1.404/2011, que introduz os artigos 190-A, 190-B, 190-C, 190-D e 190-E no Estatuto da Criança e do Adolescente (Lei 8.069/90), prevendo a infiltração de agentes de polícia na internet, para investigação de crimes contra a liberdade sexual de criança ou adolescente. Contudo, tal projeto também é omissivo quanto ao tratamento da prova digital.

⁹ HC 33.682/PR, Ministro Og Fernandes, Sexta Turma, DJe 04/05/2009.

Desse modo, permanecem sem tratamento inúmeras questões relevantes concernentes às provas digitais. Para que se possa ter dimensão dessas questões, faz-se oportuno verificar as alterações promovidas pelo desenvolvimento tecnológico, assim como a sua inserção na disciplina processual penal.

1.2 Desenvolvimento tecnológico e sociedade da informação

Ao longo da História, o homem vem constantemente se desenvolvendo, modificando o meio em que habita e alterando as relações sociais. Da sociedade primitiva, ele passou à civilização, aprimorando-se no aproveitamento dos recursos naturais e no domínio das adversidades da natureza. Desde a Antiguidade, o homem desenvolve ferramentas e métodos para auxiliarem a realização de suas tarefas, bem como a comunicação, os cálculos e a sistematização de informações.¹⁰

Do mesmo modo, progressivamente, o homem cria e aperfeiçoa meios para seu conforto, entretenimento e comunicação.

Inicialmente, na Antiguidade e Idade Média, predominavam equipamentos mecânicos e de uso manual. A Idade Moderna foi marcada pelas Revoluções Industriais, no século XVIII, em que foram desenvolvidas grandes máquinas mecanizadas, assim como evoluíram as técnicas de uso da energia, especialmente da eletricidade.¹¹

No século XX, o desenvolvimento tecnológico alcançou nível impressionante, com a criação e interligação dos computadores, diminuindo tempo e distância e rompendo fronteiras.

A Segunda Guerra Mundial ensejou grandes avanços na área da ciência, permitindo, nesse contexto, a criação dos computadores, que se deu por volta de 1940. Eles funcionavam, inicialmente, com válvulas a vácuo e atendiam a propósitos militares.¹²

¹⁰ Augusto Rossini. *Informática, Telemática e Direito Penal*. São Paulo: Memória Jurídica, 2004, p. 23.

¹¹ A respeito da evolução da sociedade agrícola até a sociedade pós-industrial, vejam-se os artigos: Roberto Senise Lisboa. Direito na Sociedade da Informação. *Revista dos Tribunais*, vol. 847, p. 78, Mai / 2006; Paulo Hamilton Siqueira Junior. Direito Informacional: Direito Da Sociedade Da Informação. *Revista dos Tribunais*, vol. 859, p. 743, Mai / 2007.

¹² Rossini, *Informática...*, p. 24.

Entre as décadas de 50 e 60, os computadores passaram a contar com maior velocidade, devido à substituição das válvulas por transistores. Nessa época, eles também começaram a ser usados para fins comerciais.¹³

Nas décadas de 70 e 80, a utilização de circuitos integrados e de microprocessadores permitiu a diminuição do tamanho dos computadores e o aumento de sua velocidade e capacidade de armazenamento, ampliando o uso comercial.¹⁴

A partir da década de 80, os computadores tiveram grande evolução, apresentando cada vez maior capacidade e variadas funções. Houve, então, a difusão desses equipamentos para uso pessoal, situação que se estabeleceu em todos os âmbitos da sociedade. O computador passou a se fazer presente nas várias dimensões da vida humana – familiar, profissional, comercial, educacional, de entretenimento, etc.¹⁵

Diversos outros dispositivos eletrônicos foram criados e desenvolvidos, ingressando na rotina humana o uso de celulares, *palm tops*, seguidos de *smartphones*, dispositivos de memória, tocadores de música e vídeos (aparelhos de mp3), minicomputadores, *tablets*, *e-readers*, câmeras digitais, gravadores digitais, GPS, jogos eletrônicos etc.

Tal hábito conduziu à criação, armazenamento e sistematização de toda espécie de informações em formato digital.

Paralelamente, houve o desenvolvimento da telefonia celular e da internet, interligando os dispositivos eletrônicos de forma abrangente e difusa, de modo que as informações passaram a ser transmitidas com maior rapidez e eficiência.

Assim como o computador, a internet também surgiu com propósitos militares, sendo resultado de um programa denominado ARPANET, da *Advanced Research Project Agency* do Departamento de Defesa norte-americano, tendo sido criada em 1968. Anos depois, a rede passou a ter finalidades acadêmicas, vedado o uso comercial. Posteriormente, houve a expansão da rede e liberação de seu uso para outros fins que não

¹³ Rossini, *Informática...*, p. 24.

¹⁴ Rossini, *Informática...*, p. 24-25.

¹⁵ Discorrendo sobre a presença da informática nos diversos âmbitos socioeconômicos, Gustavo Eduardo Aboso e María Florencia Zapata afirmam que se trata da “segunda Revolução Industrial”, mais transformadora do que a do século XIX. *Cybercriminalidad y Derecho Penal*. Buenos Aires: Editorial B de f, 2006, p. 4.

apenas militares e acadêmicos, notando-se um grande avanço na década de 1990, com os grandes provedores de internet e a criação de inúmeros *sites*.¹⁶

Atualmente, encontram-se muitos serviços disponíveis na internet, inclusive no setor público. Destacadamente, a rede e a telefonia celular exercem importante papel nas comunicações, colocando à disposição dos usuários serviços de mensagens (SMS), *e-mails*, sistemas de mensagens instantâneas, sistemas de voz sobre IP (VoIP), redes sociais (*facebook*, *twitter*, etc.), salas de bate-papo (*chats*) e fóruns de discussão, blogs, etc.

Houve, assim, a substituição, em grande medida, de meios tradicionais de expressão por novos meios tecnológicos. Apenas como ilustração, pode-se citar que: os documentos anteriormente redigidos e arquivados em papel tornaram-se eletrônicos; as músicas foram transferidas do disco de vinil e da fita cassete para o formato digital; as fotografias deixaram de ser registradas em filme para também assumirem o formato digital; do mesmo modo, a captação de imagens em vídeos; e ainda a comunicação por cartas, bilhetes, telegrama, telefone, foi transmutada em mensagens eletrônicas de texto, *e-mails*, sistemas VoIP, dentre outros.

Tais transformações caracterizam uma revolução tecnológica, a “revolução informacional”, comparável, por seus efeitos, à Revolução Industrial. Ela deu ensejo à denominada “sociedade da informação” ou “sociedade pós-industrial”, formada na segunda metade do século XX. Conforme Paulo Hamilton Siqueira Junior, “o termo sociedade da informação surgiu pela voz do então Presidente da Comissão Européia, Jacques Delors, por ocasião do Conselho Europeu (1993), ao lançar pela primeira vez a idéia das infra-estruturas da informação”.¹⁷

Nas palavras de Roberto Senise Lisboa:

“‘Sociedade da informação’, também denominada de ‘sociedade do conhecimento’, é expressão utilizada para identificar o período histórico a partir da preponderância da informação sobre os meios de produção e a distribuição dos bens na sociedade que se estabeleceu a partir da vulgarização das

¹⁶ Para um relato minucioso do desenvolvimento da Internet, consultar: Rossini, *Informática...*, p. 25-28; Marcel Leonardi. *Responsabilidade civil dos provedores de serviços de Internet*. São Paulo: Juarez de Oliveira, 2005, p. 2-4; Roberto Chacon de Albuquerque. *A criminalidade informática*. São Paulo: Juarez de Oliveira, 2006, p. 15-16; Paulo Roberto de Lima Carvalho. *Prova cibernética no Processo*. Curitiba: Juruá, 2009, 19-23.

¹⁷ Direito informacional..., p. 743.

programações de dados utiliza (sic) dos meios de comunicação existentes e dos dados obtidos sobre uma pessoa e/ou objeto, para a realização de atos e negócios jurídicos.”¹⁸

Manuel Castells, por sua vez, confere tratamento mais específico aos termos, distinguindo sociedade da informação e sociedade informacional, ponderando que a informação, como comunicação de conhecimentos, foi crucial a todas as sociedades. Nesse passo, destaca:¹⁹

“(...) o termo informacional indica o atributo de uma forma específica de organização social em que a geração, o processamento e a transmissão da informação tornam-se as fontes fundamentais de produtividade e poder devido às novas condições tecnológicas surgidas nesse período histórico. Minha terminologia tenta estabelecer um paralelo entre indústria e industrial. Uma sociedade industrial (conceito comum na tradição sociológica) não é apenas uma sociedade em que há indústrias, mas uma sociedade em que as formas sociais e tecnológicas de organização industrial permeiam todas as esferas da atividade, começando com as atividades predominantes localizadas no sistema econômico e na tecnologia militar e alcançando os objetos e hábitos da vida cotidiana. Meu emprego dos termos sociedade informacional e economia informacional tenta uma caracterização mais precisa das transformações atuais, além da sensata observação de que a informação e os conhecimentos são importantes para nossas sociedades.”

A sociedade da informação é baseada na valorização da informação, que é acessada e compartilhada de forma rápida e ilimitada pelas pessoas. Ela apresenta como características centrais a globalização e a transnacionalidade, o relacionamento social, comercial e político por meios eletrônicos, o valor econômico atribuído à informação e a impregnação do conhecimento em tudo que é produzido.²⁰

¹⁸ Direito na Sociedade da Informação, p. 78.

¹⁹ Manuel Castells. *A Sociedade em Rede*. São Paulo: Paz e Terra, 2000, p. 46.

²⁰ Para uma análise das características e efeitos da revolução informacional e da sociedade da informação, veja-se Lisboa, *Direito na Sociedade da Informação*, p. 78.

Nesse contexto, diante da massiva utilização de dispositivos digitais nas atividades cotidianas e da importância da informação, em muitas ocasiões, os fatos concernentes ao Processo Penal passaram a ocorrer no mundo virtual ou a serem registrados em formato digital. Desse modo, insere-se na sociedade da informação o tema das provas digitais, conferindo grande interesse ao seu tratamento no Direito Processual Penal.

1.3 Noções fundamentais sobre dispositivos eletrônicos e sistemas informáticos

Para se compreender o contexto em que se inserem as provas digitais, faz-se necessário examinar, em linhas gerais, os conceitos e vocabulário relacionados ao fenômeno informático.

Informática e computadores

De início, deve-se apontar que a **informática** corresponde ao tratamento automático da informação, o que se realiza por meio dos computadores.²¹

Tais equipamentos têm origem em ferramentas construídas para auxiliar no cálculo, como o ábaco, a régua de cálculo e as máquinas de calcular desenvolvidas no século XIX. Com efeito, o termo **computador** tem origem no latim *computare*, que significa “contar”, “calcular”.²²

Na definição do dicionário Houaiss, computador significa “máquina destinada ao processamento de dados; dispositivo capaz de obedecer a instruções que visam produzir certas transformações nos dados, com o objetivo de alcançar um fim determinado”.²³

²¹ Ricardo Daniel Fedeli, Enrico Giulio Franco Polloni e Fernando Eduardo Peres. *Introdução à ciência da computação*, 2ª ed. São Paulo: Cengage Learning, 2010, p. 13; Patrícia Peck Pinheiro. *Direito Digital*. 4ª ed. São Paulo: Saraiva: 2010, p. 55.

²² Deonísio da Silva. *A vida íntima das palavras: origens e curiosidades da língua portuguesa*. São Paulo: Arx, 2002, p. 115.

²³ Versão eletrônica - <http://houaiss.uol.com.br/busca.jhtm?verbete=COMPUTADOR&stype=k>. Acesso em 28.12.2011.

De acordo com Patrícia Peck Pinheiro, “o computador é uma máquina composta de elementos físicos do tipo eletrônico, capaz de realizar grande variedade de trabalhos com alta velocidade e precisão, desde que receba as instruções adequadas”.²⁴

Na definição da Seção 1030 do Título 18 do Código dos Estados Unidos (US Code), significa:

“an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical, arithmetic, or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device, but such term does not include an automated typewriter or typesetter, a portable hand held calculator, or other similar device.”²⁵

Os computadores são compostos pelo que se denomina **hardware** – componentes físicos que integram a máquina interna ou externamente – e **software** – programa processado pelo computador para executar tarefas ou instruções.²⁶

Os principais componentes do **hardware** são o **microprocessador**, denominado unidade central de processamento (CPU), e a **memória**. Enquanto a CPU representa o “cérebro” do computador, realizando as funções aritméticas, lógicas e de controle, a memória é responsável pelo armazenamento de informações a serem processadas.²⁷ A CPU executa cálculos muito simples, em grande velocidade; já a memória principal contém informações e instruções.²⁸

Também são elementos de **hardware** os **periféricos** de entrada e/ou saída, pelos quais são introduzidos dados ou comandos e são apresentados os resultados do

²⁴ *Direito Digital*, p. 55.

²⁵ Tradução livre: “Um dispositivo eletrônico, magnético, óptico, eletroquímico, ou outro dispositivo processador de dados de alta velocidade, realizando funções lógicas, aritméticas, ou de armazenamento, e inclui qualquer objeto de armazenamento de dados ou de comunicações relacionado a ou operando em conjunto com tal dispositivo, mas não se incluindo uma máquina de datilografia automática ou compositor automático, uma máquina de calcular portátil, ou outro dispositivo similar.”

²⁶ Fedeli et al. *Introdução...*, p. 5 e 9.

²⁷ Ian Walden. *Computer crimes and digital investigations*. Oxford: Oxford University Press, 2007, p. 462-464.

²⁸ Fedeli et al. *Introdução...*, p. 18.

processamento. Como exemplos, encontram-se teclado, câmera de vídeo, impressora, monitor, *pen drive*, disquete.²⁹

Além dos computadores, **outros dispositivos eletrônicos**, capazes de processar a informação, têm sido desenvolvidos, tais como *smartphones*, *e-readers*, *tablets*, etc. Cuida-se de suportes eletrônicos que desempenham tarefas diversas, de modo similar ao computador.

Vale notar que a informação pode ser armazenada em diversos dispositivos, com características próprias. Assim, na memória interna do computador, encontram-se a **memória RAM** (*Random Access Memory*) e a **memória ROM** (*Read-only Memory*). A primeira permite ao processador tanto a leitura quanto a gravação de dados e se caracteriza por ser volátil, perdendo a informação ao se desligar o equipamento. Por seu turno, a memória ROM permite apenas a leitura dos dados, pois a informação gravada não pode ser apagada ou alterada, tampouco se se perde na ausência de energia.³⁰

Uma parte da memória RAM, dita **cache**, corresponde a uma unidade de armazenamento temporário de dados que são utilizados com frequência. Nesse sentido, por exemplo, páginas de internet acessadas são armazenadas nessa memória e resgatadas quando novamente acessadas, sem a necessidade de novo carregamento.³¹

As informações também podem ser guardadas em **dispositivos externos**, como CDs, DVDs, disquetes, *pen drives*, HDs externos, *smartcards*, que podem apresentar as características de se destinarem apenas à leitura ou de permitirem a alteração e deleção.

Os computadores podem estar ligados em rede, compartilhando recursos. Para tanto, são utilizados **servidores**, ou seja, “computadores que fornecem serviços e informações em uma rede”, administrando os recursos da rede. Entre outras funções, os servidores podem armazenar arquivos dos usuários da rede, armazenar e promover envio e recebimento de mensagens eletrônicas e armazenar páginas de *sites*.³²

²⁹ Fedeli et al. *Introdução...*, p. 5-9.

³⁰ Fedeli et al. *Introdução...*, p. 7; Walden. *Computer crimes...*, p. 462-465.

³¹ Walden. *Computer crimes...*, p. 462.

³² Helena Regina Lobo da Costa e Marcel Leonardi. Busca e apreensão e acesso remoto a dados em servidores. *Revista Brasileira de Ciências Criminais*, vol. 88, p. 203, Jan/2011. Os autores referem que servidor é um gênero com diversas espécies, das quais destacam:

“a) servidor de arquivos: armazena arquivos de diversos usuários;

b) servidor web: responsável pelo armazenamento de páginas de um determinado site, requisitadas pelos clientes através de programas navegadores (browsers);

c) servidor de e-mail: responsável pelo armazenamento, envio e recebimento de mensagens de correio eletrônico;

d) servidor de impressão: responsável por controlar pedidos de impressão de arquivos dos diversos clientes;

As informações podem ainda ser armazenadas na rede mundial de computadores, o que se diz “**computação em nuvem**”. Nessa hipótese, são utilizadas a memória e a capacidade de armazenamento e cálculo de computadores e servidores compartilhados e interligados por meio da internet. Diversos programas disponíveis na rede oferecem a possibilidade de hospedar os dados informáticos do usuário, que pode acessá-los de qualquer lugar.³³

Dados e seu processamento

Os computadores e diversos dispositivos eletrônicos trabalham a informação com base no **sistema binário**, cujas bases em muito se devem aos estudos de George Boole que ensejaram a teoria da “álgebra booleana”.³⁴ Nesse sistema, todos os símbolos ou algarismos são representados pelos algarismos 0 e 1. Essa representação é referida como **digital**³⁵, posto que baseada em números, dígitos.³⁶

Por se tratar de dois números, os dois símbolos fundamentais são “designados como *dígitos binários*, mais vulgarmente conhecidos como *bit*, que representa a contração da palavra inglesa binary digit”. O *bit* corresponde à “menor quantidade de informação que pode ser armazenada na memória de um computador”.³⁷

-
- e) servidor de banco de dados: possui e manipula informações contidas em um banco de dados;
 - f) servidor de fax: transmite e recebe fax pela Internet, disponibilizando também a capacidade de enviar, receber e distribuir fax em todas as estações da rede;
 - g) servidor DNS: responsável pela conversão de endereços de sites em endereços IP, e vice-versa;
 - h) servidor proxy: armazena temporariamente páginas da internet recém-visitadas, aumentando a velocidade de exibição dessas páginas ao chamá-las novamente;
 - i) servidor de imagens: servidor especializado em armazenar imagens digitais;
 - j) servidor FTP: permite acesso de outros usuários a um disco rígido ou servidor, armazenando arquivos que podem ser acessados pela Internet;
 - k) servidor webmail: servidor para criar e gerenciar contas de e-mail na world wide web;
 - l) servidor de virtualização: permite a criação de máquinas virtuais (isoladas no mesmo equipamento), mediante compartilhamento de hardware.”

³³ Cf. <http://blogs.estadao.com.br/link/os-desafios-da-nuvem/>. Acesso em 15.01.2011.

³⁴ Pinheiro. *Direito Digital*, p. 56.

³⁵ Na definição do dicionário Houaiss, digital é “relativo a dígito (algarismo)” e ainda, em sentido informático, “que trabalha exclusivamente com valores binários (diz-se de dispositivo)”. Dicionário Houaiss da Língua Portuguesa. Disponível em: <http://houaiss.uol.com.br/busca.jhtm?verbete=digital&stype=k>. Acesso em 15.01.2011.

³⁶ Elisa Lorenzetto. Le attività urgenti di investigazione informatica e telematica. In: LUPÁRIA, Luca (Org.). *Sistema penale e criminalità informatica. Profili sostanziali e processuali nella legge attuativa della Convenzione di Budapest sul cybercrime*. Milão: Giuffrè, 2009, p. 140.

³⁷ Fedeli et al. *Introdução...*, p. 42.

Os algarismos 0 e 1, denominados *bit* zero e *bit* um, significam dois estados: desligado e ligado³⁸. Vale dizer que “o *bit* é uma representação de impulsos elétricos; se o impulso estiver presente, o computador registra 1 (ligado); se estiver ausente, registra 0 (desligado)”³⁹.

São eles símbolos opostos e mutuamente exclusivos, de modo que “em determinada posição de memória poderá existir uma e somente uma informação (*bit* zero ou *bit* um)”⁴⁰.

Os *bits* são agrupados em conjunto de oito, dando origem a uma unidade de informação chamada *byte*. O *byte* é utilizado como padrão, pois permite 256 combinações diferentes, com as quais se podem representar, na linguagem humana, todas as letras do alfabeto, os números e outros elementos gráficos.⁴¹

Há que se referir ainda que os **dados informáticos** são elementos de informação representados no sistema binário.⁴² Acerca deles, encontram-se os seguintes conceitos, na ciência da computação: “o elemento identificado em sua forma bruta, que não conduz à compreensão de uma situação”⁴³; “elementos básicos (caracteres, símbolos) de informação básica que são fornecidos ou produzidos por um computador”⁴⁴. Tais elementos trabalhados, analisados em conjunto, dão origem à **informação**⁴⁵.

A Convenção do Conselho da Europa sobre Cybercrime, de seu turno, define **dado computacional** (*computer data*) como qualquer representação de fatos, informações ou conceitos em uma forma adequada para o processamento em um sistema computacional, incluindo um programa adequado a fazer funcionar um tal sistema.⁴⁶ Na doutrina francesa, Samia Barrache e Antoine Olivier afirmam que se entende por registros

³⁸ Pinheiro. *Direito Digital*, p. 56; Fedeli et al. *Introdução...*, p. 5.

³⁹ Gabriel Cesar Zaccaria de Inellas. *Crimes na Internet*. 2ª ed. São Paulo: Juarez de Oliveira, 2009, p. 6.

⁴⁰ Fedeli et al. *Introdução...*, p. 42.

⁴¹ Inellas, *Crimes na Internet*, p. 6. O autor exemplifica com a letra A, que é representada por oito bits, um byte, na seguinte sequência: 01000001.

⁴² “O dado informatizado é uma informação numérica, de formato capaz de ser entendido, processado ou armazenado por um computador ou parte integrante de um sistema de computador.” André Augusto Mendes Machado e André Pires de Andrade Kehdi, Sigilo das comunicações e de dados In: SCARANCA FERNANDES, Antonio; ALMEIDA, José Raul Gavião de; MOARES, Maurício Zanoide de. *Sigilo no processo penal: eficiência e garantismo*. São Paulo: RT, 2008, p. 261.

⁴³ Fedeli et al. *Introdução...*, p. 10 e 56.

⁴⁴ Fernando de Souza Meirelles. *Informática: novas aplicações com microcomputadores*. 2ª ed. São Paulo: Makron Books, 1994, p. 15.

⁴⁵ Fedeli et al. *Introdução...*, p. 10.

⁴⁶ Tradução livre para o texto: “computer data means any representation of facts, information or concepts in a form suitable for processing in a computer system, including a program suitable to cause a computer system to perform a function.” Art. 1, b.

(ou dados) informáticos todos os dados que são armazenados em um computador, compreendendo os que resultem da conexão à internet.⁴⁷ No âmbito nacional, Adalberto Camargo Aranha define dados como “elementos informativos coletados num aparelhamento de informática, de forma a serem aptos a um imediato processamento, conhecimento ou comunicação”.⁴⁸

Costuma-se também referir a **arquivo informático**, que, na definição do dicionário Houaiss, consiste no “conjunto de dados digitalizados que pode ser gravado em um dispositivo de armazenamento e tratado como ente único”.⁴⁹

Para garantir a segurança das informações, existem programas que promovem a **criptografia** dos dados, fazendo-os ilegíveis para quem não tenha o código para descriptação.⁵⁰ As informações são embaralhadas, por meio de um algoritmo, necessitando do algoritmo inverso para serem descriptadas.⁵¹

Internet e transmissão da informação

As informações circulam de diversas maneiras pela rede mundial de computadores, conhecida como **internet**.

O Projeto de Lei nº 2.126/2011, denominado Marco Civil da Internet, assim define internet: “o sistema constituído de conjunto de protocolos lógicos, estruturado em escala mundial para uso público e irrestrito, com a finalidade de possibilitar a comunicação de dados entre terminais por meio de diferentes redes” (art. 5º, I).

Na dicção da doutrina, a internet consiste em “um conjunto de várias redes diferentes, unificadas para o intercâmbio de dados graças a um padrão comum de troca de

⁴⁷ “De manière générale, il faut entendre par ‘enregistrements informatiques’ toutes données qui sont stockées sur un ordinateur, y compris celles qui résultent de la connexion à internet. ” Tradução livre. L’administration de la preuve pénale et les nouvelles technologies de l’information et de la communication In: FROUVILLE, Olivier de (dir.). *La preuve pénale: internationalisation et nouvelles technologies*. Paris: La documentation française, 2007, p. 131.

⁴⁸ *Da prova no processo penal*. 7ª ed. São Paulo: Saraiva, 2008, p. 316.

⁴⁹ Disponível na versão eletrônica <http://houaiss.uol.com.br/busca.jhtm?verbete=arquivo&stype=k>. Acesso em 04.01.2012.

⁵⁰ Walden. *Computer crimes...*, p. 462.

⁵¹ Meirelles. *Informática...*, p. 63.

dados, o TCP/IP”⁵². A ligação entre os dispositivos “é feita por meio de linhas telefônicas, fibra óptica, satélite, ondas de rádio ou infravermelho”⁵³.

TCP e IP são protocolos que permitem a comunicação entre os sistemas informáticos.⁵⁴ O TCP (protocolo de controle de transmissão) efetua a divisão dos dados a serem transmitidos em pacotes, enquanto o IP (protocolo de internet) inclui neles informações sobre o remetente, o destinatário, o número total de pacotes e o número daquele pacote de dados. A transmissão dos dados é feita pelo envio de cada pacote de dados “a seu destino pela melhor rota possível, a qual pode ou não ter sido utilizada pelos demais”.⁵⁵

Importa observar a existência de **números (ou endereços) de IP**, ou seja, identificadores numéricos, formados por um código de 32 *bits* que permitem individuar os dispositivos ligados através do padrão do protocolo IP a uma rede telemática.⁵⁶ “Toda vez que um usuário se conecta à rede, seu computador recebe automaticamente de seu provedor de acesso um determinado número de IP que é único durante aquela conexão”.⁵⁷ Na transmissão dos dados, esse número é utilizado como endereço, seja como remetente, seja como destinatário.

O Projeto de Lei nº 2.126/2011 (Marco Civil da Internet) refere-se a esse número como **endereço IP**, definido como “código atribuído a um terminal de uma rede para permitir sua identificação, definido segundo parâmetros internacionais” (art. 5º, IV).

O acesso à internet e às suas funcionalidades gera o registro das informações respectivas, o que é denominado de **registro de conexão e registro de acesso a aplicações de internet** no Projeto do Marco Civil. Registro de conexão corresponde ao “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”. O registro de acesso a aplicações de internet, por sua vez, representa o “conjunto de informações referentes à data e hora de uso de uma determinada aplicação de Internet a partir de um determinado endereço IP” (art. 5º, VI e VIII).

⁵² Albuquerque. *A criminalidade informática*, p. 17.

⁵³ Pinheiro. *Direito Digital*, p. 59.

⁵⁴ Albuquerque. *A criminalidade informática*, p. 17.

⁵⁵ Leonardi. *Responsabilidade...*, p. 7. Veja-se também Inellas. *Crimes na Internet*, p. 7-8; Pinheiro. *Direito Digital*, p. 59.

⁵⁶ Giuseppe Vaciago. Internet e crimini informatici In: PICCINNI, Mario Leone; VACIAGO, Giuseppe. *Computer crimes: casi pratici e metodologie investigative dei reati informatici*. Bergamo: Moretti & Vitali, 2008, p. 29.

⁵⁷ Leonardi. *Responsabilidade...*, p. 7-8.

Costuma-se indicar a existência de diversos serviços ou diversas formas de transmissão e obtenção de informações pela internet, citando-se a *world wide web*, o correio eletrônico (*e-mail*), listas de discussão, sistemas *peer-to-peer*, programas de mensagem instantânea, salas de bate-papo (*Internet Relay Chat*), dentre outros.⁵⁸

A *world wide web* (www) consiste em um sistema de informações organizado, que engloba os outros serviços da Internet e permite o acesso a uma grande quantidade de dados armazenados em computadores ao redor do mundo. A *web* é formada pelo conjunto de *sites* públicos existentes na internet. Por sua vez, os *sites* correspondem a conjuntos de páginas da internet. Por meio do **navegador** (*browser*), um tipo de programa, o usuário acessa as páginas de internet, visualizando textos, sons, imagens.⁵⁹

Cada *site* possui um **endereço eletrônico**, pelo qual pode ser acessado. A localização de *sites* também é feita por meio de mecanismos de busca, dos quais o Google pode ser apontado como um dos mais populares.

De sua parte, os *e-mails* constituem forma de correspondência eletrônica. Dispondo de um endereço eletrônico de remessa e um de destino, um usuário pode enviar a outro uma mensagem, semelhante a uma carta ou bilhete, com textos, imagens ou sons, podendo ainda anexar arquivos.⁶⁰ Os *e-mails* contêm, além da mensagem encaminhada, os dados relativos à remessa, tais como hora e data do envio, bem como remetente e seu endereço de IP, os quais estão dispostos em seu **cabeçalho** (ou *e-mail header*).⁶¹

De modo semelhante, os usuários comunicam-se por meio de programas de **mensagens instantâneas**. Estando conectados a esses serviços, os usuários podem trocar mensagens em tempo real, enviando textos, sons, imagens, ou arquivos.

Desenvolve-se também a telefonia pela internet (ou pela intranet, rede privada). É o que se denomina de **sistema VoIP** – voz sobre IP. Essa tecnologia permite a transmissão da voz por pacotes de dados, ligando telefones e computadores, ou computadores, ou telefones entre si, desde que apropriados e conectados ao sistema.

Outra forma de transmissão de dados ocorre por meio do sistema *peer-to-peer*, em que os usuários conectados por meio de programas específicos podem acessar

⁵⁸ A propósito, Albuquerque. *A criminalidade informática*, p. 17-18; Leonardi. *Responsabilidade...*, p. 10; Carvalho. *Prova cibernética...*, p. 26-34; Fedeli et al. *Introdução...*, p. 212-215.

⁵⁹ Pinheiro. *Direito Digital*, p. 59; Leonardi. *Responsabilidade...*, p. 10; Albuquerque. *A criminalidade informática*, p. 18.

⁶⁰ Albuquerque. *A criminalidade informática*, p. 19; Leonardi. *Responsabilidade...*, p. 12-13.

⁶¹ Walden. *Computer crimes...*, p. 463.

arquivos dos demais usuários. Esse sistema caracteriza-se pela descentralização das funções, sendo que cada computador conectado ostenta o papel de servidor e de cliente, ao mesmo tempo. É muito utilizado para o compartilhamento de músicas, filmes e programas de computador.⁶²

Por fim, vale apontar que os serviços relacionados ao funcionamento da Internet, ou por meio dela, são fornecidos pelo **provedor de serviços de internet**.⁶³

1.4 Alteração do processamento e do arquivo da informação e sua influência na produção de provas

É de se registrar que as modernas tecnologias trazem alterações nas características das informações e de seu processamento, com reflexos na produção de provas.

Como apontado supra, atualmente utilizam-se com frequência dispositivos eletrônicos para processar a informação, alterá-la, armazená-la e difundi-la.

Desse modo, o indivíduo passa a contar com inúmeras ferramentas para a redação de textos, elaboração de planilhas e cálculos, organização da informação, registro de imagens e sons. Essas ferramentas são o resultado da integração entre os suportes eletrônicos físicos e os programas adequados. O produto desse processamento consiste em dados informáticos que são armazenados em dispositivos internos ou externos de memória, assim como em servidores remotos. Esses dados informáticos podem ser multiplicados, com a produção de incontáveis cópias idênticas. Assim também, podem ser enviados para inúmeros destinatários, por meio da internet.

Com a crescente capacidade de memória dos dispositivos digitais, tem-se a concentração de grande volume de informações em pequenos espaços. Há também um aumento na quantidade de dados armazenados e não descartados. Por outro lado, sua destruição mostra-se assaz simples.

⁶² Leonardi. *Responsabilidade...*, p. 16.

⁶³ Marcel Leonardi aponta que o provedor de serviços de Internet é gênero, do qual são espécies provedor de backbone, provedor de acesso, provedor de correio eletrônico, provedor de hospedagem e provedor de conteúdo. Para verificar a distinção entre essas espécies, consulte-se a obra *Responsabilidade civil dos provedores de serviços de Internet*, p. 19-31.

De outra parte, o objeto da produção humana deixa de ser material, palpável, na medida em que se apresenta como uma sequência de números, armazenada em memória eletrônica, que deve ser decodificada por um equipamento. Também por conta da imaterialidade da informação, o arquivo digital não traz ínsita correspondência com seu autor.

Nessa esteira, podem ser destacadas como principais alterações no processamento e arquivo de informações:

- a utilização de intermediários (programas) para o processamento dos dados informáticos, os quais também são necessários para a leitura e para o acesso à informação;
- aumento do volume de dados informáticos produzidos e armazenados;
- compactação da informação;
- imaterialidade do dado informático;
- volatilidade do dado informático;
- multiplicação do arquivo informático, por meio de cópias idênticas;
- facilidade de difusão da informação;
- ausência de identificação de autoria da informação.

Tais características, somadas à diversidade de dados, informações e formatos que podem ser entendidos como “provas digitais”, indicam a peculiaridade dessa prova e a necessidade de se examinar o seu impacto no processo penal.

Essa nova realidade conduz à necessidade de procedimentos próprios para a captura, armazenamento e preservação do dado eletrônico. Diversamente do papel, a apreensão do suporte físico (dispositivos eletrônicos, no caso) não indica a obtenção do dado eletrônico, nem garante sua preservação. Despontam, pois, preocupações relativas à coleta e conservação das provas, com vistas a assegurar sua autenticidade e integridade.

Em face da evolução dos dispositivos eletrônicos e diante da necessidade do programa informático para o acesso à informação, enfrentam-se novos desafios para a utilização das provas, de modo que não acabem sendo descartadas, consideradas inadmissíveis ou emprestáveis, em virtude da ausência das ferramentas adequadas.

Deve-se ainda considerar que a elevada capacidade de armazenamento das memórias e a compactação da informação refletem na obtenção de volumes inimagináveis

de informação, cujo manuseio e tratamento se torna tarefa sobre-humana. Por essa razão, procura-se identificar os métodos mais eficazes para a análise do material probatório e para a eventual descoberta da autoria delitiva.

Não menos relevante é a preocupação com a interferência na esfera dos direitos individuais, em decorrência do acesso aos arquivos digitais. Como mencionado, os dispositivos eletrônicos armazenam grande quantidade de informações, sobre as mais variadas atividades da pessoa, o que acaba por revelar aspectos reservados da vida privada. Isso se acentua com a capacidade de processamento, pesquisa e cruzamento de dados.

Surgem, portanto, situações novas, que demandam reflexão e adequado tratamento, de sorte a buscar o equilíbrio entre eficiência e garantismo no Processo Penal.

1.5 Crimes informáticos, delitos tradicionais e a prova

Ao se pensar em novas tecnologias e sua relação com as provas no Processo Penal, é possível imaginar diversas realidades de interesse. Pode-se tratar de um crime praticado na internet, como uma fraude bancária ou uma injúria propagada em rede social; de um crime praticado em dispositivo eletrônico, não necessariamente conectado à internet, como a alteração de um documento eletrônico, ensejando uma falsidade; de um crime praticado no mundo “real”, registrado em meio digital, como um *e-mail* contendo comunicação sobre a distribuição do produto do ilícito.

Do mesmo modo, quanto às provas, pode-se buscar a obtenção de informações sobre a origem de um *post* na rede social ou de um *e-mail*, acessando os dados de cadastro arquivados pelo provedor de serviços; ou pode-se utilizar o conteúdo dos arquivos eletrônicos enviados, para a prova de determinado fato.

Há, portanto, que se distinguir tais realidades, observando a classificação em delitos informáticos e delitos comuns, assim como a separação entre a prova digital e o modo de provar fatos ocorridos no mundo “virtual”.

Conforme se demonstrará, a prova digital, objeto do presente estudo, consiste em informações registradas em meio digital, armazenadas em dispositivos eletrônicos ou veiculadas por redes de computadores ou pela internet. A prova digital pode

estar relacionada com a demonstração de fatos cometidos por meio do computador, assim como de delitos tradicionais que, de algum modo, tenham sido registrados em dados digitais.⁶⁴

De outro lado, os fatos ocorridos no mundo “virtual” podem ser comprovados por diversas espécies de prova, desde a prova digital até a prova testemunhal. Assim, por exemplo, para se buscar o autor de uma ofensa, podem-se requisitar os dados do usuário de um determinado *e-mail*, os quais se encontram arquivados nos cadastros do provedor; para se demonstrar a violação ao direito de marca, pode-se fazer uma ata notarial ou uma perícia do *site* que copia o símbolo do concorrente; para se provar a divulgação de pornografia infantil, pode-se colher o testemunho de usuários do *site* criminoso⁶⁵.

Quanto aos delitos que admitem a prova digital, pode-se fazer a classificação em delitos informáticos puros, delitos informáticos impuros e delitos comuns, considerando a conduta delitiva.⁶⁶

Os delitos informáticos puros seriam as novas condutas delitivas, aquelas que só existem com o uso do computador. É o caso de invasões de sistemas, danos a equipamentos informáticos, difusão de vírus, etc. Cuida-se de infrações cujo bem jurídico tutelado, normalmente, é o sistema informático.

A seu turno, os delitos informáticos impuros seriam aqueles cometidos por meio do computador, mas que poderiam ser praticados por outra forma. Cita-se, como exemplo, a divulgação de fato difamatório por correio eletrônico.

A prova digital ainda guarda relação com os delitos comuns, que sejam demonstrados por informações digitais, incluindo as mais diversas situações. A título de exemplo, imagine-se, a troca de informações, por meios eletrônicos, para o comércio de

⁶⁴ Fabio Cassibba. L'ampliamento delle attribuzioni del pubblico ministero distrettuale. In: LUPÁRIA, Luca (Org.). *Sistema penale e criminalità informatica. Profili sostanziali e processuali nella legge attuativa della Convenzione di Budapest sul cybercrime*. Milão: Giuffrè, 2009, p. 124. Luca Luparia refere a progressiva expansão da “investigação informática”, também nos crimes em que o computador não se mostra destinatário da ofensa nem elemento do tipo penal, nem meio pelo qual o delito é perpetrado. Completa o autor: “L'evidenza digitale può infatti essere determinante oramai in ogni inchiesta criminale, dalle indagini per terrorismo (...), a quelle per reati associativi o dei colletti bianchi, così come può diventare elemento chiave addirittura nei casi di omicidio (...).” La disciplina..., p. 132.

⁶⁵ Crime previsto no artigo 241-A do Estatuto da Criança e do Adolescente (Lei 8.069/90), conforme alteração promovida pela Lei 11.829/2008.

⁶⁶ Gianluca Braghò, L'ispezione e La perquisizione di dati, informazioni e programmi informatici. In: LUPÁRIA, Luca (Org.). *Sistema penale e criminalità informatica. Profili sostanziali e processuali nella legge attuativa della Convenzione di Budapest sul cybercrime*. Milão: Giuffrè, 2009, p. 185. A distinção também é apontada por Antonio Scarance Fernandes. Crimes praticados pelo computador: dificuldade de apuração dos fatos. *Boletim do Instituto Manoel Pedro Pimentel*, São Paulo, ano 2, n. 10, p. 25-37, dez. 1999, p. 28.

drogas ilícitas; o vazamento de informações, em *e-mail*, que proporcionam a prática de *insider trading*; as imagens de circuito interno que registram um homicídio, entre outras.

Encontram-se também classificações dos delitos tendo como critério o bem jurídico tutelado e o objeto do delito. Nesse passo, Augusto Rossini classifica os delitos em informáticos puros – “aqueles em que o sujeito visa especificamente ao sistema de informática em todas as suas formas” – e em informáticos mistos – “em que o computador é mera ferramenta para a ofensa a outros bens jurídicos que não exclusivamente os do sistema informático”.

Este autor cita ainda a classificação de Túlio Lima Vianna, que aponta quatro categorias: ⁶⁷

- delitos informáticos impróprios – “aqueles nos quais o computador é usado como instrumento para a execução do crime, mas não há ofensa ao bem jurídico inviolabilidade da informação automatizada (dados)”;

- delitos informáticos próprios – “aqueles em que o bem jurídico protegido pela norma penal é a inviolabilidade das informações automatizadas (dados)”;

- delitos informáticos mistos – “crimes complexos em que, além da proteção da inviolabilidade dos dados, a norma visa a tutelar bem jurídico de natureza diversa”;

- delitos informáticos mediatos ou indiretos – “delito-fim não informático que herdou esta característica do delito-meio informático realizado para possibilitar a sua consumação”.

O presente estudo tem como escopo apenas o exame das provas digitais, que se prestam à comprovação de delitos informáticos puros e impuros, assim como de infrações comuns, não sendo parte da análise realizada outras espécies de provas de fatos “virtuais”.

1.6 Objeto do estudo e inserção na linha de pesquisa

⁶⁷ *Informática...*, p. 121.

Como visto, os novos formatos em que se mostram as provas implicam mudanças no procedimento probatório. Este deve ser ajustado para recepcionar tais provas, equacionando os problemas da autenticidade e conservação das informações, assim como para minimizar a dificuldade de descoberta da autoria de delitos informáticos.

Fazem-se necessárias normas que orientem a obtenção e produção das provas, com base em métodos e procedimentos confiáveis, que não inutilizem os elementos colhidos. Trata-se de buscar a eficiência do processo penal, com vistas à utilidade da atividade estatal.

Por outro lado, constata-se que muitas vezes os dados buscados dizem respeito à esfera da intimidade ou da privacidade do indivíduo, motivo pelo qual é de ser analisada a possibilidade de realização da prova, em face dos direitos constitucionalmente assegurados.

Assim também, o modo de realização da prova pode trazer uma restrição a direito ou garantia fundamental, como na hipótese de busca e apreensão de equipamentos eletrônicos, com a necessidade de ingresso em domicílio e a constrição de direito patrimonial.

Por isso, importa também a análise dessas provas sob o aspecto da proteção do devido processo legal e dos direitos fundamentais.

Com efeito, a preocupação com o resultado do procedimento probatório e com a proteção dos direitos fundamentais insere-se na linha de pesquisa liderada pelo Professor orientador Antonio Scarance Fernandes, relacionada ao equilíbrio entre eficiência e garantismo, cujos estudos iniciaram com a tese *Teoria geral do procedimento e o procedimento no processo penal*⁶⁸.

Trata-se de buscar a estruturação do Processo Penal, de modo a permitir que o processo alcance suas finalidades, com a aplicação da Lei Penal, sem descuidar dos direitos fundamentais, em particular do direito de defesa.

⁶⁸ Tese de titularidade, publicada com mesmo título pela Editora Revista dos Tribunais, 2005.

Nesse contexto, a eficiência é relacionada à utilidade do resultado do processo, sendo considerada como “a capacidade de um ato, de um meio de prova, de um meio de investigação, de gerar o efeito que dele se espera.”⁶⁹

Por seu turno, o garantismo é entendido como “a efetivação do devido processo legal nos prismas subjetivo e objetivo, como garantia das partes, essencialmente do acusado, e como garantias do justo processo”.⁷⁰ Trata-se, pois, de um limite moral ao efeito prático buscado na concepção do meio.⁷¹

Por meio da conjugação de eficiência e garantismo, procura-se alcançar a finalidade do processo, realizando-se as bases do Estado Democrático de Direito. Esse deve ser também o panorama buscado no que concerne às provas digitais. É à luz desses conceitos que se desenvolve o presente estudo.

⁶⁹ Antonio Scarance Fernandes. Reflexões sobre as noções de eficiência e de garantismo no processo penal. In: FERNANDES, Antonio Scarance; ALMEIDA, José Raul Gavião de; MORAES, Maurício Zanoide de (Coord.). *Sigilo no processo penal: eficiência e garantismo*. São Paulo: RT, 2008, p. 25.

⁷⁰ Idem, p. 16.

⁷¹ Os estudos sobre o garantismo, adotados neste trabalho, deitam raízes nos ensinamentos de Luigi Ferrajoli. Dentre as concepções de garantismo apresentadas pelo jurista, destaca-se aquela que contempla um modelo normativo de direito, pelo qual se tutelam as liberdades individuais, impondo limites à atuação estatal e conferindo-lhe legitimidade. *Direito e razão: teoria do garantismo penal*. 3ª ed. São Paulo: RT, 2010.

CAPÍTULO 2 – NOÇÕES SOBRE A TEORIA DA PROVA

Assim como os conceitos essenciais de informática são necessários à compreensão do tema em análise, o estudo da teoria da prova mostra-se de grande relevância para o debate acerca da caracterização e da normatização da prova digital. Nesse sentido, importa verificar a inserção da prova no processo penal.

2.1 Premissas relativas às provas e ao processo

Ao longo do tempo, verifica-se a humanização da imposição de penas, não apenas no aspecto das espécies de sanções aplicadas, mas também no que concerne à apuração dos delitos. O processo penal, cercado de garantias, assume grande relevância na proteção dos direitos individuais, preocupando-se com o modo pelo qual a verdade é buscada.

Como enfatiza Luigi Ferrajoli, “o processo, como de resto a pena, justifica-se precisamente enquanto técnica de minimizar a reação social ao delito: minimizar a violência, mas, também, o arbítrio que de outro modo seria produzido de forma ainda mais selvagem e desenfreada”⁷².

Distinguem-se, em geral, dois modelos de processo, o inquisitório e o acusatório, nos quais os papéis dos sujeitos, em especial do acusado, e as oportunidades de atuação conferidas são distintos.⁷³ Em ambos existe a finalidade de busca da verdade, mas em níveis diversos. Enquanto o processo de modelo inquisitório pode ser relacionado à busca da verdade absoluta, o processo de modelo acusatório relaciona-se com a verdade

⁷² *Direito e razão: teoria do garantismo penal*. 3ª ed. São Paulo: RT, 2010, p. 556.

⁷³ Confira-se a caracterização dos modelos dada por Ferrajoli, *Direito...*, p. 557. Para uma abordagem crítica dos traços essenciais dos sistemas inquisitório, acusatório e misto, e sua distinção em relação aos sistemas inquisitorial e adversarial, veja-se a obra *A iniciativa instrutória do juiz no processo penal*, de Marcos Alexandre Coelho Zilli. São Paulo: RT, 2003, p. 35-53.

formal.⁷⁴ Esta verdade é obtida a partir de um processo no qual há a observância de regras e garantias, valorizando-se o procedimento adotado.

Por isso, é precisa a afirmação de Luigi Ferrajoli no sentido de que “essa configuração cognitiva do processo penal e do método acusatório é uma aquisição moderna, sendo conexa – mais logicamente que historicamente – ao princípio de estrita legalidade penal e ao correlato processo de formalização e tipificação dos delitos e das penas”⁷⁵.

Nesse sistema, assume relevo a produção probatória, na medida em que a verificação da hipótese acusatória se faz com base no método da prova e da refutação, no âmbito do contraditório.⁷⁶ Como ensina o mestre italiano, “a verdade perseguida pelo método acusatório, sendo concebida como relativa ou formal, é adquirida, como qualquer pesquisa empírica, através do procedimento por prova e erro”.⁷⁷

A verificação dos fatos é pressuposto necessário da conclusão acerca da verdade e da subsequente aplicação da Lei Penal. Segundo Adalberto de Camargo Aranha, “um julgamento processa-se em dois momentos distintos e sucessivos que se completam: numa primeira fase examina-se unicamente o fato, para depois, acertado o fato, sobre ele aplicar-se uma norma de valor”.⁷⁸

A apreciação dos fatos para a conclusão acerca da verdade também é orientada diversamente nos sistemas inquisitório e acusatório. Isso porque, no sistema inquisitório, vigente na Europa nos séculos XII a XVIII, a valoração das provas seguia o sistema das provas legais, em que se encontravam muitas regras a respeito do valor das provas, exigindo-se uma certa quantidade de provas para atingir a condenação. Em verdade, esse sistema constituía uma tentativa de limitação dos poderes do juiz, com a valoração prévia das provas pelo legislador.⁷⁹

⁷⁴ Ferrajoli, *Direito...*, p. 562. A respeito dos sentidos de verdade, veja-se o artigo de nossa autoria Estudo sobre a verdade no processo penal. *Revista Brasileira de Ciências Criminais*, São Paulo, n. 83, v. 18, p. 163-183, mar/abr. 2010.

⁷⁵ *Direito...*, p. 557.

⁷⁶ Ferrajoli. *Direito...*, p. 558.

⁷⁷ Ferrajoli. *Direito...*, p. 562.

⁷⁸ *Da prova...*, p. 3.

⁷⁹ Niceto Alcalá-Zamora Y Castillo e Ricardo Levene, Hijo indicam o sistema das provas legais como um dos freios ao despotismo judicial, ao lado da possibilidade de apelação e da forma escrita do procedimento. *Derecho Procesal Penal*. Buenos Aires: Editorial Guillermo Kraft, 1945, tomo III, p. 46. Comentando sobre esse sistema enquanto limite de poder, Eugênio Pacelli de Oliveira alerta para a consequência nefasta dele advinda, correspondente à tortura, utilizada para obtenção da confissão. *Curso de Processo Penal*. 13ª ed. Rio de Janeiro: Lumen Juris, 2010, p. 352.

No sistema acusatório, nota-se a aplicação do sistema do livre convencimento, em que os juízes, não estando atrelados a regras rígidas acerca do valor das provas, valoram-nas conforme sua convicção, de maneira motivada.⁸⁰

Interessa observar que a regulamentação das provas também varia nos sistemas adversarial e inquisitorial. Essa classificação é feita sob a óptica da linha anglo-saxônica, levando em consideração a atuação judicial na marcha do processo. O sistema adversarial, normalmente relacionado à *Civil Law*, baseia-se no impulso oficial do processo, com atuação preponderante do juiz. Já o sistema inquisitorial, ligado à *Common Law*, caracteriza-se pelo “controle das partes processuais sobre a marcha processual”, diante de um julgador imparcial e passivo.⁸¹

Sendo o sistema adversarial marcado pelo julgamento popular (júri), verificam-se regras estritas e detalhadas para a admissão e avaliação das provas, vez que se trata de julgadores leigos, não familiarizados com as normas jurídicas e com a distinção do peso das provas.⁸² Já no sistema inquisitorial, no qual o julgamento é promovido por juízes togados, conhecedores do Direito, encontra-se maior flexibilidade das regras probatórias, prevalecendo a íntima convicção, com base nas provas dos autos.⁸³

No sistema brasileiro, pode-se identificar uma tendência ao modelo acusatório ou ao modelo misto, posto que se distinguem as figuras de acusador e julgador, o acusado está em posição de igualdade frente ao acusador e o julgamento ocorre publicamente, com a valoração das provas por meio do livre convencimento. Também se pode considerar que o processo brasileiro ainda se inclina para o sistema inquisitorial e não para o adversarial, mormente em razão da existência de impulso oficial, de intervenção judicial na atividade instrutória e da postura não inerte do julgador.⁸⁴

⁸⁰ Zilli. *A iniciativa...*, p. 38-40.

⁸¹ Zilli. *A iniciativa...*, p. 42-44.

⁸² Vale observar que, antes e durante o julgamento, no sistema norte-americano, os jurados são instruídos sobre suas funções, sobre o processo e sobre as provas. Nesse sentido, encontram-se manuais de instruções aos jurados, preparados pelas seções judiciárias federais americanas (“circuit courts”), os quais incluem orientações sobre a avaliação da credibilidade de testemunhas e peso da prova pericial, dentre outras. Manuais disponíveis em <http://federalevidence.com/evidence-resources/federal-jury-instructions>. Acesso em 02.01.2012.

O manual da terceira seção (“third circuit court”), com atualizações recentes, está disponível no site da Corte: <http://www.ca3.uscourts.gov/criminaljury/tocandinstructions.htm>. Acesso em 02.01.2012.

⁸³ A respeito das principais características que distinguem os sistemas inquisitorial e adversarial, confira-se o artigo *The adoption of the fundamental features of the adversarial system at the international level*, na obra *International Criminal Law*, de Antonio Cassese. Oxford: Oxford University Press, 2003, p. 365-376.

⁸⁴ Acerca do papel do julgador no processo, vale consultar a obra *A iniciativa instrutória do juiz no processo penal*, de Marcos Alexandre Coelho Zilli.

Releva notar que o artigo 155 do Código de Processo Penal, conforme redação conferida pela Lei 11.690/2008, delineou o sistema de livre convencimento, esclarecendo que não se trata da íntima convicção, baseada em quaisquer fontes de conhecimento, mas da valoração das provas produzidas em contraditório e, excepcionalmente, das informações obtidas na fase investigativa.⁸⁵

Do mesmo modo, o artigo 156 do Código agasalha a iniciativa instrutória do juiz, embora de forma complementar à atividade das partes. Nesse contexto, nota-se que a alteração legislativa deu maior ênfase à iniciativa das partes processuais, tendo em vista a adoção do exame direto e cruzado, na produção da prova testemunhal, com a formulação de perguntas diretas à testemunha. Deixou-se, porém, ao juiz a complementação da inquirição, sobre pontos não esclarecidos⁸⁶.

A iniciativa instrutória também é extraída da possibilidade de o juiz determinar a realização de prova antecipada, quando urgente e relevante ou se ameaçada de desaparecimento, consoante autorizam os artigos 156, I, e 225 do Código de Processo Penal.⁸⁷

Ademais, o sistema processual brasileiro está ancorado no conceito de devido processo legal, assegurado no artigo 5º, LIV, da Constituição da República, e que enseja a sua configuração garantista.

2.2 Direito à prova e seus limites

Conforme afirmado, o processo penal brasileiro deve atender às garantias do devido processo legal, que, na lição de Cintra, Dinamarco e Grinover, significa:

⁸⁵ Antonio Magalhães Gomes Filho. Provas – Lei 11.690, de 09.06.2008 In: MOURA, Maria Thereza Rocha de Assis (coord.). *As reformas no processo penal. As novas Leis de 2008 e os Projetos de Reforma*. São Paulo: RT, 2008, p. 248-249.

⁸⁶ Artigo 212, *caput* e parágrafo único, conforme nova redação:

“Art. 212. As perguntas serão formuladas pelas partes diretamente à testemunha, não admitindo o juiz aquelas que puderem induzir a resposta, não tiverem relação com a causa ou importarem na repetição de outra já respondida.

Parágrafo único. Sobre os pontos não esclarecidos, o juiz poderá complementar a inquirição.”

⁸⁷ De outro lado, o art. 3º da Lei 9.034/95 (Lei do Crime Organizado), que permite a realização de diligências pessoalmente pelo juiz, é duramente criticado, na medida em que excede os papéis do julgador, podendo importar em risco à imparcialidade. O tema foi abordado na Ação Direta de Inconstitucionalidade nº 1.570-2.

“o conjunto de garantias constitucionais que, de um lado, asseguram às partes o exercício de suas faculdades e poderes processuais e, do outro, são indispensáveis ao correto exercício da jurisdição. Garantias que não servem apenas aos interesses das partes, como direitos públicos subjetivos (ou poderes e faculdades processuais) destas, mas que configuram, antes de mais nada, a salvaguarda do próprio processo, objetivamente considerado, como fator legitimante do exercício da jurisdição”.⁸⁸

Com a evolução de seu conceito, o devido processo legal passou a ser considerado em duas dimensões: processual e substantiva. Em seu significado processual, o devido processo legal corresponde à ideia de um “processo estritamente legal em que se dão às partes as oportunidades amplas de alegar e provar”⁸⁹. Na acepção substantiva, o devido processo está relacionado à elaboração da lei conforme processo legislativo previamente definido, bem como à razoabilidade e ao senso de justiça de seus dispositivos.⁹⁰

Tratando particularmente do processo penal, Rogério Lauria Tucci aponta as seguintes garantias como integrantes do devido processo: acesso à Justiça Penal; juiz natural; tratamento paritário dos sujeitos parciais do processo penal; plenitude de defesa, com todos os meios e recursos a ela inerentes; publicidade dos atos processuais; motivação dos atos decisórios; fixação de prazo razoável de duração do processo penal; legalidade da execução penal.⁹¹

Tais garantias são também referidas por Luigi Paolo Comoglio, que lhes acrescenta o direito à prova.⁹²

⁸⁸ Antonio Carlos de Araújo Cintra, Ada Pellegrini Grinover e Cândido Rangel Dinamarco. *Teoria Geral do Processo*. 8ª ed. São Paulo: Malheiros, 1991, p. 78.

⁸⁹ Luis Gustavo Grandinetti Castanho de Carvalho. *O processo penal em face da Constituição*. Rio de Janeiro: Forense, 1992, p. 43.

⁹⁰ Rogério Lauria Tucci. *Direitos e garantias individuais no processo penal brasileiro*. 3ª ed. São Paulo: RT, 2009, p. 57.

⁹¹ *Direitos...*, p. 61.

⁹² I modelli di garanzia costituzionale del processo In: *Studi in onore di Vittorio Denti*. Pádua: CEDAM, 1994, volume I, p. 317.

Com efeito, em vista de sua relevância, o direito à prova é reconhecido pelos ordenamentos jurídicos, fazendo parte das garantias do devido processo legal⁹³, podendo-se vislumbrá-lo na garantia da plenitude de defesa.

Como ressalta Antonio Magalhães Gomes Filho:

“caracteriza-se, assim, um verdadeiro *direito subjetivo* à introdução do material probatório no processo, bem como de participação em todas as fases do procedimento respectivo; direito subjetivo que possui a mesma natureza constitucional e o mesmo fundamento dos direitos de *ação* e de *defesa*: o *direito de ser ouvido em juízo* não significa apenas poder apresentar ao órgão jurisdicional as próprias pretensões, mas também inclui a garantia do exercício de todos os poderes para influir positivamente sobre o convencimento do juiz”.⁹⁴

O direito à prova engloba: o direito à investigação, direito de proposição de provas, direito à admissão das provas propostas, direito de exclusão das provas inadmissíveis, impertinentes ou irrelevantes, direito de participação das partes nos atos de produção da prova e direito à valoração da prova.⁹⁵

Ada Pellegrini Grinover afirma ser essencial à validade da prova sua produção em contraditório, com a presença das partes e do juiz.⁹⁶ Na mesma direção, Giulio Ubertis destaca a importância do contraditório para o acerto fático, devendo-se garantir a possível intervenção das partes na formação do elemento cognoscitivo, implementando-se uma dialética probatória.⁹⁷

Cabe esclarecer que, embora a fonte de prova se forme fora do procedimento probatório, sua inserção no processo ocorre por um meio de prova, realizado em juízo mediante contraditório.⁹⁸

⁹³ Scarance Fernandes. *Processo penal constitucional*. 4ª ed. São Paulo: RT, 2005, p. 76.

⁹⁴ *Direito à prova no processo penal*. São Paulo: RT, 1997, p. 84.

⁹⁵ Magalhães Gomes Filho, *Direito à prova no processo penal*, São Paulo: RT, 1997, p. 85-89.

⁹⁶ *Novas tendências do direito processual (De acordo com a constituição de 1988)*. Rio de Janeiro: Forense Universitária, 1990, p. 22.

⁹⁷ La ricerca della verità giudiziale. In: UBERTIS, Giulio (Org). *La conoscenza del fatto nel processo penale*. Milano: Giuffrè, 1992, p. 12-13.

⁹⁸ Sobre as distinções entre fonte e meio de prova, ver infra.

A despeito de sua relevância, o direito à prova não é absoluto, sujeitando-se a limitações⁹⁹, que, no entender de Alcalá-Zamora Y Castillo e Levene, podem ser absolutas – quando se referem ao objeto da prova – ou relativas – quando concernentes aos meios de prova.¹⁰⁰

Com efeito, o direito à prova submete a um conjunto de regras (método probatório judiciário)¹⁰¹

“cuja função garantidora dos direitos das partes e da própria legitimação da jurisdição implica limitações ao *objeto* da prova, aos *meios* através dos quais os dados probatórios são introduzidos no processo, além de estabelecer os *procedimentos* adequados às operações relacionadas à colheita do material probatório, ou mesmo, em certas situações, o *valor* da prova obtida”.¹⁰²

Nesse contexto, as provas encontram limites com fundamentos processuais e extraprocessuais. Os limites baseados em fundamentos processuais dizem respeito ao interesse da correta apuração da verdade, sendo exemplo comum as *exclusionary rules* do Direito anglo-saxão, como a proibição da “testemunha de ouvir dizer”. As exclusões de provas por motivos extraprocessuais, por sua vez, referem-se às limitações decorrentes da proteção de outros valores e interesses, como é o caso de informações protegidas pelo sigilo.¹⁰³

Dentre as regras probatórias do processo penal brasileiro, encontram-se “a obrigatoriedade da prova pericial para constatação da materialidade da infração penal” e

⁹⁹ Segundo Novella Galantini, os limites probatórios constituem uma garantia contra abusos do livre convencimento: “I limiti probatori costituiscono una garanzia contro l’attuazione del principio del libero convincimento del giudice inteso nelle sue manifestazioni più radicali, oppure, quanto meno, possono rappresentare un deterrente alla gestione indiscriminata di tale potere giudiziale.” Inosservanza di limiti probatori e conseguenze sanzionatorie. In: UBERTIS, Giulio (Org). *La conoscenza del fatto nel processo penale*. Milano: Giuffrè, 1992, p. 169.

¹⁰⁰ *Derecho Procesal Penal*, p. 31.

¹⁰¹ No que diz respeito à disciplina da prova, cabe mencionar a distinção referida por Manuel da Costa Andrade entre proibições de prova e regras de produção da prova. Enquanto “a proibição de prova é a prescrição de um limite à descoberta da verdade”, “as regras de produção da prova visam apenas disciplinar o procedimento exterior da realização da prova na diversidade dos seus meios e métodos”, ou seja, elas determinam o modo de realização da prova. Neste caso, segundo aponta o autor, citando Figueiredo Dias, não haverá uma proibição de valoração da prova, mas apenas a eventual responsabilidade do autor da violação da regra. *Sobre as proibições de prova em processo penal*. Coimbra: Coimbra Editora, 1992, p. 83-86.

¹⁰² Magalhães Gomes Filho. *Direito à prova...*, p. 92-93.

¹⁰³ Magalhães Gomes Filho. *Direito à prova...*, p. 91-99.

“as restrições à admissibilidade do compromisso de certas testemunhas”, que, segundo Gomes Filho, têm a finalidade de evitar que “o convencimento do juiz ou dos jurados possa ser conduzido a conclusões arriscadas”, bem como para se obter “uma maior exatidão do acerto judicial”.¹⁰⁴

2.3 Conceitos de prova

Como visto, a produção probatória mostra-se de enorme relevância no processo penal. Ela está relacionada à verificação da veracidade de uma afirmação, servindo à formação da convicção do juiz. Sua origem encontra-se no latim *probatio*, derivado do verbo *probare*, cuja origem é *probus*, ou seja, bom, reto, correto.¹⁰⁵

Entretanto, ao se referir à prova, diversas ideias emergem, haja vista que a mesma palavra denomina conceitos diferentes.

Como destaca a doutrina, o termo “prova” é polissêmico¹⁰⁶, sendo utilizado em variados sentidos. Antonio Magalhães Gomes Filho aponta três acepções básicas de prova: demonstração, experimentação e desafio. Como *demonstração*, provar é apresentar elementos para estabelecer a verdade sobre determinados fatos. Na acepção de *experimentação*, refere-se à atividade ou procedimento para verificar a correção de uma afirmação. Já sob a ideia de *desafio*, significa obstáculo a ser superado como condição de reconhecimento.¹⁰⁷

Assim também, o vocábulo prova é utilizado para designar diferentes aspectos do fenômeno probatório: fonte de prova, meio de prova, elemento de prova, resultado probatório e procedimento probatório.¹⁰⁸

¹⁰⁴ *Direito à prova...*, p. 97-98.

¹⁰⁵ Gustavo Henrique Righi Ivahy Badaró. *Ônus da prova no processo penal*. São Paulo: RT, 2003, p. 156; Magalhães Gomes Filho. Notas sobre a terminologia da prova (reflexos no processo penal brasileiro). In: YARSHELL, Flavio Luiz; MORAES, Mauricio Zanoide de. (Coord.). *Estudos em homenagem à Professora Ada Pellegrini Grinover*. São Paulo: DPJ Editora, 2005, p. 305.

¹⁰⁶ Magalhães Gomes Filho. Notas..., p. 304; Badaró. *Ônus...*, p. 158; Guilherme Madeira Dezem, *Da prova penal: tipo processual, provas típicas e atípicas (atualizado de acordo com as Leis 11.689/08, 11.690/08 e 11.719/08*. Campinas: Millenium Editora, 2008, p. 80-81.

¹⁰⁷ Notas..., p. 305.

¹⁰⁸ Marina Gascón Abellán. *Los hechos en el derecho – Bases argumentales de la prueba*. Madrid/Barcelona: Marcial Pons, 1999, p. 84-86.

As **fontes de prova**¹⁰⁹ são os objetos ou seres dos quais se podem obter elementos de prova para a verificação da alegação de um fato.¹¹⁰ São elas anteriores ao processo e exteriores a ele, vez que “decorrem do fato em si, independentemente da existência do processo”.¹¹¹

As fontes de prova são, usualmente, classificadas em fontes pessoais e fontes reais. Erich Döhring agrupa as testemunhas, peritos e partes processuais em “prova pessoal”, agrupando sob a denominação de “prova real” todas as demais fontes. Para jurista alemão, o que caracteriza a fonte pessoal é que, entre o averiguador e o estado dos fatos, há a intermediação de um ser humano, portador de notícias, ao contrário da fonte real, em que o julgador recebe os elementos probatórios sem essa intermediação. Ressalta o professor que, como consequência, a prática da prova se cumpre de maneira fundamentalmente diversa nas provas reais e nas provas pessoais:

“La persona declarante, a la cual enfrenta el receptor de la declaración, puede ser impelida, mediante preguntas aclaratorias y admoniciones, a aclarar y, en su caso, a rectificar lo dicho, posibilidad que no existe en las probanzas reales. Pero la apreciación de la prueba personal tiene características especiales. Aquí hay que contar con declaraciones falsas, dolosas o no dolosas, que el receptor de la declaración debe descubrir y rectificar con ayuda de los síntomas de fidedignidad. En la prueba real, no cabe contar con esas fallas; pero sí con otros errores que deben ser detectados y subsanados con métodos especiales adecuados.”¹¹²

¹⁰⁹ Francesco Carnelutti refere-se às fontes de prova como “fatos percebidos pelo juiz, que lhe servem para a dedução do fato a ser provado”. Embora inicialmente a definição pareça indicar somente o conceito de prova indireta, infere-se que o ilustre processualista trata, indiretamente, dos objetos ou seres, a partir dos quais o julgador possa obter informações sobre o fato a ser provado. A propósito, observe-se a ilustração por ele fornecida, considerando que o fato a ser provado seria uma facada: “Ele poderá, portanto, deduzir sua existência por meio de uma fotografia, casualmente tirada por um espectador, ou, ao invés, pela narração dos próprios contendores ou de quem os viu no ato: aqui o fato que o juiz percebe, isto é, a fotografia ou a narração das partes ou das testemunhas, não têm, relativamente ao fato a ser provado, uma existência autônoma; é, se pode dizer, a respeito deste um fato *secundário*, porque a fotografia ou a narração não são cumpridas, porém, senão para representar, com sinais e com palavras, o fato fotografado ou narrado.” O autor utiliza tal conceito em comparação com *fontes de presunção*, que seriam fatos não constituídos para a representação do fato a ser provado. *A prova civil: parte geral: o conceito jurídico da prova*. São Paulo: Liv. e Ed. Universitária de Direito, 2002, p. 117-119.

¹¹⁰ Magalhães Gomes Filho. Notas..., p. 308.

¹¹¹ Badaró. *Ônus...*, p. 164-166.

¹¹² Tradução livre. Erich Döhring. *La prueba: su practica y apreciacion*. Ediciones Juridicas Europa-America: Buenos Aires, 1972, p. 20-21.

Alcalá-Zamora Y Castillo e Levene consideram que os seres humanos constituem prova pessoal e funcionam como meio de prova (quando em atitude ativa) ou como objeto de inspeção (em atitude passiva, como quando vítima de lesões).¹¹³

As fontes de prova são introduzidas no processo pelos **meios de prova**. Nesse sentido, Marina Gascón Abellán aponta para a distinção entre fonte e meio de prova, citando J. Monteiro Aroca:

“La distinción arranca de la constatación de que en el proceso se realiza una actividad de verificación, y de que para que ésta sea posible tiene que existir algo (la fuente de prueba) con lo que verificar... El medio de prueba es así esencialmente actividad, actuación procesal por la que una fuente se introduce en el proceso”.¹¹⁴

Eugenio Florian esclarece que o meio de prova representa o momento, no qual a contribuição da prova se explica em sua maior eficiência. Por isso atua-se o contato entre o objeto de prova e o juiz; por isso o objeto da prova vem recolhido à cognição do juiz e dos outros sujeitos processuais.¹¹⁵

Sentís Melendo, citado por Gustavo Badaró, define os meios de prova como “as atuações judiciais com as quais as fontes se incorporam ao processo”¹¹⁶. De modo semelhante, Cândido Rangel Dinamarco se refere aos meios de prova como “as técnicas destinadas a atuar sobre as fontes e delas efetivamente extrair o conhecimento dos fatos relevantes para a causa”.¹¹⁷ Nas palavras de Gomes Filho, são “os *instrumentos* ou *atividades* por intermédio dos quais os dados probatórios (*elementos* de prova) são introduzidos e fixados no processo (*produção* da prova).”¹¹⁸ Na definição de Alcalá-Zamora y Castillo e Levene, “são meios de prova os modos ou formas em que se

¹¹³ *Derecho procesal penal*, p. 33.

¹¹⁴ *Los hechos...*, p. 84

¹¹⁵ “Il mezzo di prova rappresenta il momento, in cui il contributo della prova si esplica nella sua maggiore efficienza. Per esso si attua Il contatto fra l’oggetto di prova ed il giudice: per esso l’oggetto di prova viene recato a cognizione del giudice e degli altri soggetti processuali.” *Delle prove penali: in specie*. Milano: Francesco Vallardi, 1924, vol. II, p. 1.

¹¹⁶ Badaró. *Ônus...*, p. 166.

¹¹⁷ *Instituições de Direito Processual Civil*. São Paulo: Malheiros, 2001, vol. III, p. 47.

¹¹⁸ *Notas...*, p. 308.

exterioriza sua prática e que se utilizam para chegar ao conhecimento da verdade no processo.”¹¹⁹

Os meios de prova podem ser especificados em **meios de obtenção de prova** (ou meios de pesquisa) e **meios de produção da prova**, como fez o Código de Processo Penal italiano de 1988¹²⁰. Os primeiros são destinados à pesquisa e colheita da prova, servindo à aquisição das fontes de prova. Já os meios de produção da prova “são os instrumentos por meio dos quais as fontes de prova são levadas para o processo”¹²¹.

A distinção é ressaltada por Marcos Alexandre Coelho Zilli: ¹²²

“Nesse campo, não há como se confundir os meios de prova com os denominados meios de busca de prova. De fato, enquanto os primeiros constituem os instrumentos (documentos, depoimentos de testemunhas, exames periciais etc.) que levam ao conhecimento dos sujeitos processuais os fatos, os segundos são as próprias medidas tendentes à busca, à coleta, à obtenção, enfim, de provas (busca e apreensão, interceptação telefônica, quebras de sigilo bancário e fiscal e as inspeções judiciais) as quais serão, posteriormente, instrumentalizadas e transportadas até o processo para conhecimento e apreciação de todos.”

Nesse sentido, também leciona Antonio Magalhães Gomes Filho: ¹²³

“Os meios de prova referem-se a uma atividade *endoprocessual* que se desenvolve perante o juiz, com o conhecimento e participação das partes, visando a introdução e a fixação de dados probatórios *no processo*. Os *meios de pesquisa* ou *investigação* dizem respeito a certos procedimentos (em geral, *extraprocessuais*) regulados pela lei, com o objetivo de conseguir provas materiais, e que podem ser realizados por outros funcionários (policiais, por exemplo)”.

¹¹⁹ *Derecho procesal penal*, p. 34. Tradução livre.

¹²⁰ Magalhães Gomes Filho. Notas..., p. 309.

¹²¹ Badaró. *Ônus...*, p. 166.

¹²² *A iniciativa...*, p. 183.

¹²³ Magalhães Gomes Filho. Notas..., p. 309.

Além disso, afirma-se que, enquanto os meios de obtenção de prova normalmente são acompanhados pela surpresa e afetam direitos individuais, os meios de produção de prova pressupõem a obediência ao contraditório e à ampla defesa, com a efetiva participação das partes.¹²⁴

Paolo Tonini indica quatro aspectos que distinguem os “meios de investigação” dos “meios de prova”. Enquanto os meios de investigação permitem a aquisição de um elemento probatório pré-existente, nos meios de prova, o elemento probatório forma-se após sua realização. Além disso, os meios de prova devem ser produzidos perante o juiz na fase processual, ao passo que os meios de investigação podem ser produzidos por outras autoridades, ainda durante a fase de investigação. A terceira distinção reside no fato de que os meios de investigação baseiam-se na surpresa, ao invés dos meios de prova, que são produzidos em contraditório. Ainda, os meios de investigação são irrepetíveis e podem ser juntados ao processo, mas os meios de prova, se produzidos antes do processo, devem consistir em prova antecipada.¹²⁵

Embora seja adequada a distinção entre meios de investigação e meios de prova, não se pode concordar com a asserção de que aqueles são dotados de surpresa e realizados na fase de investigação e que os últimos são realizados na fase processual, em contraditório. Isso porque nada obsta que meios de investigação, como uma quebra de sigilo fiscal ou bancário, por exemplo, sejam realizados em contraditório. Estando as informações em poder do Estado ou de terceiros, não há prejuízo no conhecimento e manifestação prévia do interessado. Assim também, a obtenção de fontes de prova pode ocorrer durante a fase processual, sendo de se observar que a Lei 9.296/96 estabelece que a interceptação telefônica pode ser deferida para a investigação criminal ou para a instrução processual penal.

Registre-se, de igual modo, que os meios de prova, como o testemunho, podem se realizar previamente ao processo, na forma de prova antecipada, como autorizam os artigos 156, I, e 225 do Código de Processo Penal.

Ainda acerca dos sentidos de prova, na acepção de **atividade ou procedimento probatório**, a prova relaciona-se à ideia de “experimentação”,

¹²⁴ Magalhães Gomes Filho. Notas..., p. 309.

¹²⁵ *A prova no processo penal italiano*. São Paulo: RT, 2002, p. 242-243.

correspondendo aos meios e atos praticados no processo visando à demonstração da veracidade de uma alegação sobre um fato.¹²⁶

Vincenzo Manzini define o termo prova como atividade: “La prova è l’attività processuale immediatmanete diretta allo scopo di ottenere la certezza giudiziale, secondo il critério della veritè reale, circa l’imputazione o altra affermazione o negazione interessante la decisione del giudice.”¹²⁷

De sua parte, os dados probatórios introduzidos no processo são os **elementos de prova**, ou seja, “dados objetivos que confirmam ou negam uma asserção a respeito de um fato que interessa à decisão da causa”.¹²⁸

A prova, como **resultado probatório**, indica a conclusão obtida pela conjunção dos diversos elementos de prova, pelo que se diz que um fato está “provado” ou não.¹²⁹

Por fim, também guarda relevância para o estudo a expressão **objeto da prova**, que, no processo penal, é referido como o *thema probandum*. Segundo a doutrina, o objeto da prova consiste nos fatos que interessam à solução da causa ou, mais propriamente, nas afirmações que se fazem sobre um fato eventualmente típico. Trata-se, em suma, de apurar a veracidade ou falsidade da afirmação a respeito de um fato.¹³⁰

2.4 Momentos do procedimento probatório e espécies de provas

O procedimento probatório é definido, por Adalberto de Camargo Aranha, como “a marcha dos atos processuais relativos à prova, na forma prevista pela lei e de

¹²⁶ Badaró. *Ônus...*, p. 158.

¹²⁷ *Istituzioni di Diritto Processuale Penale*. Torino: Fratelli Bocca, 1917, p. 161.

¹²⁸ Magalhães Gomes Filho. *Notas...*, p. 307.

¹²⁹ Magalhães Gomes Filho. *Notas...*, p. 308. Michele Taruffo registra a diversidade de significados de “prova” e a conceitua, na acepção de resultado probatório: “Prova’ è allora l’inferenza probatória, ossia il ragionamento con cui il giudice stabilisce che il fatto è provato sulla base degli elementi di prova di cui dispone”. *La prova dei fatti giuridici – Nozioni generali*. Milão: Giuffrè, 1992, p. 424.

¹³⁰ Magalhães Gomes Filho. *Notas...*, p. 316-317. O Código de Processo Penal português, em seu artigo 124, estabelece: “Constituem objecto da prova todos os factos juridicamente relevantes para a existência ou inexistência do crime, a punibilidade ou não punibilidade do arguido e a determinação da pena ou da medida de segurança aplicáveis.”

maneira coordenada e concatenada”. O autor identifica três momentos nesse andamento: a proposição, a admissão e a produção da prova.¹³¹

Já Antonio Magalhães Gomes Filho identifica quatro momentos do procedimento probatório: a proposição, a admissão, a produção e a valoração. O autor relaciona ainda os direitos compreendidos no direito à prova, a saber: direito à investigação, direito de proposição de provas, direito à admissão das provas requeridas, direito sobre o meio de prova e direito à valoração das provas existentes no processo.¹³²

A proposição de provas contempla a iniciativa tendente à introdução do material probatório no processo. O direito respectivo é previsto às partes, assim como a terceiros interessados, como o ofendido e o assistente de acusação (arts. 14 e 271, CPP). Conforme Antonio Magalhães Gomes Filho, “esse direito também inclui a eventual antecipação dos atos de obtenção da prova, nos casos em que se verificar um risco de desaparecimento das fontes de prova (*periculum in mora*).”¹³³

A proposição das provas mostra-se fundamental no sistema dito acusatório, na medida em que se espera a passividade do julgador na busca das provas, de modo a não se vincular com qualquer das teses em pauta. Tratando da distinção entre fonte e meio de prova, Gustavo Badaró sinaliza que caberia às partes processuais a disposição sobre as fontes de prova, podendo, por outro lado, o juiz determinar a realização do meio de prova adequado:

“Em síntese, as partes teriam disponibilidade sobre as fontes de prova, podendo deixar de levá-las ao conhecimento do juiz, se assim lhes aprouver. Em tal caso, sem as fontes, não há que se falar em meio de prova. Por outro lado, não caberia ao juiz averiguar ou buscar fontes de prova, sob pena de perder a sua imparcialidade e desnaturar a sua verdadeira função. Porém, tendo chegado aos autos informações sobre fontes de provas, o juiz poderá determinar, de ofício, a

¹³¹ *Da prova...*, p. 35. Tal é também a classificação de José Frederico Marques, citado por Guilherme Madeira Dezem, *Da prova...*, p. 89.

¹³² *Direito à prova...*, p. 59-89.

¹³³ *Direito à prova...*, p. 88.

realização do meio de prova que achar pertinente e adequado para que tais fontes sejam incorporadas ao processo.”¹³⁴

Não obstante, parece mais adequado reservar às partes processuais a indicação das fontes de prova existentes e a proposição do meio de prova respectivo, destinando ao magistrado a tarefa de administrar a marcha processual e o procedimento probatório, bem como de ordenar a realização dos meios de prova. A par disso, deve-se admitir a atuação do juiz na incorporação de fontes de prova ao processo somente de maneira complementar, em consonância com os limites da iniciativa instrutória.

No que respeita à admissão da prova, cuida-se da “efetiva permissão para o ingresso dos elementos pretendidos pelos interessados”¹³⁵. Em vista do amplo direito à prova, a rejeição deve restar devidamente motivada, tendo por fundamento a permissão legal ou constitucional para a exclusão da prova. Esta última se dá em decorrência da inadmissibilidade de certas provas – como expressamente apontado pela Constituição da República (art. 5º, LVI) e pelo Código de Processo Penal (art. 157) em relação às provas ilícitas – ou da impertinência e da irrelevância (arts. 400, §1º, e 411, §2º, CPP).

No caso da inadmissibilidade, tem-se um sopesamento entre o direito à prova e à busca da verdade, de um lado, e os interesses protegidos pela não realização da prova ou exclusão da prova ilicitamente produzida, de outro. Trata-se da imposição de limites, obedecendo-se ao devido processo legal.

A exclusão das provas irrelevantes e impertinentes, por seu turno, tem por objetivo a economia processual e a eficiência do processo, afastando-se o que não contribua para o esclarecimento dos fatos e aplicação da lei.

O momento da produção da prova corresponde à sua introdução no processo, pela juntada - como ocorre na prova documental -, ou pela execução da prova,

¹³⁴ *Ônus...*, p. 167-168. Deve-se, porém, observar que, considerando as funções desempenhadas pelo Ministério Público, nos termos da Constituição da República, não se pode admitir a sonegação de fontes de prova favoráveis ao acusado, já que o *Parquet* deve objetivar a busca da verdade, não a condenação.

¹³⁵ *Direito à prova...*, p. 88-89. No processo penal norte-americano, a fim de se preservar o julgamento pelo júri, atendem-se diversas regras sobre a admissão de provas. No curso das audiências, por vezes, ao ser oposta objeção por uma das partes, instala-se uma conferência reservada com o juiz togado (“bench conference”) ou determina-se um recesso, a fim de decidir sobre a admissibilidade da prova, sem contaminar a imparcialidade dos jurados. O procedimento consta das instruções aos jurados, conforme os manuais as seções judiciárias federais. Manuais disponíveis em <http://federalevideance.com/evidence-resources/federal-jury-instructions>. Acesso em 02.01.2012

sendo essencial a participação do juiz e das partes, vez que somente se considera prova aquela realizada em juízo e mediante contraditório.¹³⁶

Com efeito, ressalta Antonio Magalhães Gomes Filho a esse respeito:

“É através dessa participação [dos interessados], com impugnações, perguntas, críticas, e eventual oferecimento de *contra-prova*, que se realiza, em sua plenitude, o contraditório na instrução criminal, requisito essencial à legitimação da própria atividade jurisdicional (...).”¹³⁷

Por fim, para que a prova produzida seja útil e atenda ao objetivo de influir no convencimento judicial, a prova há de ser valorada pelo magistrado, quando da prolação da sentença. A valoração deve transparecer na motivação da decisão¹³⁸, indicando-se por que a prova corrobora a conclusão adotada ou por que, inversamente, ela deve ser desconsiderada.

Tendo em vista o sistema de livre convencimento motivado e a inexistência de provas tarifadas, mostra-se essencial a valoração da prova, com a revisão de todos os atos promovidos durante a instrução e a análise dos elementos colhidos.

Antonio Magalhães Gomes Filho aponta a existência de dois momentos na fase da valoração da prova:

“(...) o primeiro é constituído por uma apreciação isolada sobre a aptidão de cada elemento obtido para servir de fundamento ao convencimento judicial (*atendibilidade, idoneidade, credibilidade, autenticidade* da prova); o segundo é representado pelo conjunto de operações inferenciais, realizadas a partir do

¹³⁶ *Novas tendências do direito processual (De acordo com a constituição de 1988)*. Rio de Janeiro: Forense Universitária, 1990, p. 22.

¹³⁷ *Direito à prova...*, p. 89.

¹³⁸ Conforme ensina Antonio Magalhães Gomes Filho, a motivação das decisões judiciais exibe-se como garantia política e como garantia processual. Sob o aspecto político, está a limitar e legitimar o poder estatal, assegurando “a participação popular, a soberania da lei, a certeza do direito, a separação de poderes e a supremacia dos direitos individuais”. Na perspectiva processual, tem-se em vista a efetividade da cognição judicial, a independência e imparcialidade do juiz, o contraditório, a viabilização do duplo grau de jurisdição e a publicidade processual. *A motivação das decisões penais*. São Paulo: RT, 2001, p. 75-105.

material informativo reputado idôneo, com o objetivo de atingir o *resultado* da prova, que é a reconstrução dos fatos sobre os quais incidirá a decisão.”¹³⁹

A produção de provas ocorre pela realização dos diversos meios de prova, os quais propiciam que elas passem a fazer parte do conjunto probatório a ser analisado pelo juiz. Em geral, classificam-se os meios de prova em: prova documental, prova testemunhal e prova pericial. Não obstante as inovações técnicas, entende-se que todas as provas poderiam ser incluídas em uma dessas espécies de provas. É o que manifestam Alcalá-Zamora y Castillo e Levene:¹⁴⁰

“La realidad, sin embargo, es que si bien surgen a menudo nuevas técnicas y nuevos instrumentos de prueba, todos ellos pueden incluirse sin dificultad dentro de los medios probatorios tradicionalmente admitidos, sobre todo dentro de la pericia, que tiene una extraordinaria capacidad de absorción.”

Assim, todas as espécies de provas estariam abrangidas por alguma dessas categorias.

O atual Código de Processo Penal prevê os seguintes meios de prova: exame do corpo do delito e outras perícias (art. 158 e sgs), oitiva do ofendido (art. 201), inquirição de testemunhas (art. 202 e sgs), reconhecimento de pessoas ou coisas (arts. 226 a 228), acareação (arts. 229 e 230), documentos (art. 231 e sgs).

Adiante, será aprofundado o estudo da classificação dos meios de prova e de sua abrangência, assim como a possibilidade de aplicação dos meios de prova previstos no Código em relação à prova digital.

2.5 Tipicidade da prova e distinção com provas nominadas, anômalas e irrituais

¹³⁹ A motivação..., p. 154.

¹⁴⁰ *Derecho procesal penal*, p. 34-35.

Ultimamente, vem ganhando atenção o estudo da tipicidade das provas e das consequências atribuíveis às provas atípicas.

De maneira geral, a doutrina entende que vige, no Processo Penal brasileiro, a liberdade probatória, admitindo-se todos os meios de prova legítimos, ainda que não previstos na legislação.¹⁴¹

A liberdade probatória decorreria da redação do art. 155 do Código de Processo Penal, que prevê a livre apreciação da prova, impondo apenas as restrições da lei civil ao estado das pessoas. Do mesmo modo, pode-se sustentar que a aceitação de todos os meios de prova legítimos decorre da aplicação, por analogia, do art. 332 do Código de Processo Civil (cc. art. 3º do Código de Processo Penal). Referindo este dispositivo, afirma Gustavo Badaró:¹⁴²

“Embora não haja um dispositivo semelhante no Código de Processo Penal, há consenso de que também não vigora no campo penal um sistema rígido de taxatividade dos meios de prova, sendo admitida a produção de provas não disciplinadas em lei, desde que obedecidas determinadas restrições.”

Todavia, o procedimento probatório previsto na legislação representa uma garantia ao indivíduo, em virtude da previsibilidade da atividade processual, assim como traduz uma forma considerada eficaz para o resultado pretendido.¹⁴³

Tratando do papel das provas produzidas no contexto do devido processo legal para a legitimidade das decisões penais, Antonio Magalhães Gomes Filho realça a importância da disciplina jurídica da prova:¹⁴⁴

¹⁴¹ Fernando da Costa Tourinho Filho, *Processo penal*. 28ª Ed. São Paulo: Saraiva, 2006, vol. III, p. 219-220. Gustavo Henrique Righi Ivahy Badaró, *Direito Processual Penal*. Rio de Janeiro: Elsevier, 2008, vol. I, p. 200.

¹⁴² Provas atípicas e provas anômalas: inadmissibilidade da substituição da prova testemunhal pela juntada de declarações escritas de quem poderia ser testemunha. In: YARSHELL, Flavio Luiz; MORAES, Mauricio Zanoide de. (Coord.). *Estudos em homenagem à Professora Ada Pellegrini Grinover*. São Paulo: DPJ Editora, 2005, p. 344.

¹⁴³ Nesse sentido, Gustavo Henrique Righi Ivahy Badaró: “Nos casos em que a lei estabelece um determinado procedimento para a produção de uma prova, o respeito dessa disciplina legal assegura a genuinidade e a capacidade demonstrativa de tal meio de prova.” *Direito...*, vol. I, p. 200.

¹⁴⁴ *Direito à prova no processo penal*. São Paulo: RT, 1997, p. 56.

“Daí também a necessidade de que os institutos probatórios sejam informados pela *legalidade*, pois a observância desse modelo *cognitivo* deve estar assegurada por regras previamente fixadas pelo legislador, que, por isso, são *normas de garantia*, constituindo decorrência direta dos preceitos constitucionais, conferindo-lhes aplicabilidade. Como pondera Verde, uma disciplina jurídica da prova é tão inevitável como a própria disciplina jurídica do processo, para assegurar o *caráter racional* dessa atividade.”

O autor complementa, apontando que os excessos das provas legais não devem “conduzir ao vício oposto de uma liberdade absoluta, próxima ao arbítrio, em que se confunde a livre *valoração* pelo magistrado, que constitui inegavelmente uma conquista, com a ausência de vínculos legais também nos procedimentos de *admissão e produção* das provas.”¹⁴⁵

De forma similar, analisando o sistema italiano, destaca Paolo Tonini:¹⁴⁶

“o modo de produção é previsto para permitir que o juiz e as partes valorem, da melhor forma, a credibilidade da fonte e a idoneidade do elemento de prova. Os meios de prova típicos são considerados, pelo Código, idôneos a viabilizar o acerto dos fatos.”

A respeito da disciplina dos meios de prova, Hernando Devis Echandía refere a existência de dois sistemas para a fixação dos meios de prova: o da prova livre, que deixa o juiz em liberdade para admitir ou ordenar os que considere aptos para a formação de seu convencimento, e o das provas legais, que estabelece legislativamente quais são. Pode também haver um sistema misto, em que se enumeram os meios de prova que o juiz não pode desconhecer, mas se lhe outorga a faculdade de admitir ou ordenar outros que avalie úteis.¹⁴⁷

Nesse contexto, pode-se afirmar que o ordenamento italiano adota o sistema misto. O Código de Processo Penal de 1988, visando conciliar a confiabilidade dos meios

¹⁴⁵ *Direito à prova...*, p. 56-57.

¹⁴⁶ *A prova...*, p. 108.

¹⁴⁷ *Teoría general de la prueba judicial*. 5ª Ed. Buenos Aires: Victor P. de Zavalía, 1981, vol. I, p. 553.

típicos e a impossibilidade de previsão exaustiva dos meios de prova, fez uma escolha intermediária entre a liberdade e a taxatividade dos meios de prova¹⁴⁸, prevendo a admissão dos meios atípicos mediante a manifestação das partes e o preenchimento de dois requisitos: idoneidade do meio de prova para o acerto dos fatos e respeito à liberdade moral (art. 189).

Nessa esteira, com base na doutrina italiana, tem-se debatido, no âmbito nacional, a existência de parâmetros legais para o procedimento probatório. Entende-se que, a exemplo dos tipos penais, que definem as condutas incriminadas, haveria, na disciplina processual, padrões dos meios de prova definidos em lei, levando a certa restrição quanto aos meios não disciplinados. Discute-se, então, a admissibilidade e valoração dos meios de prova atípicos.

Embora não se encontre previsão legal da tipicidade processual, sustenta Guilherme Madeira Dezem sua aplicação no processo penal brasileiro, tendo como fundamento o princípio da legalidade (art. 5º, II, CR) e o devido processo legal (art. 5º, LIV, CR).¹⁴⁹

O tema relaciona-se com a teoria das nulidades, que se funda na existência de um delineamento de modelo legal para os atos processuais, conforme a doutrina de Ada Pellegrini Grinover, Antonio Magalhães Gomes Filho e Antonio Scarance Fernandes. Segundo tais professores, a atividade processual é regulada pelo ordenamento jurídico, “através de formas que devem ser obedecidas pelos que nela intervêm”, sob pena de ser sancionada pela nulidade. A finalidade das formas reside em “conferir segurança às partes e objetividade ao procedimento”¹⁵⁰.

Pode-se afirmar que assim também sucede com as provas, havendo de se observar o direcionamento legal para a produção probatória.

Apesar do desenvolvimento de teorias sobre o tema, não existe consenso em torno do conceito de prova atípica, encontrando-se variadas definições.

No Direito italiano, embora não haja menção ao termo “prova atípica”, encontra-se, como mencionado, a previsão, no art. 189 do Código de Processo Penal, do procedimento aplicável para as provas “*não disciplinadas na lei*”.

¹⁴⁸ Cf. Antonio Laronga. *Le prove atipiche nel processo penale*. Milão: CEDAM, 2002, p. 5.

¹⁴⁹ *Da prova penal...*, p. 55.

¹⁵⁰ *As nulidades no processo penal*. 11ª ed. São Paulo: RT, 2009, p. 17.

De modo similar, Antonio Laronga, após examinar a posição da doutrina e da jurisprudência, conclui que a atipicidade se presta a designar qualquer meio de prova ou de investigação, não *disciplinado* nas normas processuais penais, funcionalmente destinado à verificação do enunciado fático, desde que não vedado expressamente.¹⁵¹

Diversamente, Paolo Tonini refere que existiriam, ao menos, três significados para provas atípicas. Numa primeira acepção, tratar-se-ia da prova que visa obter um resultado diverso do perseguido pelos meios de prova tipificados no Código, que seria mais apropriadamente chamada de prova inominada. De outro prisma; seria a prova produzida de forma diversa daquela prevista para o meio típico. Ainda, em terceira perspectiva, prova atípica seria aquela que visa obter, mediante um meio de prova típico, o resultado de um meio diverso, também típico, que seria mais adequadamente chamada de prova anômala.¹⁵²

Ainda, analisando a doutrina italiana, Guilherme Madeira Dezem identifica uma posição restritiva e uma posição ampliativa sobre o tema. A primeira, que seria majoritária e incluiria Taruffo, Nobili e Cavallone, considera atípica a prova quando ausente a previsão legal da fonte de prova. O autor acertadamente refuta tal posição, considerando que, sendo as fontes de provas reais ou pessoais, não se conceberiam fontes de provas atípicas.¹⁵³

Já para a posição ampliativa, por ele acolhida, a atipicidade se configuraria em duas situações: quando a prova seja nominada no ordenamento, mas não seja definido seu procedimento; quando nem seja nominada nem tenha procedimento previsto.¹⁵⁴

Este autor não indica, porém, se as provas atípicas incluiriam tanto os meios de obtenção da prova quanto os meios de prova, ou se apenas contemplariam estes. No Direito italiano, Antonio Laronga relata que, no silêncio da norma do art. 189 do Código, questiona-se se o dispositivo também se aplica aos meios de pesquisa da prova, concluindo positivamente, eis que referido artigo contém um princípio geral.¹⁵⁵

Com efeito, deve-se considerar o conceito da tipicidade e atipicidade processual aplicável, com ainda maior razão, aos meios de obtenção da prova, tendo em vista que, em geral, afetam com maior gravidade os direitos individuais.

¹⁵¹ *Le prove atipiche...*, p. 32.

¹⁵² *A prova...*, p. 110-111.

¹⁵³ *Da prova penal...*, p. 150-151.

¹⁵⁴ *Da prova penal...*, p. 147.

¹⁵⁵ *Le prove atipiche...*, p. 28-32.

Antonio Magalhães Gomes Filho refere que as provas atípicas ou inominadas são aquelas de que, ao contrário das típicas, o legislador não cogitou. Distingue, porém, o caso em que não se prevê o instrumento pelo qual o elemento de prova é introduzido no processo - o que conduziria à inadmissibilidade -, daquele em que se utiliza um procedimento diverso do previsto em lei - quando se fala em nulidade.¹⁵⁶

Para que se possa indicar o conceito mais apropriado no âmbito deste estudo, releva cotejar as provas atípicas com as denominadas provas nominada, irritual e anômala.

No que se refere à prova nominada, Guilherme Madeira Dezem afirma consistir no meio de prova que é mencionado no ordenamento jurídico, tendo ou não descrição do procedimento correspondente. Em suas palavras, “há, aqui, apenas a previsão do *nomen juris* do meio de prova”, sendo que exemplo de prova nominada, no Direito brasileiro, seria a reconstituição, prevista no art. 7º do Código de Processo Penal. O autor ainda refere que a prova nominada não significa, necessariamente, prova típica.¹⁵⁷ A prova nominada poderia ser típica ou atípica.

A despeito dessa posição, adota-se, neste estudo, entendimento de que a prova nominada consiste no meio de investigação ou meio de prova que é apenas citado no ordenamento jurídico, sem procedimento próprio, sendo, portanto prova atípica. Quando nominada e regulamentada, trata-se de prova típica.

Por prova irritual, tem-se a prova que - sendo típica, pois prevista no ordenamento jurídico - é produzida sem a observância do modelo legal.¹⁵⁸

Por seu turno, a prova anômala corresponde a uma distorção do modelo legal. Trata-se de “uma prova típica, utilizada ou para fins diversos daqueles que lhes são próprios, ou para fins característicos de outras provas típicas”.¹⁵⁹ Em estudo específico sobre o tema, Gustavo Badaró exemplifica a prova anômala pela juntada de declarações escritas de testemunhas (prova documental), em substituição ao depoimento oral (prova testemunhal).¹⁶⁰

¹⁵⁶ Notas..., p. 314-315.

¹⁵⁷ *Da prova penal...*, p. 155-157.

¹⁵⁸ *Da prova penal...*, p. 153; Badaró. Provas atípicas..., p. 344.

¹⁵⁹ Badaró. Provas atípicas..., p. 345. No mesmo sentido, com base em Laronga, Dezem. *Da prova penal...*, p. 152.

¹⁶⁰ Provas atípicas..., p. 351.

Tendo em vista a finalidade da previsão legal dos meios de produção e de obtenção da prova, ou seja, a garantia de direito individual e a eficiência/utilidade do procedimento¹⁶¹, parece mais apropriado considerar que a ausência de definição de um procedimento probatório acarreta a atipicidade da prova, ainda que haja a mera nomeação do meio. Desse modo, ao se referir a prova atípica, neste trabalho, estar-se-á considerando o meio de investigação ou meio de prova cujo procedimento não é disciplinado pelo ordenamento jurídico, ainda que seja nele mencionado.

Observe-se que as provas atípicas, irrituais e anômalas apresentam consequências diversas. Considerando a teoria das nulidades, as provas irrituais e anômalas devem ensejar a nulidade da prova, posto que não se conformam ao modelo legal.¹⁶²

No que atine às provas atípicas, não se pode afirmar com segurança qual a consequência a lhes atribuir, vez que o sistema processual brasileiro não cuida delas especificamente. Poder-se-ia cogitar de nulidade ou inadmissibilidade. No entanto, as nulidades são dispostas como sanções ao desvio do modelo legal.

Aury Lopes Junior manifesta-se no sentido da aceitação excepcional das provas atípicas – por ele referidas como inominadas -, desde que “estejam em estrita observância com os limites constitucionais e processuais da prova”, respeitando-se as regras de coleta, admissão e produção em juízo.¹⁶³

¹⁶¹ Benjamim Silva Rodrigues refere que o procedimento probatório no sistema português é orientado pelo princípio da legalidade, prevendo o artigo 125 do Código de Processo Penal que “são admissíveis as provas que não forem proibidas por lei”. A respeito do estabelecimento de regras probatórias, cita o autor o Preâmbulo do Código de Processo Penal português, segundo o qual se estabeleceu “um regime de conciliação particularmente exigente das finalidades do processo em conflito. Se, por um lado, se visa a máxima eficiência da investigação, por outro define-se um regime rigoroso (sistema) de protecção de direitos fundamentais em que o princípio da liberdade de prova sofre restrições típicas relativas aos métodos de prova concretizados num sistema exigente de proibições de prova”. *Das escutas telefônicas: A monitorização dos fluxos informacionais e comunicacionais*. 2ª Ed., Coimbra: Coimbra Editora, 2008, p. 73-74.

¹⁶² Guilherme Madeira Dezem sustenta que tais provas conduzem à nulidade ou à ilicitude. *Da prova penal...*, p. 155.

¹⁶³ O autor, no entanto, sustenta a taxatividade do rol de provas admitidas em processo penal, afirmando que, como regra, somente as provas típicas poderiam ser admitidas, mas que excepcionalmente provas atípicas poderiam ser permitidas, sob a condição de que não representem subversão da forma estabelecida para uma prova e que estejam em conformidade com as regras constitucionais e processuais atinentes à prova penal. *Direito processual penal e sua conformidade constitucional*. 5ª ed. Rio de Janeiro: Lumen Juris, 2010, vol. I, p. 571-572.

Em verdade, não se vedam as provas atípicas no Processo Penal brasileiro, vigendo, como visto, certa liberdade probatória.¹⁶⁴ No entanto, como sustentava José Frederico Marques:¹⁶⁵

“De um modo geral, são inadmissíveis os meios de prova que a lei proíba e aqueles que são incompatíveis com o sistema processual em vigor. Tais são: a) os meios probatórios de invocação ao sobrenatural; b) os meios probatórios que sejam incompatíveis com os princípios de respeito ao direito de defesa e à dignidade da pessoa humana.”

Para além da incompatibilidade, há de se considerar inadmissíveis as provas atípicas quando a própria ausência de procedimento legal não permitir a segurança das partes, a proteção dos direitos e garantias fundamentais e a eficiência do processo.¹⁶⁶

Como visto, o processo constitui garantia do indivíduo e da sociedade, visando à busca da verdade possível, dentro dos parâmetros legais. Não se pode, então, sob a justificativa da busca da verdade, admitir todo e qualquer meio de prova atípico, com risco à credibilidade do resultado do processo e aos direitos fundamentais, especialmente quando se trata de meio restritivo dos direitos fundamentais.¹⁶⁷ Não havendo a lei, que proporciona previsibilidade e segurança jurídica, é preciso adotar critérios, a exemplo do

¹⁶⁴ Nesse sentido, Adalberto Camargo Aranha, *Da prova...*, p. 37. O autor refere que existiriam o sistema das provas taxativas e o sistema das provas meramente exemplificativas, no qual o ordenamento brasileiro se incluiria.

¹⁶⁵ *Elementos de Direito Processual Penal*. 3ª atualização, vol. II, Campinas: Millenium Editora, 2009, p. 270-271.

¹⁶⁶ De maneira semelhante, pondera Guilherme de Souza Nucci, ao se referir aos meios ilícitos de prova: “É lógico que alguns mecanismos, ainda que não previstos em lei, pois o legislador pode não ter pensado em todas as hipóteses possíveis, podem ser usados, desde que não contrariem o próprio ordenamento jurídico. Existe, portanto, uma liberdade quase plena para produzir provas em processo penal, onde se busca a verdade real ou material, não se contentando com a formal.” *O valor da confissão como meio de prova no Processo Penal*. 2ª Ed., São Paulo: RT, 1999, p. 63-64.

¹⁶⁷ Benjamim Silva Rodrigues enumera os requisitos para a utilização de métodos ocultos de investigação, os quais correspondem a “todos aqueles métodos que representam uma intromissão nos processos de acção, interacção, informação e comunicação das pessoas concretamente visadas, sem que as mesmas disso tenham consciência, conhecimento ou disso sequer se apercebam”. Tais requisitos são a reserva de lei, fragmentaridade (com a seleção de um catálogo de infrações que permitam o método), fundada suspeita da ocorrência da referida infração, subsidiariedade dos métodos ocultos, o princípio da proporcionalidade, proibição do aniquilamento do âmbito nuclear da intimidade, “reserva de juiz” (exigência de decisão judicial autorizadora), dentre outros requisitos específicos. *Da prova penal: Tomo II - Bruscamente...a(s) face(s) oculta(s) dos métodos ocultos de investigação criminal*. Lisboa: Rei dos Livros, 2010, p. 37 e 53-64.

procedimento fixado no ordenamento italiano, que permitam aferir a conformação do meio utilizado ao devido processo penal.

Nesse sentido, havendo restrição a direito fundamental, impõe-se a existência de decisão judicial, particularmente motivada, de modo a justificar a necessidade de referido meio de prova e sua adequação ao resultado esperado, assim como a proporcionalidade da medida em relação ao direito afetado. Ainda, não se apresentando risco ao sucesso da medida, deve-se proceder à prévia oitiva das partes processuais.

No caso das provas digitais, não se encontra previsão legal dos meios específicos para sua obtenção, havendo que se recorrer ao uso da analogia e à adoção de procedimento de aferição, como acima proposto.

CAPÍTULO 3 – PROVAS DIGITAIS: CONCEITO, CARACTERÍSTICAS E NATUREZA JURÍDICA

Ao se tratar de provas digitais, é comum o emprego da expressão “documento eletrônico” para referir os dados e arquivos digitais. Faz-se, assim, uma aproximação do produto do processamento eletrônico com os documentos em sua concepção tradicional.

Não obstante, o presente estudo tem por finalidade demonstrar que as provas digitais possuem características diferenciadas, que conduzem ao seu enquadramento em uma classificação própria, muito embora as semelhanças entre a prova digital e o documento permitam a utilização do meio de prova documental como procedimento probatório em juízo.

Desse modo, mostra-se apropriado verificar o conceito que pode ser atribuído às provas digitais, para então examinar suas características e compará-las aos documentos tradicionais, analisando-se ao final sua natureza jurídica e o tratamento a ser-lhes conferido.

3.1 Prova digital: conceito

No campo das provas digitais, pode-se vislumbrar aplicações do termo “prova” nos diversos sentidos que ela apresenta¹⁶⁸.

Veja-se que é possível mencionar, sob a ideia de fonte real, prova eletrônica ou digital para designar os suportes físicos em que se encontram armazenados os dados – computadores, *pen drives*, CDs, DVDs, telefones celulares, aparelhos de MP3, as urnas

¹⁶⁸ Veja-se, a propósito, item 2.3 *supra*.

eletrônicas, câmeras de vídeo ou fotográficas, etc.¹⁶⁹ Do mesmo modo, com relação aos arquivos neles contidos – imagens, vídeos, músicas, documentos de texto, correspondências eletrônicas, páginas de *sites*, dentre outros.

Para a aquisição dessas fontes, são utilizados vários meios de pesquisa, como buscas e apreensões, interceptações, infiltrações em redes ou suportes, os quais podem ser entendidos como meios de obtenção de provas digitais.

Posteriormente, ocorre a introdução das fontes no processo, com a perícia e a prova documental, que constituem os meios de produção da prova digital.

Os elementos obtidos das fontes digitais, em conjunto com os demais elementos do processo, conduzem, então, ao resultado probatório, por meio da verificação das asserções feitas pelas partes.

No entanto, faz-se necessário delinear um conceito mais preciso de prova digital.

Encontram-se, na doutrina, algumas definições de prova digital (referida na doutrina norte-americana e inglesa como *digital evidence*), as quais, geralmente, possuem múltiplos sentidos ou correspondem ao sentido de “elemento de prova”.

Eoghan Casey define *digital evidence* como “qualquer dado armazenado ou transmitido usando um computador que confirma ou rejeita uma teoria a respeito de como ocorreu um fato ofensivo ou que identifica elementos essenciais da ofensa como intenção ou o álibi”¹⁷⁰.

Benjamim Silva Rodrigues define “prova electrónico-digital” como “qualquer tipo de informação, com valor probatório, armazenada (em repositórios electrónicos-digitais de armazenamento) ou transmitida (em sistemas e redes informáticas ou rede de comunicações electrónicas, privadas ou publicamente acessíveis, sob a forma binária ou digital”.¹⁷¹

¹⁶⁹ “Data may be held on a huge variety of types of data media.” Walden. *Computer crimes...*, p. 212.

¹⁷⁰ *Digital evidence and computer crime: forensic science, computers, and the Internet*. 2ª ed. San Diego/London: Elsevier Academic Press, 2004, p. 12. Tradução livre.

¹⁷¹ *Da prova penal: Tomo IV – Da prova-electrónico-digital e da criminalidade informático-digital*. Lisboa: Rei dos Livros, 2011, p. 39.

De modo similar, a *International Organization of Computer Evidence* (IOCE) refere-se à prova digital como “informação transmitida ou memorizada em formato binário que pode ser utilizada na Justiça”¹⁷².

Entretanto, pode-se observar que a peculiaridade da prova digital consiste na forma de arquivamento da informação e suas respectivas características. Isso levará a cuidados e procedimentos especiais na obtenção e produção dessa prova, o que constitui consequência de sua configuração. Quanto ao elemento de prova e ao resultado probatório, cuida-se da análise da informação, em cotejo com as demais provas do processo, não apresentando traços distintivos de relevo, mas apenas a influência das características da prova digital na valoração da prova.

Conclui-se, portanto, que a alusão à prova digital designa, na verdade, fonte de prova; o objeto a partir do qual se podem extrair informações de interesse à persecução penal.¹⁷³ O valor probatório, contudo, será analisado no âmbito do processo, motivo pelo qual não deve integrar o conceito de prova digital.

A partir dessas premissas, pode-se definir “**prova digital**” da seguinte maneira: “os dados em forma digital (no sistema binário) constantes de um suporte eletrônico ou transmitidos em rede de comunicação, os quais contêm a representação de fatos ou ideias.”

Releva destacar que essa definição não compreende os meios de prova que se utilizam de sistemas informáticos para auxiliar na interpretação e análise dos dados contidos no processo. É o caso de animações ou simulações elaboradas no computador, assim como reconstituições de fatos em programas informáticos. Esses meios de prova são

¹⁷² Giovanni Ziccardi, Le tecniche informatico-giuridiche di investigazione digitale. In: LUPARIA, Luca; ZICCARDI, Giovanni (Org.). *Investigazione penale e tecnologia informatica. L'accertamento del reato tra progresso scientifico e garanzie fondamentali*. Milão: Giuffrè, 2007, p. 60.

¹⁷³ Sob a nomenclatura de “prova cibernética”, encontra-se, em âmbito nacional, a seguinte definição, mais próxima à ideia de fonte de prova: “(...) o registro de um fato, originariamente, por meios eletrônicos ou tecnológicos, documentado sob a forma digital, através de codificação binária, capaz de ser traduzido para uma linguagem inteligível ao homem, dotado de abstração quanto ao meio em que ocorreu o fato objeto do registro e a respectiva forma de armazenagem, presente a portabilidade do código binário para suporte material diverso, conservando a integridade original do registro, sua autenticidade e possibilidade de utilização sob a forma de pelo menos outra mídia que não a originalmente obtida.” Embora mais próxima do conceito apropriado de prova digital, tal definição inclui características do dado digital e referências a sua duplicação, nem sempre presentes e que não compõem o conceito. Paulo Roberto de Lima Carvalho. *Prova cibernética...*, p. 87.

referidos por Luca Luparia, com base na doutrina anglo-saxônica, como *computer-generated-evidence*, distinguindo-se da *computer-derived-evidence*.¹⁷⁴

Do mesmo modo, não se incluem entre as provas digitais as informações que possam ser obtidas de entidades públicas ou de terceiros, por meio de requisição, apenas porque sejam registradas em meios digitais. Assim, não se entendem por prova digital os dados bancários de um indivíduo sob investigação, que sejam armazenados em computadores da instituição financeira e encaminhados mediante requisição do Juízo.

Por outro lado, seriam provas digitais arquivos informáticos obtidos nos servidores de instituição financeira, mediante busca e apreensão, para investigação do próprio banco, de funcionários ou terceiros.

Logo, a prova digital não se confunde com a prestação de informações em formato digital. Trata-se, isso sim, de prova que tem por base os arquivos informáticos, em poder do investigado ou de terceiros ou enviados pelas redes informáticas, que possam conter informações úteis à busca da verdade. O que interessa é o próprio arquivo informático.

Importa, nesse ponto, observar que o dado digital pode ser obtido quando está armazenado em um dispositivo eletrônico ou quando está sendo transmitido. As duas situações estão inseridas, respectivamente, no que se denomina **informática** e **telemática**. Segundo a doutrina, a primeira constitui gênero, abarcando todos os fatos ocorridos no âmbito dos computadores, ao passo que a telemática é espécie, constituindo o inter-relacionamento entre computadores, em um ambiente de rede.¹⁷⁵ À luz desse conceito, haveria a captação telemática quando se tratasse da obtenção de dados durante sua transmissão entre dispositivos, à distância.¹⁷⁶ Assim, haverá meios de obtenção da prova que se dirigem aos suportes físicos e aos dados estáticos, como também haverá os que captam as informações quando estão em movimento.¹⁷⁷

¹⁷⁴ Luca Luparia. La disciplina processuale e le garanzie difensive. In: LUPARIA, Luca; ZICCARDI, Giovanni (Org.). *Investigazione penale e tecnologia informatica. L'accertamento del reato tra progresso scientifico e garanzie fondamentali*. Milão: Giuffrè, 2007, p. 145.

¹⁷⁵ Rossini, *Informática...*, p. 42-43 e 110.

¹⁷⁶ Dicionário Houaiss da Língua Portuguesa. Disponível em: <http://houaiss.uol.com.br/busca.jhtm?verbete=digital&stipe=k>. Acesso em 15.01.2011.

¹⁷⁷ “In generale, assume comunque significato la distinzione operata tra sistema informatico e sistema telematico quali autonome sedi di raccolta di dati, informazioni e programmi informatici oggetto di attività inquirenti urgenti: sviluppando la nozione di *computer* dalla dimensione statica di macchina che memorizza dati alla prospettiva dinamica di strumento attivo per un collegamento di rete, si proietta la capacità dimostrativa dell'evidenza digitale nella grandezza virtuale dello sconfinato *cyber* spazio.” Lorenzetto, *Le attività...*, p. 140.

Cabe ainda ressaltar que, em diversas obras, utilizam-se indistintamente os termos prova digital, prova eletrônica, prova informática e prova tecnológica. Faz-se, porém, necessário, distinguir a **prova digital** de outros termos comumente utilizados.

Assim, pode-se diferenciar a **prova digital** e a **prova eletrônica**. Enquanto a prova digital corresponde aos dados binários, a prova eletrônica está relacionada aos suportes físicos que armazenam os arquivos digitais. Essa distinção é feita por Eoghan Casey:¹⁷⁸

“Os termos prova digital e prova eletrônica, às vezes, são usados de forma intercambiável. Entretanto, um esforço deve ser feito para distinguir entre equipamentos eletrônicos, tais como telefones celulares, e os dados digitais que eles contêm.”

Embora sem diferenciá-la da prova digital, Eduardo de Urbano Castrillo oferece definição de prova eletrônica que enfatiza os suportes físicos:¹⁷⁹

“(...) la que permite acreditar hechos a través de ‘los medios de reproducción de la palabra, el sonido y la imagen, así como los instrumentos que permiten archivar y conocer o reproducir palabras, datos, cifras y operaciones matemáticas llevadas a cabo con fines contables o de otra clase, relevantes para el proceso’”.

Com relação à **prova informática**, pode-se afirmar que ela constitui categoria mais ampla do que a prova digital. Nesse sentido, a prova informática pode ser entendida como toda prova que seja originada, processada ou reproduzida por computador, incluindo tanto a *computer-generated-evidence* quanto a *computer-derived-evidence*.

Giovanni Ziccardi também resalta que a fonte de prova digital pode ser afeta a um ambiente estático ou dinâmico. *Informatica Giuridica: privacy, sicurezza informatica, computer forensics e investigazioni digitali*. Milão: Giuffrè, 2008, Tomo II, p. 323.

Veja-se ainda Walden. *Computer crimes...*, p. 207.

¹⁷⁸ *Digital evidence...*, p. 12.

¹⁷⁹ *La valoración de la prueba electrónica*. Valencia: Tirant Lo Blanch, 2009, p. 47.

Por seu turno, a **prova tecnológica** também se exhibe ampla, referindo-se aos elementos obtidos a partir de qualquer instrumento desenvolvido pelas modernas tecnologias.¹⁸⁰

3.2 Características da prova digital

As provas digitais, na acepção de fontes de prova, constituem uma nova realidade no que diz respeito ao seu registro, extração, conservação e apresentação em juízo. Possuem, pois, características próprias que as individualizam como categoria específica de fonte de prova.

Giovanni Ziccardi aponta como características da fonte de prova digital a imaterialidade e a fragilidade intrínseca do dado.¹⁸¹

Luca Lupária destaca a natureza “ontologicamente volátil, alterável e falsificável do dado digital”.¹⁸²

Benjamim Silva Rodrigues identifica as seguintes características dessa prova:¹⁸³

- efemeridade, temporalidade, precariedade e não durabilidade;
- fragilidade e fácil alterabilidade;

¹⁸⁰ Diante dos delineamentos feitos, parecem equivocadas as definições adotadas por José María Illán Fernández acerca de meios eletrônicos, documento eletrônico e documento digital, na medida em que se confundem conceitos diversos. Segundo o autor:

Meios eletrônicos são: “todos aquellos instrumentos creados para obtener un intercambio de información de forma automatizada, tales como Internet, fax, correo electrónico, etc.”

Documento eletrônico “son todos aquellos objetos materiales en los que puede percibirse una manifestación de voluntad o representativos de un hecho de interés para el proceso que pueda obtenerse a través de los modernos medios reproductivos, como la fotografía, la fonografía, la cinematografía, el magnetófono, las cintas de video, los discos de ordenador y cualesquiera otros similares”.

Documento digital “es un conjunto seleccionado y organizado de objetos o materiales digitales (documentos electrónicos) junto con los metadatos que los describen y una interfaz o conjunto de interfaces que facilitan su acceso”.

La prueba electrónica, eficacia y valoración en el proceso civil: Nueva oficina judicial, comunicaciones telemáticas (lexnet) y el expediente judicial electrónico – Análisis comparado legislativo y jurisprudencial. Navarra: Editorial Aranzadi, 2009, p. 241-242.

¹⁸¹ Ziccardi. Le techniche..., p. 7-8.

¹⁸² Lupária. La disciplina..., p. 148.

¹⁸³ *Da prova penal: Tomo IV...*, p. 41-44.

- volatilidade ou instabilidade, diante da possibilidade de desaparecimento e alteração;
- aparente imaterialidade ou invisibilidade;
- complexidade ou codificação, pela necessidade de “uso/conhecimento de palavras-chave ou técnicas de descriptação”;
- dispersão, disseminação ou pulverização;
- dinamismo e mutabilidade.

De fato, a principal característica da prova digital reside no fato de se tratar de objeto imaterial (sequência numérica¹⁸⁴), que pode ser facilmente alterado, como também pode ser copiado e difundido, necessitando de um equipamento intermediário para ser acessado.

Por outro lado, não se pode afirmar que a não durabilidade seja característica de toda prova digital, pois os dados informáticos armazenados em dispositivos eletrônicos são submetidos a técnicas de preservação. De igual modo, os dados transmitidos em rede são captados e fixados em suportes eletrônicos, de forma a os tornar permanentes.

A disseminação dos dados, pulverizados em diferentes ambientes eletrônicos tampouco constitui característica comum e essencial a toda prova digital. O objeto de interesse para a persecução penal pode se encontrar armazenado em um único dispositivo, em um só arquivo. No entanto, a dispersão corresponde a uma possibilidade, que deve ser considerada durante a investigação.

Em vista de tais constatações, pode-se apontar a existência das seguintes características das provas digitais: imaterialidade e desprendimento do suporte físico originário, volatilidade, suscetibilidade de clonagem e necessidade de intermediação de equipamento para ser acessada.

Imaterialidade

¹⁸⁴ “In informatica, l’aggettivo ‘digitale’ si riferisce a tutto ciò che viene rappresentato con numeri o che opera manipolando numeri. Il termine deriva dall’inglese *digit* (cifra), che a sua volta deriva dal latino *digitus* (dito). Il dato informatico è l’entità su cui opera un *computer* e si esprime in linguaggio binario, risultando composto da una successione di 0 e 1.” Lorenzetto. *Le attività...*, p. 140. Veja-se no primeiro capítulo a definição de digital e de dados informáticos.

A imaterialidade é a característica do que “não é composto de matéria”, do “que não se pode tocar”, o que é “impalpável”¹⁸⁵, o que “não tem consistência material, não é da natureza da matéria, não tem existência palpável”¹⁸⁶.

O sentido de “imaterial”, no que concerne à prova digital, corresponde à sua natureza impalpável, vez que, embora invisíveis a olho nu, os dados informáticos consistem em impulsos elétricos.

O dado digital mostra-se, portanto, imaterial, intangível.¹⁸⁷ Nesse sentido, não depende do suporte físico originário para existir, podendo ser transferido a outros dispositivos eletrônicos, sem perder sua essência. Daí o desprendimento, ou seja, a separação, entre o suporte físico originário e o dado digital.

A imaterialidade possibilita aos sistemas informáticos o armazenamento de imensa quantidade de informações, já que os dados não ocupam espaço físico relevante, mostrando-se compactos. Isso permite grande acumulação de dados, em capacidade muito superior aos documentos tradicionais.

Volatilidade

A volatilidade caracteriza o que é “volúvel”, “inconstante”, “que muda com facilidade”, “que não é firme ou permanente”¹⁸⁸, o que é “variável”, “que pode desaparecer ou dissipar-se”¹⁸⁹.

Em virtude de sua imaterialidade, o dado digital apresenta-se frágil, pois facilmente se submete a alterações ou desaparecimento, bastando a modificação da sequência numérica que o compõe.¹⁹⁰

¹⁸⁵ Dicionário Aulete, em sua versão digital. Disponível em: http://aulete.uol.com.br/site.php?mdl=aulete_digital&op=loadVerbete&palavra=imaterial. Acesso em 04.01.2012.

¹⁸⁶ Dicionário Houaiss, em sua versão digital. Disponível em: <http://houaiss.uol.com.br/busca.jhtm?verbete=imaterial&stipe=k>. Acesso em 04.01.2012

¹⁸⁷ Ian Walden faz referência à natureza intangível e transitória dos dados, em especial em um ambiente de rede, do que decorre a dificuldade e complexidade da investigação informática. *Computer crimes...*, p. 205

¹⁸⁸ Dicionário Houaiss, em sua versão digital. Disponível em: <http://houaiss.uol.com.br/busca.jhtm?verbete=vol%E1til&cod=191288>. Acesso em 04.01.2012.

¹⁸⁹ Dicionário Aulete, em sua versão digital. Disponível em: http://aulete.uol.com.br/site.php?mdl=aulete_digital&op=loadVerbete&pesquisa=1&palavra=vol%E1til. Acesso em 04.01.2012.

É, portanto, volátil, sujeito a variações e dissipação com facilidade. Como resultado, pode-se perder a informação guardada de forma digital, assim como pode haver alterações que prejudiquem sua confiabilidade.

A alteração pode ocorrer propositalmente ou acidentalmente, como destaca Eoghan Casey: “(...) the fact that digital evidence can be manipulated so easily raises new challenges for digital investigators. Digital evidence can be altered either maliciously by offenders or accidentally during collection without leaving any obvious signs of distortion.”¹⁹¹

Suscetibilidade de clonagem

A clonagem constitui uma técnica da genética pela qual se produzem organismos idênticos. O termo é aplicado à informática, denominando a elaboração de cópia fiel de um arquivo digital, contendo todos os *bits* que o compõem. Refere-se a este processo também como espelhamento ou imagem.¹⁹²

Por se tratar de um objeto imaterial, consistente em sequência numérica, os dados digitais permitem a sua transferência a outros dispositivos eletrônicos, em sua integralidade. Por essa razão, ele admite a execução de infinitas cópias, todas iguais, sem que se possa falar em um exemplar original¹⁹³.

Necessidade de intermediação

Sendo o dado digital uma sequência numérica, constituindo, assim, um código digital, faz-se necessário o uso de um equipamento que possa processar a informação e disponibilizá-la de maneira compreensível pelo ser humano.

¹⁹⁰ “È opinione comune che l’informazione digitale è per sua natura immateriale ed impalpabile, per cui è soggetta ad intrinseca modificazione e repentina alterazione.” Braghò. *L’ispezione...*, p. 191.

¹⁹¹ *Digital evidence...* p. 16.

¹⁹² O guia de boas práticas da Associação dos Chefes de Polícia do Reino Unido assim define o processo de “imagem”: “the process used to obtain all of the data present on a storage media (e.g. hard disk) whether it is active data or data in free space, in such a way as to allow it to be examined as if it were the original data”. Ian Walden. *Computer crimes...*, p. 463.

¹⁹³ Renato Luis Benucci. *A tecnologia aplicada ao processo judicial*. Campinas: Millenium Editora: 2006, p. 78.

Não é possível a leitura dos dados diretamente pelo receptor da informação, vez que está é imaterial, invisível e codificada.

3.3 Comparação entre prova digital e documento. Análise da natureza jurídica da prova digital

Ao se depararem com a prova digital, os operadores do direito vêm se utilizando dos conceitos relacionados ao documento e aplicando as normas respectivas, sem questionamentos aprofundados. O tema, porém, mostra-se complexo, em vista das mencionadas particularidades da prova digital.

Ademais, a dificuldade aprofunda-se pelo fato de não haver uma definição clara sobre a concepção de documento, nem uma disciplina acurada de seu procedimento probatório.

Com efeito, o Código de Processo Penal brasileiro definiu como documentos “quaisquer escritos, instrumentos ou papéis, públicos ou particulares” (art. 232), pelo que apenas escritos corresponderiam a essa espécie de prova.¹⁹⁴

De outro lado, com a alteração promovida pela Lei 11.689/2008, o Código passou a considerar como documento, para efeito da proibição inscrita no procedimento do júri de leitura ou exibição de documento não previamente juntado, os seguintes objetos: jornais ou qualquer outro escrito, vídeos, gravações, fotografias, laudos, quadros, croqui “ou qualquer outro meio assemelhado, cujo conteúdo versar sobre a matéria de fato submetida à apreciação e julgamento dos jurados” (art. 479).

De toda sorte, como relata Guilherme Madeira Dezem, a jurisprudência vem admitindo a ampliação do conceito, aceitando como documento outras formas de fixação do pensamento.¹⁹⁵

Nesse passo, encontram-se, na doutrina, correntes ampliativas e restritivas do conceito, com diversas definições de documento.¹⁹⁶

¹⁹⁴ O Projeto do novo Código de Processo Penal optou por não adotar uma definição de documento.

¹⁹⁵ *Da prova penal...*, p. 265.

¹⁹⁶ Tal o que referem Dezem, *Da prova penal...*, p. 264-265; Tourinho Filho, *Processo penal*, vol. III, p. 349-350; Virginia Pardo Iranzo, *La prueba documental en el proceso penal*. Valencia: Tirant Lo Blanch, 2008, p.

Segundo a teoria do escrito (ou concepção latina), o documento é sempre escrito, sujeito às ideias de permanência e durabilidade^{197 198}.

Por outro lado, segundo a posição ampliativa, em consonância com a teoria da representação (ou concepção germânica), considera-se documento “todo elemento que ofereça alguma informação com independência do suporte onde se encontre”¹⁹⁹.

Neste sentido, é clássica a lição de Francesco Carnelutti, que postula ser documento “uma coisa capaz de representar um fato”.²⁰⁰ Com base nessa acepção, sustenta-se que matérias diversas do papel podem ser consideradas documentos, se contiverem representação através da escritura ou por outros meios (figuras, desenhos, sons, imagens, etc.).

De maneira semelhante, encontram-se, na doutrina nacional, definições de documento baseadas na ideia de representação, em qualquer base material, com fins de prova.²⁰¹

Nesse sentido, Magalhães Noronha refere uma definição lata e uma estrita de documento, “compreendendo-se na primeira todo objeto hábil para provar uma verdade, ao passo que, no segundo sentido, é o objeto que contém a manifestação do pensamento ou da vontade da pessoa, bem como a menção de um fato, a narração de um acontecimento etc.”, sendo que, nessa acepção, “é o objeto que contém um *escrito*, uma expressão gráfica de valor probatório”.²⁰²

Assim também, para Guilherme de Souza Nucci: “é toda base materialmente disposta a concentrar e expressar um pensamento, uma idéia ou qualquer manifestação de

49-51; Andrés Jaume Bennasar. *La validez del documento electrónico y su eficacia en sede procesal*. Valladolid: Lex Nova, 2010, p. 47.

¹⁹⁷ Bennasar, *La validez...*, p. 47.

¹⁹⁸ Vincenzo Manzini define documento pela percepção de escritura e indica a aptidão de servir à prova: “Documento, in senso proprio, è ogni scrittura fissata sopra um mezzo idoneo, dovuta ad um autore determinato, contenente manifestazioni o dichiarazioni di volontà ovvero attestazioni di verità, atte a fondare o a sufragare uma pretesa giuridica, o a provare un fatto giuridicamente rilevante, in un rapporto processuale o in altro rapporto giuridico.” *Trattato di Diritto Processuale Penale Italiano*. 6ª Ed. Torino: UTET, 1970, p.545, vol. III.

¹⁹⁹ Bennasar, *La validez...*, p. 47-48. Tradução livre.

²⁰⁰ A definição é citada por muitos autores, a exemplo de Humberto Theodoro Junior. *Curso de Direito Processual Civil*, 18ª Ed. Rio de Janeiro: Forense, 1996, vol. I, p. 442.

²⁰¹ José Frederico Marques é um dos autores que adotam a definição de documento elaborada por Carnelutti. *Elementos...*, p. 343.

²⁰² *Curso de Direito Processual Penal*. 13ª Ed. São Paulo: Saraiva, 1981, p. 126.

vontade do ser humano, que sirva para demonstrar e provar um fato ou acontecimento juridicamente relevante.”²⁰³

Nas palavras de Adalberto Camargo Aranha, considera-se documento “todo meio legal pelo qual a representação se faz pela escrita, por sinais da palavra falada ou pela reprodução de um fato ou acontecimento em um objeto físico, possível de servir como prova em juízo”.²⁰⁴

Também segundo Humberto Theodoro Junior, documento “é o resultado de uma obra humana que tenha por objetivo a fixação ou retratação material de algum acontecimento.”²⁰⁵

Julio Fabbrini Mirabete afirma que, “em sentido estrito, documento (de *doceo*, ensinar, mostrar, indicar) é o escrito que condensa graficamente o pensamento de alguém, podendo provar um fato ou realização de algum ato dotado de significação ou relevância jurídica”.²⁰⁶

Utilizando o critério da representação e também referindo o fato delituoso, expõe Galdino Siqueira acerca do sentido amplo de documento: “Em sua mais ampla acepção, chama-se *documento* todo e qualquer objecto phisico e sensível que estampe ou revele os traços do facto delituoso, ou que a este se refira circumstancialmente.”²⁰⁷

Diante das diferentes concepções de documento, Virginia Pardo Iranzo propõe a verificação dos elementos essenciais que o constituem. De acordo com a autora, seriam eles: a corporeidade, ou seja, a base material do objeto; a docência, que significa a capacidade de demonstrar algo, a representação; e a “incorporação da mensagem ao suporte de maneira artificial, por obra do ser humano, não da natureza”.²⁰⁸

A respeito da “docência”, cabe observar que Adalberto Camargo Aranha indica que o termo documento “tem a sua origem em *documentum*, do verbo latino *doceo*, significando ensinar, mostrar, indicar, vale dizer, tudo aquilo que tem em si a virtude de fazer conhecer outra coisa”.

²⁰³ *Manual de Processo Penal e Execução Penal*. 4ª Ed., São Paulo: RT, 2008, p. 480.

²⁰⁴ *Da prova...*, p. 258.

²⁰⁵ *Curso...*, vol. I, p. 442.

²⁰⁶ *Processo penal*. 18ª Ed. São Paulo: Atlas, 2008, p. 312.

²⁰⁷ *Curso de processo criminal*. 2ª Ed. Rio de Janeiro: Magalhães, 1939, p. 185. Já definição estrita de documento oferecida pelo autor mais se assemelha à documentação.

²⁰⁸ *La prueba documental...*, p. 51-52.

Hernando Devis Echandía, por sua vez, aponta os requisitos necessários para a existência jurídica do documento: que se trate de uma coisa ou um objeto, com aptidão representativa, formado mediante um ato humano; que represente um fato qualquer; que tenha uma significação probatória; a assinatura.²⁰⁹

De sua parte, Andrés Jaime Bennasar assinala as funções essenciais que o documento deve cumprir para ser reconhecido como tal:²¹⁰

- função probatória - com a veiculação de uma informação;
- função de perpetuação - com o registro em um suporte que permita conservar, manter ou fixar a informação;
- e função de garantia - com a identificação da fonte ou autores da declaração de vontade, dos dados ou fatos, conferindo-lhe autenticidade.

Como se nota, destaca-se, por vezes, a finalidade probatória do documento. No entanto, é preciso atentar para a diferenciação, proposta por Manzini e referida por Alcalá-Zamora y Castillo e Levene, entre os documentos *originariamente destinados à prova* e os *originariamente não destinados à prova*. Os primeiros “são aqueles criados intencionalmente para servir de meios de prova” (sic), enquanto os segundos, “alheios em seu nascimento a todo propósito probatório, adquirem tal caráter posteriormente”. Dentre estes últimos, estariam o corpo do delito e os documentos que provenham do imputado.²¹¹

Em vista do exposto, conclui-se que se pode adotar uma ampla variedade de concepções sobre o documento, das mais restritivas às mais amplas: documento é somente o papel, ou qualquer base material (papel, madeira, pedra, filme, disco, fita de vídeo, CDs, etc.); somente o escrito ou qualquer forma de manifestação humana (desenhos, fotografia, escultura, sons, imagens, etc.); qualquer representação de uma ideia ou fato ou somente a declaração de vontade humana; um objeto criado para fins probatórios ou que adquire este caráter posteriormente.

A adoção de uma noção intermediária revela-se adequada. Não se pode admitir que o documento seja qualquer coisa, nem se pode reduzi-lo ao papel escrito. Ainda, mostra-se demasiadamente restritiva a exigência de que se trate de uma declaração de vontade ou que seja ele destinado à prova. Por outro lado, mostra-se muito ampla a

²⁰⁹ *Teoría...*, vol. II, p. 526-527.

²¹⁰ *La validez...*, p. 49-50.

²¹¹ *Derecho Procesal Penal*, p. 151. Tradução livre.

aceitação de qualquer representação de fato ou idéia como documento. Outrossim, são consistentes os elementos da corporeidade, da representação e da incorporação da mensagem de maneira artificial. Por fim, deve-se distinguir o objeto material que contém a representação de um fato ou ideia daquele que constitui o corpo do delito, e, portanto, o objeto da prova (como um documento falso).

Desta feita, o conceito de documento está relacionado ao registro da representação de um fato ou ideia, pela intervenção humana, por meio de escrito, imagem ou som, em base material móvel²¹², de maneira duradoura e realizado fora do processo.²¹³

Utilizando-se do conceito de documento como registro de um fato, Augusto Tavares Rosa Marcacini sustenta sua atualização, de modo a se dar maior ênfase à perpetuação do pensamento ou do fato do que à sua materialidade. Com isso, inclui o documento eletrônico no conceito jurídico de documento, propondo nova classificação: documento físico e documento eletrônico. Confirma-se a explanação:²¹⁴

“Um conceito atual de documento, para abranger também o documento eletrônico, deve privilegiar o pensamento ou fato que se quer perpetuar e não a coisa em que estes se materializam. Isto porque o documento eletrônico é totalmente dissociado do meio em que foi originalmente armazenado.

(...)

Documento, assim, é o registro de um fato. (...). A característica de um documento é a possibilidade de ser futuramente observado; o documento narra, para o futuro, um fato ou pensamento presente. Daí ser também definido como prova histórica. Diversamente, representações cênicas ou narrativas orais, feitas ao vivo, representam um fato no momento em que são realizadas, mas não se perpetuam, não registram o fato para o futuro. Se esta é a característica marcante do documento, é lícito dizer que, na medida em que a técnica evolui

²¹² Veja-se, a propósito, a comparação mencionada por Virginia Pardo Iranzo entre documento e monumento, cujo traço distintivo é a mobilidade. *La prueba documental...*, p. 48-49. Diversamente, Adalberto Camargo Aranha distingue documento e monumento pelo significado: “enquanto o primeiro reproduz o real, o segundo transmite-se por meio de um simbolismo”. *Da prova...*, p. 259. A asserção, porém, não parece acurada, vez que o documento se apresenta como representação ampla, podendo conter variadas formas de manifestação.

²¹³ A exterioridade ao processo é destacada por Paolo Tonini, que distingue *documento* e *documentação*. Enquanto os documentos são “provas pré-constituídas formadas fora do processo”, a documentação constitui representação de um ato do mesmo procedimento no qual é juntada, como os termos de declarações. *A prova...*, p. 192-193.

²¹⁴ O documento eletrônico como meio de prova. *Revista de Direito Imobiliário*, vol. 47, p. 70, Jul / 1999.

permitindo registro permanente dos fatos sem fixá-lo de modo inseparável em alguma coisa corpórea, tal registro também pode ser considerado documento. A tradicional definição de documento enquanto coisa é justificada pela impossibilidade, até então, de registrar fatos de outro modo, que não apegado de modo inseparável a algo tangível.

Assim, renovando o conceito de documento - e até retornando à origem do vocábulo - documento é o registro de um fato. Se a técnica atual, mediante o uso da criptografia assimétrica, permite registro inalterável de um fato em meio eletrônico, a isto também podemos chamar de documento.

Incluído o documento eletrônico no conceito jurídico de documento, dadas as suas características peculiares mostra-se possível propor mais uma classificação - além das que já são estabelecidas pela doutrina - para distinguir o documento entre documento físico e documento eletrônico. O documento físico bem pode continuar a ser definido como uma coisa representativa de um fato (Moacyr Amaral Santos). Se documento, em sentido lato, é o registro de um fato, o documento físico é o registro de um fato inscrito em meio físico e a ele inseparavelmente ligado.

Já o documento eletrônico, como dito acima, não se prende ao meio físico em que está gravado, possuindo autonomia em relação a ele. O documento eletrônico é, então, uma seqüência de bits que, traduzida por meio de um determinado programa de computador, seja representativa de um fato. Da mesma forma que os documentos físicos, o documento eletrônico não se resume em escritos: pode ser um texto escrito, como também pode ser um desenho, uma fotografia digitalizada, sons, vídeos, enfim, tudo que puder representar um fato e que esteja armazenado em um arquivo digital.”

Ocorre que essa proposição leva em consideração os contornos do Processo Civil, baseando-se na utilização da criptografia para o registro inalterável de um fato em meio eletrônico. Logo, para esse autor, nem todo arquivo digital será considerado documento.

O Processo Penal, contudo, possui conformação diferente, não se podendo desprezar os dados digitais que não atendam ao requisito da durabilidade. Outrossim, nota-

se uma diferença conceitual entre o documento eletrônico, conforme proposto pelo autor mencionado, e a prova digital, aqui examinada.

A partir do conceito de documento acima exposto, pode-se afirmar que, no Processo Penal, a prova digital constitui fonte de prova assemelhada ao documento, mas com natureza própria, em virtude das particularidades que a caracterizam.

Assim, embora no mais das vezes a prova digital contenha a representação sobre um fato ou ideia, ela se exhibe mais ampla, abrangendo a informação de maneira geral.

Ela ainda se distingue do documento tradicional pela imaterialidade e pelo desprendimento da base material, base essa que se mostra essencial em relação ao documento tradicional. Nesse ponto, note-se que a prova digital pode ser alterada ou destruída sem efeitos para seu suporte, enquanto a intervenção no conteúdo do documento, em regra, também afeta a base material.

Acrescente-se que a prova digital não constitui necessariamente o registro da representação de forma duradoura. É o que se observa, por exemplo, pelo tráfego de dados na internet, hipótese em que a preservação só é possível pela captura da informação.

Por essas razões, considera-se que a prova digital constitui espécie de fonte real de prova, assemelhada ao documento, mas formadora de categoria própria.²¹⁵

²¹⁵ Davi Monteiro Diniz, sob o raciocínio do Direito Civil, reconhece que os arquivos digitais não apresentam os elementos integrantes dos documentos. No entanto, considera que as técnicas de criptografia permitem seu uso como meio de prova, defendendo também a alteração legislativa, de modo a contemplar os arquivos digitais como instrumentos aptos à formalização dos atos em geral.

Confira-se sua conclusão: “Os documentos sofrem uma diferenciação de tratamento legal expressiva, uma vez que direitos públicos e direitos privados os tomam como objeto de suas disposições. Os elementos de autoria, integridade de conteúdo e corporalidade dos documentos são abordados pelo legislador ora de modo concentrado, ora de modo particular, de acordo com a relevância da função que exercem em diferentes situações jurídicas.

Os arquivos digitais não atendem, com exatidão, às integrais funções previstas pela nossa legislação aos documentos. No entanto, as técnicas de criptografia disponíveis já oferecem condições materiais para a identificação de sua autoria e a verificação da integridade de seu conteúdo, possibilitando o seu intenso uso como meio probatório.

A caracterização do arquivo digital como objeto imaterial - uma vez que a sua principal utilidade reside na representação de seu conteúdo, como demonstra o seu manejo independentemente da base material que eventualmente o encerre - o coloca como inadequado para as situações em que o documento é legalmente pressuposto como um objeto corpóreo.

Faz-se necessária a adaptação dos diplomas legais que impõem, como elemento essencial ao reconhecimento da existência de um documento, sua corporalidade, o que se constata pelo estudo dos requisitos presentes nos tipos, gerais ou especiais, disponíveis para a instrumentação dos atos jurídicos.

Em conformidade com o exposto, qualificar os arquivos digitais como documentos terá maior ou menor coerência não apenas de acordo com a confiança que lhe for emprestada como meio probatório, mas também dependerá da revisão de textos positivos, de modo a que reconheçam a idoneidade desses arquivos para a

3.4 Necessidade de normas próprias para a prova digital

A natureza da prova digital e suas características produzem reflexos diretos sobre o Processo Penal, particularmente na atividade probatória, demandando maior cautela na obtenção da prova e o estabelecimento de regras próprias para essa fonte de prova.

Em primeiro lugar, deve-se cuidar de capturar os dados digitais, seja por meio de interceptação, seja pelo *download* ou cópia. A seguir, dada a imaterialidade da prova digital, faz-se necessário proceder à sua fixação em um suporte eletrônico, que seja colocado à disposição da justiça. Diferentemente dos documentos tradicionais, não basta a apreensão dos suportes físicos.

Ademais, a volatilidade e alterabilidade das fontes de prova recomendam a rapidez na atuação para sua captura, a fim de preservar os possíveis elementos de prova, especialmente quando se tratar de dados em tráfego na rede.

A esse respeito, Elisa Lorenzetto avalia que a disciplina das medidas urgentes para a investigação informática, presente no sistema jurídico italiano foi concebida levando em consideração o perigo de que “os vestígios e as coisas concernentes ao delito e ao estado do lugar ‘se alterem, se dispersem ou de qualquer modo se modifiquem’ e identifica em tal caso o principal pressuposto para a consecução dos ‘acertamentos e buscas’ à iniciativa da polícia judiciária”. Isso porque, como ressalta a autora, “o caráter digital dos dados, das informações e dos programas inerentes a um sistema informático ou telemático integra *in re ipsa* o perigo de volatilização, tratando-se de elementos alteráveis em nível máximo”.²¹⁶

formalização dos atos em geral. O sistema jurídico precisará internalizar o fato de que a existência de um escrito não mais significa pressupor seu vínculo permanente a um objeto corpóreo.”

Documentos eletrônicos, assinaturas digitais: um estudo sobre a qualificação dos arquivos digitais como documentos. *Revista de Direito Privado*, vol. 6, p. 52, Abr / 2001.

²¹⁶ Le attività..., p. 143. Tradução livre. No original: “Il *corpus* normativo...è tutto improntato...alla situazione di ‘pericolo’ che le tracce e le cose pertinenti al reato e lo stato dei luoghi ‘si alterino, si disperdano o comunque si modifichino’ e identifica in tale evenienza il principale presupposto per il compimento di ‘accertamenti e rilievi’ a iniziativa di polizia giudiziaria. (...) Invero, il carattere digitale dei dati, delle informazioni e dei programmi inerenti a un sistema informatico o telematico integra *in re ipsa* il pericolo di volatilizzazione, trattandosi di elementi alterabili al massimo grado”.

Faz-se, por isso, necessária a previsão e especificação de medidas cautelares que, amparadas pela justa causa, possibilitem a coleta das provas digitais, no tempo adequado.

De outra parte, a alterabilidade exige a cautela na obtenção, conservação e análise das provas digitais, de modo a preservar sua integridade e autenticidade. Alerta Giovanni Ziccardi que “a potencial fonte de prova digital pode ser facilmente contaminada. A gestão da fonte de prova digital com instrumentos de *computer forensics* é muito delicada, vez que apresenta uma grande taxa de vulnerabilidade e de exposição a erros”.²¹⁷

Assim, a manipulação inadequada da prova digital pode acarretar a imprestabilidade da prova, que não deverá ser valorada no conjunto probatório, prejudicando o objetivo de eficiência do processo ou o exercício da defesa, como também pode levar a uma apreciação incorreta dos fatos, com base em provas alteradas²¹⁸. Esta situação pode decorrer de alteração consciente ou inconsciente da prova, com prejuízos à acusação ou à defesa.

Outrossim, a prova digital deve se tornar duradoura, garantida sua originalidade. Para tanto, além de ser fixada em uma base material acessível no futuro, impende a aplicação de dispositivos que preservem a integridade do conteúdo, como, por exemplo, o cálculo do *hash*.²¹⁹

Vale ainda observar que, em decorrência da capacidade de armazenamento de arquivos, a possibilidade de recuperação de dados, o registro de operações do sistema, bem como a acumulação de dados proporciona a aquisição de imensa quantidade de informações. Ao mesmo tempo em que esse fato é positivo, por admitir o acesso a mais elementos relevantes para a verificação dos fatos sob apuração, cria-se grande dificuldade na análise desses dados e em sua apresentação em juízo.²²⁰

Por fim, considerando a grande variedade de sistemas e a evolução da tecnologia, além da imprescindibilidade da intermediação de equipamentos eletrônicos, é preciso providenciar para que os dados digitais se façam acessíveis, permitindo o uso das informações armazenadas, mesmo em sistemas diversos ou mais avançados.

²¹⁷ *Informatica giuridica...*, p. 325. Tradução livre. No original: “la potenziale fonte di prova digitale può essere facilmente contaminata. La gestione della fonte di prova digitale con strumenti di *computer forensics* è molto delicata, dal momento che presenta un ampio tasso di vulnerabilità e di esposizione agli errori”.

²¹⁸ Lorenzetto. *Le attività...*, p. 162.

²¹⁹ A respeito do cálculo do *hash*, veja-se item adiante.

²²⁰ Segundo Giovanni Ziccardi, uma das características das fontes de prova digitais seria a existência de “potenciais provas demais”. *Informatica...*, p. 325.

Assim, com vistas à busca da verdade e à eficiência do processo, a obtenção e a produção da prova digital devem ser orientadas pelas finalidades de preservação, autenticidade ou genuinidade²²¹, durabilidade e acessibilidade dos dados digitais, assim como pela possibilidade de análise conjunta das informações coletadas. Esses procedimentos devem também ser pautados pelas garantias do devido processo legal, respeitando-se os direitos fundamentais, de modo a se obter prova válida e legítima.

Para isso, são imprescindíveis normas que prescrevam os procedimentos adequados para a aquisição, conservação, análise e produção dos dados digitais, complementando as regras probatórias existentes no ordenamento atual.

²²¹ “Non vi è dubbio, infatti, che la genuinità del dato digitale (concetto che convenzionalmente ricomprende in sé quelli di integrità e autenticità) costituisca un valore assoluto al quale devono conformarsi tutti i protagonisti del rito penale.” Lupária. La disciplina..., p. 147.

Giovanni Ziccardi refere como objeto de estudo da *computer forensics* o valor de um dado digital, concebendo-o como a “capacidade de resistência” a eventuais contestações e capacidade de convencimento do juiz, em relação à genuinidade, não repudiabilidade, imputabilidade e integridade do dado em si e do fato demonstrado. Le tecniche..., p. 11.

CAPÍTULO 4 - MEIOS DE OBTENÇÃO E DE PRODUÇÃO DA PROVA DIGITAL

Os dados digitais de interesse à persecução penal tanto podem estar armazenados em um dispositivo eletrônico, como podem estar trafegando por uma rede, em especial a internet. Assim, a coleta da fonte de prova para posterior introdução no processo penal pode ser realizada visando ao suporte físico ou apenas aos dados.

Giovanni Ziccardi refere três modalidades típicas de aquisição dos dados: “sequestro”, cópia e interceptação. Citando Ghirardini e Faggioli, o autor italiano afirma que “o sequestro nada mais é do que apreender fisicamente o suporte em que está o dado”; na cópia, “o suporte original é adquirido sob a forma de cópia das informações contidas nele e transferidas em outro suporte”; já a interceptação “prevê que o dado seja adquirido durante sua passagem de um sistema a outro”.²²²

Adaptando a lição ao contexto brasileiro, pode-se afirmar que a obtenção da prova digital ocorre por meio da apreensão dos suportes físicos, da apreensão remota de dados e da interceptação telemática.

No que se refere à produção, a prova pode ser apresentada em juízo, como os documentos, ou pode ser objeto de perícia, quando se mostrar necessário recorrer a conhecimentos técnicos específicos para a extração dos elementos de prova. Desse modo, aplicam-se os meios de prova documental e pericial.

O ordenamento jurídico brasileiro não contempla normas específicas sobre a obtenção e a produção da prova digital, o que conduz ao uso da analogia para o procedimento probatório ou à proibição do método probatório.

No plano internacional, por sua vez, destaca-se a Convenção sobre o Cibercrime do Conselho da Europa, firmada em Budapeste em 23 de novembro de 2001, pela qual os Estados-Partes se comprometeram a adotar as medidas legislativas para prever, em seu ordenamento, os crimes informáticos e o procedimento penal necessário à

²²² Le techniche..., p. 76-77. Tradução livre.

investigação ou instrução criminal. Nesse sentido, em 2008, a Itália editou a Lei nº 48 e, em 2009, Portugal promulgou a Lei nº 109.

Quanto à obtenção da prova digital, a Convenção prescreve a adoção de medidas para a preservação expedita de dados (art. 16), a preservação e a revelação expedita de dados de tráfego (art. 17), a ordem para apresentação de dados (art. 18), a busca e a apreensão de dados computacionais (art. 19), a obtenção de dados de tráfego em tempo real (art. 20) e a interceptação de comunicações de dados (art. 21).

A preservação expedita de dados consiste em uma ordem de “congelamento”, dirigida àquele que tenha a disponibilidade ou controle de dados informáticos armazenados em um sistema computacional, incluindo dados de tráfego, para que preserve esses dados até que as autoridades obtenham autorização para seu acesso.²²³

A preservação e a revelação expedita de dados de tráfego concernem a transmissão de dados. Trata-se de ordem para a preservação e a revelação dos dados de tráfego, de modo a permitir a identificação dos provedores de serviço e do caminho utilizado para a transmissão de tal comunicação.²²⁴

²²³ “Article 16 – Expedited preservation of stored computer data

1 Each Party shall adopt such legislative and other measures as may be necessary to enable its competent authorities to order or similarly obtain the expeditious preservation of specified computer data, including traffic data, that has been stored by means of a computer system, in particular where there are grounds to believe that the computer data is particularly vulnerable to loss or modification.

2 Where a Party gives effect to paragraph 1 above by means of an order to a person to preserve specified stored computer data in the person’s possession or control, the Party shall adopt such legislative and other measures as may be necessary to oblige that person to preserve and maintain the integrity of that computer data for a period of time as long as necessary, up to a maximum of ninety days, to enable the competent authorities to seek its disclosure. A Party may provide for such an order to be subsequently renewed.

3 Each Party shall adopt such legislative and other measures as may be necessary to oblige the custodian or other person who is to preserve the computer data to keep confidential the undertaking of such procedures for the period of time provided for by its domestic law.

4 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.”

²²⁴ “Article 17 – Expedited preservation and partial disclosure of traffic data

1 Each Party shall adopt, in respect of traffic data that is to be preserved under Article 16, such legislative and other measures as may be necessary to:

a) ensure that such expeditious preservation of traffic data is available regardless of whether one or more service providers were involved in the transmission of that communication; and

b) ensure the expeditious disclosure to the Party’s competent authority, or a person designated by that authority, of a sufficient amount of traffic data to enable the Party to identify the service providers and the path through which the communication was transmitted.

2 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.”

A ordem de apresentação de dados é dirigida à pessoa que tem a posse ou o controle dos dados computacionais ou ainda ao provedor de serviços em relação às informações de usuário, para que os apresente às autoridades competentes.²²⁵

No que se refere à busca e à apreensão, a Convenção não distingue a diligência efetuada sobre os suportes físicos daquela realizada remotamente. Os Estados devem prever medidas que confirmem poder às autoridades para apreender ou de maneira similar assegurar a preservação de um sistema computacional ou de um meio de armazenamento de dados, promover e custodiar a cópia dos dados computacionais, manter a integridade dos dados relevantes e tornar inacessível ou remover os dados computacionais no sistema informático acessado.²²⁶

²²⁵ “Article 18 – Production order

1 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to order:

- a) a person in its territory to submit specified computer data in that person’s possession or control, which is stored in a computer system or a computer-data storage medium; and
- b) a service provider offering its services in the territory of the Party to submit subscriber information relating to such services in that service provider’s possession or control.

2 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.

3 For the purpose of this article, the term “subscriber information” means any information contained in the form of computer data or any other form that is held by a service provider, relating to subscribers of its services other than traffic or content data and by which can be established:

- a) the type of communication service used, the technical provisions taken thereto and the period of service;
- b) the subscriber’s identity, postal or geographic address, telephone and other access number, billing and payment information, available on the basis of the service agreement or arrangement;
- c) any other information on the site of the installation of communication equipment, available on the basis of the service agreement or arrangement.”

²²⁶ “Article 19 – Search and seizure of stored computer data

1 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to search or similarly access:

- a) a computer system or part of it and computer data stored therein; and
- b) a computer-data storage medium in which computer data may be stored in its territory.

2 Each Party shall adopt such legislative and other measures as may be necessary to ensure that where its authorities search or similarly access a specific computer system or part of it, pursuant to paragraph 1.a, and have grounds to believe that the data sought is stored in another computer system or part of it in its territory, and such data is lawfully accessible from or available to the initial system, the authorities shall be able to expeditiously extend the search or similar accessing to the other system.

3 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to seize or similarly secure computer data accessed according to paragraphs 1 or 2. These measures shall include the power to:

- a) seize or similarly secure a computer system or part of it or a computer-data storage medium;
- b) make and retain a copy of those computer data;
- c) maintain the integrity of the relevant stored computer data;
- d) render inaccessible or remove those computer data in the accessed computer system.

4 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to order any person who has knowledge about the functioning of the computer system or measures applied to protect the computer data therein to provide, as is reasonable, the necessary information, to enable the undertaking of the measures referred to in paragraphs 1 and 2.

5 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.”

A obtenção de dados de tráfego em tempo real corresponde à coleta ou registro de dados de tráfego de determinadas comunicações, pelo emprego de meios técnicos ou pela adoção de medidas dirigidas ao provedor de serviços com o intuito de compeli-lo a disponibilizar esses dados.²²⁷

Por fim, a Convenção prevê a interceptação de dados, para a coleta ou registro de dados informáticos de conteúdo, em tempo real, também por meios técnicos ou por medidas dirigidas ao provedor de serviços.²²⁸

Passa-se, então, ao exame específico dos procedimentos para obtenção e produção da prova digital no Processo Penal brasileiro, comparando-se com as previsões do Direito estrangeiro. Não serão examinadas as medidas relacionadas à obtenção de dados de tráfego, vez que se situam fora do escopo do trabalho.

²²⁷ “Article 20 – Real-time collection of traffic data

1 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to:

a) collect or record through the application of technical means on the territory of that Party, and
b) compel a service provider, within its existing technical capability:
i) to collect or record through the application of technical means on the territory of that Party; or
ii) to co-operate and assist the competent authorities in the collection or recording of, traffic data, in real-time, associated with specified communications in its territory transmitted by means of a computer system.

2 Where a Party, due to the established principles of its domestic legal system, cannot adopt the measures referred to in paragraph 1.a, it may instead adopt legislative and other measures as may be necessary to ensure the real-time collection or recording of traffic data associated with specified communications transmitted in its territory, through the application of technical means on that territory.

3 Each Party shall adopt such legislative and other measures as may be necessary to oblige a service provider to keep confidential the fact of the execution of any power provided for in this article and any information relating to it.

4 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.”

²²⁸ “Article 21 – Interception of content data

1 Each Party shall adopt such legislative and other measures as may be necessary, in relation to a range of serious offences to be determined by domestic law, to empower its competent authorities to:

a) collect or record through the application of technical means on the territory of that Party, and
b) compel a service provider, within its existing technical capability:
i) to collect or record through the application of technical means on the territory of that Party, or
ii) to co-operate and assist the competent authorities in the collection or recording of, content data, in real-time, of specified communications in its territory transmitted by means of a computer system.

2 Where a Party, due to the established principles of its domestic legal system, cannot adopt the measures referred to in paragraph 1.a, it may instead adopt legislative and other measures as may be necessary to ensure the real-time collection or recording of content data on specified communications in its territory through the application of technical means on that territory.

3 Each Party shall adopt such legislative and other measures as may be necessary to oblige a service provider to keep confidential the fact of the execution of any power provided for in this article and any information relating to it.

4 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.”

4.1 Busca e apreensão

A busca e a apreensão são medidas relacionadas ao intuito de recolha e preservação de possíveis provas úteis ao processo penal. Trata-se, porém, de institutos diversos, dotados de autonomia, vez que um pode ocorrer independentemente do outro.

Como leciona Sergio Marcos de Moraes Pitombo:²²⁹

“(...) a apreensão, no mais das vezes, segue a busca. Emerge, daí, o costume de vê-las unidas. Conceitos que se teriam fundido, como se fossem uma e mesma coisa, ou objetivamente, inseparáveis. As buscas, contudo, se distinguem da apreensão, como os meios diferem dos fins.”

Essa lição é complementada por Cleunice Bastos Pitombo que, em estudo específico sobre o tema, lembra que a busca pode ter finalidades diversas da apreensão, como a prisão, por exemplo. A autora afirma que “a autonomia dos institutos verifica-se, também, pela eventualidade de apreensão sem busca, ocorrente na exibição voluntária do que se procura”.²³⁰

A busca é definida por Cleunice Bastos Pitombo como “ato do procedimento persecutivo penal, restritivo de direito individual (inviolabilidade da intimidade, vida privada, domicílio e da integridade física ou moral), consistente em procura, que pode ostentar-se na *revista* ou no *varejamento*”, conforme se trate de pessoa, coisa ou vestígio.²³¹

Quanto à apreensão, assim define a autora: “ato processual penal, subjetivamente complexo, de apossamento, remoção e guarda de coisas – objetos, papéis ou documentos -, de semoventes e de pessoas, ‘do poder de quem as retém ou detém’;

²²⁹ *Do seqüestro no processo penal brasileiro*. São Paulo: Bushatsky, 1973, p. 60.

²³⁰ *Da busca e da apreensão no processo penal*. 2ª Ed. São Paulo: RT, 2005, p. 103.

²³¹ *Da busca e da apreensão...*, p. 109.

tornando-as indisponíveis, ou as colocando sob custódia, enquanto importarem à instrução criminal ou ao processo”, podendo ser coercitiva ou espontânea.²³²

A busca e a apreensão consistem em medidas cautelares, tendo em vista que procuram assegurar a coleta de elementos necessários à persecução penal.²³³ De acordo com Adalberto de Camargo Aranha, trata-se de “medida cautelar de natureza criminal visando a assegurar a obtenção e a perpetuação de uma prova”, pois “consiste em assegurar não só a existência de uma prova criminal, como também evitar seu perecimento”.²³⁴

O Código de Processo Penal disciplina conjuntamente a busca e a apreensão no Capítulo XI de seu Título VII do Livro I. Contudo, a apreensão não é devidamente regulamentada, estabelecendo-se apenas a colocação da pessoa ou coisa sob custódia da autoridade (art. 245, §6º) e a lavratura de auto circunstanciado assinado por duas testemunhas presenciais (art. 245, §7º).

A finalidade e o objeto da busca são indicados pelo art. 240, §1º, do Código:

“§ 1º Proceder-se-á à busca domiciliar, quando fundadas razões a autorizarem, para:

- a) prender criminosos;
- b) apreender coisas achadas ou obtidas por meios criminosos;
- c) apreender instrumentos de falsificação ou de contrafação e objetos falsificados ou contrafeitos;
- d) apreender armas e munições, instrumentos utilizados na prática de crime ou destinados a fim delituoso;
- e) descobrir objetos necessários à prova de infração ou à defesa do réu;

²³² *Da busca e da apreensão...*, p. 230.

²³³ Pitombo, *Do seqüestro...*, p. 81. José Frederico Marques assim se refere a tais medidas: “Esses poderes [coercitivos] são exercidos através da chamada *busca e apreensão*, que é procedimento cautelar destinado a formar o corpo de delito e sobretudo o *corpus instrumentorum* do fato delituoso, mediante atos de coação da Polícia Judiciária.” *Elementos...*, vol. II, p. 309.

²³⁴ *Da prova...*, p. 270. Interessante a analogia feita por Cernelutti: “Ir en busca de las pruebas se asemeja muy a menudo, aun cuando la comparación pueda parecer pintoresca, a ir a la caza de mariposas: cuando se las ha cazado, es necesario conservarlas, y es una operación difícil por el peligro de inutilizarles las alas.” *Principios del proceso penal*. Buenos Aires: Ediciones Jurídicas Europa-América, 1971, p. 181.

- f) apreender cartas, abertas ou não, destinadas ao acusado ou em seu poder, quando haja suspeita de que o conhecimento do seu conteúdo possa ser útil à elucidação do fato;
- g) apreender pessoas vítimas de crimes;
- h) colher qualquer elemento de convicção.”

Efetua-se a busca, portanto, para o descobrimento de pessoa, coisa ou vestígios, em especial fontes de prova, que possam servir tanto à acusação quanto à defesa.²³⁵

A busca pode ser pessoal ou domiciliar²³⁶, devendo, como regra, ser precedida de mandado judicial, a não ser que se realize pessoalmente pela autoridade judicial²³⁷ ou que haja consentimento do envolvido.²³⁸

A busca pessoal dispensa o mandado, contanto que realizada no caso de prisão ou diante de fundada suspeita de que a pessoa esteja na posse de arma proibida ou de objetos ou papéis que constituam o corpo do delito, ou ainda no curso da busca domiciliar (art. 244).

A busca domiciliar, por seu turno, deve ser executada durante o dia, mediante mandado judicial devidamente fundamentado; e excepcionalmente, sem mandado, em caso de flagrante delito.

As limitações ao poder estatal para a realização da busca encontram fundamento na previsão constitucional do direito à intimidade e à privacidade (art. 5º, X) e da garantia da inviolabilidade do domicílio (art. 5º, XI).

²³⁵ Pitombo. *Da busca e da apreensão...*, p. 118.

²³⁶ O conceito de domicílio deve ser entendido de forma ampla, contemplando as disposições do Código Penal (art. 150) e do Código de Processo Penal (art. 246). Segundo Cleunice Bastos Pitombo, “a expressão ‘casa’ deve abranger: (a) a habitação definitiva, ou morada transitória; (b) casa própria, alugada, ou cedida; (c) dependências da casa, sendo cercadas, gradeadas ou muradas; (d) qualquer compartimento habitado; (e) aposento ocupado de habitação coletiva, em pensões, hotéis e em casas de pousada; (f) estabelecimentos comerciais e industriais, fechados ao público; (g) local onde se exerce atividade profissional, não aberto ao público; (h) barco, trailer, cabine de trem ou navio e barraca de acampamento; (i) áreas comuns de condomínio, vertical ou horizontal”. *Da busca e da apreensão...*, p. 72.

²³⁷ Camargo Aranha, *Da prova...*, p. 273. A respeito da atividade instrutória do juiz e da realização de diligências pessoalmente, em vista do resguardo da imparcialidade, veja-se o item 2.1 acima.

²³⁸ Com base no art. 139, V, da Constituição da República, costuma-se apontar que a exigência do mandado para a busca e apreensão em domicílio é suspensa durante o estado de sítio, em decorrência da restrição à inviolabilidade do domicílio.

Com relação ao procedimento da busca domiciliar, o Código de Processo Penal dispõe que se proceda à exibição e leitura do mandado, seguindo-se a entrada no local e a realização da procura. Se se tratar de pessoa ou coisa determinada, a busca ocorrerá se, intimado a mostrá-la, o morador se recusar a fazê-lo. Ao final, deve ser lavrado auto circunstanciado, assinado por duas testemunhas presenciais da diligência.²³⁹

A Lei nº 9.279/96, que cuida da proteção da propriedade industrial, estabelece regras especiais para a busca e a apreensão relacionadas à prova dos crimes ali tipificados. Assim, em complemento às normas ordinárias, essa Lei determina que, em caso de crime contra patente que tenha por objeto a invenção de processo, o oficial do juízo seja acompanhado por perito, que verificará, preliminarmente, a existência do ilícito, podendo ser feita a apreensão dos produtos em quantidade suficiente à elaboração do exame de corpo do delito.²⁴⁰ A Lei também se preocupa em determinar que, “tratando-se de estabelecimentos industriais ou comerciais legalmente organizados e que estejam funcionando publicamente”, as diligências devem se limitar à vistoria e apreensão, “não podendo ser paralisada a sua atividade lícitamente exercida” (art. 204). Além da diligência preliminar, prevê-se a apreensão e a destruição da marca falsificada, alterada ou imitada (art. 202).

No que se refere à prova digital, também se faz necessária a previsão de regras especiais, a exemplo do que ocorre com o procedimento probatório nos crimes contra a propriedade industrial.

Neste caso, a diligência poderá ter a finalidade de apreender informações que sirvam à prova dos fatos (art. 240, §1º, *e e h*); apreender arquivos digitais obtidos por meios criminosos (art. 240, §1º, *b*), como o vazamento de informações reservadas (art. 153, §1º-A, do Código Penal); apreender arquivos digitais falsificados, assim como programas falsificados ou contrafeitos ou utilizados para esse fim (art. 240, §1º, *c*); apreender os dispositivos eletrônicos que tenham sido utilizados na prática do crime (art. 240, §1º, *d*).

Da mesma forma que na cautelar dirigida aos documentos, a busca e a apreensão da prova digital devem ser autorizadas por decisão judicial devidamente fundamentada, expedindo-se o respectivo mandado. Este deve conter o local da diligência e a pessoa a ele relacionada, assim como o motivo e os fins da medida, precisando-se quais

²³⁹ Adalberto Camargo Aranha ressalta que as testemunhas presenciais “são pessoas que assistiram à apreensão e que, no futuro, se necessário, poderão depor e testemunhar a realização do ato assistido, sua forma de execução”. *Da prova...*, p. 275.

²⁴⁰ Pitombo. *Da busca e da apreensão...*, p. 288.

os fatos e delitos investigados e os objetos a serem buscados. O mandado há que esclarecer, ademais, quais equipamentos podem ser apreendidos, se deve ocorrer a apreensão física ou o espelhamento, qual a destinação a ser dada a essas mídias, e demais informações que possam definir claramente os contornos da medida cautelar.

A diligência poderá ocorrer no domicílio do investigado ou envolvido, assim como em outros locais onde se encontrem servidores externos que armazenem a informação que se quer obter.²⁴¹

A busca será dirigida à localização dos dispositivos eletrônicos²⁴² – tais como, computadores, *netbooks*, *tablets*, *smartphones*, etc. - que possam conter os elementos de interesse para a investigação. Não se deve, porém, proceder à apreensão indiscriminada de todos e quaisquer objetos eletrônicos que se encontrem no local. É preciso que haja relação com os fatos e com os sujeitos envolvidos. Assim, em uma apuração de *insider trading*, não é cabível a apreensão de aparelho de mp3 do investigado, a não ser que haja indício de armazenamento de informações relevantes nesse dispositivo. Do mesmo modo, no exemplo citado, não se mostra possível a apreensão de equipamentos de todos os moradores do local, como os filhos do investigado, ou de terceiros desvinculados da pessoa atingida pela medida ou dos fatos apurados.

Em virtude da volatilidade do dado digital destacada anteriormente, é preciso que a diligência seja acompanhada por perito ou técnico em informática, a fim de garantir a preservação e a autenticidade da prova²⁴³. Referida exigência deve constar do mandado de busca e apreensão.

Além disso, não deve haver a intervenção no dispositivo eletrônico, para verificação de seu conteúdo, posto que esta operação pode ocasionar a alteração dos dados. Ao contrário, devem ser identificados os equipamentos de interesse, para que sejam apreendidos ou copiados pelo *expert*.

²⁴¹ Como asseveram Helena Regina Lobo da Costa e Marcel Leonardi, não poderá haver apreensão de dados armazenados em servidor externo se o endereço onde se localiza o equipamento não consta do mandado de busca e apreensão, ou se não há ordem judicial autorizando que a diligência se realize de forma remota. *Busca e apreensão...*, p. 203.

²⁴² Giovanni Ziccardi, citando Eoghan Casey, enumera os itens que devem ser procurados na cena do crime: *hardwares* que possam conter informações; *softwares*, caso a prova tenha sido criada com a utilização de programas pouco comuns; mídias removíveis, como fitas de *backup*; documentos relacionados ao hardware, software e mídias removíveis; senhas, números de telefone e informações sobre contas de usuário; impressões jogadas no lixo; outros vestígios digitais. *Le tecniche...*, p. 78.

²⁴³ Mittermaier utiliza o termo “legitimidade” ao tratar do valor do documento, asseverando que: “Para que un documento haga entera fe, debe satisfacer una condición esencial, a saber: la de la legitimidad; esto es, que se reproduzca exacta y fielmente en el estado en que salió de manos de su autor.” *Tratado de la prueba en matéria criminal*. 9ª Ed. Madrid: Instituto Editorial Reus, 1959, p. 413.

Os procedimentos a serem adotados devem seguir os protocolos internacionais, que dispõem sobre as *best practices* da atividade de *computer forensics*.

Nesse passo, interessa indicar que o ordenamento jurídico italiano, com escopo de se conformar com as previsões da Convenção sobre Cibercrime do Conselho da Europa, sofreu alterações em seu Código de Processo Penal, por meio da Lei nº 48/2008, no que respeita à inspeção, busca e apreensão, ali denominadas *ispezione*, *perquisizione* e *sequestro*.

Essa mudança na legislação italiana não estabeleceu, contudo, procedimentos técnicos²⁴⁴. De maneira geral, previu-se a possibilidade de as medidas recaírem sobre sistemas informáticos e telemáticos, bem como a exigência de conservação dos dados originais e de se impedir sua alteração.²⁴⁵

Ademais, dispôs-se sobre a possibilidade de a autoridade judiciária determinar a realização de cópia dos dados informáticos em suporte adequado, com a preservação do original.²⁴⁶

²⁴⁴ Referindo-se à inspeção e à busca, Gianluca Braghò anota que “il minimo comune denominatore della disciplina stabilita per i due mezzi di ricerca della prova rimane l’obbligatoria adozione delle misure tecniche che salvaguardino la genuinità dei dati originali e che siano atte ad impedirne l’alterazione (...) La scelta dei protocolli procedurali è rimessa all’discrezionalità e alle capacità professionali degli organi inquirenti, in relazione alle migliori pratiche che gli standard internazionali hanno affermato sino a un determinato termine operativo.” L’ispezione..., p. 195.

²⁴⁵ Nesse sentido, o artigo 247, que trata das hipóteses de busca:

“Art. 247 Casi e forme delle perquisizioni.

1. Quando vi è fondato motivo di ritenere che taluno occulti sulla persona il corpo del reato o cose pertinenti al reato, è disposta perquisizione personale. Quando vi è fondato motivo di ritenere che tali cose si trovino in un determinato luogo ovvero che in esso possa eseguirsi l’arresto dell’imputato o dell’evaso, è disposta perquisizione locale. 1-bis. Quando vi è fondato motivo di ritenere che dati, informazioni, programmi informatici o tracce comunque pertinenti al reato si trovino in un sistema informatico o telematico, ancorchè protetto da misure di sicurezza, ne è disposta la perquisizione, adottando misure tecniche dirette ad assicurare la conservazione dei dati originali e ad impedirne l’alterazione. 2. La perquisizione è disposta con decreto motivato. 3. L’autorità giudiziaria può procedere personalmente ovvero disporre che l’atto sia compiuto da ufficiali di polizia giudiziaria delegati con lo stesso decreto.”

Assim também, o artigo 259, ao tratar da custódia do objeto da apreensão:

“Art. 259 Custodia delle cose sequestrate.

1. Le cose sequestrate sono affidate in custodia alla cancelleria o alla segreteria. Quando ciò non è possibile o non è opportuno, l’autorità giudiziaria dispone che la custodia avvenga in luogo diverso, determinandone il modo e nominando un altro custode, idoneo a norma dell’articolo 120. 2. All’atto della consegna, il custode è avvertito dell’obbligo di conservare e di presentare le cose a ogni richiesta dell’autorità giudiziaria nonché delle pene previste dalla legge penale per chi trasgredisce ai doveri della custodia. Quando la custodia riguarda dati, informazioni o programmi informatici, il custode è altresì avvertito dell’obbligo di impedirne l’alterazione o l’accesso da parte di terzi, salva, in quest’ultimo caso, diversa disposizione dell’autorità giudiziaria. Al custode può essere imposta una cauzione. Dell’avvenuta consegna, dell’avvertimento dato e della cauzione imposta è fatta menzione nel verbale. La cauzione è ricevuta, con separato verbale, nella cancelleria o nella segreteria.”

²⁴⁶ Nesse sentido, os artigos 254-bis e 260:

No ordenamento português, igualmente, não houve previsão do procedimento a ser adotado. Porém, com base na Convenção, foram indicadas as formas da apreensão, ordenando-se a duplicação da cópia, no caso da eleição dessa forma de coleta da prova. É o que se extrai dos itens 7 e 8 do artigo 16 da Lei nº 109/2009:

“7 - A apreensão de dados informáticos, consoante seja mais adequado e proporcional, tendo em conta os interesses do caso concreto, pode, nomeadamente, revestir as formas seguintes:

- a) Apreensão do suporte onde está instalado o sistema ou apreensão do suporte onde estão armazenados os dados informáticos, bem como dos dispositivos necessários à respectiva leitura;
- b) Realização de uma cópia dos dados, em suporte autónomo, que será junto ao processo;

“Art. 254-bis Sequestro di dati informatici presso fornitori di servizi informatici, telematici e di telecomunicazioni.

1. L'autorità giudiziaria, quando dispone il sequestro, presso i fornitori di servizi informatici, telematici o di telecomunicazioni, dei dati da questi detenuti, compresi quelli di traffico o di ubicazione, può stabilire, per esigenze legate alla regolare fornitura dei medesimi servizi, che la loro acquisizione avvenga mediante copia di essi su adeguato supporto, con una procedura che assicuri la conformità dei dati acquisiti a quelli originali e la loro immodificabilità. In questo caso è, comunque, ordinato al fornitore dei servizi di conservare e proteggere adeguatamente i dati originali.”

“Art. 260 Apposizione dei sigilli alle cose sequestrate. Cose deperibili.

1. Le cose sequestrate si assicurano con il sigillo dell'ufficio giudiziario e con le sottoscrizioni dell'autorità giudiziaria e dell'ausiliario che la assiste ovvero, in relazione alla natura delle cose, con altro mezzo, anche di carattere elettronico o informatico, idoneo a indicare il vincolo imposto a fini di giustizia. 2. L'autorità giudiziaria fa estrarre copia dei documenti e fa eseguire fotografie o altre riproduzioni delle cose sequestrate che possono alterarsi o che sono di difficile custodia, le unisce agli atti e fa custodire in cancelleria o segreteria gli originali dei documenti, disponendo, quanto alle cose, in conformità dell'articolo 259. Quando si tratta di dati, di informazioni o di programmi informatici, la copia deve essere realizzata su adeguati supporti, mediante procedura che assicuri la conformità della copia all'originale e la sua immodificabilità; in tali casi, la custodia degli originali può essere disposta anche in luoghi diversi dalla cancelleria o dalla segreteria. 3. Se si tratta di cose che possono alterarsi, l'autorità giudiziaria ne ordina, secondo i casi, l'alienazione o la distruzione. 3-bis. L'autorità giudiziaria procede, altresì, anche su richiesta dell'organo accertatore alla distruzione delle merci di cui sono comunque vietati la fabbricazione, il possesso, la detenzione o la commercializzazione quando le stesse sono di difficile custodia, ovvero quando la custodia risulta particolarmente onerosa o pericolosa per la sicurezza, la salute o l'igiene pubblica ovvero quando, anche all'esito di accertamenti compiuti ai sensi dell'articolo 360, risulti evidente la violazione dei predetti divieti. L'autorità giudiziaria dispone il prelievo di uno o più campioni con l'osservanza delle formalità di cui all'articolo 364 e ordina la distruzione della merce residua. 3-ter. Nei casi di sequestro nei procedimenti a carico di ignoti, la polizia giudiziaria, decorso il termine di tre mesi dalla data di effettuazione del sequestro, può procedere alla distruzione delle merci contraffatte sequestrate, previa comunicazione all'autorità giudiziaria. La distruzione può avvenire dopo 15 giorni dalla comunicazione salva diversa decisione dell'autorità giudiziaria. E' fatta salva la facoltà di conservazione di campioni da utilizzare a fini giudiziari.”

c) Preservação, por meios tecnológicos, da integridade dos dados, sem realização de cópia nem remoção dos mesmos; ou

d) Eliminação não reversível ou bloqueio do acesso aos dados.

8 - No caso da apreensão efectuada nos termos da alínea b) do número anterior, a cópia é efectuada em duplicado, sendo uma das cópias selada e confiada ao secretário judicial dos serviços onde o processo correr os seus termos e, se tal for tecnicamente possível, os dados apreendidos são certificados por meio de assinatura digital.”

De outra senda, ambos os ordenamentos não dispõem sobre a forma de registro do objeto da apreensão.

Contudo, é de se ressaltar a importância da lavratura, ao final do cumprimento da medida, de auto detalhado sobre a diligência e os objetos apreendidos, como nos documentos tradicionais.

Examinando o Código brasileiro, sustenta Adalberto Camargo Aranha que, tendo em vista a menção a “auto circunstanciado” e considerando circunstância “tudo o que se considera como fato principal”, “a peça deve conter uma narrativa plena sobre o que foi apreendido, com descrição completa, onde e como”.²⁴⁷

Não obstante, os requisitos do auto não são delineados pelo Código de Processo Penal. Essa conclusão decorre da leitura de seu art. 245, §7º, que se limita a ordenar a lavratura do auto, sem tratar de seu conteúdo.²⁴⁸

Nesse passo, acolhe-se a lição de Cleunice Bastos Pitombo, que sustenta a necessidade de individualização daquilo que foi apreendido, com apontamento de todas as suas características, asseverando, ainda, que a lei comum deveria incorporar (e alargar) os requisitos do auto que se encontram dispostos no Código de Processo Penal Militar, em seu artigo 189, parágrafo único²⁴⁹:

²⁴⁷ *Da prova...*, p. 275.

²⁴⁸ O projeto do novo Código de Processo Penal não resolve a questão, repetindo, nesse ponto, os dispositivos do Código atual.

²⁴⁹ *Da busca e da apreensão...*, p. 272-273.

“Art. 189. Finda a diligência, lavrar-se-á auto circunstanciado da busca e apreensão, assinado por duas testemunhas, com declaração do lugar, dia e hora em que se realizou, com citação das pessoas que a sofreram e das que nelas tomaram parte ou as tenham assistido, com as respectivas identidades, bem como de todos os incidentes ocorridos durante a sua execução.

Conteúdo do auto

Parágrafo único. Constarão do auto, ou dêle farão parte em anexo devidamente rubricado pelo executor da diligência, a relação e descrição das coisas apreendidas, com a especificação:

- a) se máquinas, veículos, instrumentos ou armas, da sua marca e tipo e, se possível, da sua origem, número e data da fabricação;
- b) se livros, o respectivo título e o nome do autor;
- c) se documentos, a sua natureza.”

Como a autora ressalta:

“A elaboração de auto minucioso ostenta-se como garantia de todos os envolvidos no ato processual, subjetivamente complexo: presidente, futor, sujeito paciente e testemunhas.

Presta-se, ainda, o auto a fixar o estado real do que se apreendeu, forçando-lhe a guarda e proteção; primeiro, no interesse do processo; depois, por motivo de eventual depósito, entrega ou restituição.”²⁵⁰

Na apreensão de dispositivos eletrônicos, é preciso que haja a descrição do equipamento, com indicação da marca, modelo, número de série e do lacre que se lhe anexe, bem como do local e condições em que se encontrava e da hora exata da diligência.

Caso se proceda à cópia da memória do dispositivo, cumpre registrar o procedimento adotado, a descrição do equipamento originário, bem como do suporte que recebeu a cópia, anotando-se o valor do *hash* calculado para a preservação do conteúdo.²⁵¹

²⁵⁰ *Da busca e da apreensão...*, p. 273.

Releva, ainda, a elaboração de uma **cadeia de custódia** (*chain of custody*), documento que registra a transferência do equipamento entre custodiantes, bem como os procedimentos adotados por cada um deles. Esclarece Giovanni Ziccardi a esse respeito²⁵²:

“Uma cadeia de custódia, inclusive no âmbito das empresas, é um simples processo usado para manter e documentar, em detalhes, a história cronológica da investigação, compreendidas a coleta, gestão e preservação da prova, juntamente com um registro de quaisquer pessoas que tenham tido contato com ela. A cadeia de custódia deve mostrar em cada momento que a prova foi coletada do sistema em referência e que foi memorizada e gerida sem alterações.”

Como indica Luca Lupária, a cadeia de custódia visa a assegurar a continuidade probatória, para proteger a genuinidade da prova digital. Segundo ele, “a manutenção da *chain of custody* em matéria de investigação informática demanda então uma completa anotação das várias passagens ‘físicas’ e ‘informáticas’ ocorridas no momento da apreensão do dado e na sucessiva fase de conservação”.²⁵³

Como se nota, a busca e a apreensão da prova digital podem ser realizadas segundo as regras atualmente existentes no Código de Processo Penal. Todavia, são imprescindíveis normas específicas que contemplem a exigência de perito na diligência, a forma a ser adotada para o procedimento e os requisitos do registro da apreensão. Essas normas são essenciais para a segurança dos envolvidos no procedimento, para a acuidade das informações referentes ao cumprimento da medida e para a proteção da autenticidade da prova.

²⁵¹ O glosário do Manual de Boas Práticas da Associação dos Chefes de Polícia do Reino Unido explica que o *hash* é um algoritmo que, quando aplicado a um disco rígido, cria um valor único. Se houver a alteração dos dados contidos no disco, o valor do *hash* será alterado. Walden, *Computer crimes...*, p. 464.

²⁵² Le tecniche..., p. 92-93. Tradução livre. No original: “Una catena di custodia, anche nella *corporate forensics*, è un semplice processo usato per mantenere e documentare, nel dettaglio, la storia cronologica dell’investigazione, compresa la raccolta, gestione, e preservazione della prova, insieme a un *record* di chiunque sia venuto in contatto con la prova. La catena di custodia dovrebbe mostrare in ogni momento che la prova è stata raccolta dal sistema in oggetto, e che è stata memorizzata e gestita senza alterazioni.”

²⁵³ La disciplina..., p. 149. Tradução livre. No original: “Il mantenimento della *chain of custody* in materia di investigazioni informatiche richiede allora una completa annotazione dei vari passaggi ‘fisici’ e ‘informatici’ compiuti al momento dell’apprensione del dato e nella successiva fase di conservazione (...).”

4.2 Apreensão remota de dados e infiltração

No item precedente, foram abordados os temas da obtenção dos suportes físicos e da extração dos dados digitais pertinentes. Cabe, então, analisar as formas pelas quais as informações contidas em meios digitais podem ser obtidas de maneira remota.

Nesse sentido, cuida-se de verificar os meios que permitem o monitoramento eletrônico de pessoas ou empresas. Como explanado, além do registro de informações em formato digital, tem-se atualmente a constante troca de dados pelas redes virtuais, havendo também a possibilidade de acesso a dados armazenados em um dispositivo, através da conexão em rede. Por essa razão, surgem outras possibilidades de obtenção de dados digitais, sem necessidade de violação do domicílio e restrição do direito de propriedade. Trata-se de medidas que também se caracterizam pela discrição, podendo ser realizadas sem o conhecimento de seus alvos.²⁵⁴

Pode-se apontar as seguintes formas de obtenção de dados digitais, de maneira remota ou virtual:

- interceptação telemática, objeto do item seguinte, por meio da qual se coletam informações transmitidas em rede;
- busca e apreensão remota de dados, que consiste no acesso a sistema informático, de maneira remota, para se proceder à pesquisa e cópia dos dados informáticos;

²⁵⁴ Sustentando a possibilidade, no ordenamento atual, de se promoverem buscas e apreensões digitais, mediante “circunstanciada decisão judicial”, Diego Fajardo Maranhã Leão de Souza descreve a relevância e as vantagens do procedimento:

“Ocorre que, em tempo presente, é cada vez mais rotineiro presenciar operações policiais em que dezenas de computadores são apreendidos apenas com o escopo de serem capturados os dados armazenados em seus discos rígidos. Em se tratando de grupos organizados, criminalidade econômica e financeira ou delitos virtuais, como a propagação de pornografia infantil, é factível que dados da mais alta importância para a constituição do quadro probatório estejam armazenados remotamente, em servidores situados em outras cidades, estados ou até mesmo países. Esses dados estariam disponíveis apenas nos breves momentos em que acessados pelo investigado, sendo quaisquer vestígios locais eliminados imediatamente, o que tornaria inócua a busca e apreensão tradicional. Numa atividade de ação controlada, também poderia ser de interesse do órgão de investigação ter acesso aos dados do crime sem que o investigado percebesse, fazendo coleta periódica de informações à distância, por meio de acesso virtual, até o melhor momento do ponto de vista da formação da prova. Do lado do imputado, uma busca digital permitiria que continuasse de posse de sua estrutura de informática, já que a apreensão prolongada de computadores e milhares e arquivos pode inviabilizar irreversivelmente a atividade econômica de uma empresa.” Busca e apreensão digital: prova penal atípica. *Boletim IBCCRIM*, São Paulo, ano 15, n. 181, p.14-15, dez. 2007.

- infiltração em sistema informático, mediante a implantação de dispositivo (*software*) que permita o monitoramento do sistema atingido, visualizando-se todas as ações praticadas e eventualmente copiando-se os dados respectivos;

- captação de dados informáticos, por meio da instalação de programas maliciosos, que enviam informações do sistema atingido.

Contemplando as novas tecnologias, encontram-se, no direito comparado, previsões de medidas de obtenção remota de dados.

No Direito português, tem-se a Lei n.º 109/2009, Lei do Cibercrime, que transpõe “para a ordem jurídica interna a Decisão Quadro n.º 2005/222/JAI, do Conselho, de 24 de Fevereiro, relativa a ataques contra sistemas de informação, e adapta o direito interno à Convenção sobre Cibercrime do Conselho da Europa”. A Lei prevê a pesquisa de dados informáticos (art. 15) e sua apreensão (art. 16), assim como a ação encoberta em “ambiente electrónico-digital” (art. 19).

A pesquisa de dados informáticos²⁵⁵ consiste em uma forma oculta de investigação, pela qual se pretende a obtenção de dados específicos e determinados, armazenados em certo sistema informático. O enunciado normativo deixa claro que a pesquisa é realizada quando necessária à produção da prova, durante o processo, ou seja, não se autoriza uma busca livre e desenfreada apartada de um procedimento inquisitório.

²⁵⁵ “Artigo 15.º

Pesquisa de dados informáticos

1 - Quando no decurso do processo se tornar necessário à produção de prova, tendo em vista a descoberta da verdade, obter dados informáticos específicos e determinados, armazenados num determinado sistema informático, a autoridade judiciária competente autoriza ou ordena por despacho que se proceda a uma pesquisa nesse sistema informático, devendo, sempre que possível, presidir à diligência.

2 - O despacho previsto no número anterior tem um prazo de validade máximo de 30 dias, sob pena de nulidade.

3 - O órgão de polícia criminal pode proceder à pesquisa, sem prévia autorização da autoridade judiciária, quando:

a) A mesma for voluntariamente consentida por quem tiver a disponibilidade ou controlo desses dados, desde que o consentimento prestado fique, por qualquer forma, documentado;

b) Nos casos de terrorismo, criminalidade violenta ou altamente organizada, quando haja fundados indícios da prática iminente de crime que ponha em grave risco a vida ou a integridade de qualquer pessoa.

4 - Quando o órgão de polícia criminal proceder à pesquisa nos termos do número anterior:

a) No caso previsto na alínea b), a realização da diligência é, sob pena de nulidade, imediatamente comunicada à autoridade judiciária competente e por esta apreciada em ordem à sua validação;

b) Em qualquer caso, é elaborado e remetido à autoridade judiciária competente o relatório previsto no artigo 253.º do Código de Processo Penal.

5 - Quando, no decurso de pesquisa, surgirem razões para crer que os dados procurados se encontram noutra sistema informático, ou numa parte diferente do sistema pesquisado, mas que tais dados são legitimamente acessíveis a partir do sistema inicial, a pesquisa pode ser estendida mediante autorização ou ordem da autoridade competente, nos termos dos n.os 1 e 2.

6 - À pesquisa a que se refere este artigo são aplicáveis, com as necessárias adaptações, as regras de execução das buscas previstas no Código de Processo Penal e no Estatuto do Jornalista.”

A medida deve ser precedida de autorização judicial, que ostenta prazo de validade de 30 dias. Havendo indicação de que os dados procurados se encontrem em outro sistema informático ou em parte diferente do mesmo sistema, desde que acessíveis a partir do sistema inicial, permite-se a extensão da pesquisa mediante autorização judicial.

A Lei excepciona a obrigatoriedade da precedência de ordem judicial para a pesquisa quando esta for “voluntariamente consentida por quem tiver a disponibilidade ou controlo desses dados, desde que o consentimento prestado fique, por qualquer forma, documentado”²⁵⁶ ou nos “casos de terrorismo, criminalidade violenta ou altamente organizada, quando haja fundados indícios da prática iminente de crime que ponha em grave risco a vida ou a integridade de qualquer pessoa”.

Ainda, a Lei restringe a medida, com fundamento na proteção ao sigilo, consoante as disposições do Estatuto do Jornalista.

O mesmo ocorre com a apreensão de dados contidos em “sistemas informáticos utilizados para o exercício da advocacia e das actividades médica e bancária” ou “para o exercício da profissão de jornalista”, quando se aplicam as normas do Código de Processo Penal e do Estatuto do Jornalista.

Como regra, o procedimento a ser adotado para a pesquisa é aquele previsto para a execução de buscas, segundo o Código de Processo Penal português.

A apreensão pode ocorrer no decurso de uma pesquisa informática ou de outro acesso legítimo a um sistema informático, mediante autorização judicial. A apreensão pode ser feita pela polícia, sem prévia ordem judicial, se no curso de pesquisa legitimamente ordenada, ou quando haja urgência ou perigo na demora.

Em qualquer caso, as apreensões feitas pela polícia devem sempre ser sujeitas à validação judicial no prazo máximo de 72 horas.

Visando à proteção da intimidade e da privacidade, a Lei prescreve a análise do juiz sobre a eventual juntada aos autos dos “dados ou documentos informáticos cujo

²⁵⁶ A esse respeito, consigna Benjamim Silva Rodrigues: “No que respeita à alínea a), do n.º 3, do artigo 15.º, da LCiber 2009), ela merece-nos algumas reticências já que há um perigo, que não é meramente académica (sic), de os agentes actuarem de forma desleal, no sentido de que já tendo uma suspeita minimamente fundada, relativamente a um suspeito, e que já seria suficiente para o constituir arguido, se dirijam ao mesmo e, de forma ‘engenhosa, desleal e alguma artimanha’, lhe solicitem dados que o irão ‘auto-incriminar’ sem o informarem que lhe assiste o direito de prestar ou não a referida colaboração e que, por muito que seja, sempre existe um certo mínimo de perigo de a sua colaboração – consentimento – permitir o acesso a dados que doutro modo os órgãos nunca teriam acesso e, no entanto, serão fundamentais para a condenação do suspeito.” *Da prova penal: Tomo IV*, p. 527.

conteúdo seja susceptível de revelar dados pessoais ou íntimos, que possam pôr em causa a privacidade do respectivo titular ou de terceiro”.

Com relação à ação encoberta, admite-se sua aplicação, de acordo com as regras da interceptação, para os crimes previstos na própria Lei do Cibercrime e aqueles “cometidos por meio de um sistema informático, quando lhes corresponda, em abstracto, pena de prisão de máximo superior a 5 anos ou, ainda que a pena seja inferior, e sendo dolosos, os crimes contra a liberdade e autodeterminação sexual nos casos em que os ofendidos sejam menores ou incapazes, a burla qualificada, a burla informática e nas comunicações, a discriminação racial, religiosa ou sexual, as infracções económico-financeiras, bem como os crimes consagrados no título iv do Código do Direito de Autor e dos Direitos Conexos”.²⁵⁷

No Reino Unido, o monitoramento eletrônico é feito com base na lei que regula os poderes investigatórios, *Regulation of Investigatory Powers Act 2000* (RIPA), elaborada para adequar a legislação inglesa à orientação da Convenção Europeia de Direitos Humanos.²⁵⁸

O RIPA prevê o instituto da vigilância, que compreende: o monitoramento, observação e escuta de pessoas, seus movimentos, suas conversas e outras atividades ou comunicações; a gravação de qualquer coisa monitorada, observada ou ouvida durante a vigilância; e a vigilância por meio de ou com o auxílio de um equipamento próprio para esse fim.²⁵⁹

A vigilância pode ser direta, intrusiva ou pelo uso de uma fonte humana de inteligência encoberta.

²⁵⁷ “Artigo 19.º

Acções encobertas

1 - É admissível o recurso às acções encobertas previstas na Lei n.º 101/2001, de 25 de Agosto, nos termos aí previstos, no decurso de inquérito relativo aos seguintes crimes:

a) Os previstos na presente lei;

b) Os cometidos por meio de um sistema informático, quando lhes corresponda, em abstracto, pena de prisão de máximo superior a 5 anos ou, ainda que a pena seja inferior, e sendo dolosos, os crimes contra a liberdade e autodeterminação sexual nos casos em que os ofendidos sejam menores ou incapazes, a burla qualificada, a burla informática e nas comunicações, a discriminação racial, religiosa ou sexual, as infracções económico-financeiras, bem como os crimes consagrados no título iv do Código do Direito de Autor e dos Direitos Conexos.

2 - Sendo necessário o recurso a meios e dispositivos informáticos observam-se, naquilo que for aplicável, as regras previstas para a interceptação de comunicações.”

²⁵⁸ Walden, *Computer crimes...*, p. 215.

²⁵⁹ Walden, *Computer crimes...*, p. 215.

De acordo com Ian Walden, a vigilância direta não se mostra intrusiva e ocorre em um local público ou quase público, o que, no contexto da prova digital, pode corresponder a um cybercafé ou a uma rede remota, fora do local do investigado, como um provedor de internet. A medida, que normalmente resulta na obtenção de informações privadas sobre uma pessoa, é relacionada a uma investigação ou operação e deve ser necessária e proporcional ao alcance de objetivos determinados. Ela deve ser autorizada pelas autoridades indicadas na lei, tendo a duração de três meses, passível de renovação.²⁶⁰

Já a vigilância intrusiva volta-se a qualquer evento que ocorra em um local residencial ou em um veículo privado, podendo ser, no caso da prova digital, o computador do investigado. Nesse caso, a pessoa que conduz a vigilância está presente no local investigado ou utiliza-se um dispositivo de monitoramento, como um *spyware*²⁶¹. Por ser mais gravoso, este meio somente pode ser usado no caso de interesse da segurança nacional, crimes graves e bem-estar econômico do Reino Unido, necessitando de autorização do Secretário de Estado ou de um oficial sênior autorizador.²⁶²

Por último, o uso de uma fonte humana de inteligência encoberta consiste no uso de agente infiltrado. Esta medida deve ter uma autorização distinta, dada por oficiais autorizadores específicos, servindo para propósitos de segurança nacional, prevenção e detecção de crime ou desordem, o bem-estar econômico do Reino Unido, a saúde pública; questões fiscais, ou como especificado pelo Secretário de Estado. Ela dura por um período mínimo de doze meses.²⁶³

Na França, o Código de Processo Penal sofreu alterações, promovidas pela Lei “Perben II”, de 09 de março de 2004, que estabeleceu o procedimento aplicável à criminalidade organizada. Este procedimento foi objeto de alterações posteriores, dentre as quais, a previsão de obtenção de dados informáticos (seção 6-bis do capítulo II do título XXV do livro IV do Código), introduzida pela Lei nº 267, de 14 de março de 2011.

Segundo essa norma, o juiz de instrução pode, em decisão motivada, autorizar os oficiais e agentes de polícia judiciária a instalar um dispositivo técnico, tendo como objeto aceder, sem o consentimento dos interessados, a dados informáticos,

²⁶⁰ Walden, *Computer crimes...*, p.216-218.

²⁶¹ Trata-se de um programa malicioso, que é instalado no computador e capta informações do usuário, sem seu conhecimento.

²⁶² Walden, *Computer crimes...*, p. 218.

²⁶³ Walden, *computer crimes...*, p. 221-222.

gravando-os, conservando-os e transmitindo-os.²⁶⁴ A decisão deve conter a infração sob investigação, a localização exata ou a descrição detalhada do sistema informático alvo e a duração da medida. O prazo máximo legal é de 4 meses, podendo ser renovado, excepcionalmente, por igual período.²⁶⁵ Os dados privados que não se relacionem à infração não podem ser juntados aos autos.

O Direito brasileiro, por sua vez, somente disciplina a interceptação telemática, conforme se examinará no item seguinte. O Projeto de Lei nº 1.404/2011, que altera o Estatuto da Criança e do Adolescente prevê a infiltração de agentes na internet, seguindo procedimento mais assemelhado ao de infiltração de agentes propriamente e sem especificação de procedimento técnico.

Diante da inexistência de disciplina legal, tem-se que a obtenção remota de dados, com exceção da interceptação telemática, não pode ser utilizada como meio de pesquisa da prova digital, no Processo Penal brasileiro. A uma, porque se trata de medida assaz intrusiva, pela qual é possível o acesso a infinitos dados, atingindo severamente a esfera de intimidade e privacidade do indivíduo. A duas, porque apresenta o risco de alteração dos dados originais, não se podendo garantir a autenticidade da prova.

Como asseverado no capítulo 2, há de se considerar inadmissíveis as provas atípica - como a obtenção remota de dados, que nem sequer é nomeada no ordenamento -, quando a própria ausência de procedimento legal não permitir a segurança das partes, a proteção dos direitos e garantias fundamentais e a eficiência do processo.

²⁶⁴ “Article 706-102-1

Lorsque les nécessités de l'information concernant un crime ou un délit entrant dans le champ d'application de l'article 706-73 l'exigent, le juge d'instruction peut, après avis du procureur de la République, autoriser par ordonnance motivée les officiers et agents de police judiciaire commis sur commission rogatoire à mettre en place un dispositif technique ayant pour objet, sans le consentement des intéressés, d'accéder, en tous lieux, à des données informatiques, de les enregistrer, les conserver et les transmettre, telles qu'elles s'affichent sur un écran pour l'utilisateur d'un système de traitement automatisé de données ou telles qu'il les y introduit par saisie de caractères. Ces opérations sont effectuées sous l'autorité et le contrôle du juge d'instruction.”

²⁶⁵ “Article 706-102-2

A peine de nullité, les décisions du juge d'instruction prises en application de l'article 706-102-1 précisent l'infraction qui motive le recours à ces opérations, la localisation exacte ou la description détaillée des systèmes de traitement automatisé de données ainsi que la durée des opérations.”

“Article 706

Les décisions mentionnées à l'article 706-102-2 sont prises pour une durée maximale de quatre mois. Si les nécessités de l'instruction l'exigent, l'opération de captation des données informatiques peut, à titre exceptionnel et dans les mêmes conditions de forme, faire l'objet d'une prolongation supplémentaire de quatre mois.

Le juge d'instruction peut, à tout moment, ordonner l'interruption de l'opération.”

Excepcionalmente, pode-se admitir a busca e apreensão remota, em servidor determinado, no cumprimento de busca e apreensão tradicional, mediante ordem judicial específica e com o acompanhamento do interessado e eventualmente de seu advogado, vez que a medida não é cumprida de maneira oculta e permite o controle e a oposição da parte.

4.3 Intercepção telemática

A intercepção telemática²⁶⁶ constitui a única forma de apreensão de dados digitais mencionada na legislação brasileira. A par do debate sobre a constitucionalidade da medida, que será objeto de exame adiante, cumpre verificar as normas legais que disciplinam a intercepção das comunicações, a fim de examinar se atendem às finalidades de segurança das partes, proteção dos direitos fundamentais e eficiência do meio de prova.

Tal medida consiste na captação de dados em trânsito, que estejam sendo transmitidos por uma rede de dispositivos eletrônicos. Ela pode recair sobre um determinado serviço, como uma conta de *e-mail*, ou sobre toda a troca de dados por um endereço de IP²⁶⁷, hipótese em que são coletados *e-mails*, conversas em comunicadores instantâneos, sistemas VoIP, etc.

A Lei nº 9.296/96, que regulamentou a parte final do inciso XII do artigo 5º da Constituição da República, previu, no parágrafo único de seu artigo 1º, que suas disposições se aplicam “à intercepção do fluxo de comunicações em sistemas de informática e telemática”. Bem anotam Grinover, Magalhães Gomes Filho e Scarance Fernandes a inadequação do texto: “Em sentido técnico, só pela telemática pode haver a comunicação do fluxo de dados via telefone, donde já se vê a impropriedade da referência da lei à informática.”²⁶⁸

Diante da menção à intercepção das comunicações, vale observar que a comunicação significa a troca de mensagens entre indivíduos. Ela pode ela ser feita

²⁶⁶ A respeito do sentido do termo “telemática” e sua distinção com a “informática”, veja-se o item 3.1.

²⁶⁷ Veja-se o significado de endereço de IP no item 1.3.

²⁶⁸ *As nulidades...*, p.171.

pessoalmente, entre presentes, o que se denomina comunicação ambiental²⁶⁹, assim como por meio de correspondência, telefone e troca de dados.

Quanto à captação das comunicações, costumam ser utilizados os termos *interceptação*, *escuta* e *gravação clandestina*, para distinguir os diferentes modos de obtenção da prova.

A *interceptação* é referida como a captação da mensagem, por terceiro, sem o conhecimento dos interlocutores. A *escuta* consiste na captação feita por terceiro, com o conhecimento de, ao menos, um dos interlocutores. Por seu turno, a *gravação clandestina* configura-se com a gravação da conversa por um dos interlocutores, sem o conhecimento do(s) outro(s).^{270 271}

A Lei disciplinou apenas a interceptação, que tem por finalidade a prova em investigação criminal e em instrução processual penal. Apresenta-se, portanto, como medida cautelar orientada à obtenção de fonte de prova.²⁷²

Em consonância com a determinação constitucional, a Lei exige ordem judicial prévia, devidamente fundamentada, para a restrição do direito fundamental, como se extrai de seus artigos 1º, 3º e 5º.

No que se refere às hipóteses de cabimento desse meio de investigação, observa-se a má técnica legislativa, por serem definidas por exclusão. Isso porque a lei

²⁶⁹ Grinover et al. *As nulidades...*, p. 164; André Augusto Mendes Machado e André Pires de Andrade Kehdi, *Sigilo...*, p. 257.

²⁷⁰ Grinover et al. *As nulidades...*, p. 164; Damásio E. de Jesus. Interceptações de comunicações telefônicas: notas à Lei 9.296, de 24.07.1996. *Revista dos Tribunais*, São Paulo, ano 86, vol. 735, p. 458-473, jan. 1997, p. 460; Paulo Rangel. Breves considerações sobre a Lei 9.296/96. Interceptação telefônica. *Revista Brasileira de Ciências Criminais*, São Paulo, ano 7, n. 26, p. 143-151, abr/jun. 1999, p. 145.

Sergio Marcos de Moraes Pitombo (Sigilo nas comunicações: aspecto processual penal. *Boletim IBCCRIM*. São Paulo, n.49, p. 07-08, dez. 1996) ressalva que: “Assentam os dicionários que interceptar é interromper o curso de algo; impedir, cortar ou cruzar a passagem. A toda luz, não se deseja impedir o fluxo da comunicação telefônica; menos ainda cortar a interlocução. Quer-se ouvir, autorizado, sem interferência, rolares as palavras, capturando-as, ou recolhendo-as, tanto que possível, e para ‘prova em investigação criminal e em instrução processual penal’ (art. 1º, da Lei nº 9.296/96). Pretende-se, lícitamente, pôr a descoberto a palavra confidenciada, que só importa ao esclarecimento da verdade criminal.” Ressalta, porém, que: “A palavra interceptação, se não emerge a melhor, já se acha e aceita consagrada.”

²⁷¹ Abordando a Lei Geral de Telecomunicações do Chile, María Cecilia Ramírez Guzmán refere que “interceptar”, segundo o dicionário da real academia, significa “apoderar-se de uma coisa antes que chegue a seu destino”, “deter uma coisa em seu caminho” e “interromper, obstruir uma via de comunicação”. Para o caso de conversas telefônicas, a autora defende o significado de “acesso não consentido de um terceiro à conversa telefônica, com a intenção de apreender seu conteúdo”. O “grampo” (“pinchazo”, em espanhol) diz respeito à interceptação pela manipulação direta dos cabos telefônicos. *Protección de las comunicaciones telefónicas en Chile* In: MARTÍN, Adán Nieto (coord.). *Homenaje al Dr. Marino Barbero Santos: in memoriam*. Cuenca: Ediciones de La Universidad Castilla-La Mancha/Ediciones Universidad Salamanca, 2001, vol. II, p. 534-535.

²⁷² Grinover refere que a interceptação telefônica é meio de apreensão imprópria e que seu resultado é fonte de prova. *As nulidades...*, p. 165.

estabeleceu, em seu art. 2º, apenas os casos em que a interceptação não é admitida, sendo necessário fazer raciocínio inverso para se chegar às possibilidades de quebra do sigilo.

Assim, a interceptação mostra-se possível apenas para os crimes apenados com reclusão e presentes os requisitos de cautelaridade, quais sejam, indícios razoáveis de autoria ou participação em infração penal e impossibilidade de realizar a coleta da prova por outros meios disponíveis.

Tanto no pedido apresentado ao juiz quanto na decisão proferida, deve-se descrever, precisamente, “a situação objeto da investigação, inclusive com a indicação e qualificação dos investigados”, e a necessidade da medida para a apuração da infração penal, com indicação dos meios a serem empregados (arts. 2º, par. único, 4º e 5º).²⁷³

A interceptação das comunicações deve ser adotada diante de sua estrita necessidade, quando a investigação não for possível por outros meios (art. 2º, II).²⁷⁴ A invasão da intimidade costuma ser justificada, pela doutrina, em virtude da instantaneidade da fonte de prova, já que as mensagens transmitidas só podem ser colhidas enquanto a comunicação ocorre.²⁷⁵ Porém, esse argumento é contestável no que se refere aos dados informáticos. Em muitos casos, a informação transmitida remanesce nos dispositivos eletrônicos, permitindo outros meios de colheita da prova, como as buscas e apreensões.

A medida pode ser decretada no curso de inquérito policial ou processo penal, como indica o artigo 3º da Lei. Não se admite, assim, a sua decretação como primeira providência ou sem que haja procedimento apuratório instaurado. A previsão é adequada, posto que a interceptação deve consistir em medida excepcional, adotada quando os outros meios disponíveis não houverem sido suficientes para a investigação. Outrossim, com uma investigação em curso, é possível reunir os indícios de autoria ou participação em infração penal, necessários à decretação da medida.²⁷⁶

²⁷³ No que diz respeito à gravação clandestina, em face da ausência de tratamento legal, costuma-se apontar a admissibilidade da prova e exclusão do crime do art. 153 do Código Penal em se constatando justa causa a respaldar a gravação. Veja-se, nesse sentido, ensinamento de Ada Pellegrini Grinover, Antonio Scarance Fernandes e Antonio Magalhães Gomes Filho (*As nulidades...*, p. 186-187).

²⁷⁴ Nesse sentido, Ada Pellegrini Grinover, Antonio Scarance Fernandes e Antonio Magalhães Gomes Filho (*As nulidades...*, p. 174) destacam: “É que as interceptações representam não apenas poderoso instrumento, freqüentemente insubstituível, no combate aos crimes mais graves, mas também uma insidiosa ingerência na intimidade não só do suspeito ou acusado, mas até de terceiros, pelo que só devem ser utilizadas como *ultima ratio*.”

²⁷⁵ Tércio Sampaio Ferraz Jr. Sigilo de dados: o direito à privacidade e os limites à função fiscalizadora do Estado. *Cadernos de Direito Constitucional e Ciência Política*, São Paulo, ano 1, n. 1, p. 77-90, out/dez. 1992, p. 82.

²⁷⁶ Nesse sentido a posição de Antonio Scarance Fernandes (*Processo penal constitucional*, p. 106): “Para que o juiz possa avaliar a presença no caso concreto destas duas exigências (materialidade e autoria), haverá

Quanto à duração da medida, a Lei 9.296/96, em seu art. 5º, estabelece que a diligência “não poderá exceder o prazo de quinze dias, renovável por igual tempo uma vez comprovada a indispensabilidade do meio de prova”.

Desde a promulgação da Lei, a doutrina debateu a possibilidade de prorrogação da medida por mais de uma vez. Grande parte da doutrina defendeu a prorrogação por indeterminadas vezes, conforme se mostrasse necessária.²⁷⁷ Em sentido contrário, Sergio Marcos de Moraes Pitombo, em artigo publicado em 1996, sustentou o prazo máximo de 30 dias para a interceptação, vez que a norma que restringe direito individual deve ser interpretada restritivamente.²⁷⁸

No mesmo sentido encontra-se a posição de Geraldo Prado, ao fazer interpretação sistemática da Lei em face da Constituição, levando em consideração o prazo de duração do estado de defesa, em que se podem suspender os direitos fundamentais. Tal situação excepcional não pode ultrapassar 60 dias. Assim, no estado de normalidade, qualquer garantia constitucional não poderia ser restringida por tempo superior a este.²⁷⁹

Até momento recente, a jurisprudência admitia amplamente a renovação indeterminada das interceptações das comunicações. No entanto, o panorama foi alterado pelo acórdão proferido pelo Superior Tribunal de Justiça, no Habeas Corpus nº 76686, de relatoria do Ministro Nilson Naves, publicado em 10 de novembro de 2008. Neste julgado, foi mudado o entendimento da Corte, que considerou ilícita a prova produzida, vez que inexistia na Lei a previsão de renovações. O acórdão tomou por base os argumentos doutrinários acima citados.²⁸⁰

necessidade de investigação em andamento ou processo instaurado (art. 3º, I), ficando, em princípio, excluída a possibilidade de interceptação para iniciar a investigação.” Damásio E. de Jesus (*Interceptações...*, p. 466) assume entendimento contrário, admitindo a interceptação como início de investigação.

²⁷⁷ Grinover et al. *As nulidades...*, p. 177; Greco Filho. *Interceptações telefônicas...*, p. 51; Rangel. *Breves considerações...*, p. 150; Gomes e Cervini. *Interceptação telefônica...*, p. 219; Damásio E. de Jesus. *Interceptações...*, p. 469.

Fábio Ramazzini Bechara, comentando o julgamento do RHC 13.274, pelo Superior Tribunal de Justiça, defendeu a renovação ilimitada da interceptação, em face da gravidade dos crimes praticados por organizações criminosas. Crime organizado e interceptação telefônica. *Revista Síntese de Direito Penal e Processual Penal*, São Paulo, ano IV, nº 25, abr/maio. 2004, p. 158-160.

²⁷⁸ Sigilo..., p. 7-8.

²⁷⁹ *Limite às interceptações telefônicas e a jurisprudência do Superior Tribunal de Justiça*. 2ª ed. Rio de Janeiro: Lumen Juris, 2006, p. 25-45.

²⁸⁰ Constou da ementa do julgado:

“(...) 3. Inexistindo, na Lei nº 9.296/96, previsão de renovações sucessivas, não há como admiti-las.

4. Já que não absoluto o sigilo, a relatividade implica o conflito entre normas de diversas inspirações ideológicas; em caso que tal, o conflito (aparente) resolve-se, semelhantemente a outros, a favor da liberdade, da intimidade, da vida privada, etc. É que estritamente se interpretam as disposições que restringem a liberdade humana (Maximiliano).

O julgamento é paradigmático, pois traz alteração profunda no entendimento sobre a limitação temporal das interceptações, adotando a posição que mais atende à garantia do direito individual.

No que se refere ao procedimento desse meio de obtenção da prova, a Lei não apresenta normas que especifiquem a forma da interceptação telemática, como, por exemplo, sua implementação e armazenamento, tampouco contempla as particularidades dos dados digitais, de modo a garantir sua autenticidade.

Mesmo com relação à interceptação telefônica, a Lei não disciplina detalhadamente a forma de realização da diligência, prevendo apenas que esta seja indicada na decisão judicial e que seja conduzida pela autoridade policial, que pode requisitar serviços e técnicos especializados às concessionárias de serviço público (arts. 5º, 6º e 7º).

Essa lacuna acaba por gerar insegurança jurídica, não permitindo ainda controle sobre a legitimidade e autenticidade da prova produzida, bem como sobre o sigilo das informações. Sem a previsão da forma de realização da interceptação, o jurisdicionado não sabe quem a realiza, onde a mensagem é armazenada, qual seu inteiro teor, e quando a comunicação foi captada.

Falhou, portanto, a Lei ao não prescrever exatamente a atuação a ser adotada pela polícia ou pelas concessionárias de telefonia e provedores de serviços de internet, que normalmente são responsáveis por efetivar a medida. Prudente seria também a centralização da operação e a exigência de compromisso de seu responsável. Medidas dessa natureza poderiam auxiliar na contenção de abusos cometidos nas interceptações das comunicações, como o vazamento de informações.

Outra questão relevante diz respeito à forma de introdução da prova no procedimento ou processo criminal. Interpretando a previsão legal (art. 6º, §1º), a doutrina entende que a gravação das mensagens interceptadas poderá ou não ocorrer. Caso não seja possível a gravação, a prova ocorreria por meio do testemunho de quem ouviu as

5. Se não de trinta dias, embora seja exatamente esse, com efeito, o prazo de lei (Lei nº 9.296/96, art. 5º), que sejam, então, os sessenta dias do estado de defesa (Constituição, art. 136, § 2º), ou razoável prazo, desde que, é claro, na última hipótese, haja decisão exaustivamente fundamentada. Há, neste caso, se não explícita ou implícita violação do art. 5º da Lei nº 9.296/96, evidente violação do princípio da razoabilidade.

conversas, podendo ainda ser registradas por meio do auto circunstanciado a ser enviado ao juiz.²⁸¹

Todavia, é de se ponderar que a gravação da comunicação constitui meio de prova diverso da narração de quem a ouviu²⁸², possuindo ambos valores probatórios diferentes.²⁸³ No segundo caso, não se pode referir propriamente a registro de interceptação de comunicação, de modo que se estaria diante de prova anômala²⁸⁴.

Em sendo feita a gravação, prevê a Lei que seja determinada a sua transcrição (art. 6º, §1º). No entanto, a prática vem sendo de apenas se elaborar auto circunstanciado, nos termos do §2º do art. 6º da Lei, no qual são referidos trechos selecionados das gravações. Essa conduta vem sendo ratificada por parte da jurisprudência, havendo julgados que consideraram desnecessária a transcrição das gravações.²⁸⁵

Discute-se a possibilidade de as gravações ou transcrições de interceptação autorizada no âmbito criminal servirem como prova emprestada em outros processos ou procedimentos.

Em se cuidando de outro processo criminal contra o mesmo acusado, a doutrina aponta para a aceitação da prova.²⁸⁶ A questão é mais controvertida quando se trata de processo ou procedimento de outra natureza, havendo posicionamento contrário à

²⁸¹ Pitombo. *Sigilo...*, p. 7-8; Greco Filho. *Interceptações telefônicas...*, p. 53.

²⁸² Como indica Sergio Marcos de Moraes Pitombo, havendo gravação da comunicação, ter-se-á documento. Em caso contrário, testemunho. *Sigilo...*, p. 7-8.

²⁸³ Esta é a anotação feita por Ada Pellegrini Grinover, Antonio Scarance Fernandes e Antonio Magalhães Gomes Filho. *As nulidades...*, p. 177.

Consigne-se que o valor do testemunho deverá atender às condições do caso concreto, sendo necessário anotar que o agente público envolvido na investigação, tal como o agente de polícia federal que acompanha as interceptações telefônicas, não poderá ser considerado testemunha desvinculada dos fatos e desinteressada.

²⁸⁴ Veja-se, a respeito, o capítulo 2.

²⁸⁵ STF, HC 91207, Tribunal Pleno, Rel. para acórdão Min. Cármen Lúcia, DJe 20.09.2007, HC 83515, Tribunal Pleno, Rel. Min. Nelson Jobim, DJ 04.03.2005; STJ, MS 13501, Rel. Min. Felix Fischer, DJe 09.02.2009; HC 37.227/SP, Quinta Turma, Rel. Min. José Arnaldo da Fonseca, DJ 16.11.2004.

No Tribunal Regional Federal da 3ª Região, é predominante o entendimento da desnecessidade da transcrição integral das comunicações interceptadas, citando-se, como exemplos: HC 2008.03.00.037866-2, Primeira Turma, DJ 11.05.2009; HC 2007.03.00.097724-3, Segunda Turma, DJ 30.04.2009; HC 2009.03.00.004600-1, Quinta Turma, DJ 14.04.2009; Inquérito 2007.60.00.003258-4, Órgão Especial, DJ 06.01.2009; HC 2008.03.00.018551-3, Segunda Turma, DJ 14.08.2008.

Exigindo a transcrição da interceptação: STF, HC 83983/PR, Primeira Turma, Rel. Min. Marco Aurélio, DJe 21.05.2008.

²⁸⁶ Greco Filho. *Interceptações telefônicas...*, p. 39; Scarance Fernandes, *Processo penal constitucional*, p. 110.

Ao contrário, Luiz Vicente Cernicchiaro entende que “a prova colhida conforme o procedimento mencionado só pode ser utilizada na hipótese mencionada no requerimento de autorização judicial. Ou seja, imprestável para outro inquérito, ou outro processo.” Lei 9.296/96 : interceptação telefônica. *Boletim IBCCRIM*. São Paulo, n.47, p. 03, out. 1996.

sua utilização, em virtude da finalidade específica da prova, consignada na Constituição da República.²⁸⁷

Releva ainda destacar que a Lei não previu expressamente oportunidade para exercício do contraditório e da ampla defesa, estabelecendo, por outro lado, o apensamento dos autos da interceptação ao inquérito ou ao processo somente por ocasião do relatório final das investigações ou da pronúncia ou sentença. Em face da garantia assegurada no art. 5º, LV, da Constituição da República, não se pode admitir que a interceptação telefônica ou telemática seja mantida em segredo, sem possibilidade de reação do investigado ou acusado, até o fim do procedimento.

Como bem acentuam Ada Pellegrini Grinover, Antonio Scarance Fernandes e Antonio Magalhães Gomes Filho, o incidente relativo à introdução do resultado da interceptação deve ser conduzido em contraditório, “contraditório diferido, em face da natureza cautelar (assecuratória da prova) do procedimento de interceptação, necessariamente realizado *inaudita altera parte*, mas que deverá instaurar-se tão logo se considere que o conhecimento do resultado da diligência não importará em prejuízo ao prosseguimento das investigações ou do processo”.²⁸⁸

Em se tratando de processo penal, desenvolvendo-se já a instrução com base na denúncia oferecida, não se pode aceitar a surpresa, ao final do procedimento, a respeito de elementos de prova, sobre os quais as partes não puderam se manifestar e se contrapor.

Quanto ao inquérito policial, é de estatura constitucional a garantia do direito de defesa, que só pode ser exercido mediante a ciência do conteúdo das investigações. É interesse do investigado apresentar elementos e requerer provas (art. 14 do Código de Processo Penal), de forma a evitar uma denúncia fundada em provas ilícitas ou em elementos tendenciosos ou deturpados. Tem ele, assim, o direito de apontar vícios da

²⁸⁷ A respeito da finalidade específica da interceptação das comunicações, veja-se análise em item anterior. Ada Pellegrini Grinover, Antonio Scarance Fernandes e Antonio Magalhães Gomes Filho (*As nulidades...*, p. 182-184) entendem ser possível o transporte da prova, pois o valor protegido, a intimidade, já teria sido rompido, de sorte que nada mais restaria a preservar.

Contudo, é preciso ponderar que, não obstante já ter ocorrido a invasão em espaço da intimidade do indivíduo, a restrição do acesso apenas ao processo penal permite que se proteja essa esfera da intimidade de uma divulgação mais ampla, pelo que a prova emprestada não seria recomendável.

De todo modo, mostra-se interessante a advertência feita pelos autores: “Nessa linha de interpretação, cuidados especiais devem ser tomados para evitar que o processo penal sirva exclusivamente como meio oblíquo para legitimar a prova no processo civil. Se o juiz perceber que esse foi o único objetivo da ação penal, não deverá admitir a prova na causa cível.”

²⁸⁸ *As nulidades...*, p. 178-179.

interceptação das comunicações. Do mesmo modo, com a ciência das interceptações, pode exercer a autodefesa, por meio do interrogatório.

A despeito de ser nomeada no ordenamento brasileiro e receber o tratamento da interceptação telefônica, nota-se que a disciplina da interceptação telemática carece de especificação, de modo a melhor garantir os direitos fundamentais e a valoração da prova.

A insuficiência de normatização não proíbe o uso desse meio de obtenção da prova. No entanto, conclui-se ser imperiosa a previsão de regras específicas que afiancem a autenticidade e a validade da prova, inclusive para garantia de seu valor probatório.

Falta, assim, delimitar o objeto da interceptação, restringindo a possibilidade de captação de todo o fluxo de dados de um endereço de IP. Do mesmo modo, cumpre determinar a inutilização dos dados privados e os que não tenham relação com a investigação, apontando as hipóteses excepcionais em que o material possa ser aproveitado para processo diverso. É preciso também indicar os possíveis procedimentos a serem adotados na execução da medida, ordenando-se a preservação dos dados originais. Deve-se também descrever a forma de introdução dos dados no processo e consignar o dever de fornecimento do material ao acusado ou investigado.

4.4 Produção da prova digital pelo meio documental

Obtidos os dados digitais, resta verificar como ocorre a introdução da fonte de prova no processo penal. Ou seja, qual meio de produção de prova se mostra adequado à formação do resultado probatório para o esclarecimento da verdade.

Como explanado, os dados digitais, embora constituam categoria própria, assemelham-se aos documentos, podendo receber tratamento equivalente, com adaptações. Isso porque a extração das informações ou dos elementos de prova ocorre, de maneira geral, pelo contato do destinatário com o dado, sem a necessidade de sua reprodução por outro ser humano.

Na prova testemunhal, a informação é extraída de um relato produzido por um ser humano, durante a produção da prova. Por meio de perguntas das partes processuais

e da manifestação da fonte de prova, são obtidas as informações relevantes ao esclarecimento dos fatos sob exame.

Diferentemente, quando se trata de fonte real como os documentos e as provas digitais, está-se diante da representação dos fatos, existente anteriormente ao processo, a qual deve ser acedida diretamente pelo destinatário, da escuta dos sons ou da visualização da imagem, desenho ou vídeo, realizando-se a interpretação desses registros.

289

Nos ordenamentos de origem anglo-saxônica, observa-se o pouco relevo conferido aos documentos, ao passo que o testemunho oral se apresenta como prova primordial. Isso se deve ao fato de os julgamentos se realizarem perante o júri, bem como à tradição oral do processo. A prova testemunhal é produzida em plenário, mediante o exame direto e cruzado pelas partes processuais, segundo o contraditório. Já os documentos são apresentados, durante o julgamento, como *exhibits*, para a inspeção dos jurados.²⁹⁰

Adalberto Camargo Aranha leciona que o uso da prova documental é recente, tendo em vista a dificuldade de reprodução escrita e o analfabetismo de grande parte das pessoas nos tempos antigos. O início do prestígio da prova documental teria coincidido com a invenção da imprensa.²⁹¹ O autor também manifesta que a prova documental teria maior relevância no processo civil do que no processo penal.²⁹²

Não obstante, na atualidade do processo penal brasileiro, pode-se notar grande importância do documento, em especial com a frequente realização de buscas e apreensões. Em realidade, chega-se ao extremo de conferir absoluta credibilidade aos escritos, aos *e-mails*, aos arquivos eletrônicos, sem se ponderar o contexto de sua produção. Por outro lado, embora a prova testemunhal ainda exerça papel de destaque, vislumbra-se uma certa desconfiança dos julgadores nas declarações das testemunhas.

²⁸⁹ A propósito, Eugenio Florian classifica os meios de prova segundo o critério de intermediação, conforme sirvam para o juiz adquirir o conhecimento da prova mediante informações de outros ou mediante sua própria e direta percepção. Como exemplos de meios que dependam de intermediação, encontram-se o testemunho e a perícia. *Delle prove...*, p. 3.

²⁹⁰ A esse respeito, Paul Roberts e Adrian Zuckerman: “Objects and documents, if relevant and not rendered inadmissible by any applicable exclusionary rule, may be adduced in the trial as ‘exhibits’ for the jury’s inspection, but they do not literally *testify* as human witnesses do, and are therefore aptly described as ‘non-testimonial’ evidence. (...) Live oral witness testimony is still the paradigmatic form (sic) of evidence in criminal trials, and merits detailed examination.” Os autores ainda discutem o papel do testemunho no julgamento diante das novas tecnologias. *Criminal evidence*. Oxford: Oxford University Press, 2004, reimpressão em 2008, p. 184-187 e 212-213.

²⁹¹ *Da prova...*, p. 259.

²⁹² Essa comparação também é feita por Eugenio Florian. *Elementos de Derecho Procesal Penal*. Barcelona: Bosch, 1934, p. 329.

No que se refere à disciplina da prova documental, o ordenamento pátrio não se ocupa do procedimento a ser adotado; em vez disso, fornece o conceito e as limitações ao uso do documento.

Assim, o Código traz uma norma de exclusão da prova, declarando inadmissíveis as cartas particulares, interceptadas ou obtidas por meios criminosos (art. 233). Ressalva, contudo, que as cartas poderão ser exibidas por seu destinatário, para defesa de seu direito, mesmo sem o consentimento do signatário.

A mesma norma deve ser aplicada às provas digitais, tendo em vista a semelhança dos *e-mails* com as cartas.

Como regra geral, o Código de Processo Penal admite a apresentação de documentos em qualquer fase do processo, não a vedando mesmo na fase recursal (art. 231).

A exceção vem disposta no procedimento do júri, no qual se exige a antecedência mínima de três dias na apresentação do documento e ciência à outra parte, para que possa ser lido ou exibido em plenário (art. 479).

Além da iniciativa das partes na apresentação do documento, o Código também dispõe sobre a atuação do juiz, na busca da verdade²⁹³, conforme o art. 234:

“Se o juiz tiver notícia da existência de documento relativo a ponto relevante da acusação ou da defesa, providenciará, independentemente de requerimento de qualquer das partes, para sua juntada aos autos, se possível.”

Com relação aos documentos em língua estrangeira, haverá, “se necessário”, sua tradução, por tradutor público ou, na falta, por pessoa idônea nomeada pela autoridade, sem prejuízo da imediata juntada. Porém, conforme ressalta Guilherme Madeira Dezem, criticando entendimento esposado por Guilherme Nucci, a tradução só pode ser dispensada quando os dados do documento se mostrarem evidentes:²⁹⁴

²⁹³ Sobre os limites dos poderes instrutórios do juiz, veja-se o item 2.4.

²⁹⁴ *Da prova...*, p. 269.

“O conhecimento pessoal das partes do idioma estrangeiro não deve ser motivo de dispensa de sua tradução. Com efeito, as partes não são as únicas destinatárias do processo, mas toda a sociedade que exerce o democrático controle sobre o processo. Pensamos que a tradução pode ser dispensada quando se fizerem evidentes os dados constantes do documento a dispensar a tradução.”

No mesmo sentido, afirmam Grinover, Magalhães Gomes Filho e Scarance Fernandes que se tem entendido que a tradução deve ser realizada, sob pena de nulidade, “pois o conteúdo do documento, dada a natureza pública do processo, deve ser acessível a todos”.²⁹⁵

Esse posicionamento encontra-se em sintonia com as determinações do Código Civil²⁹⁶ e do Código de Processo Civil²⁹⁷, pelas quais a tradução é imperativa.

Quanto à forma de apresentação, o Código confere à cópia devidamente autenticada o mesmo valor do original (art. 232, par. único). Assim também, dispõe que, em caso de processo findo, não havendo motivo relevante para conservação, os documentos originais poderão ser restituídos, mediante traslado nos autos (art. 238).

No caso das provas digitais, não se pode distinguir original e cópia produzida por espelhamento. Desse modo, os suportes eletrônicos originais, que contenham os dados digitais de interesse ao processo e que tenham sido apreendidos, não precisam ser mantidos sob custódia. Basta que se proceda à cópia dos arquivos, segundo os métodos apropriados, de preferência em duplicidade, com a transferência a dispositivos que se destinem à custódia judicial. Tal cópia será equivalente à reprodução autenticada do documento.

Com relação aos documentos particulares, extrai-se que o Código confere validade à prova²⁹⁸, exceto se contestada sua autenticidade (art. 235).²⁹⁹ Nesta hipótese, procede-se ao exame pericial da letra e firma do documento, nos termos do art. 174 do Código.

²⁹⁵ *As nulidades...*, p. 159.

²⁹⁶ “Art. 224. Os documentos redigidos em língua estrangeira serão traduzidos para o português para ter efeitos legais no País.”

²⁹⁷ “Art. 157. Só poderá ser junto aos autos documento redigido em língua estrangeira, quando acompanhado de versão em vernáculo, firmada por tradutor juramentado.”

²⁹⁸ *Dezem, Da prova...*, p. 270.

²⁹⁹ “Art. 235. A letra e firma dos documentos particulares serão submetidas a exame pericial, quando contestada a sua autenticidade.”

Pode-se ainda instaurar incidente de falsidade, autuado em apartado, no qual as partes se manifestam em contraditório e são realizadas as diligências pertinentes (art. 145 a 148). Como ressalta Adalberto Camargo Aranha, o incidente diz respeito apenas ao falso instrumental, na forma de falsidade material e na forma de falsidade ideológica, não contemplando vícios da vontade.³⁰⁰

Relativamente às provas digitais, cumpre observar que, a despeito de sua fragilidade, existe a possibilidade de rastreamento, de modo a se verificar a autenticidade da prova, e de resgate de provas pretensamente destruídas. Assim, alterações dos dados digitais podem eventualmente ser constatadas, confirmando-se ou não a autenticidade da prova.

Outro ponto relevante relaciona-se aos documentos anônimos. Segundo Adalberto Camargo Aranha, “a assinatura é o elemento formal pelo qual se reconhece a autenticidade e origem de um documento.” O autor divide os documentos não assinados em três grupos: livros societários, papéis e registros domésticos³⁰¹ e anotações em documento assinado³⁰².

As provas digitais podem conter identificação de autoria, como a aposição da assinatura digital. No entanto, grande parte dos dados digitais não carrega intrinsecamente traços distintivos que apontem para o seu criador.³⁰³ Diferentemente da escrita humana, os dados digitais não são configurados de maneira que se possa, por métodos científicos como a grafoscopia, apontar o seu criador. Dados idênticos podem ser criados indistintamente por pessoas diversas, sem que o resultado possa ser atribuído corretamente ao seu autor.

A situação complica-se, pois computadores podem ser compartilhados, endereços de IP podem ser mascarados, contas de *e-mail* com dados incorretos de usuário podem ser criadas. Enfrenta-se, assim, o problema de descobrir a origem de um arquivo, na

³⁰⁰ O autor detalha que, no documento particular, o incidente só pode ser invocado diante de uma falsidade material, pois a afirmativa falsa em escrito privado constituiria vício da vontade. *Da prova...*, p. 264.

³⁰¹ “Papéis e registros domésticos são instrumentos particulares utilizados por pessoas para a fixação de determinados fatos; são lembranças de uma parte da vida; são anotações de ocorrências ou acontecimentos.” Camargo Aranha, *Da prova...*, p. 266.

³⁰² “Algumas pessoas têm o hábito de fazer anotações em documentos de autoria de terceiros, contestando ou confirmando as anotações ali existentes.” Camargo Aranha, *Da prova...*, p. 267.

³⁰³ “I reati commessi attraverso Internet sono difficilmente perseguibili, in quanto è spesso problematica l’identificazione dell’autore e questo proprio a causa delle stesse caratteristiche strutturali della rete (transnazionalità e immateriabilità).” Vaciego. *Internet...*, p. 25.

internet, ou de demonstrar a pertinência entre um dado coletado em um dispositivo eletrônico e uma determinada pessoa.³⁰⁴

O ordenamento italiano cuida expressamente do documento que contenha declaração anônima, vedando sua aquisição e utilização.³⁰⁵ São dispostas duas exceções: as declarações que constituem o corpo do delito e as que provêm de qualquer forma do acusado.³⁰⁶

Mesmo anônimas, as declarações podem ser utilizadas se houver identificação de seu autor, por perícia ou reconhecimento expreso. Tem-se, porém, um problema com relação ao valor probatório, como assevera Tonini³⁰⁷:

“Diverso é o problema do valor probatório que se deve dar às declarações nas quais não exista subscrição, quando o seu autor tenha sido identificado mediante perícia ou reconhecimento expreso. A ausência de assinatura do próprio nome demonstra que o autor não quis vincular sua responsabilidade à respectiva declaração. Portanto, não há um problema de utilizabilidade, pois, após a identificação, a declaração formalmente anônima deixa de sê-lo em substância;

³⁰⁴ A respeito, pronuncia-se Giovanni Ziccardi: “L’ultima fase, che appare naturale nel mondo della prova tradizionale, è quella forse più complicata durante le investigazioni informatiche: è il processo di connettere un fatto elettronico a un elemento fisico, che sia una persona o, almeno, un’utenza telefonica, un *account* di posta elettronica reale.” Le tecniche..., p. 59. O mesmo autor, em outra obra (*Informatica Giuridica*, p. 324) aponta a existência de diversos potenciais suspeitos como uma característica das fontes de prova digitais.

³⁰⁵ “Art. 240 Documenti anonimi ed atti relativi ad intercettazioni illegali.

1. I documenti che contengono dichiarazioni anonime non possono essere acquisiti nè in alcun modo utilizzati, salvo che costituiscano corpo del reato o provengano comunque dall'imputato. 2. Il pubblico ministero dispone l'immediata sequestro e la custodia in luogo protetto dei documenti, dei supporti e degli atti concernenti dati e contenuti di conversazioni o comunicazioni, relativi a traffico telefonico e telematico, illegalmente formati o acquisiti. Allo stesso modo provvede per i documenti formati attraverso la raccolta illegale di informazioni. Di essi è vietato effettuare copia in qualunque forma e in qualunque fase del procedimento ed il loro contenuto non può essere utilizzato. 3. Il pubblico ministero, acquisiti i documenti, i supporti e gli atti di cui al comma 2, entro quarantotto ore, chiede al giudice per le indagini preliminari di disporre la distruzione. 4. Il giudice per le indagini preliminari entro le successive quarantotto ore fissa l'udienza da tenersi entro dieci giorni, ai sensi dell'articolo 127, dando avviso a tutte le parti interessate, che potranno nominare un difensore di fiducia, almeno tre giorni prima della data dell'udienza. 5. Sentite le parti comparse, il giudice per le indagini preliminari legge il provvedimento in udienza e, nel caso ritenga sussistenti i presupposti di cui al comma 2, dispone la distruzione dei documenti, dei supporti e degli atti di cui al medesimo comma 2 e vi dà esecuzione subito dopo alla presenza del pubblico ministero e dei difensori delle parti. 6. Delle operazioni di distruzione è redatto apposito verbale, nel quale si dà atto dell'avvenuta intercettazione o detenzione o acquisizione illecita dei documenti, dei supporti e degli atti di cui al comma 2 nonchè delle modalità e dei mezzi usati oltre che dei soggetti interessati, senza alcun riferimento al contenuto degli stessi documenti, supporti e atti.”

³⁰⁶ De acordo com Paolo Tonini, essa disposição deve ser interpretada de modo a se compreender o documento cuja declaração seja de autoria do acusado, assim como as declarações anônimas apresentadas pelo acusado. *A prova...*, p. 202-203.

³⁰⁷ *A prova...*, p. 201.

entretanto, há um problema de credibilidade da fonte e de idoneidade da representação.”

O Código de Processo Penal brasileiro, por sua vez, não disciplina a questão. Encontra-se apenas, na Constituição da República, a vedação ao anonimato, ao se garantir a livre manifestação do pensamento (art. 5º, IV).³⁰⁸ A prova, contudo, não é vedada, sendo, a princípio, admissível.

De outro lado, há de se delinear parâmetro para sua valoração, o qual se recomendaria restar positivado no ordenamento.

Interessa examinar as regras propostas por Adalberto Camargo Aranha para a apreciação do documento não assinado. No caso dos livros societários: “fazem prova todos os livros, comerciais, fiscais e trabalhistas, desde que revestidos das formalidades (intrínsecas e extrínsecas) exigíveis”; “a força probante é de livre apreciação, apenas reportando-se às legislações específicas”; “os livros fazem prova contra seus responsáveis e em seu favor”; “os livros irregulares, pela simples existência da irregularidade, fazem prova contra seus responsáveis”; “o objeto da prova deve estar relacionado com a natureza do próprio livro”.³⁰⁹

Quanto aos papéis e registros domésticos, propugna o autor por duas operações: “a primeira visa determinar a autoria, firmar a origem, estabelecer um relacionamento com o seu autor material”; a segunda diz respeito ao valor em si como prova, sendo que se parte “de um princípio universalmente aceito, de uma regra geral: por primeiro, fazem prova contra o seu autor, como consequência da aplicação do princípio *nemo sibi titulum constituit*; por segundo, não valem a favor do autor, servindo apenas como um começo de prova que deve ser vestida por outros elementos”.³¹⁰

Estas duas regras também valeriam para as anotações em documentos alheios.³¹¹

³⁰⁸ Importa observar, nesse ponto, que o Superior Tribunal de Justiça, apreciando o dispositivo em comento, considerou ilícita prova obtida por meios gravosos deferidos a partir de notícia anônima, embora tenha admitido que referida comunicação pode servir de propulsor para o início da atuação do aparato policial. HC 137.349, Rel. Min. Maria Thereza de Assis Moura, Sexta Turma, j. 05.0.2011, DJe 30.05.011.

³⁰⁹ *Da prova...*, p 266.

³¹⁰ *Da prova...*, p 267.

³¹¹ *Da prova...*, p 267.

As observações do jurista brasileiro alinham-se com o ensinamento de Édouard Bonnier, que examina as regras aplicáveis aos documentos não assinados. O professor francês assevera que, de qualquer forma, se o documento é contestado, impõe-se a sua verificação, caso contrário, não poderá servir nem como início de prova.³¹²

No caso das provas digitais, as principais preocupações estão relacionadas com a autenticidade, a identificação da autoria e a consequente atribuição de valor probatório, bem como com o acesso dos sujeitos processuais à fonte de prova.

Havendo a correta obtenção e preservação da prova, de acordo com os protocolos técnicos, pode-se afirmar a existência de uma presunção de autenticidade da prova. Em caso de contestação, o material deve ser submetido a exame pericial, a fim de aferir a alteração dos dados digitais.

Por sua vez, a identificação da autoria e a atribuição de valor probatório constituem pontos de maior dificuldade na análise da prova, cujo enfrentamento passa pela distinção entre os diversos tipos de arquivos digitais.

No caso de imagens e sons, deve-se verificar se não foram manipulados e, então, avaliar sua verossimilhança. Documentos oficiais fazem prova no contexto em que são criados. Os documentos públicos são presumidamente verdadeiros. Quanto às mensagens enviadas a partir de endereço de *e-mail* oficial (ou corporativo), em que há controle da identidade do usuário, pode-se presumir que este último seja seu autor. Os arquivos de texto, tabelas, apresentações, notas, de seu turno, dependem da análise de seu contexto e das circunstâncias em que foram obtidos. Assim como se faz relevante a identificação do usuário do dispositivo que continha os dados, também se deve averiguar se esse usuário poderia estar utilizando o equipamento no horário da criação ou alteração do arquivo, se o objeto da representação se relaciona com suas atividades ou hábitos, se outras ações que podem ser ligadas a tal usuário foram efetuadas no mesmo período, dentre outras informações.

A par disso, deve-se examinar a ideia ali representada, para verificar sua verossimilhança, constatar peculiaridades da manifestação reconhecíveis em outras declarações do sujeito, a compatibilidade com outros elementos de prova, etc.

³¹² *Traité théorique et pratique des preuves en droit civil et en droit criminel*. 5ª Ed. Paris: E. Plon, Nourrit et Cie, 1888, p. 621.

Por fim, a prova digital deve ser submetida ao contraditório, ponderando-se as afirmações das partes processuais a seu respeito. Para tanto, impõe-se a previsão de formas eficazes de juntada dos arquivos digitais aos autos, bem como do fornecimento de cópia aos sujeitos processuais, assegurando-se, se o caso, os equipamentos e programas necessários para o acesso aos dados.

4.5 Produção da prova digital pelo meio pericial

Além de ser acostada aos autos, por meio da prova documental, a prova digital pode ser submetida ao exame pericial.

A perícia consiste no trabalho desenvolvido por pessoa capacitada, detentora de competências técnicas, científicas ou artísticas, para a extração de conclusão sobre determinados fatos.³¹³

Bem esclarece Eugenio Florian que “é a perícia o meio particularmente utilizado para transmitir ou aportar ao processo noções técnicas sobre o objeto de prova para cuja evidenciação são necessárias ciência especial ou habilidade técnica”.³¹⁴

Nessa esteira, o perito é definido como “uma pessoa que, pelas qualidades especiais que possui, geralmente de natureza científica ou artística, supre as insuficiências do juiz no que tange à verificação ou apreciação daqueles fatos da causa que para tal exijam conhecimentos especiais ou técnicos”, atuando, pois, como um auxiliar do juízo.³¹⁵

Encontram-se posições diversas sobre a natureza da perícia. Ela normalmente é referida como meio de prova³¹⁶, mas também como meio de valoração da prova³¹⁷ e como algo mais do que simples meio de prova³¹⁸. Na visão de Francesco Carnelutti, trata-se de elaboração de provas³¹⁹.

³¹³ “A perícia é necessária quando deve ser realizada uma valoração que requer específicas competências técnicas, científicas ou artísticas.” Tonini, *A prova...*, p. 183.

³¹⁴ *Delle prove...*, p. 323.

³¹⁵ Moacyr Amaral Santos. *Comentários ao Código de Processo Civil*, vol. IV, 4ª Ed., Rio de Janeiro, Forense, 1986, p. 317.

³¹⁶ Santos, *Comentários...*, p. 309.

³¹⁷ Tonini, *A prova...*, p. 184.

De acordo com Ítalo Virotta, por outro lado, a classificação da perícia entre os meios de prova ou a referência do perito como auxiliar do juízo são equivocadas, porque se cuidaria de “colaboração judicial”.³²⁰

Segundo Paolo Tonini, “a perícia tem três funções que, para serem exercitadas, requerem conhecimentos específicos: 1) desenvolver investigações para adquirir dados probatórios; 2) adquirir referidos dados, selecionando-os e interpretando-os; 3) realizar a valoração em relação aos dados produzidos (art. 220, inciso I, do CPP)”.³²¹

Em relação às provas digitais, pode-se observar a necessidade de perícia: (i) para a pesquisa da prova, como nas hipóteses de apreensão remota de dados; (ii) para a captação da prova, com a realização de procedimentos técnicos para a interceptação de dados ou para cópia de um dispositivo; (iii) para a análise dos dados apreendidos, com uso de equipamentos de busca e de separação de arquivos; (iv) para a constatação da autenticidade dos dados e de eventual alteração da prova.

Nas duas primeiras hipóteses, o trabalho pericial auxiliará a obtenção da prova digital, em colaboração com a busca e apreensão, com a captação remota ou com a interceptação. Conforme exposto anteriormente, diante da fragilidade da prova digital, a segunda hipótese de necessidade da perícia deverá sempre estar presente para a obtenção dos dados digitais.

A análise dos dados apreendidos e a constatação da autenticidade da prova, por seu turno, constituem propriamente meio de prova pericial.

Essa análise decorrerá da necessidade de extração de informações específicas, por meio de procedimentos técnicos, bem como de descoberta de informações em um universo grande de dados, ou ainda de cruzamento de informações para extração de conclusões sobre os fatos. Como exemplo de situações que demandam o meio de prova em questão, tem-se, a verificação de registros de ações no sistema informático (os chamados

³¹⁸ Tornaghi e Mirabete *apud* Dezem, *Da prova...*, p. 159. Tal é também o entendimento de Adalberto Camargo Aranha, que situa a perícia em “uma posição intermediária entre a prova e a sentença”. *Da prova...*, p. 190.

³¹⁹ *Apud* Moacyr Amaral Santos. *Prova judiciária no cível e comercial*. Volume V. São Paulo, Max Limonad, 1949.

³²⁰ *La perizia nel processo penale italiano*. Padova: CEDAM, 1968, p. 86-150.

³²¹ *A prova...*, p. 183.

logs³²²), o resgate de dados deletados, a busca de arquivos por palavras-chave, a análise de arquivos transferidos, observando-se suas similitudes e padrões.

Esclareça-se que o ato de apagar um arquivo corresponde ao seu reposicionamento ou renomeação dentro do dispositivo, o que significa que esse arquivo pode se mostrar recuperável, ainda que parcialmente. É possível, desse modo, obter fragmentos de arquivos deletados que revelem informações potencialmente relevantes.³²³

No que tange à constatação da autenticidade da prova, realiza-se exame pericial sobre o material em questão, a fim de procurar por indícios de alterações.

Como visto no item precedente, a perícia deverá ser realizada, à luz do que determina o art. 235 do Código de Processo Penal, quando for contestada a autenticidade de “documentos” (arquivos digitais) particulares, os quais se pretenda utilizar como prova.

Assim também, a perícia será obrigatória quando os arquivos digitais constituírem o corpo do delito (art. 158), como, por exemplo, um *software* utilizado para perpetrar fraudes bancárias.

À perícia, enquanto meio de prova, aplicam-se as normas contidas no Código de Processo Penal. Assim, exige-se que seja realizada por perito oficial, portador de diploma de curso superior (art. 159), ou, em sua falta, por duas pessoas idôneas portadoras de diploma de curso superior preferencialmente na área específica (art. 159, §1º), as quais devem ser devidamente compromissadas (art. 159, §2º).

Nos termos da alteração promovida pela Lei nº 11.690/2008, é garantida a participação das partes processuais, que podem formular quesitos e indicar assistente técnico, que podem ter acesso ao material probatório.

³²² Os sistemas mantêm o que se chama de “log”, um registro de funcionamento com os eventos ocorridos em um dispositivo, com indicação de data, arquivos criados, modificados, impressos, deletados, etc. Andrea Monti. La nuova disciplina del sequestro informatico. In: LUPÁRIA, Luca (Org.). *Sistema penale e criminalità informatica. Profili sostanziali e processuali nella legge attuativa della Convenzione di Budapest sul cybercrime*. Milão: Giuffrè, 2009, p. 204.

³²³ “The deletion of files in standard desktop applications will generally only result in the removal of the addressing information associated with each block of data, which logically links the various blocks comprising the contents of the file; or the files are simply treated as deleted and are renamed in another directory, such as the ‘Recycle Bin’ or ‘Trash’. As such, the data remains on the media, and is potentially recoverable, until it has been either completely overwritten by new data, or been deleted by other means. This residual physical representation of erased data is sometimes referred to as ‘data remanence’, and is one cause of the ‘stickiness’ data problem.” Walden. *Computer crimes...*, p. 213.

A respeito do *recovery* de dados, veja-se Giovanni Ziccardi. L’ingresso della *computer forensics* nel sistema processuale italiano: alcune considerazioni informatico-giuridiche. In: LUPÁRIA, Luca (Org.). *Sistema penale e criminalità informatica. Profili sostanziali e processuali nella legge attuativa della Convenzione di Budapest sul cybercrime*. Milão: Giuffrè, 2009, p. 175.

Antes restrita ao processo civil, a figura do assistente técnico, embora timidamente disposta no Código de Processo Penal atual, reforça a instalação do contraditório e da busca da verdade. Como o perito, trata-se também de pessoa dotada de conhecimentos técnicos, atuando, porém, no interesse das partes processuais. Ele possui a função de fiscalizar e questionar o trabalho do perito, com a possibilidade de consultar, apenas posteriormente, o material submetido a perícia.

Nesse passo, ainda que não previsto, o acompanhamento da perícia por representante da parte ou advogado, na medida do possível, deve também ser assegurado.

É possível ainda a inquirição do perito e dos assistentes técnicos em audiência, para a prestação de esclarecimentos (art. 159, §5º).

O prazo para a elaboração do laudo pericial é de 10 dias, prorrogável em casos excepcionais (art. 160, par. único). Entretanto, com exceção dos crimes contra a propriedade imaterial³²⁴, o Código não especifica o momento em que a perícia deve ser produzida. Infere-se, a partir dos artigos 400 e 531, que a perícia deve se realizar até a audiência de instrução, vez que se prevê a oitiva dos peritos, para esclarecimentos, nessa ocasião.

O trabalho da perícia deve ser documentado, por meio do laudo pericial, que, como costuma indicar a doutrina, apresenta quatro partes:³²⁵

- preâmbulo – contendo os elementos identificadores dos peritos e do objeto da perícia;
- exposição ou descrição – relatando o que foi examinado;
- discussão – em que se expõe a análise técnica do caso;
- conclusão – com a exposição da opinião dos peritos e a resposta aos quesitos.

Embora o Código não tenha estabelecido seus requisitos, é essencial que o laudo descreva os métodos, técnicas e equipamentos empregados, bem como as regras, leis e princípios científicos aplicáveis. A opinião deve ser fundamentada e demonstrada. Os

³²⁴ Nesse caso, o artigo 525 prescreve que a denúncia ou queixa não pode ser recebida se não for instruída com o exame pericial dos objetos que constituam o corpo do delito.

³²⁵ Dezem, *Da prova...*, p. 177.

quesitos também devem ser respondidos com clareza. Ademais, deve-se utilizar linguagem acessível aos sujeitos envolvidos no processo.³²⁶

Releva, por fim, anotar que, no sistema brasileiro, o laudo pericial não é vinculatório, devendo ser livremente apreciado pelo juiz, em cotejo com as demais provas. É o que prevê o artigo 182 do Código de Processo Penal: “O juiz não ficará adstrito ao laudo, podendo aceitá-lo ou rejeitá-lo, no todo ou em parte.” Com efeito, o laudo constitui uma conclusão sobre os fatos, a partir de determinados dados e emprego de certa técnica, devendo ser avaliado seu valor probatório. Por essa razão, faz-se imprescindível a descrição detalhada dos métodos adotados, dos exames realizados e dos motivos que conduzem à conclusão exposta.

³²⁶ “A parte conclusiva é o laudo propriamente dito. É a parte na qual os expertos respondem aos quesitos que lhes foram apresentados, dando a sua fundamentação e conclusão. Encerra a *opinio*, motivo determinante do exame. As respostas devem ser fundamentadas, indicando as razões pelas quais as conclusões apresentadas são reais, tornando possível avaliar o acerto. Por seu turno, a redação deve ser clara, concisa e com a menor quantidade possível de termos técnicos, pois os peritos estão escrevendo para leigos.” Camargo Aranha, *Da prova...*, p. 209.

CAPÍTULO 5 – QUESTÕES RELEVANTES SOBRE A PROVA DIGITAL E PROPOSIÇÕES

Além da conceituação do dado digital e da verificação de sua natureza e do procedimento probatório apropriado para sua obtenção e para a produção da prova, cumpre analisar os direitos e garantias fundamentais relacionados ao tema, bem como seu reflexo nos limites à prova digital.

Deve-se, ainda, examinar a questão sob a luz da proposição de equilíbrio entre eficiência e garantismo.

Por fim, faz-se pertinente a proposição de disciplina própria, que contemple as conclusões extraídas do exame do tema.

5.1 A inviolabilidade dos dados e a validade de sua captação

A Constituição da República, em seu artigo 5º, XII, assegura a inviolabilidade do sigilo de dados. O dispositivo vem assim vazado:

“é inviolável o sigilo da correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas, salvo, no último caso, por ordem judicial, nas hipóteses e na forma que a lei estabelecer para fins de investigação criminal ou instrução processual penal”.

Permite-se, pois, a violação do sigilo para fins de investigação criminal ou instrução processual penal, nas hipóteses estabelecidas por lei. A redação do inciso, porém, dá azo a diversas dúvidas e interpretações.

Inicialmente, no que se refere aos “dados”, não se divisa, com clareza, se a expressão se refere a dados cadastrais, informações ou propriamente dados informáticos. De acordo com Antonio Scarance Fernandes:³²⁷

“Os dados, em uma exegese restrita, seriam apenas os registros constantes do computador de um indivíduo, os quais contêm segredos a respeito de sua vida. Numa visão mais ampla, abrangeriam quaisquer anotações pessoais e reservadas, como as constantes de um diário.”

Na acepção de Manoel Gonçalves Ferreira Filho, o sigilo de dados foi previsto “em decorrência do desenvolvimento da informática. Os dados *aqui* são os dados informáticos”.³²⁸ De fato, mostra-se mais adequada a interpretação de que o dispositivo cuida dos dados no âmbito da computação. De todo modo, dados cadastrais e demais informações privadas também se encontram assegurados pela proteção genérica da intimidade e da privacidade, conforme o inciso X do art. 5º.³²⁹

De outro lado, discute-se se a inviolabilidade atine aos dados em si ou à comunicação de dados.

Em artigo amplamente conhecido, Tércio Sampaio Ferraz Junior sustenta que:³³⁰

“Obviamente o que se regula é *comunicação* por correspondência e telegrafia, *comunicação* de dados e telefônica. O que fere a liberdade de omitir pensamento é, pois, entrar na *comunicação* alheia, fazendo com que o que devia ficar entre sujeitos que se comunicam privadamente passe ilegitimamente ao domínio de um terceiro.

(..) o objeto protegido no direito à inviolabilidade do sigilo não são os dados em si, mas a sua comunicação restringida (liberdade de negação). A troca de

³²⁷ *Processo...*, p. 100.

³²⁸ *Apud* Ferraz Jr., Sigilo de dados..., p. 81.

³²⁹ Tal é a lição de Antonio Scarance Fernandes. *Processo...*, p. 100.

³³⁰ Sigilo de dados..., p. 81-82.

informações (comunicação) *privativa* é que não pode ser violada por sujeito estranho à comunicação.”

Inversamente, parte da doutrina entende que a garantia em comento se refere tanto às comunicações quanto aos dados em si³³¹, posição que merece acolhida. De fato, uma leitura atenta do artigo 5º, XII, da Constituição da República favorece a interpretação mais ampla sobre o alcance dessa garantia

Embora o contexto da garantia aludida seja o das comunicações, a redação do dispositivo conduz à conclusão de que a proteção se dirige aos dados, de maneira geral. Isso porque, quando entendeu necessário, o legislador após a palavra “comunicações” junto ao adjetivo (telegráficas e telefônicas). Além disso, repetiu a palavra nos dois casos e as empregou no plural. Acrescente-se também que o termo “de dados” complementa o substantivo “sigilo” e não o substantivo “comunicações”.

Sendo assim, não é possível supor que tenha omitido a palavra “comunicações” antes de “dados”, nem que tal termo, precedendo “telegráficas”, tenha sido empregado no plural para também abarcar os dados. Se pretendesse tratar das comunicações de dados, o legislador teria escrito: “comunicações telegráficas, de dados e telefônicas”.

Ainda que não fosse essa a interpretação correta, caberia ressaltar que os arquivos digitais se encontram protegidos pelas garantias da intimidade e da privacidade, pelo direito de imagem, pelo sigilo da fonte, pelo direito autoral, pelo direito de propriedade, pelo sigilo bancário, etc. Ainda, o sigilo dos dados informáticos vem referido na Lei nº 7.232/84, que dispõe sobre a política nacional de informática.³³²

Com base na garantia do inciso XII do art. 5º, cabe discutir o alcance da exceção à inviolabilidade do sigilo, assim expressa: “salvo, no último caso, por ordem judicial, nas hipóteses e na forma que a lei estabelecer para fins de investigação criminal ou instrução processual penal”.

³³¹ É o que apontam André Augusto Mendes Machado e André Pires de Andrade Kehdi, *Sigilo...*, p. 243.

³³² “Art. 2º A Política Nacional de Informática tem por objetivo a capacitação nacional nas atividades de informática, em proveito do desenvolvimento social, cultural, político, tecnológico e econômico da sociedade brasileira, atendidos os seguintes princípios:

(...)

VIII - estabelecimento de mecanismos e instrumentos legais e técnicos para a proteção do sigilo dos dados armazenados, processados e veiculados, do interesse da privacidade e de segurança das pessoas físicas e jurídicas, privadas e públicas;”

Em síntese, três são as posições sobre a ressalva citada.

A primeira entende que a expressão “último caso” se refere apenas às comunicações telefônicas, que seriam as únicas que poderiam ser restringidas.³³³

A segunda separa as inviolabilidades em duas partes: sigilo da correspondência e das comunicações telegráficas, de um lado; sigilo de dados e das comunicações telefônicas, de outro. De acordo com essa interpretação, a exceção à inviolabilidade diria respeito à segunda parte, abrangendo os dados e as comunicações telefônicas.³³⁴

A terceira interpretação sustenta que haveria duas situações de sigilo: da correspondência, e das comunicações telegráficas, de dados e telefônicas. A quebra do sigilo seria permitida nos três últimos casos.³³⁵

Poucos anos após a promulgação da Constituição de 1988, o Supremo Tribunal Federal manifestou-se a respeito da norma em referência, na Ação Penal nº 307/DF, do chamado caso PC Farias, que envolvia o ex-Presidente Collor de Mello³³⁶, tendo concluído pela inviolabilidade absoluta do sigilo de dados. Transcrevem-se, a seguir, os trechos de maior interesse da ementa:

“AÇÃO CRIMINAL. CÓDIGO PENAL. CORRUPÇÃO PASSIVA (ART. 317, CAPUT), CORRUPÇÃO ATIVA DE TESTEMUNHA (ART. 343), COAÇÃO NO CURSO DO PROCESSO (ART. 344), SUPRESSAO DE DOCUMENTO (ART. 305) E FALSIDADE IDEOLOGICA (ART. 299). PRELIMINARES: INADMISSIBILIDADE DE PROVAS CONSIDERADAS OBTIDAS POR MEIO ILICITO E INCOMPETENCIA DO SUPREMO TRIBUNAL FEDERAL PARA OS CRIMES DO ART. 299, A AUSÊNCIA DE CONEXAO COM O DE CORRUPÇÃO PASSIVA, QUE DETERMINOU A INSTAURAÇÃO DO

³³³ Esta posição é adotada por Vicente Greco Filho. *Interceptações telefônicas: considerações sobre a Lei nº 9.296, de 24 de julho de 1996*. 2ª ed. São Paulo: Saraiva, 2008, p. 13-17; Grinover et al. *As nulidades...*, p. 168; Luiz Flávio Gomes e Raúl Cervini. *Interceptação telefônica: Lei 9.296, de 24.07.1996*. São Paulo: RT, 1997, p. 91-92; José Henrique Barbosa Moreira Lima Neto. Da inviolabilidade de dados: inconstitucionalidade da Lei 9.296/96 (Lei de Interceptação de Comunicações Telefônicas). *Cadernos de Direito Constitucional e Ciência Política*, São Paulo, ano 6, n. 23, p. 187-196, abr/jun. 1998, p. 187-188.

³³⁴ Rangel. *Breves considerações...*, p. 143.

³³⁵ A interpretação é referida por Ada Pellegrini Grinover, Antonio Scarance Fernandes e Antonio Magalhães Gomes Filho. *As nulidades...*, p. 168.

³³⁶ Relator Min. Ilmar Galvão, Tribunal Pleno, j. 13.12.1994, DJ 13.10.1995.

PROCESSO PERANTE ESSA CORTE, POSTO QUE ATRIBUIDO, ENTRE OUTROS, A PRESIDENTE DA REPUBLICA.

1.1 Inadmissibilidade, como prova, de laudos de degravação de conversa telefônica e de registros contidos na memória de micro computador, obtidos por meios ilícitos (art. 5º, LVI, da Constituição Federal); no primeiro caso, por se tratar de gravação realizada por um dos interlocutores, sem conhecimento do outro, havendo a degravação sido feita com inobservância do princípio do contraditório, e utilizada com violação a privacidade alheia (art. 5., X, da CF); e, no segundo caso, por estar-se diante de micro computador que, além de ter sido apreendido com violação de domicílio, teve a memória nele contida sido degradada ao arrepio da garantia da inviolabilidade da intimidade das pessoas (art. 5º, X e XII, da CF). (...)”

Observa-se, ainda, no voto do Ministro relator:

“Mas, mesmo que a apreensão material do micro-computador, no recinto da empresa, se houvesse dado em uma das situações fáticas previstas no inc. XI, do art. 5º, da Carta Federal, ou houvesse sido feita em cumprimento a determinação judicial, ainda assim, não estaria nela compreendido o conteúdo ideológico de sua memória, razão pela qual a Polícia Federal não poderia ter-se apropriado dos dados contidos naquele micro-computador, para mandar decodificá-los ao seu alvedrio, como fez, acobertados que se achavam pelo sigilo, o qual, conquanto se possa ter por corolário da inviolabilidade do próprio recinto dos escritórios da empresa, acha-se especificamente contemplado no inc. XII, do mesmo artigo, ao lado da correspondência e das comunicações telegráficas e telefônicas.”

“Aliás, nos tempos modernos, em que todos os trabalhos datilográficos das empresas é realizado por meio de digitação, a invasão da memória dos computadores implica fatalmente a quebra do sigilo não apenas de dados em geral, desde os relativos a simples agenda até os relacionados a fórmulas e cálculos, mas também de toda correspondência epistolar e telegráfica, em relação aos quais o manto constitucional é de natureza absoluta, já que não deixou espaço

reservado ao trabalho normativo do legislador ordinário, como se fez com as comunicações telefônicas.”

Posteriormente, contudo, a Corte expressou posicionamento contrário, mitigando o sentido do julgado e diferenciando o sigilo dos dados do sigilo das comunicações de dados, conforme se observa da ementa do RE 418.416/SC:³³⁷

“IV - Proteção constitucional ao sigilo das comunicações de dados - art. 5º, XVII, da CF: ausência de violação, no caso. 1. Impertinência à hipótese da invocação da AP 307 (Pleno, 13.12.94, Galvão, DJU 13.10.95), em que a tese da inviolabilidade absoluta de dados de computador não pode ser tomada como consagrada pelo Colegiado, dada a interferência, naquele caso, de outra razão suficiente para a exclusão da prova questionada - o ter sido o microcomputador apreendido sem ordem judicial e a conseqüente ofensa da garantia da inviolabilidade do domicílio da empresa - este segundo fundamento bastante, sim, aceito por votação unânime, à luz do art. 5º, XI, da Lei Fundamental. 2. Na espécie, ao contrário, não se questiona que a apreensão dos computadores da empresa do recorrente se fez regularmente, na conformidade e em cumprimento de mandado judicial. 3. Não há violação do art. 5º, XII, da Constituição que, conforme se acentuou na sentença, não se aplica ao caso, pois não houve "quebra de sigilo das comunicações de dados (interceptação das comunicações), mas sim apreensão de base física na qual se encontravam os dados, mediante prévia e fundamentada decisão judicial". 4. A proteção a que se refere o art.5º, XII, da Constituição, é da comunicação 'de dados' e não dos 'dados em si mesmos', ainda quando armazenados em computador. (cf. voto no MS 21.729, Pleno, 5.10.95, red. Néri da Silveira - RTJ 179/225, 270).” (grifo nosso)

Com base na divergência aludida acima, parte da doutrina sustenta que a interceptação dos fluxos de dados não encontraria amparo constitucional. Nessa linha de raciocínio, o parágrafo 1º do art. 1º da Lei 9.296/96, que estende a sua aplicação ao fluxo de comunicações em sistemas de informática e telemática, consistiria em

³³⁷ Relator Min. Sepúlveda Pertence, Tribunal Pleno, j. 10.05.2006, DJ 19.12.2006.

inconstitucionalidade, vez que apenas o sigilo das comunicações telefônicas seria excepcionado.³³⁸

Não bastasse a dificuldade de interpretação imposta pela redação do inciso em comento, enfrenta-se atualmente a questão de definir o que seja comunicação telefônica e o que seja comunicação informática ou telemática.³³⁹

No que concerne à comunicação telefônica, a doutrina diverge a respeito de sua abrangência. Em suma, encontram-se duas correntes doutrinárias sobre o tema: uma, que defende ser a comunicação telefônica a que se caracteriza pela transmissão de voz entre os interlocutores³⁴⁰; outra, que considera incluídas, na comunicação telefônica, “todas as formas de transmissão, emissão, recepção de símbolos, caracteres, sinais, escritos, imagens, sons ou informações de qualquer natureza, por meio da telefonia, estática ou móvel (celular)”.³⁴¹

A divergência teve por origem a possibilidade surgida de transmissão de dados, e acesso à internet, por meio das linhas telefônicas. Assim, discutiu-se se a exceção ao sigilo deveria se aplicar ao meio (linha telefônica) ou à forma de comunicação (oral).

Problema similar decorre da criação e desenvolvimento de serviços de troca de mensagens em formato digital, na internet, com a possibilidade de envio de textos escritos e também de comunicação oral, como ao telefone.³⁴²

³³⁸ A esse respeito, veja-se Vicente Greco Filho, *Interceptações...*, p. 13-20; Grinover et al., *As nulidades...*, p. 171; Barbosa Moreira Lima Neto, *Da inviolabilidade...*, p. 187-196.

Em sentido contrário, Gustavo Bandeira sustenta a constitucionalidade do dispositivo em comento, pois: garantiria eficácia plena e a finalidade da própria exceção, atenderia ao princípio da proporcionalidade, supriria lacuna constitucional, bem como por sua razoabilidade. A interceptação do fluxo de comunicações por sistemas de informática e sua constitucionalidade. *Revista da EMERJ*, Rio de Janeiro, v. 6, n. 22, p. 150-163, 2003.

³³⁹ A propósito, observe-se que a expressão “fluxo de comunicações em sistemas de informática e telemática”, contida na Lei 9.296/96, é criticada por Ada Pellegrini Grinover, Antonio Scarance Fernandes e Antonio Magalhães Gomes Filho. Conforme os autores, “a *informática* tem por objeto o tratamento da informação através do uso de equipamentos e procedimentos da área de processamento de dados”, enquanto “a *telemática* versa sobre a manipulação e utilização da informação através do uso combinado do computador e meios de telecomunicação”. *As nulidades...*, p. 171.

³⁴⁰ Nesse sentido, Vicente Greco Filho: “Comunicação telefônica não se confunde com comunicação por meio de linha telefônica. Telefone é aparelho de comunicação de voz, de modo que os outros instrumentos que se utilizam da linha telefônica somente por essa razão não podem ser a ele equiparados.” *Interceptações...*, p. 17-20.

O mesmo entendimento é esposado por Ada Pellegrini Grinover, Antonio Scarance Fernandes e Antonio Magalhães Gomes Filho (*As nulidades...*, p. 171) e Sergio Marcos de Moraes Pitombo (*Sigilo...*, p. 7-8).

³⁴¹ Gomes et al. *Interceptação telefônica...*, p. 100. A posição é também defendida por Damásio E. de Jesus (*Interceptações...*, p. 464): “A exceção, quando menciona ‘comunicações telefônicas’, estende-se a qualquer forma de comunicação que empregue a via telefônica como meio, ainda que haja transferência de ‘dados’.”

³⁴² Veja-se, no capítulo 1, a observação sobre os serviços de voz sobre IP.

Não menos relevante é a questão da natureza dos *e-mails*. Como afirmado, os *e-mails* constituem forma de correspondência eletrônica, assemelhando-se a uma carta ou bilhete. Não se compreende, então, por que não seriam eles incluídos na proteção dada às correspondências escritas.

Em vista da disposição constitucional, é de se concluir que está assegurada a inviolabilidade do sigilo de dados (não apenas da comunicação de dados) e que a exceção feita pela norma se refere às comunicações telefônicas, porquanto se trata de interpretação restritiva, condizente com a limitação a direito constitucional.

Com efeito, do mal lançado texto do inciso XII, pode-se colher o intuito de proteção da esfera da intimidade, impondo como regra o sigilo. A sua restrição deve ocorrer em caso excepcionalíssimo e com o menor dano ao direito individual, mormente no caso dos dados digitais, que possuem amplo espectro e atingem ainda mais severamente a intimidade e a privacidade.

Isso não enseja, porém, o caráter absoluto desse direito.³⁴³ Como leciona Antonio Scarance Fernandes, “a utilização como prova do dado protegido pelo sigilo depende da aceitação do princípio da proporcionalidade, que a justificaria para preservar outro valor amparado constitucionalmente e de maior relevância”.³⁴⁴ Cuida-se, pois, de refletir sobre restrição a direitos fundamentais com base na construção que Robert Alexy denomina de “máxima da proporcionalidade”³⁴⁵ e que Virgílio Afonso da Silva chama de “regra da proporcionalidade”³⁴⁶.

Não se pode ignorar a alteração nos hábitos e condutas das pessoas, promovida pelo desenvolvimento tecnológico, com a formação da sociedade da informação. Não há razoabilidade em vedar de maneira absoluta o acesso aos dados. No entanto, não se pode permitir a desconsideração do sigilo de dados e seu levantamento de maneira ampla.

Nesse diapasão, o afastamento do sigilo só deve ocorrer quando se constatar que essa medida atende aos requisitos de adequação, necessidade – isto é, quando representar o meio menos gravoso para a consecução de uma determinada finalidade – e

³⁴³ Sustentando a posição segundo a qual os dados se incluem na expressão “no último caso”, assevera Rogério Lauria Tucci: “Daí, a afirmação de que, relativamente a *dados*, também, o mandamento constitucional proibitivo *não tem caráter absoluto*.” *Direitos...*, p. 338.

³⁴⁴ *Processo...*, p. 100.

³⁴⁵ *Teoria dos Direitos Fundamentais*. Trad. Virgílio Afonso da Silva. São Paulo: Malheiros, 2008, p. 116-120.

³⁴⁶ *Direitos Fundamentais: conteúdo essencial, restrições e eficácia*. São Paulo: Malheiros, 2009, p. 169.

proporcionalidade em sentido estrito³⁴⁷. Evidentemente, trata-se de análise a ser realizada em decisão judicial fundamentada à luz das peculiaridades jurídicas e fáticas de cada caso concreto, pela autoridade competente. Ainda, deve-se verificar a viabilidade do meio de levantamento do sigilo, observando-se a existência de procedimento probatório apropriado e sua admissibilidade no processo penal brasileiro, como referido no capítulo anterior.

5.2 Os limites à obtenção e à utilização da prova digital

A par da inviolabilidade do sigilo, outras questões surgem a respeito da obtenção e da utilização da prova digital.

A primeira delas refere-se ao conceito de domicílio e ao local de guarda dos dados. Como se sabe, a Constituição da República garante a inviolabilidade do domicílio, em seu art. 5º, inciso XI:

“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.”

Com fundamento na autorização constitucional, encontram-se previstas a busca e a apreensão, que exigem decisão judicial fundamentada e expedição de mandado, conforme observado no item 4.1 acima.

Ocorre que, atualmente, os meios tecnológicos permitem o acesso aos dados digitais, sem a necessidade de adentrar o domicílio físico do indivíduo, como no caso da infiltração, conforme item 4.2 supra. De outro lado, os dados podem ser armazenados “em nuvem” ou em servidores remotos, não se localizando dentro da residência do indivíduo.

Por essa razão, emerge a ideia de “domicílio virtual”, conforme propõe Benjamin Silva Rodrigues:³⁴⁸

³⁴⁷ Cf. Robert Alexy, *Teoria...*, p. 116-120; cf. também Virgílio Afonso da Silva, *Direitos Fundamentais*, p. 167-182.

³⁴⁸ *Da prova penal: Tomo II...*, p. 473.

“O computador surge-nos, cada vez com maior insistência e persistência, como o ‘*domicílio informático*’ ou a ‘*casa digital*’ onde mora a nossa ‘*alma digital*’ cujo desapossamento poderá configurar uma irremediável ‘*falsificação existencial*’ (e ‘*informativa e comunicacional*’). Entrar no computador é colocar um pé em casa do seu titular e, simplesmente *para isso*, e *por isso*, exigir-se-ia que *somente entre quem tem convite ou que se apresenta, declaradamente, ‘às claras’, na porta dianteira* e não através da porta traseira e de forma algo subreptícia, aleivosa e maliciosa (para não dizermos mesmo ‘às ocultas’).”

De fato, diante do valor da informação na sociedade atual e da quantidade e relevância de dados armazenados nos dispositivos eletrônicos, é de se reconhecer uma proteção especial a esses locais, que constituem um novo espaço da esfera de intimidade e de privacidade.³⁴⁹

Assim, caso sejam previstos meios de obtenção remota de dados, com o estabelecimento do procedimento probatório, faz-se necessária a imposição de limites à atividade a ser desenvolvida, visando ao resguardo dos aludidos direitos fundamentais. Nesse sentido, a exigência de detalhamento da operação permitida, descrevendo com precisão o sistema alvo, os locais que podem ser acessados, as ações que podem ser adotadas e os dados que podem ser recolhidos. Além disso, mostra-se imperiosa a previsão de duração máxima da medida.

A fim de permitir o controle da atividade estatal, bem como o exercício do direito de defesa e o contraditório, há de se prever a comunicação ao interessado sobre o cumprimento da medida, dando-lhe conhecimento do procedimento adotado e dos dados recolhidos.

Tanto na interceptação quanto na busca e apreensão tradicionais e na busca remota, é preciso definir limites da apreensão, vez que a facilidade de coleta do dado digital abre a possibilidade de obtenção de infinitos dados a respeito do indivíduo ou da empresa, e até mesmo de todos os dados que estes possuem armazenados – imagine-se,

³⁴⁹ Segundo Antonio Scarance Fernandes, “a intimidade é o espaço mais reservado do indivíduo, no qual ele guarda os seus segredos e espera que não sejam descobertos. O âmbito da vida privada é maior, abrangendo a área dos relacionamentos pessoais e particulares da pessoa, com a sua família, os seus amigos.” *Processo...*, p. 113.

nesse ponto, um dispositivo de *backup* ou uma memória externa. Com isso, pretende-se preservar a intimidade e a privacidade.

A propósito, vale observar a aplicação do sigilo da correspondência, que abrange a comunicação por *e-mail*.³⁵⁰ Caso não se entenda existir vedação absoluta à obtenção da correspondência fechada³⁵¹, tratando-se de forma de comunicação, insta obedecer aos preceitos da Lei nº 9.296/96, assim como às disposições do Código de Processo Penal referentes aos documentos (arts. 231 a 238).

Outro ponto relevante reside nos dados que constituem segredo. É possível que, ao se efetuar uma busca em um sistema de um indivíduo, encontrem-se dados atinentes à sua atividade profissional, os quais sejam gravados pelo sigilo legal.³⁵²

“O segredo profissional é derivado da proteção constitucional da intimidade da pessoa, proteção que além de abarcar interesses particulares ligados à intimidade e à vida privada, por via reflexa tutela valores de ordem ética, cuja inobservância poderia abalar a vida social.”³⁵³

Nesse sentido, a Lei nº 8.906/94, em seu art. 7º, inciso II, dispõe sobre o sigilo garantido ao advogado, assentando “a inviolabilidade de seu escritório ou local de trabalho, bem como de seus instrumentos de trabalho, de sua correspondência escrita, eletrônica, telefônica e telemática, desde que relativas ao exercício da advocacia”. A exceção - muitas vezes dilatada e utilizada indevidamente, em afronta à figura do defensor, como restou evidente das discussões publicadas na mídia sobre a invasão de escritórios - encontra-se no caso de o advogado constar como investigado.³⁵⁴

³⁵⁰ Nesse sentido, Adalberto Camargo Aranha, após mencionar definição, de Magalhães Noronha, de correspondência (“comunicação ou transmissão de pensamento de uma pessoa a outra, reproduzida ou fixada numa coisa”), arremata: “Logo, pode-se entender como correspondência as cartas e os postais, os telegramas, os impressos e as encomendas por via postal, bem como por um meio eletrônico como o telex e o *e-mail*.” *Da prova...*, p. 303.

³⁵¹ Adalberto Camargo Aranha defende que a correspondência é sigilosa e goza de proteção absoluta enquanto fechada. Depois de aberta, deve ser tratada como documento particular. *Da prova...*, p. 303-304.

³⁵² Segundo Sergio Carlos Covello, o sigilo é a proteção jurídica do segredo, ou seja, da notícia não comunicável, que está sob reserva. O autor distingue sigilo de segredo, pois enquanto aquele é a proteção jurídica, este é “um estado de fato pelo qual uma notícia permanece conhecida somente por uma ou por algumas pessoas”. *As normas de sigilo como proteção à intimidade*, São Paulo, Sejac, 1999, p. 11.

³⁵³ Mario Sergio Sobrinho e Thais Aroca Datcho Lacava. O sigilo profissional e a produção de prova. In: SCARANCA FERNANDES, Antonio; ALMEIDA, José Raul Gavião de; MOARES, Maurício Zanoide de. *Sigilo no processo penal: eficiência e garantismo*. São Paulo: RT, 2008, p. 174.

³⁵⁴ “Art. 7º (...)

§ 6º Presentes indícios de autoria e materialidade da prática de crime por parte de advogado, a autoridade judiciária competente poderá decretar a quebra da inviolabilidade de que trata o inciso II do caput deste artigo, em decisão motivada, expedindo mandado de busca e apreensão, específico e pormenorizado, a ser cumprido na presença de representante da OAB, sendo, em qualquer hipótese, vedada a utilização dos

De sua parte, o sigilo médico é estabelecido pelo art. 102 do Código de Ética Médica, aprovado pela Resolução nº 1.246/88, do Conselho Federal de Medicina. Já o jornalista tem assegurado o sigilo da fonte, pelo art. 5º, XIV, da Constituição da República. O sacerdote também tem sua atuação protegida, consoante art. 207 do Código Penal.

Ainda, o sigilo bancário decorre do art. 1º da Lei Complementar nº 105/2001.

De maneira geral, os dados protegidos por sigilo devem ser preservados, não sendo submetidos à apreensão ou, se já efetuada, sendo inutilizados. No entanto, se esses dados tiverem relação com os fatos e precisarem ser conhecidos, sua obtenção e sua produção dependerão de ordem judicial devidamente fundamentada.

Outrossim, deve-se enfrentar a questão do denominado “conhecimento fortuito”, que consiste na identificação de fatos em relação a terceiros ou de fatos que não fundamentaram a decisão autorizadora da medida. A questão acentua-se, na prova digital, diante do volume de dados disponíveis e da abrangência do acesso em relação aos variados âmbitos da vida, bem como do recolhimento de discos rígidos inteiros.

Tratando da interceptação telefônica, analisa Vicente Greco Filho, quanto a terceiros, que é da essência da comunicação que a interceptação ocorra em face de dois interlocutores, de forma que não se pode recusar que a autorização da medida abranja a participação de qualquer interlocutor.³⁵⁵ Do mesmo modo, Ada Pellegrini Grinover, Antonio Scarance Fernandes e Antonio Magalhães Gomes Filho admitem a utilização dos elementos obtidos em face de terceiros, desde que ligados ao fato que está sendo investigado.³⁵⁶

No que concerne a fatos diversos, a doutrina aponta que se poderia vislumbrar na Lei nº 9.296/96 a intenção de restringir a interceptação ao objeto da investigação que a embasou (arts. 2º, par. único, e 4º). Contudo, os juristas tendem a acolher a possibilidade de utilizar a interceptação para fatos diversos, desde que

documentos, das mídias e dos objetos pertencentes a clientes do advogado averiguado, bem como dos demais instrumentos de trabalho que contenham informações sobre clientes.

§ 7º A ressalva constante do § 6º deste artigo não se estende a clientes do advogado averiguado que estejam sendo formalmente investigados como seus partícipes ou co-autores pela prática do mesmo crime que deu causa à quebra da inviolabilidade.”

³⁵⁵ *Interceptações telefônicas...*, p. 33-35.

³⁵⁶ Ada Pellegrini Grinover, Antonio Scarance Fernandes e Antonio Magalhães Gomes Filho. *As nulidades...*, p. 175-176.

relacionados com o fato sob investigação.³⁵⁷ Nesse sentido, encontra-se o posicionamento de Antonio Scarance Fernandes:³⁵⁸

“A questão, como faz a doutrina, deve ser situada num ponto médio. Em princípio, haverá ilicitude por desvio do objeto da interceptação ou busca autorizada, mas nem toda prova obtida em relação a crime diverso daquele da autorização será ilícita e, por isso, inadmissível. O critério deve ser o da existência de nexo entre os dois crimes.”

Diante da relevância da questão e de sua seriedade no que concerne à prova digital, faz-se imprescindível a fixação de critérios que orientem a admissão dos dados coletados mediante encontro fortuito, sob pena de se instalar devassa generalizada. Certamente, deve-se tomar como parâmetro a conexão entre os delitos e a equivalência de gravidade do delito descoberto ao acaso em relação ao originalmente investigado. É de ser admitida também a apreensão do dado que constitua corpo do delito, no sentido de *corpus criminis*³⁵⁹, vez que a situação equivaleria a um flagrante.

5.3 A busca pelo equilíbrio entre eficiência e garantismo nas provas digitais

³⁵⁷ Vicente Greco Filho admite o uso da interceptação nesses casos, mas “desde que a infração possa ser ensejadora de interceptação, ou seja, não se encontre entre as proibições do art. 2º e desde que seja fato relacionado com o primeiro, ensejando concurso de crimes, continência ou conexão.” *Interceptações telefônicas...*, p. 35-36. Ada Pellegrini Grinover, Antonio Scarance Fernandes e Antonio Magalhães Gomes Filho indicam a utilização dos requisitos do art. 2º da Lei como critério para o aproveitamento do resultado da interceptação, devendo se tratar de crime de igual ou maior gravidade. *As nulidades...*, p. 175.

Damásio E. de Jesus adota posição contrária, defendendo que a prova obtida sem autorização judicial específica não serve para demonstração desse “novo” delito. *Interceptações...*, p. 467.

³⁵⁸ *Processo...*, p. 108.

³⁵⁹ Em obra específica sobre o assunto, Rogerio Lauria Tucci afirma que a verificação do conceito de corpo de delito deve ser feita em vista dos elementos que o compõem: “a) *corpus criminis*, como tal considerada a pessoa ou coisa sobre a qual praticado o ato criminoso; b) *corpus instrumentorum*, respeitante à averiguação de coisas – objetos ou instrumentos, - utilizados na atuação delituosa, pelo autor ou autores do mesmo; e c) *corpus probatorium*, concernente à constatação de todas as circunstâncias hábeis à reconstrução do crime investigado”. *Do corpo de delito no Direito Processual Penal brasileiro*. São Paulo: Saraiva, 1978, p. 70.

A partir do que se expôs, podem-se extrair os principais aspectos relacionados à tentativa de atingir os objetivos de eficiência e garantismo com relação à prova digital.

A eficiência “expressa a capacidade, a força, o poder de algo que o leva a produzir um efeito”³⁶⁰. Como expressa Fábio Ramazzini Bechara, “eficiência é fazer bem as coisas”. Sobre o tema, tratando também da eficácia e da efetividade, o autor bem resume: “Assim, por eficiência entender-se-á a aptidão para um resultado; por eficácia entender-se-á a obtenção do resultado; por efetividade entender-se-á a qualidade externa que se projeta para além do resultado.”³⁶¹

De acordo com Antonio Scarance Fernandes, deve-se distinguir a eficiência *do* processo penal e a eficiência *no* processo penal. A eficiência do processo penal levaria em conta a eficiência na atuação dos sujeitos processuais e a eficiência dos atos que compõem o procedimento, “quando vistos principalmente na sequência que devem seguir”. A eficiência no processo penal seria “a capacidade de um ato, de um meio de prova, de um meio de investigação, de gerar o efeito que dele se espera.”³⁶²

O autor exemplifica a ideia em relação aos meios de obtenção da prova: “Por outro lado, a eficiência de um meio de investigação que tem como finalidade buscar uma fonte de prova será medida em razão de sua capacidade de propiciar a descoberta da fonte.”³⁶³

Relativamente à prova digital, a eficiência está afeta à capacidade da busca e apreensão, infiltração e interceptação em obterem os dados de interesse ao esclarecimento da verdade, conjugada com a preservação da autenticidade e integridade do material, armazenado de maneira que se torne duradouro.

Assim, tais medidas, seguindo os adequados protocolos técnicos, devem conseguir extrair os dados digitais e fixá-los em suporte apropriado para o uso no processo. Essas operações, repise-se, devem ser feitas sem alterar os dados originais. Cumpre, ainda, tornar o material acessível ao longo do tempo, mantendo seu conteúdo genuíno.

³⁶⁰ Scarance Fernandes. Reflexões..., p. 18.

³⁶¹ *Cooperação Jurídica Internacional em Matéria Penal: eficácia da prova produzida no exterior*. Tese de doutorado apresentada à Faculdade de Direito da Universidade de São Paulo, sob orientação do Professor Titular Antonio Scarance Fernandes, 2009, p. 19.

³⁶² Reflexões..., p. 24-25.

³⁶³ Reflexões..., p. 25.

Quanto à produção da prova, importa que o meio previsto permita o acesso dos sujeitos processuais aos dados que servem à comprovação dos fatos. Assim também, é fundamental que se possam analisar todas as informações relevantes, que se complementam sobre o objeto da prova.

Nessa linha, cuida-se de dar solução ao problema do tratamento do enorme volume de dados colocados à disposição da Justiça, por meio das buscas e apreensões e interceptações.

Ian Walden aborda a questão com precisão:³⁶⁴

“Related to the ‘stickiness’ problem is the ‘analysis’ problem created by the volume and nature of the data that an investigator may be required to handle in the course of an investigation. Modern data media, such as hard drives, DVDs and memory sticks are capable of storing vast amounts of data, while networks are capable of transmitting huge bitstreams of data over channels and across nodes. While an investigator may be able to obtain and preserve such data in a relatively straightforward manner, through the exercise of seizure or interception powers, the ability to access, manage and analyse it for subsequent presentation in court can present very significant problems, from the need to overcome protection mechanisms, to the availability of appropriate resource within any time limits imposed by law.”³⁶⁵

De fato, tem-se visto, na prática processual, a realização de buscas e apreensões, sem se falar em interceptações telemáticas, em que incomensurável número de arquivos é obtido, ao que se segue a elaboração de cópia e simples anexação ao processo. Os elementos de prova incorporados aos autos, em geral, são apenas aqueles pinçados pela autoridade policial, ignorando-se todas as demais informações disponíveis. À defesa

³⁶⁴ *Computer crimes...*, p. 208.

³⁶⁵ Tradução livre: “Relacionado com o problema da ‘aderência’ está o problema da ‘análise’ criado pelo volume e natureza dos dados que um investigador pode ser obrigado a lidar no decorrer de uma investigação. Mídias modernas de dados, como discos rígidos, DVDs e cartões de memória são capazes de armazenar grandes quantidades de dados, enquanto as redes são capazes de transmitir grande quantidade de dados através de canais e nós. Enquanto um investigador pode ser capaz de obter e preservar esses dados de uma forma relativamente simples, por meio da realização de apreensão ou interceptação, a capacidade de acessar, gerenciar e analisá-la para posterior apresentação em juízo pode apresentar problemas muito significativos, desde a necessidade de superar os mecanismos de proteção, à disponibilidade de recursos apropriados respeitando os limites de tempo impostos pela lei.”

também resta inviável a análise de todo o material coletado, por ausência de tempo e meios adequados.

Para se enfrentar o problema, têm sido desenvolvidas ferramentas de busca e catalogação de arquivos, de modo a facilitar sua análise. No entanto, o instrumento parece insuficiente diante da necessidade de exame conjunto das informações existentes. Nesse panorama, a prova digital ainda carece de eficiência.

De outro lado, releva a observação dos questionamentos relativos à aplicação do garantismo na prova digital. O garantismo reflete a concepção de um processo penal seguidor dos princípios constitucionais e garantidor dos direitos fundamentais, levando à proteção dos indivíduos e à legitimação da atuação estatal.

Esse princípio abrange a imposição de limites ao processo penal, opondo-se, em certa medida, ao objetivo de eficiência.

Entretanto, deve haver uma conjugação dos dois objetivos, conduzindo a um processo penal equilibrado.

Na prova digital, ao passo em que se permite seu uso, verificam-se limites à forma de obtenção dos dados – como a inadmissibilidade de meios não regulamentados que causem grave restrição a direito fundamental –, à apreensão de dados – em vista da proteção da intimidade, da privacidade e dos sigilos –, e à utilização dos dados – como a vedação do “conhecimento fortuito”.

De outro lado, como exemplo de coincidência entre eficiência e garantismo, tem-se a proposição da manutenção dos dados digitais em suportes destinados à custódia judicial, sem a apreensão dos suportes físicos originais. Com efeito, na história recente, é comum a apreensão de computadores, servidores, telefones celulares, dentre outros dispositivos, quase sempre com prejuízo a quem sofre a medida. Em muitos casos, a atividade empresarial vê-se paralisada em razão da apreensão de seus equipamentos.

No entanto, tendo-se em conta a autenticidade da cópia obtida por espelhamento para a produção da prova, é possível atender ao escopo de produção de prova válida com a assecuração do direito de propriedade³⁶⁶ e o resguardo da continuidade

³⁶⁶ Note-se que, não apenas o proprietário fica privado de seu bem por razoável período de tempo, “enquanto interessar ao processo”, como também acaba por perder o valor de mercado do bem, em vista da constante evolução da tecnologia.

dos trabalhos da empresa ou órgão público, evitando também a lotação dos depósitos judiciais.

A propósito, vale notar que esse procedimento foi contemplado na Portaria nº 1.287/2005 do Ministério da Justiça. Ao registrar instruções sobre a execução de diligências da Polícia Federal para cumprimento de mandados judiciais de busca e apreensão, previu-se acertadamente que:

“Art. 3º Salvo expressa determinação judicial em contrário, não se fará a apreensão de suportes eletrônicos, computadores, discos rígidos, bases de dados ou quaisquer outros repositórios de informação que, sem prejuízo para as investigações, possam ser analisados por cópia (back-up) efetuada por perito criminal federal especializado.

Parágrafo único. O perito criminal federal, ao copiar os dados objeto da busca, adotará medidas para evitar apreender o que não esteja relacionado ao crime sob investigação.”

Não obstante, lamentavelmente, tal norma foi revogada pela Portaria MJ nº 759/2009. Manteve-se apenas a faculdade de o interessado extrair cópia dos documentos apreendidos, “inclusive dos dados eletrônicos” (art. 4º, §1º).

Ponto pouco discutido na doutrina brasileira diz respeito ao princípio do *nemo tenetur se detegere* no que respeita aos meios ocultos de prova. Em virtude do princípio de não autoincriminação, sustenta-se que a produção da prova por meio das manifestações do próprio investigado ofenderia o direito ao silêncio e a dignidade da pessoa humana. O questionamento decorre do fato de que, com cada vez maior frequência, diante da facilidade das técnicas modernas, vêm as autoridades policiais e judiciais utilizando material probatório submetido pelo próprio investigado ou acusado, involuntariamente e sem que o saiba. Produz, assim, provas que serão valoradas contra si.³⁶⁷

O mesmo princípio envolve a questão do fornecimento de senha de sistemas protegidos por criptografia. Esclarece Giovanni Ziccardi que, “com o termo criptografia,

³⁶⁷ Tratando da interceptação telefônica, Francisco Muñoz Conde. *De las prohibiciones probatorias al Derecho procesal penal del enemigo*. Buenos Aires: Hammurabi, 2008, p. 65-66.

derivado etimologicamente do grego *krypto* (esconder) e *graphein* (escrever), identifica-se aquela disciplina científica que estuda as técnicas idôneas a proteger um texto, tornando-o incompreensível por quem não conheça a chave de interpretação correta”. Geralmente, a técnica é baseada nos mecanismos de transposição ou permutação (com a mudança da ordem dos elementos literais que o compõem) e de substituição (com a substituição dos caracteres por outros).³⁶⁸

Por essa razão, o acesso à informação contida nos arquivos digitais encriptados depende da aplicação do código correto para a reorganização dos dados.

Pode-se discutir, então, se é permitido requisitar essa informação do investigado ou acusado. Em face do direito à não auto-incriminação, não se mostra cabível a exigência do fornecimento do código, sob pena de forçar o indivíduo a produzir prova em seu desfavor, caso a diligência resulte na coleta de dados confirmadores da hipótese acusatória. Do mesmo modo, o sujeito não pode ser considerado incurso no crime de desobediência, previsto no art. 330 do Código Penal.

Nada impede que, ao invés, a senha seja apenas solicitada ao indivíduo atingido pela medida, advertindo-o, porém, do direito ao silêncio, consoante art. 5º, LXIII, da Constituição da República.

A fim de preservar esse direito, tem-se, como alternativa para a obtenção do código de descriptação, a requisição de informações aos fornecedores dos equipamentos e programas utilizados para a codificação de arquivos.

De outro lado, considerando as questões expostas, cabe ponderar que, embora se deva fornecer às autoridades instrumental hábil à persecução penal, a utilização de técnicas ocultas demasiadamente intrusivas extrapola a proporcionalidade e o justo processo. Do mesmo modo, mostra-se inaceitável o uso de monitoramento digital, de maneira contínua ou por largo espaço de tempo, ou ainda desatrelado de investigação criminal objetiva.

Por todos os aspectos analisados, urge a elaboração de norma legal, que oriente a atuação estatal e fixe limites ao procedimento probatório, protegendo os direitos fundamentais e conferindo segurança jurídica.

³⁶⁸ *Informatica giuridica...* vol. II, p. 260.

5.4 Proposição de regras para regulamentação da prova digital

Cumpre, ao final, propor possíveis pontos a serem incorporados pela legislação, para regulamentação da prova digital.

Com efeito, a doutrina reconhece atualmente a importância do procedimento como fator de legitimação dos atos estatais e da imposição da sanção criminal. Do mesmo modo, infere que as normas procedimentais constituem balizas para o devido acerto fático e para o resguardo dos direitos fundamentais. Como exposto, a previsão legal da atuação estatal permite a adoção dos meios mais úteis para uma determinada finalidade, garantindo ainda a segurança jurídica, na medida em que é de conhecimento geral o modo de se proceder. Asseguram-se, também, os direitos fundamentais, em especial as garantias do devido processo legal, vez que as regras probatórias se estabelecem contemplando tais direitos.³⁶⁹

No campo da prova digital, os aspectos a seguir abordados merecem positividade.

Inicialmente, cabe a introdução da prova digital, no Processo Penal brasileiro, sob a forma de uma categoria própria de fonte de prova, assemelhada ao documento.

Mostra-se conveniente que haja a definição do que se considera prova digital para o processo penal.

Além disso, é preciso haver previsão de meios próprios para a obtenção dessa fonte, especificando-se o respectivo procedimento. Propõe-se, para tanto, a adoção da busca e apreensão, física e remota, e da interceptação telemática. As hipóteses em que um ou outro meio se ache adequado e cabível devem ser apontadas em lei. Nesse sentido, a busca e apreensão remota deve ser admitida como meio excepcionalíssimo, realizada sob rígido controle da autoridade judicial.

Os meios de obtenção forçada da prova digital devem sempre ser precedidos de autorização judicial, devidamente fundamentada, que descreva a situação fática ensejadora da medida, com a indicação da materialidade e possível autoria delitiva, indique

³⁶⁹ A propósito, interessa consultar a análise de Guilherme Madeira Dezem, *Da prova penal...*, p. 59 e 73-77.

a necessidade desse meio de prova e estabeleça os limites da atividade a ser empreendida e sua duração.

Quanto à busca e à apreensão físicas, faz-se premente estabelecer como regra o espelhamento dos dispositivos eletrônicos, evitando-se a apreensão da propriedade. Em caso de impossibilidade de espelhamento, é preciso garantir que o sujeito afetado pela medida possa obter cópia do material recolhido, estabelecendo-se ainda um prazo limite para a manutenção da apreensão dos equipamentos eletrônicos.

Quanto à interceptação, releva deixar esclarecido na lei o prazo da medida e as hipóteses restritas de prorrogação, a fim de se evitar a banalização do meio de obtenção referido. Do mesmo modo, impõe-se estabelecer que a interceptação de todo o espectro de um endereço de IP se reserva a casos excepcionais, devidamente justificados em decisão própria.

Importa também prever que as atividades destinadas à pesquisa e à obtenção da prova digital devam ser realizadas, ou ao menos acompanhadas, por perito ou técnico em informática, que se torne responsável pela escolha de procedimento técnico abalizado, para a preservação da integridade e autenticidade dos dados digitais.

No caso de fornecimento espontâneo de dados digitais, seja pelo investigado ou acusado, seja pela vítima, é de se prever o formato e os requisitos técnicos a serem preenchidos para a apresentação desse material, com vistas a permitir verificar sua origem.

Providência da maior importância consiste na documentação das medidas.

De início, a documentação ocorre pela expedição de mandado suficientemente instruído com informações sobre os fatos sob investigação, o indivíduo alvo da medida, os equipamentos potencialmente atingidos, o objeto da busca, os procedimentos autorizados a serem efetuados, os limites da apreensão. Em caso de busca física, o mandado especificará se e em quais circunstâncias pode ocorrer a apreensão dos equipamentos eletrônicos. O mandado conterà advertência aos seus executantes para que, ao se cumprir a medida, a integridade e a autenticidade dos dados digitais sejam preservadas.

Realizada a diligência, deve ser documentado o relato sobre o transcorrer dos trabalhos, indicando seus responsáveis e as testemunhas do ato e detalhando as atividades desenvolvidas, os dados coletados e os equipamentos atingidos.

Comporta também elaborar a cadeia de custódia, colocando o material obtido sob a guarda de agente público capacitado, que promoverá o encaminhamento do objeto conforme a finalidade adequada.

Há ainda de se lacrar os equipamentos eletrônicos e apor dispositivos de segurança nas cópias digitais, de modo a se garantir a genuinidade dos dados.

Com a mesma finalidade, deve ser feita uma cópia de trabalho, sobre a qual serão realizadas as pesquisas e exames, mantendo-se intacta uma cópia fiel do material obtido.

Em razão do caráter intrusivo dos meios de obtenção da prova digital, é imprescindível dar imediata ciência à autoridade judicial competente sobre o cumprimento da medida, o seu resultado e o encaminhamento conferido aos objetos coletados.

Em caso de medida oculta, como a interceptação e eventualmente a busca e a apreensão remotas, é imperioso que a lei determine que seja dada ciência ao indivíduo alvo da medida, bem como aos investigados e acusados, tão-logo seu conhecimento não apresente risco ao sucesso do meio de obtenção da prova.

Outrossim, em respeito ao direito de defesa, mostra-se obrigatória a concessão de cópia dos dados coletados aos investigados ou acusados, ainda na fase de inquérito policial, antes de eventual interrogatório, e juntamente com a denúncia, na fase processual.

Com relação à eventual coleta de dados privados do investigado ou acusado ou ainda de pessoas a ele relacionadas, que sejam relevantes ao caso, mas que não digam respeito aos demais sujeitos processuais, deve-se cuidar de separar esse material, mantendo-o acessível apenas aos interessados.

Para o caso de encontro fortuito de dados relacionados a fatos diversos, a Lei deve definir as hipóteses de possível utilização da prova. Sugere-se que se estabeleça o aproveitamento da prova em caso de conexão entre o fato descoberto e aquele originalmente apurado e quando se tratar do próprio corpo do delito.

É preciso, ainda, consignar, na lei destinada à regulamentação do tema em comento, que deve ser assegurada a preservação dos sigilos bancário, fiscal, telefônico, médico, advocatício, religioso, etc., ao se promover as medidas de obtenção da prova, ressaltando-se os casos em que haja ordem judicial específica para a obtenção de tais

informações diante de sua relevância e pertinência para o esclarecimento dos fatos ou em que a investigação se relacione a possíveis crimes cometidos na prática profissional correlata ao sigilo.

Quanto aos exames realizados sobre o material apreendido, para a extração de informações, deve-se determinar que o agente público encarregado dessas tarefas registre as pesquisas feitas, os equipamentos e programas utilizados, as palavras-chave empregadas para a busca e a localização do arquivo encontrado.

No que concerne à produção da prova em juízo, o exame pericial da prova digital deve ser catalogado entre aqueles admitidos no processo penal, ressaltando que sua realização tem de se pautar pela preservação da autenticidade e da durabilidade da prova.

De outro lado, cumpre estabelecer em lei que a produção da prova digital ocorra conforme o procedimento da prova documental, adicionando-se a previsão do momento de proposição, admissão e realização desse meio de prova, bem como a forma a ser adotada para a introdução ao processo, de modo a permitir o acesso dos sujeitos processuais e interessados, de maneira eficiente.

Ao final, cabe registrar uma incipiente proposta de redação das principais normas legais relativas à obtenção da prova digital, contemplando as questões mais tormentosas. Vislumbrando-se sua integração a um capítulo do Código de Processo Penal, propõe-se:

DA PROVA DIGITAL

Art. – Considera-se prova digital todo dado em sistema binário constante de um suporte eletrônico ou transmitido em rede de comunicação que contenha a representação de fatos ou ideias.

Parágrafo único – À prova digital aplicam-se as disposições relativas aos documentos, com as previsões constantes deste Capítulo.

Art. Constituem meios de obtenção da prova digital:

I – a busca e a apreensão de suportes eletrônicos que contenham dados digitais;

II – a busca e apreensão, de maneira remota, de dados digitais contidos em um sistema informático acessado à distância;

III – a interceptação telemática.

Art. Exceto no caso de apresentação espontânea dos dados digitais por seu autor ou receptor, a obtenção da prova digital será precedida de decisão judicial, devidamente fundamentada, que descreva os fatos sob investigação, com a indicação da materialidade e possível autoria delitiva, indique os motivos, a necessidade e os fins da diligência, estabeleça os limites da atividade a ser empreendida e o prazo para seu cumprimento.

Parágrafo único – Em caso de monitoramento do fluxo de dados, a medida não poderá exceder o prazo de 15 (quinze) dias. Será permitida a renovação do prazo, por igual período, mediante apresentação de relatório circunstanciado dos dados até então coletados e da justificativa detalhada da imprescindibilidade da prorrogação da medida. O período total de monitoramento não poderá exceder a 90 (noventa) dias.

Art. A decisão judicial será instrumentalizada por mandado judicial, dirigido aos seus executores e às pessoas físicas ou jurídicas que irão sofrê-la, suficientemente instruído com informações sobre os fatos sob investigação, o indivíduo alvo da diligência, os equipamentos potencialmente atingidos, o objeto da medida, os procedimentos autorizados a serem efetuados, os limites da apreensão e o prazo para cumprimento.

Parágrafo único – No caso de monitoramento de sistema informático ou interceptação de fluxo de dados, será expedido mandado de intimação aos interessados, nos termos do *caput*, logo após o cumprimento da medida.

Art. Os meios de obtenção da prova digital serão implementados por perito oficial da área de informática ou por perito ou técnico em informática nomeados pelo juízo, que prestarão compromisso de bem e fielmente desempenhar o encargo. O perito ou técnico em informática deverá proceder conforme as melhores práticas

aplicáveis aos procedimentos a serem desenvolvidos, cuidando para que se preserve a integridade, a autenticidade e a durabilidade da prova digital.

Art. Ao fim da diligência para obtenção da prova digital, a autoridade policial encarregada da supervisão do cumprimento da medida lavrará auto circunstanciado, assinado por duas testemunhas, com declaração do lugar, dia e hora em que se realizou, com menção das pessoas que a sofreram e das que nela tomaram parte ou a tenham assistido, com as respectivas identidades, bem como de todos os incidentes ocorridos durante a sua execução, especificando-se os procedimentos adotados e equipamentos utilizados.

Art. Caso a diligência para obtenção da prova digital seja positiva, constará do auto circunstanciado a relação e descrição das coisas apreendidas, especificando-se o dispositivo eletrônico apreendido ou copiado, com indicação da marca, modelo, número de série e do lacre que se lhe anexe, bem como do local e condições em que se encontrava e da hora exata da operação. No caso de ser procedida à cópia da memória do dispositivo, constará o equipamento e o programa utilizados para o espelhamento do suporte eletrônico, a descrição do equipamento originário e do suporte que recebeu a cópia, anotando-se o valor do *hash* calculado para a preservação do conteúdo.

Art. O cumprimento da diligência será comunicado à autoridade judicial competente, no prazo de 48 horas, informando-se do seu resultado e do encaminhamento conferido aos objetos coletados e apresentando-se cópia do auto circunstanciado.

Art. Além do auto circunstanciado, será elaborado registro da custódia do material resultante da diligência, indicando os custodiantes e as transferências do material, bem como as operações realizadas em cada momento da custódia.

Art. A cópia do material resultante da diligência, feita por espelhamento, será guardada pela autoridade judicial competente, para eventual confronto. As análises, as pesquisas e os exames periciais devem ser realizados sobre cópia de trabalho, produzida a partir da cópia primária.

Art. Salvo expressa determinação judicial em contrário ou impossibilidade de cumprimento da medida desta forma, a apreensão dos dados digitais ocorrerá por espelhamento, não se fazendo a apreensão de suportes eletrônicos, computadores, discos rígidos, bases de dados ou quaisquer outros repositórios de informação.

Parágrafo único - O perito criminal encarregado da medida, ao copiar os dados objeto da busca, adotará medidas para evitar apreender o que não esteja relacionado aos fatos sob investigação.

Art. Em caso de impossibilidade de apreensão por espelhamento, será garantida ao indivíduo atingido pela apreensão dos dispositivos eletrônicos cópia do material recolhido. A apreensão dos equipamentos eletrônicos não poderá superar 120 (cento e vinte) dias.

Art. A interceptação telemática seguirá o procedimento estabelecido na Lei nº 9.296/96, com as modificações constantes deste Capítulo.

Art. A interceptação telemática será destinada a um determinado serviço de internet, especificando-se o usuário atingido. A interceptação de um endereço de IP somente poderá ocorrer no caso de crimes praticados por múltiplos usuários desse endereço ou quando se fizer necessária a coleta de dados comprovadamente transmitidos por diversos serviços de internet, o que deverá ser devidamente justificado em decisão própria.

Art. Os meios de obtenção da prova digital observarão o devido processo legal, respeitando-se o sigilo de informações protegidas por privilégio legal, incluindo-

se, mas não se limitando, ao sigilo médico, religioso e da relação advogado-cliente.

Parágrafo único – As informações sigilosas mencionadas no *caput* serão objeto de apreensão mediante ordem judicial específica, em face de sua relevância e pertinência para o esclarecimento dos fatos, ou nos casos de crimes cometidos pelo portador do sigilo.

Art. Os dados sigilosos ou afetos à intimidade ou à privacidade do investigado ou acusado ou pessoas a ele relacionadas, que sejam relevantes ao caso, mas que não digam respeito aos demais sujeitos processuais, serão separados dos autos principais, mantendo-se acessíveis apenas aos interessados.

Art. Se, na coleta da prova digital judicialmente autorizada, houver o encontro fortuito de dados relacionados a fatos diversos, admitir-se-á o aproveitamento da prova apenas em caso de conexão entre o fato descoberto e aquele originalmente apurado e quando se tratar do próprio corpo do delito.

CONCLUSÃO

O impressionante avanço tecnológico referente ao tratamento e registro de informações, iniciado no Século XX, ensejou a formação da denominada sociedade da informação, na qual se firma a preponderância da informação sobre os meios de produção e a distribuição dos bens na sociedade

A sociedade da informação é centralizada na valorização da informação, que apresenta enorme valor econômico e representa poder.

Essa forma de organização social tem como características centrais a globalização e a transnacionalidade, o relacionamento social, comercial e político por meios eletrônicos, o valor econômico atribuído à informação e a impregnação do conhecimento em tudo que é produzido.

Nesse contexto, a utilização de dispositivos eletrônicos pela população, inclusive com acesso à internet, e a informatização do registro de fatos apresentaram grande expansão na primeira década do Século XXI.

Conforme informações do IBGE, com base no Censo Demográfico 2010, a presença do computador em residências brasileiras triplicou desde o ano 2000, atingindo o número de cerca de 22 milhões de lares, dos quais 80% com acesso à internet.

Nessa esteira, observam-se como principais alterações no processamento e arquivo de informações:

- a utilização de intermediários (programas) para o processamento dos dados informáticos, os quais também são necessários a leitura e o acesso à informação;
- aumento do volume de dados informáticos produzidos e armazenados;
- compactação da informação;
- imaterialidade do dado informático;
- volatilidade do dado informático;
- multiplicação do arquivo informático, por meio de cópias idênticas;
- facilidade de difusão da informação;

- ausência de identificação de autoria da informação.

Igualmente, cresce o uso dos dados digitais no Processo Penal, como fonte de prova, tendo em vista a adoção de medidas de interceptação telemática e de busca e apreensão de equipamentos eletrônicos em relevante número de investigações.

Não obstante, a matéria carece de normatização e de uniformização jurisprudencial.

Faz-se imprescindível a classificação desses dados digitais, no contexto da prova penal, assim como a sistematização do procedimento probatório adequado à obtenção dos arquivos digitais e à produção da prova.

Para tanto, deve-se ter em mente que os dados digitais ou informáticos são elementos de informação representados no sistema binário. São eles a base do conceito de prova digital ora proposto: “os dados em forma digital (no sistema binário) constantes de um suporte eletrônico ou transmitidos em rede de comunicação, os quais contêm a representação de fatos ou idéias.”

A prova digital presta-se à comprovação tanto de delitos informáticos puros e impuros, quanto de infrações comuns.

Entretanto, a definição de prova digital não compreende os meios de prova que se utilizam de sistemas informáticos para auxiliar na interpretação e análise dos dados contidos no processo.

Do mesmo modo, não se incluem nas provas digitais as informações que possam ser obtidas de entidades públicas ou de terceiros, por meio de requisição, apenas porque sejam registradas em meios digitais.

De outro lado, pode-se concluir pela existência das seguintes características da prova digital: imaterialidade e desprendimento do suporte físico originário, volatilidade, suscetibilidade de clonagem, necessidade de intermediação de equipamento para ser acessada.

Outrossim, cumpre destacar que o dado digital pode ser obtido quando está armazenado em um dispositivo eletrônico ou quando está sendo transmitido. As duas situações estão insertas, respectivamente, no que se denomina *informática* e *telemática*.

Para a classificação da prova digital, importa definir o conceito de documento, a fim de se examinar sua pertinência ou não a esta categoria de fonte de prova.

A despeito da multiplicidade de posicionamentos, tem-se que o documento corresponde ao registro da representação de um fato ou ideia, pela intervenção humana, por meio de escrito, imagem ou som, em base material móvel, de maneira duradoura e realizado fora do processo.

A partir desse conceito, pode-se afirmar que a prova digital constitui fonte de prova assemelhada ao documento, mas com natureza própria, em virtude das particularidades que lhe caracterizam.

Embora no mais das vezes a prova digital contenha a representação sobre um fato ou ideia, ela se exhibe mais ampla, abrangendo a informação de maneira geral.

Ela ainda se distingue do documento tradicional pela imaterialidade e desprendimento da base material, a qual é essencial àquele. Nesse ponto, note-se que a prova digital pode ser alterada ou destruída sem efeitos para seu suporte, enquanto a intervenção no conteúdo do documento deve também afetar a base material.

Acrescente-se que a prova digital não constitui necessariamente o registro da representação de forma duradoura. Tal o que pode ser observado, por exemplo, pelo tráfego de dados na internet, caso em que a preservação apenas é possível pela captura da informação.

Por essas razões, considera-se que a prova digital constitui espécie de fonte real de prova, assemelhada ao documento, mas formadora de categoria própria.

Assim, com vistas à busca da verdade e à eficiência do processo, a obtenção e a produção da prova digital devem ser realizadas por meio de procedimentos específicos, sendo orientadas pelas finalidades de preservação, autenticidade/genuinidade, durabilidade e acessibilidade dos dados digitais, assim como pela possibilidade de análise conjunta das informações coletadas.

Tais procedimentos devem ser pautados pelas garantias do devido processo legal, respeitando-se os direitos fundamentais, de modo a se obter prova válida e legítima.

Para isso, são imprescindíveis normas que prescrevam os procedimentos adequados para a aquisição, conservação, análise e produção dos dados digitais, complementando as regras probatórias existentes no ordenamento atual.

A obtenção da prova digital ocorre por meio da apreensão dos suportes físicos, pela apreensão remota de dados ou infiltração e pela interceptação telemática.

No que se refere à produção, a prova pode ser apresentada em juízo, como os documentos, ou pode ser objeto de perícia, quando necessário recorrer a conhecimentos técnicos específicos para a extração dos elementos de prova. Desse modo, aplicam-se os meios de prova documental e pericial.

O ordenamento jurídico brasileiro atual não contempla normas específicas sobre a obtenção e a produção da prova digital, apenas mencionando a possibilidade de interceptação telemática. Isso conduz ou ao uso da analogia ou à proibição do método probatório.

A busca e a apreensão da prova digital podem ser realizadas segundo as regras atualmente existentes no Código de Processo Penal. Todavia, são imprescindíveis normas específicas que contemplem a exigência de perito na diligência, a forma a ser adotada para o procedimento e os requisitos do registro da apreensão.

De outro lado, diante da inexistência de regulamento legal, a obtenção remota de dados, com exceção da interceptação telemática, não pode ser utilizada como meio de pesquisa da prova digital, no Processo Penal brasileiro. Isso porque se trata de medida assaz intrusiva, pela qual é possível o acesso a infinitos dados, atingindo severamente a esfera de intimidade e privacidade do indivíduo, com o risco de alteração dos dados originais, não se podendo garantir a autenticidade da prova.

Como asseverado no capítulo 2, há de se considerar inadmissíveis as provas atípicas - como a obtenção remota de dados, que nem sequer é nomeada no ordenamento -, quando a própria ausência de procedimento legal não permitir a segurança das partes, a proteção dos direitos e garantias fundamentais e a eficiência do processo.

Excepcionalmente, pode-se admitir a busca e apreensão remota, em servidor determinado, no cumprimento de busca e apreensão tradicional, mediante ordem judicial específica e com o acompanhamento do interessado e eventualmente de seu advogado, vez que a medida não é cumprida de maneira oculta e permite o controle e a oposição da parte.

No que se refere à interceptação telemática, a despeito de ser nomeada no ordenamento brasileiro e receber o tratamento da interceptação telefônica, essa medida carece de especificação, de modo a melhor garantir os direitos fundamentais e a valoração da prova.

A insuficiência de normatização não proíbe o uso desse meio de obtenção da prova. No entanto, conclui-se ser imperiosa a previsão de regras específicas que afiancem a autenticidade e a validade da prova, inclusive para salvaguardar seu valor probatório.

A produção da prova digital, em geral, deve seguir a disciplina da prova documental. Entretanto, diante de suas peculiaridades e da escassa normatização desse meio de prova, tem-se a necessidade de previsão de normas específicas sobre a forma de introdução das provas digitais no processo, o momento da produção dessa prova, a validade da cópia feita por espelhamento, os critérios para a admissibilidade dos dados anônimos, assim como a previsão de parâmetros para auxiliar a valoração da prova.

Por seu turno, a perícia das provas digitais pode-se fazer necessária: (i) para a pesquisa da prova, como nas hipóteses de apreensão remota de dados; (ii) para a captação da prova, com a realização de procedimentos técnicos para a interceptação de dados ou para cópia de um dispositivo; (iii) para a análise dos dados apreendidos, com uso de equipamentos de busca e de separação de arquivos; (iv) para a constatação da autenticidade dos dados e de eventual alteração da prova.

Nas duas primeiras hipóteses, o trabalho pericial auxiliará a obtenção da prova digital, em colaboração com a busca e apreensão, com a captação remota ou com a interceptação. Conforme exposto anteriormente, diante da fragilidade da prova digital, a segunda hipótese de necessidade da perícia deverá sempre estar presente para a obtenção dos dados digitais.

A análise dos dados apreendidos e a constatação da autenticidade da prova, por seu turno, constituem propriamente meio de prova pericial.

À perícia da prova digital aplicam-se as normas do Código de Processo Penal.

Por fim, deve-se consignar a necessidade de normatização da prova digital e do exame das questões relativas a ela sob a perspectiva da busca pelo equilíbrio entre eficiência e garantismo no processo penal.

Nesse sentido, reconhecida a inviolabilidade do sigilo de dados e de sua comunicação, há de se reconhecer que esse direito não possui caráter absoluto. De outro lado, não se pode permitir a desconsideração do sigilo de dados e seu levantamento de maneira ampla.

Ainda, diante das novas formas de relacionamento social e de armazenamento de dados, deve-se atentar para a proteção da intimidade e da privacidade, interessando a concepção de domicílio virtual como local que também gozaria de inviolabilidade.

Com vistas aos mesmos direitos aludidos, mostra-se imperiosa a imposição de limites às pesquisas dos dados digitais e de sua apreensão, alertando-se também para a necessidade de preservação dos sigilos profissionais.

Dentro do mesmo escopo, urge a fixação de critérios de admissibilidade da prova digital oriunda do denominado conhecimento fortuito. Sua utilização somente é aceitável se houver conexão entre o fato descoberto e o originalmente apurado ou se o dado digital constituir o corpo d delito.

Ressalta-se, por último, que a disciplina da obtenção da prova digital deve observar a garantia contra a autoincriminação, pelo que não se admite seja o investigado ou acusado compelido a fornecer informações para a pesquisa de dados ou senhas de descriptação.

Pela relevância do tema, é recomendável a previsão de normas próprias sobre a prova digital, seja no Código de Processo Penal, seja em lei especial. A fim de iniciar a discussão sobre a positivação das regras probatórias da prova digital, consigna-se proposta de redação normativa.

BIBLIOGRAFIA REFERIDA

ABELLÁN, Marina Gascón. *Los hechos em el derecho – Bases argumentales de la prueba*. Madrid/Barcelona: Marcial Pons, 1999.

ABOSO, Gustavo Eduardo; ZAPATA, María Florencia. *Cybercriminalidad y Derecho Penal*. Buenos Aires: Editorial B de f, 2006.

ALBUQUERQUE, Roberto Chacon de. *A criminalidade informática*. São Paulo: Juarez de Oliveira, 2006.

ALEXY, Robert. *Teoria dos Direitos Fundamentais*. Trad. Virgílio Afonso da Silva. São Paulo: Malheiros, 2008.

ALMEIDA, José Raul Gavião de; MORAES, Maurício Zanoide de; FERNANDES, Antonio Scarance (Coord.). *Sigilo no processo penal: eficiência e garantismo*. São Paulo: RT, 2008.

ANDRADE, Manuel da Costa. *Sobre as proibições de prova em processo penal*. Coimbra: Coimbra Editora, 1992.

ARANHA, Adalberto José Q. T. de Camargo. *Da prova no processo penal*. 7ª ed. São Paulo: Saraiva, 2008.

BADARÓ, Gustavo Henrique Righi Ivahy. *Ônus da prova no processo penal*. São Paulo: RT, 2003.

_____. Provas atípicas e provas anômalas: inadmissibilidade da substituição da prova testemunhal pela juntada de declarações escritas de quem poderia ser

testemunha. In: YARSHELL, Flavio Luiz; MORAES, Mauricio Zanoide de. (Coord.). *Estudos em homenagem à Professora Ada Pellegrini Grinover*. São Paulo: DPJ Editora, 2005.

_____. *Direito Processual Penal*. Rio de Janeiro: Elsevier, 2008.

BANDEIRA, Gustavo. *Revista da EMERJ*, Rio de Janeiro, v. 6, n. 22, p. 150-163, 2003.

BARBOSA MOREIRA LIMA NETO, José Henrique. Da inviolabilidade de dados: inconstitucionalidade da Lei 9.296/96 (Lei de Interceptação de Comunicações Telefônicas). *Cadernos de Direito Constitucional e Ciência Política*, São Paulo, ano 6, n. 23, p. 187-196, abr/jun. 1998.

BARRACHE, Samia; OLIVIER, Antoine. L'administration de la preuve pénale et les nouvelles technologies de l'information et de la communication In: FROUVILLE, Olivier de (dir.). *La preuve pénale: internationalisation et nouvelles technologies*. Paris: La documentation française, 2007.

BECHARA, Fábio Ramazzini. Crime organizado e interceptação telefônica. *Revista Síntese de Direito Penal e Processual Penal*, São Paulo, ano IV, nº 25, p. 158-160, abr/maio. 2004.

_____. *Cooperação Jurídica Internacional em Matéria Penal: eficácia da prova produzida no exterior*. Tese de doutorado apresentada à Faculdade de Direito da Universidade de São Paulo, sob orientação do Professor Titular Antonio Scarance Fernandes, 2009.

BENNASAR, Andrés Jaume. *La validez del documento electrónico y su eficacia en sede procesal*. Valladolid: Lex Nova, 2010.

BENUCCI, Renato Luis. *A tecnologia aplicada ao processo judicial*. Campinas: Millenium Editora: 2006.

BONNIER, Édouard. *Traité théorique et pratique des preuves en droit civil et en droit criminel*. 5^a Ed. Paris: E. Plon, Nourrit et Cie, 1888.

BRAGHÒ, Gianluca. L'ispezione e La perquisizione di dati, informazioni e programmi informatici. In: LUPÁRIA, Luca (Org.). *Sistema penale e criminalità informatica. Profili sostanziali e processuali nella legge attuativa della Convenzione di Budapest sul cybercrime*. Milão: Giuffrè, 2009.

CARNELUTTI, Francesco. *Principios del proceso penal*. Buenos Aires: Ediciones Juridicas Europa-America, 1971.

_____. *A prova civil: parte geral: o conceito jurídico da prova*. São Paulo: Liv. e Ed. Universitária de Direito, 2002.

CARVALHO, Luis Gustavo Grandinetti Castanho de. *O processo penal em face da Constituição*. Rio de Janeiro: Forense, 1992.

CARVALHO, Paulo Roberto de Lima. *Prova cibernética no Processo*. Curitiba: Juruá, 2009.

CASEY, Eoghan. *Digital evidence and computer crime: forensic science, computers, and the Internet*. 2^a ed. San Diego/London: Elsevier Academic Press, 2004.

CASSESSE, Antonio. *International Criminal Law*. Oxford: Oxford University Press, 2003.

CASSIBBA, Fabio. L'ampliamento delle attribuzioni del pubblico ministero distrettuale. In: LUPÁRIA, Luca (Org.). *Sistema penale e criminalità informatica. Profili sostanziali e*

processuali nella legge attuativa della Convenzione di Budapest sul cybercrime. Milão: Giuffrè, 2009.

CASTELLS, Manuel. *A Sociedade em Rede*. São Paulo: Paz e Terra, 2000.

CASTILLO, Niceto Alcalá-Zamora Y; LEVENE HIJO, Ricardo. *Derecho Procesal Penal*. Buenos Aires: Editorial Guillermo Kraft, 1945, tomo III.

CASTRILLO, Eduardo de Urbano. *La valoración de la prueba electrónica*. Valencia: Tirant Lo Blanch, 2009.

CERNICCHIARO, Luiz Vicente. Lei 9.296/96: interceptação telefônica. *Boletim IBCCRIM*. São Paulo, n.47, p. 03, out. 1996.

CERVINI, Raúl; GOMES, Luiz Flávio Gomes. *Interceptação telefônica: Lei 9.296, de 24.07.1996*. São Paulo: RT, 1997.

CINTRA, Antonio Carlos de Araújo; GRINOVER, Ada Pellegrini; DINAMARCO, Cândido Rangel. *Teoria Geral do Processo*. 8^a ed. São Paulo: Malheiros, 1991.

COMOGLIO, Luigi Paolo. I modelli di garanzia costituzionale del processo In: *Studi in onore di Vittorio Denti*. Pádua: CEDAM, 1994, vol. I.

CONDE, Francisco Muñoz. *De las prohibiciones probatorias al Derecho procesal penal del enemigo*. Buenos Aires: Hammurabi, 2008.

COVELLO, Sergio Carlos. *As normas de sigilo como proteção à intimidade*, São Paulo, Sejac, 1999.

DEZEM, Guilherme Madeira. *Da prova penal: tipo processual, provas típicas e atípicas (atualizado de acordo com as Leis 11.689/08, 11.690/08 e 11.719/08)*. Campinas: Millenium Editora, 2008.

DINAMARCO, Cândido Rangel. *Instituições de Direito Processual Civil*. São Paulo: Malheiros, 2001, vol. III.

_____.CINTRA, Antonio Carlos de Araújo; GRINOVER, Ada Pellegrini. *Teoria Geral do Processo*. 8^a ed. São Paulo: Malheiros, 1991.

DINIZ, Davi Monteiro. Documentos eletrônicos, assinaturas digitais: um estudo sobre a qualificação dos arquivos digitais como documentos. *Revista de Direito Privado*, vol. 6, p. 52, Abr / 2001.

DÖHRING, Erich. *La prueba: su practica y apreciacion*. Ediciones Juridicas Europa-America: Buenos Aires, 1972.

ECHANDÍA, Hernando Devis. *Teoría general de la prueba judicial*. 5^a Ed. Buenos Aires: Victor P. de Zavalía, 1981, vol. I e II.

FEDELI, Ricardo Daniel; POLLONI, Enrico Giulio Franco; PERES, Fernando Eduardo. *Introdução à ciência da computação*. 2^a ed. São Paulo: Cengage Learning, 2010.

FERNÁNDEZ, José María Illán. *La prueba electrónica, eficacia y valoración en el proceso civil: Nueva oficina judicial, comunicaciones telemáticas (lexnet) y el expediente judicial electrónico – Análisis comparado legislativo y jurisprudencial*. Navarra: Editorial Aranzadi, 2009

FERRAJOLI, Luigi. *Direito e razão: teoria do garantismo penal*. 3ª ed. São Paulo: RT, 2010.

FERRAZ JR, Tércio Sampaio. Sigilo de dados: o direito à privacidade e os limites à função fiscalizadora do Estado. *Cadernos de Direito Constitucional e Ciência Política*, São Paulo, ano 1, n. 1, p. 77-90, out/dez. 1992.

FLORIAN, Eugenio. *Delle prove penali: in ispecie*. Milano: Francesco Vallardi, 1924, vol. II.

_____. *Elementos de Derecho Procesal Penal*. Barcelona: Bosch, 1934.

FROUVILLE, Olivier de (dir.). *La preuve pénale: internationalisation et nouvelles technologies*. Paris: La documentation française, 2007.

GALANTINI, Novella. Inosservanza di limiti probatori e conseguenze sanzionatorie. In: UBERTIS, Giulio (Org). *La conoscenza del fatto nel processo penale*. Milano: Giuffrè, 1992.

GOMES, Luiz Flávio Gomes; CERVINI, Raúl. *Interceptação telefônica: Lei 9.296, de 24.07.1996*. São Paulo: RT, 1997.

GRECO FILHO, Vicente. *Interceptações telefônicas: considerações sobre a Lei nº 9.296, de 24 de julho de 1996*. 2ª ed. São Paulo: Saraiva, 2008.

GRINOVER, Ada Pellegrini. *Novas tendências do direito processual (De acordo com a constituição de 1988)*. Rio de Janeiro: Forense Universitária, 1990.

_____. CINTRA, Antonio Carlos de Araújo; DINAMARCO, Cândido Rangel. *Teoria Geral do Processo*. 8ª ed. São Paulo: Malheiros, 1991.

_____. MAGALHÃES GOMES FILHO, Antonio; SCARANCE FERNANDES, Antonio. *As nulidades no processo penal*. 11ª ed. São Paulo: RT, 2009.

GUZMÁN, María Cecilia Ramírez. Protección de las comunicaciones telefónicas en Chile In: MARTÍN, Adán Nieto (coord.). *Homenaje al Dr. Marino Barbero Santos: in memoriam*. Cuenca: Ediciones de La Universidad Castilla-La Mancha/Ediciones Universidad Salamanca, 2001, vol. II, p. 531-550.

INELLAS, Gabriel Cesar Zaccarias de. *Crimes na Internet*. 2ª ed. São Paulo: Juarez de Oliveira, 2009.

IRANZO, Virginia Pardo. *La prueba documental en el proceso penal*. Valencia: Tirant Lo Blanch, 2008.

JESUS, Damásio E. de. Interceptações de comunicações telefônicas: notas à Lei 9.296, de 24.07.1996. *Revista dos Tribunais*, São Paulo, ano 86, vol. 735, p. 458-473, jan. 1997.

KEHDI, André Pires de Andrade; MACHADO, André Augusto Mendes. Sigilo das comunicações e de dados In: SCARANCE FERNANDES, Antonio; ALMEIDA, José Raul Gavião de; MOARES, Maurício Zanoide de. *Sigilo no processo penal: eficiência e garantismo*. São Paulo: RT, 2008.

LACAVA, Thais Aroca Datcho; SOBRINHO, Mario Sergio. O sigilo profissional e a produção de prova. In: SCARANCE FERNANDES, Antonio; ALMEIDA, José Raul Gavião de; MOARES, Maurício Zanoide de. *Sigilo no processo penal: eficiência e garantismo*. São Paulo: RT, 2008.

LARONGA, Antonio. *Le prove atipiche nel processo penale*. Milão: CEDAM, 2002.

LEONARDI, Marcel. *Responsabilidade civil dos provedores de serviços de Internet*. São Paulo: Juarez de Oliveira, 2005.

_____; COSTA, Helena Regina Lobo da. Busca e apreensão e acesso remoto a dados em servidores. *Revista Brasileira de Ciências Criminais*, vol. 88, p. 203, Jan/2011.

LEVENE HIJO, Ricardo; CASTILLO, Niceto Alcalá-Zamora Y. *Derecho Procesal Penal*. Buenos Aires: Editorial Guillermo Kraft, 1945, tomo III.

LISBOA, Roberto Senise. Direito na Sociedade da Informação. *Revista dos Tribunais*, vol. 847, p. 78, Mai / 2006.

LOPES JUNIOR, Aury. *Direito processual penal e sua conformidade constitucional*. 5ª ed. Rio de Janeiro: Lumen Juris, 2010, vol. I.

LORENZETTO, Elisa. Le attività urgenti di investigazione informatica e telematica. In: LUPÁRIA, Luca (Org.). *Sistema penale e criminalità informatica. Profili sostanziali e processuali nella legge attuativa della Convenzione di Budapest sul cybercrime*. Milão: Giuffrè, 2009, p. 135-164.

LUPÁRIA, Luca. La disciplina processuale e le garanzie difensive. In: LUPARIA, Luca; ZICCARDI, Giovanni (Org.). *Investigazione penale e tecnologia informatica. L'accertamento del reato tra progresso scientifico e garanzie fondamentali*. Milão: Giuffrè, 2007.

_____; ZICCARDI, Giovanni (Org.). *Investigazione penale e tecnologia informatica. L'accertamento del reato tra progresso scientifico e garanzie fondamentali*. Milão: Giuffrè, 2007.

_____. (Org.). *Sistema penale e criminalità informatica. Profili sostanziali e processuali nella legge attuativa della Convenzione di Budapest sul cybercrime*. Milão: Giuffrè, 2009.

MACHADO, André Augusto Mendes; KEHDI, André Pires de Andrade. Sigilo das comunicações e de dados In: SCARANCE FERNANDES, Antonio; ALMEIDA, José Raul Gavião de; MOARES, Maurício Zanoide de. *Sigilo no processo penal: eficiência e garantismo*. São Paulo: RT, 2008.

MAGALHÃES GOMES FILHO, Antonio. *Direito à prova no processo penal*. São Paulo: RT, 1997.

_____. *A motivação das decisões penais*. São Paulo: RT, 2001.

_____. Notas sobre a terminologia da prova (reflexos no processo penal brasileiro). In: YARSHELL, Flavio Luiz; MORAES, Mauricio Zanoide de. (Coord.). *Estudos em homenagem à Professora Ada Pellegrini Grinover*. São Paulo: DPJ Editora, 2005.

_____. Provas – Lei 11.690, de 09.06.2008 In: MOURA, Maria Thereza Rocha de Assis (coord.). *As reformas no processo penal. As novas Leis de 2008 e os Projetos de Reforma*. São Paulo, RT, 2008.

_____. GRINOVER, Ada Pellegrini; SCARANCE FERNANDES, Antonio. *As nulidades no processo penal*. 11ª ed. São Paulo: RT, 2009.

MARCACINI, Augusto Tavares Rosa. O documento eletrônico como meio de prova. *Revista de Direito Imobiliário*, vol. 47, p. 70, Jul / 1999.

MARQUES, José Frederico. *Elementos de Direito Processual Penal*. 3ª atualização, Campinas: Millenium Editora, 2009, vol. II.

MANZINI, Vincenzo. *Istituzioni di Diritto Processuale Penale*. Torino: Fratelli Bocca, 1917.

_____. *Trattato di Diritto Processuale Penale Italiano*. 6ª Ed. Torino: UTET, 1970, vol. III.

MEIRELLES, Fernando de Souza. *Informática: novas aplicações com microcomputadores*. 2ª ed. São Paulo: Makron Books, 1994.

MIRABETE, Julio Fabbrini. *Processo penal*. 18ª Ed. São Paulo: Atlas, 2008.

MITTERMAIER, C.J.A. *Tratado de la prueba en matéria criminal*. 9ª Ed. Madrid: Instituto Editorial Reus, 1959.

MONTI, Andrea. La nuova disciplina del sequestro informatico. In: LUPÁRIA, Luca (Org.). *Sistema penale e criminalità informatica. Profili sostanziali e processuali nella legge attuativa della Convenzione di Budapest sul cybercrime*. Milão: Giuffrè, 2009.

MORAES, Mauricio Zanoide de; YARSHELL, Flavio Luiz. (Coord.). *Estudos em homenagem à Professora Ada Pellegrini Grinover*. São Paulo: DPJ Editora, 2005.

_____. FERNANDES, Antonio Scarance; ALMEIDA, José Raul Gavião de; (Coord.). *Sigilo no processo penal: eficiência e garantismo*. São Paulo: RT, 2008.

MOURA, Maria Thereza Rocha de Assis (coord.). *As reformas no processo penal. As novas Leis de 2008 e os Projetos de Reforma*. São Paulo, RT, 2008.

NORONHA, E. Magalhães. *Curso de Direito Processual Penal*. 13ª Ed. São Paulo: Saraiva, 1981.

NUCCI, Guilherme de Souza. *O valor da confissão como meio de prova no Processo Penal*. 2ª Ed., São Paulo: RT, 1999.

_____. *Manual de Processo Penal e Execução Penal*. 4ª Ed., São Paulo: RT, 2008.

OLIVEIRA, Eugênio Pacelli de. *Curso de Processo Penal*. 13ª ed. Rio de Janeiro: Lumen Juris, 2010.

OLIVIER, Antoine; BARRACHE, Samia. L'administration de la preuve pénale et les nouvelles technologies de l'information et de la communication In: FROUVILLE, Olivier de (dir.). *La preuve pénale: internationalisation et nouvelles technologies*. Paris: La documentation française, 2007.

PERES, Fernando Eduardo; FEDELI, Ricardo Daniel; POLLONI, Enrico Giulio Franco. *Introdução à ciência da computação*. 2ª ed. São Paulo: Cengage Learning, 2010.

PICCINNI, Mario Leone; VACIAGO, Giuseppe. *Computer crimes: casi pratici e metodologie investigative dei reati informatici*. Bergamo: Moretti & Vitali, 2008.

PINHEIRO, Patrícia Peck. *Direito Digital*. 4ª ed. São Paulo: Saraiva, 2010.

PITOMBO, Sergio Marcos de Moraes. Sigilo nas comunicações: aspecto processual penal. *Boletim IBCCRIM*. São Paulo, n.49, p. 07-08, dez. 1996.

_____. *Do seqüestro no processo penal brasileiro*. São Paulo: Bushatsky, 1973.

PITOMBO, Cleunice A. Valentim Bastos. *Da busca e da apreensão no processo penal*. 2ª Ed. São Paulo: RT, 2005.

POLLONI, Enrico Giulio Franco; FEDELI, Ricardo Daniel; PERES, Fernando Eduardo. *Introdução à ciência da computação*. 2ª ed. São Paulo: Cengage Learning, 2010.

PRADO, Geraldo. *Limite às interceptações telefônicas e a jurisprudência do Superior Tribunal de Justiça*. 2ª ed. Rio de Janeiro: Lumen Juris, 2006.

RANGEL, Paulo. Breves considerações sobre a Lei 9.296/96. Interceptação telefônica. *Revista Brasileira de Ciências Criminais*, São Paulo, ano 7, n. 26, p. 143-151, abr/jun. 1999.

ROBERTS, Paul; ZUCKERMAN, Adrian. *Criminal evidence*. Oxford: Oxford University Press, 2004, reimpressão de 2008.

RODRIGUES, Benjamim Silva. *Das escutas telefônicas: A monitorização dos fluxos informacionais e comunicacionais*. 2ª Ed., Coimbra: Coimbra Editora, 2008.

_____. *Da prova penal: Tomo II - Bruscamente...a(s) face(s) oculta(s) dos métodos ocultos de investigação criminal*. Lisboa: Rei dos Livros, 2010.

_____. *Da prova penal: Tomo IV – Da prova-electrónico-digital e da criminalidade informático-digital*. Lisboa: Rei dos Livros, 2011.

ROSSINI, Augusto. *Informática, Telemática e Direito Penal*. São Paulo: Memória Jurídica, 2004.

SANTOS, Moacyr Amaral. *Comentários ao Código de Processo Civil*. vol. IV, 4ª Ed., Rio de Janeiro, Forense, 1986.

_____. *Prova judiciária no cível e comercial*. Volume V. São Paulo, Max Limonad, 1949.

SCARANCE FERNANDES, Antonio. Crimes praticados pelo computador: dificuldade de apuração dos fatos. *Boletim do Instituto Manoel Pedro Pimentel*, São Paulo, ano 2, n. 10, p. 25-37, dez. 1999.

_____. *Teoria geral do procedimento e o procedimento no processo penal*. São Paulo: RT, 2005.

_____. *Processo penal constitucional*. 4ª ed. São Paulo: RT, 2005.

_____. Reflexões sobre as noções de eficiência e de garantismo no processo penal. In: FERNANDES, Antonio Scarance; ALMEIDA, José Raul Gavião de; MORAES, Maurício Zanoide de (Coord.). *Sigilo no processo penal: eficiência e garantismo*. São Paulo: RT, 2008, p. 9-28.

_____; ALMEIDA, José Raul Gavião de; MORAES, Maurício Zanoide de (Coord.). *Sigilo no processo penal: eficiência e garantismo*. São Paulo, RT, 2008.

_____. GRINOVER, Ada Pellegrini; MAGALHÃES GOMES FILHO, Antonio. *As nulidades no processo penal*. 11ª ed. São Paulo: RT, 2009.

SILVA, Deonísio da. *A vida íntima das palavras: origens e curiosidades da língua portuguesa*. São Paulo: Arx, 2002.

SILVA, Virgílio Afonso da. *Direitos Fundamentais: conteúdo essencial, restrições e eficácia*. São Paulo: Malheiros, 2009.

SIQUEIRA, Galdino. *Curso de processo criminal*. 2ª Ed. Rio de Janeiro: Magalhães, 1939.

SIQUEIRA JUNIOR, Paulo Hamilton. Direito Informacional: Direito Da Sociedade Da Informação. *Revista dos Tribunais*, vol. 859, p. 743, Mai / 2007.

SOBRINHO, Mario Sergio; LACAVA, Thais Aroca Datcho. O sigilo profissional e a produção de prova. In: SCARANCE FERNANDES, Antonio; ALMEIDA, José Raul Gavião de; MOARES, Maurício Zanoide de. *Sigilo no processo penal: eficiência e garantismo*. São Paulo: RT, 2008.

SOUZA, Diego Fajardo Maranhã L. de. Busca e apreensão digital: prova penal atípica. *Boletim IBCCRIM*, São Paulo, ano 15, n. 181, p.14-15, dez. 2007.

TARUFFO, Michele. *La prova dei fatti giuridici – Nozioni generali*. Milão: Giuffrè, 1992.

THEODORO JUNIOR, Humberto. *Curso de Direito Processual Civil*. 18ª Ed., vol I, Rio de Janeiro: Forense, 1996.

TONINI, Paolo. *A prova no processo penal italiano*. São Paulo: RT, 2002.

TOURINHO FILHO, Fernando da Costa. *Processo penal*. 28ª Ed. São Paulo: Saraiva, 2006, vol. III.

TUCCI, Rogério Lauria. *Do corpo de delito no Direito Processual Penal brasileiro*. São Paulo: Saraiva, 1978.

_____. *Direitos e garantias individuais no processo penal brasileiro*. 3ª ed. São Paulo: RT, 2009.

UBERTIS, Giulio. La ricerca della verità giudiziale. In: _____. (Org). *La conoscenza del fatto nel processo penale*. Milano: Giuffrè, 1992.

VACIAGO, Giuseppe. Internet e crimini informatici In: PICCINNI, Mario Leone; VACIAGO, Giuseppe. *Computer crimes: casi pratici e metodologie investigative dei reati informatici*. Bergamo: Moretti & Vitali, 2008.

VAZ, Denise Provasi. Estudo sobre a verdade no processo penal. *Revista Brasileira de Ciências Criminais*, São Paulo, n. 83, v. 18, p. 163-183, mar/abr. 2010.

VIROTTA, Ítalo. *La perizia nel processo penale italiano*. Padova: CEDAM, 1968.

WALDEN, Ian. *Computer crimes and digital investigations*. Oxford: Oxford University Press, 2007.

YARSHELL, Flavio Luiz; MORAES, Mauricio Zanoide de. (Coord.). *Estudos em homenagem à Professora Ada Pellegrini Grinover*. São Paulo: DPJ Editora, 2005.

ZAPATA, María Florência; ABOSO, Gustavo Eduardo. *Cybercriminalidad y Derecho Penal*. Buenos Aires: Editorial B de f, 2006.

ZICCARDI, Giovanni. Le tecniche informatico-giuridiche di investigazione digitale. In: LUPARIA, Luca; ZICCARDI, Giovanni (Org.). *Investigazione penale e tecnologia informatica. L'accertamento del reato tra progresso scientifico e garanzie fondamentali*. Milão: Giuffrè, 2007.

_____. *Informatica Giuridica: privacy, sicurezza informatica, computer forensics e investigazioni digitali*. Milão: Giuffrè, 2008, tomo II.

_____. L'ingresso della *computer forensics* nel sistema processuale italiano: alcune considerazioni informático-giuridiche. In: LUPÁRIA, Luca (Org.). *Sistema penale e criminalità informatica. Profili sostanziali e processuali nella legge attuativa della Convenzione di Budapest sul cybercrime*. Milão: Giuffrè, 2009.

ZILLI, Marcos Alexandre Coelho. *A iniciativa instrutória do juiz no processo penal*. São Paulo: RT, 2003.

ZUCKERMAN, Adrian; ROBERTS, Paul. *Criminal evidence*. Oxford: Oxford University Press, 2004, reimpressão de 2008.

Sites consultados

Dicionário Houaiss da Língua Portuguesa.

Disponível em: <http://houaiss.uol.com.br/busca.jhtm?verbete=digital&stype=k>. Acesso em 15.01.2011, 28.12.2011, 04.01.2012.

História do Comitê Gestor da Internet

Disponível em: <http://www.cg.org.br/sobre-cg/historia.htm>. Acesso em 10.11.2011.

Informações sobre os resultados do Censo 2010.

Disponível em: http://www.ibge.gov.br/home/estatistica/populacao/censo2010/resultados_preliminares_amostra/default_resultados_preliminares_amostra.shtm. Acesso em 28.12.2011.

Disponível em: <http://www1.folha.uol.com.br/mercado/1007350-triplica-numero-de-casas-com-computador-diz-ibge.shtml>. Acesso em 28.12.2011.

Instruções das Cortes Federais norte-americanas aos jurados.

Disponível em: <http://federalevidence.com/evidence-resources/federal-jury-instructions>. Acesso em 02.01.2012.

Disponível em: <http://www.ca3.uscourts.gov/criminaljury/tocandinstructions.htm>. Acesso em 02.01.2012

Matéria sobre computação em nuvem.

Disponível em: <http://blogs.estadao.com.br/link/os-desafios-da-nuvem/>. Acesso em 15.01.2011.

Matéria sobre o estado da informática em 1981.

Disponível em: http://veja.abril.com.br/arquivo_veja/capa_10061981.shtml. Acesso em 10.11.2011.

Matéria sobre as vendas de computadores em 2011.

Disponível em: <http://video.globo.com/Videos/Player/Noticias/0,,GIM1598561-7823-BRASIL+ULTRAPASSA+O+JAPAO+NO+NUMERO+DE+COMPUTADORES+VENDIDOS,00.html>. Acesso em 10.11.2011.

Notícia sobre interceptações autorizadas em 2011.

Disponível em: <http://www.cnj.jus.br/noticias/cnj/17795-justica-autoriza-grampo-em-195-mil-telefones-em-2011>. Acesso em 14.01.2012.

Operações da Polícia Federal.

Disponível em: <http://www7.pf.gov.br/DCS/operacoes/indexop.html>. Acesso em 10.11.2011.

ANEXO – CONVENÇÃO SOBRE O CIBERCRIME

CONVENÇÃO SOBRE O CIBERCRIME

Budapeste, 23.XI.2001

Preâmbulo

Os Estados membros do Conselho da Europa e os seguintes Estados signatários,

Considerando que o objectivo do Conselho da Europa é realizar uma união mais estreita entre os seus membros;

Reconhecendo a importância de intensificar a cooperação com os outros Estados Partes da presente Convenção;

Convictos da necessidade de prosseguir, com carácter prioritário, uma política criminal comum, com o objectivo de proteger a sociedade contra a criminalidade no ciberespaço, designadamente, através da adopção de legislação adequada e da melhoria da cooperação internacional;

Conscientes das profundas mudanças provocadas pela digitalização, pela convergência e pela globalização permanente das redes informáticas;

Preocupados com o risco de que as redes informáticas e a informação electrónica, sejam igualmente utilizadas para cometer infracções criminais e de que as provas dessas infracções sejam armazenadas e transmitidas através dessas redes;

Reconhecendo a necessidade de uma cooperação entre os Estados e a indústria privada no combate à cibercriminalidade, bem como a necessidade de proteger os interesses legítimos ligados ao uso e desenvolvimento das tecnologias da informação;

Acreditando que uma luta efectiva contra a cibercriminalidade requer uma cooperação internacional em matéria penal acrescida, rápida e eficaz;

Convictos de que a presente Convenção é necessária para impedir os actos praticados contra a confidencialidade, integridade e disponibilidade de sistemas informáticos, de redes e dados informáticos, bem como a utilização fraudulenta de desses sistemas, redes e dados, assegurando a incriminação desses comportamentos tal como descritos na presente Convenção, e da adopção de poderes suficientes para combater eficazmente essas infracções, facilitando a detecção, a investigação e o procedimento criminal relativamente às referidas infracções, tanto ao nível nacional como internacional, e estabelecendo disposições materiais com vista a uma cooperação internacional rápida e fiável;

Tendo presente a necessidade de garantir um equilíbrio adequado entre os interesses da aplicação da lei e o respeito pelos direitos fundamentais do ser

humano, tal como garantidos pela Convenção para a Protecção dos Direitos do Homem e das Liberdades Fundamentais do Conselho da Europa de 1950, pelo Pacto Internacional sobre os Direitos Civis e Políticos das Nações Unidas de 1966, bem como por outros tratados internacionais aplicáveis em matéria de direitos do Homem, que reafirmam o direito à liberdade de opinião sem qualquer ingerência, o direito à liberdade de expressão, incluindo a liberdade de procurar, de receber e transmitir informações e ideias de qualquer natureza sem considerações de fronteiras e, ainda, o direito ao respeito pela vida privada;

Tendo igualmente presente o direito à protecção de dados pessoais, tal como é conferido, por exemplo, pela Convenção do Conselho da Europa de 1981, para a Protecção das Pessoas relativamente ao Tratamento Automatizado de Dados de Carácter Pessoal;

Considerando a Convenção das Nações Unidas sobre os Direitos da Criança de 1989, e a Convenção da Organização Internacional do Trabalho sobre as Piores Formas do Trabalho Infantil de 1999;

Tendo em conta as convenções existentes do Conselho da Europa sobre a cooperação em matéria penal, bem como outros tratados similares celebrados entre os Estados membros do Conselho da Europa e outros Estados, e sublinhando que a presente Convenção tem por finalidade complementar as referidas convenções, de modo a tornar mais eficazes as investigações e as acções penais relativas a infracções penais relacionadas com sistemas e dados informáticos, bem como permitir a recolha de provas em forma electrónica de uma infracção penal;

Saudando os recentes desenvolvimentos destinados a aprofundar o entendimento e cooperação internacionais no combate à criminalidade no ciberespaço, nomeadamente, as acções empreendidas pelas Nações Unidas, pela OCDE, pela União Europeia e pelo G8;

Recordando as Recomendações do Comité de Ministros N.º R (85) 10 relativa à aplicação prática da Convenção Europeia sobre Auxílio Judiciário Mútuo em Matéria Penal quanto às cartas rogatórias para a interceptação de telecomunicações, N.º R (88) 2 sobre as medidas destinadas a combater a pirataria no domínio do direito de autor e dos direitos conexos, N.º R (87) 15 que regula a utilização de dados de carácter pessoal no sector da polícia, N.º R (95) 4 relativa à protecção dos dados de carácter pessoal no sector das telecomunicações, tendo em conta, designadamente os serviços telefónicos e a N.º R (89) 9 sobre a criminalidade informática que estabelece directrizes para os legisladores nacionais respeitantes à definição de certos crimes informáticos e, ainda, a N.º R (95) 13 relativa a problemas processuais penais relacionados com as tecnologias da informação;

Tendo em conta a Resolução n.º 1 adoptada pelos Ministros Europeus da Justiça na sua 21ª Conferência (Praga, 10 e 11 de Junho de 1997), que recomenda ao Comité de Ministros para apoiar o trabalho desenvolvido pelo Comité Europeu para os Problemas Criminais (CDPC) sobre a cibercriminalidade a fim de aproximar as legislações penais nacionais e de permitir a utilização de meios de investigação eficazes em matéria de crimes informáticos, bem como a Resolução n.º 3, adoptada na 23ª Conferência dos Ministros Europeus da Justiça (Londres, 8 e 9 de Junho de 2000), que incentiva as partes intervenientes nas negociações a prosseguirem os seus esforços para encontrar soluções apropriadas que permitam o maior número

possível de Estados a tornarem-se Partes da Convenção e reconhece a necessidade de dispor de um mecanismo rápido e eficaz de cooperação internacional, que tenha devidamente em conta as exigências específicas da luta contra a cibercriminalidade;

Tendo igualmente em conta o Plano de Acção adoptado pelos Chefes de Estado e de Governo do Conselho da Europa, por ocasião da sua Segunda Cimeira (Estrasburgo, 10 e 11 de Outubro de 1997), para procurar respostas comuns face ao desenvolvimento das novas tecnologias da informação, com base nas normas e princípios do Conselho da Europa;

Acordaram no seguinte:

Capítulo I – Terminologia

Artigo 1º - Definições

Para os fins da presente Convenção:

- a) “Sistema informático” significa qualquer dispositivo isolado ou grupo de dispositivos relacionados ou interligados, em que um ou mais de entre eles, desenvolve, em execução de um programa, o tratamento automatizado dos dados;
- b) “Dados informáticos” significa qualquer representação de factos, de informações ou de conceitos sob uma forma susceptível de processamento num sistema de computadores, incluindo um programa, apto a fazer um sistema informático executar uma função;
- c) “Fornecedor de serviço” 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.
- d) “Dados de tráfego” significa todos os dados informáticos relacionados com uma comunicação efectuada por meio de um sistema informático, gerados por este sistema como elemento de uma cadeia de comunicação, indicando a origem da comunicação, o destino, o trajecto, a hora, a data, o tamanho, a duração ou o tipo do serviço subjacente.

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

Artigo 2º - Acesso ilegítimo

Cada Parte adoptará as medidas legislativas e outras que se revelem necessárias para estabelecer como infracção penal, no seu direito interno, o acesso intencional e ilegítimo à totalidade ou a parte de um sistema informático. As Partes podem exigir que a infracção seja cometida com a violação de medidas de segurança, com a intenção de obter dados informáticos ou outra intenção ilegítima, ou que seja relacionada com um sistema informático conectado a outro sistema informático.

Artigo 3º - Intercepção ilegítima

Cada Parte adoptará as medidas legislativas e outras que se revelem necessárias para estabelecer como infracção penal, no seu direito interno, a intercepção intencional e ilegítima de dados informáticos, efectuada por meios técnicos, em transmissões não públicas, para, de ou dentro de um sistema informático, incluindo emissões electromagnéticas provenientes de um sistema informático que veicule esses dados. As Partes podem exigir que a infracção seja cometida com dolo ou que seja relacionada com um sistema informático conectado com outro sistema informático.

Artigo 4º - Interferência em dados

1. Cada Parte adoptará as medidas legislativas e outras que se revelem necessárias para estabelecer como infracção penal, no seu direito interno, o acto de intencional e ilegitimamente danificar, apagar, deteriorar, alterar ou eliminar dados informáticos.
2. Uma Parte pode reservar-se o direito de exigir que a conduta descrita no n.º 1 provoque danos graves.

Artigo 5º - Interferência em sistemas

Cada Parte adoptará as medidas legislativas e outras que se revelem necessárias para estabelecer como infracção penal, no seu direito interno, a obstrução grave, intencional e ilegítima, ao funcionamento de um sistema informático, através da introdução, transmissão, danificação, eliminação, deterioração, modificação ou supressão de dados informáticos.

Artigo 6º - Uso abusivo de dispositivos

1. Cada Parte adoptará as medidas legislativas e outras que se revelem necessárias para estabelecer como infracções penais, em conformidade com o seu direito interno, quando cometidas intencional e ilegitimamente:
 - a) A produção, a venda, a obtenção para utilização, a importação, a distribuição, ou outras formas de disponibilização de:
 - i. Um dispositivo, incluindo um programa informático, concebido ou adaptado essencialmente para permitir a prática de uma das infracções definidas em conformidade com os artigos 2º a 5º;

ii. Uma palavra-passe, um código de acesso ou dados informáticos semelhantes que permitam aceder a todo, ou a parte de um sistema informático

com a intenção de serem utilizados para cometer qualquer uma das infracções definidas nos Artigos 2º a 5º; e

- b) A posse de um elemento referido nos alínea a), i. ou ii., com a intenção de ser utilizado com o objectivo de cometer qualquer uma das infracções referidas nos artigos 2º a 5º. As Partes podem exigir que no direito interno se reúna um certo número desses elementos para que seja determinada a responsabilidade criminal.
2. O presente artigo não deve ser interpretado como impondo responsabilidade criminal quando a produção, a venda, a aquisição para utilização, a importação, a distribuição, ou outra forma de disponibilização ou posse, mencionadas no n.º1 do presente artigo não tenham por objectivo cometer uma infracção estabelecida em conformidade com os artigos 2º a 5º da presente Convenção, como é o caso de ensaios autorizados ou de protecção de um sistema informático.
3. Cada Parte pode reservar-se o direito de não aplicar o disposto no n.º 1 do presente artigo desde que essa reserva não diga respeito à venda, distribuição, ou a qualquer outra forma de disponibilização dos elementos referidos no n.º 1, a), ii.

Título 2 – Infracções relacionada com computadores

Artigo 7º - Falsidade informática

Cada Parte adoptará as medidas legislativas e outras que se revelem necessárias para estabelecer como infracção penal, em conformidade com o seu direito interno, a introdução, a alteração, a eliminação ou a supressão intencional e ilegítima de dados informáticos, produzindo dados não autênticos, com a intenção de que estes sejam considerados ou utilizados para fins legais como se fossem autênticos, quer sejam ou não directamente legíveis e inteligíveis. Uma Parte pode exigir no direito interno uma intenção fraudulenta ou uma intenção ilegítima similar para que seja determinada a responsabilidade criminal.

Artigo 8º - Burla informática

Cada Parte adoptará as medidas legislativas e outras que se revelem necessárias para estabelecer como infracção penal, em conformidade com o seu direito interno, o acto intencional e ilegítimo, que origine a perda de bens a terceiros através:

- a) Da introdução, da alteração, da eliminação ou da supressão de dados informáticos,
- b) De qualquer intervenção no funcionamento de um sistema informático,

com a intenção de obter um benefício económico ilegítimo para si ou para terceiros.

Título 3 – Infracções relacionadas com o conteúdo

Artigo 9º - Infracções relacionadas com pornografia infantil

1. Cada Parte adoptará as medidas legislativas e outras que se revelem necessárias para estabelecer como infracção penal, em conformidade com o seu direito interno, as seguintes condutas, quando cometidas de forma intencional e ilegítima:
 - a) Produzir pornografia infantil com o objectivo da sua difusão através de um sistema informático;
 - b) Oferecer ou disponibilizar pornografia infantil através de um sistema informático;
 - c) Difundir ou transmitir pornografia infantil através de um sistema informático;
 - d) Obter pornografia infantil através de um sistema informático para si próprio ou para terceiros;
 - e) Possuir pornografia infantil num sistema informático ou num meio de armazenamento de dados informáticos.
2. Para efeitos do n.º 1, a expressão “pornografia infantil” inclui qualquer material pornográfico que represente visualmente:
 - a) Um menor envolvido num comportamento sexualmente explícito;
 - b) Uma pessoa que aparente ser menor envolvida num comportamento sexualmente explícito;
 - c) Imagens realísticas que representem um menor envolvido num comportamento sexualmente explícito;
3. Para efeitos do n.º 2, a expressão “menor” inclui qualquer pessoa com idade inferior a 18 anos. Uma Parte, pode, no entanto, exigir um limite de idade inferior, que não será menos que 16 anos.
4. Cada Parte pode reservar-se o direito de não aplicar, no todo ou em parte, o disposto nos n.ºs 1, alínea d), e., 2, alíneas b) e c).

Título 4 – Infracções relacionadas com a violação do direito de autor e direitos conexos

Artigo 10º - Infracções relacionadas com a violação do direito de autor e dos direitos conexos

1. Cada Parte adoptará as medidas legislativas e outras que se revelem necessárias para estabelecer como infracção penal, em conformidade com o seu direito interno, a violação do direito de autor definido pela legislação dessa Parte, em conformidade com as obrigações que a mesma assumiu em aplicação da Convenção Universal sobre o Direito de Autor, revista em Paris, em 24 de Julho de 1971, da Convenção de Berna para a Protecção das Obras Literárias e Artísticas, do Acordo sobre os Aspectos dos Direitos de Propriedade Intelectual Relacionados com o Comércio, e do Tratado da OMPI sobre o Direito de Autor, com excepção de quaisquer direitos morais conferidos por essas Convenções, quando esses actos forem praticados intencionalmente, a uma escala comercial e por meio de um sistema informático.
2. Cada Parte adoptará as medidas legislativas e outras que se revelem necessárias para estabelecer como infracção penal, em conformidade com o seu direito interno, a violação dos direitos conexos definidos pela legislação dessa Parte, em conformidade com as obrigações assumidas por força da Convenção Internacional para a Protecção dos Artistas Intérpretes ou Executantes, dos Produtores de Fonogramas e dos Organismos de Radiodifusão (Convenção de Roma) do Acordo sobre Aspectos dos Direitos de Propriedade Intelectual Relacionados com o Comércio, e do Tratado da OMPI sobre Interpretações, Execuções e Fonogramas, com excepção de qualquer direito moral conferido por essas Convenções, quando esses actos forem praticados intencionalmente, a uma escala comercial e por meio de um sistema informático.
3. Uma Parte pode, em circunstâncias bem delimitadas, reservar-se o direito de não determinar a responsabilidade penal nos termos dos n.ºs 1 e 2 do presente artigo, na condição de estarem disponíveis outros meios eficazes e essa reserva não prejudique as obrigações internacionais que incumbem a essa Parte, em aplicação dos instrumentos internacionais mencionados nos n.ºs 1 e 2 do presente artigo.

Título 5 – Outras formas de Responsabilidade e Sanções

Artigo 11º - Tentativa e cumplicidade

1. Cada Parte adoptará as medidas legislativas e outras que se revelem necessárias para estabelecer como infracção penal, em conformidade com o seu direito interno, a cumplicidade, quando cometida intencionalmente, na prática de qualquer uma das infracções estabelecidas de acordo com os artigos 2º a 10º da presente Convenção, com a intenção de que essa infracção seja cometida.
2. Cada Parte adoptará as medidas legislativas e outras que se revelem necessárias para estabelecer como infracção penal, em conformidade com o seu direito interno, a tentativa de cometer uma das infracções estabelecidas nos artigos 3º, 5º, 7º, 8º, 9º, 1., alínea a) e 9, 1. alínea c) da presente Convenção.
3. Cada Parte pode reservar-se o direito de não aplicar, no todo ou em parte, o disposto no n.º 2 do presente artigo.

Artigo 12º - Responsabilidade de pessoas colectivas

1. Cada Parte adoptará as medidas legislativas e outras que se revelem necessárias para assegurar que as pessoas colectivas possam ser consideradas responsáveis por infracções estabelecidas de acordo com a presente Convenção, quando cometidas em seu benefício por uma pessoa singular agindo quer individualmente, quer como membro de um órgão da pessoa colectiva que exerça no seu seio uma posição de direcção, com base no seguinte:
 - a) Poder de representação da pessoa colectiva;
 - b) Autoridade para tomar decisões em nome da pessoa colectiva;
 - c) Autoridade para exercer controlo no seio da pessoa colectiva.
2. Além dos casos já previstos no n.º 1 deste artigo, cada Parte adoptará as medidas necessárias para assegurar que uma pessoa colectiva possa ser considerada responsável quando a ausência de supervisão ou de controlo por parte de uma pessoa singular, mencionada no n.º 1 tornou possível a prática de infracções previstas na presente Convenção, em benefício da referida pessoa colectiva por uma pessoa singular agindo sob a sua autoridade.
3. De acordo com os princípios jurídicos da Parte, a responsabilidade de uma pessoa colectiva pode ser criminal, civil ou administrativa.
4. Essa responsabilidade deve ser determinada sem prejuízo da responsabilidade criminal das pessoas singulares que cometeram a infracção.

Artigo 13º - Sanções e medidas

1. Cada Parte adoptará as medidas legislativas e outras que se revelem necessárias para assegurar que as infracções penais verificadas em aplicação dos Artigos 2º a 11º sejam passíveis de sanções eficazes, proporcionais e dissuasivas, incluindo penas privativas da liberdade.
2. Cada Parte assegurará que as pessoas colectivas consideradas responsáveis nos termos do artigo 12º, fiquem sujeitas à aplicação de sanções ou medidas, penais ou não penais eficazes, proporcionais e dissuasivas, incluindo sanções pecuniárias.

Secção 2 – Direito Processual

Título 1 – Disposições comuns

Artigo 14º - Âmbito das disposições processuais

1. Cada Parte adoptará as medidas legislativas e outras que se revelem necessárias, para instituir os poderes e os procedimentos previstos na presente Secção, para fins de investigação ou de procedimento penal.

2. Salvo disposição em contrário constante do artigo 21º, cada Parte aplicará os poderes e procedimentos referidos no n.º 1:
 - a) Às infracções penais em conformidade com o disposto nos artigos 2º a 11º da presente Convenção;
 - b) A outras infracções penais cometidas por meio de um sistema informático; e
 - c) À recolha de prova em suporte electrónico provas electrónicas de qualquer infracção penal.
3. a) Cada Parte pode reservar-se o direito de apenas aplicar as medidas referidas no artigo 20º às infracções ou categorias de infracções especificadas na reserva, desde que o conjunto dessas infracções ou categorias de infracções não seja mais reduzido do que o conjunto de infracções às quais aplica as medidas referidas no artigo 21º. Cada Parte procurará limitar essa reserva de modo a permitir a aplicação mais ampla possível da medida referida no Artigo 20º.
 - b) Nos casos em que uma Parte, devido a restrições impostas pela sua legislação em vigor no momento da adopção da presente Convenção, não puder aplicar as medidas referidas nos Artigos 20º e 21º às comunicações transmitidas num sistema informático de um fornecedor de serviços, que
 - i. Esteja em funcionamento para benefício de um grupo fechado de utilizadores, e
 - ii. Não utilize redes públicas de telecomunicações e não esteja em conexão com outro sistema informático, quer seja público ou privado,
 essa Parte pode reservar-se o direito de não aplicar essas medidas às referidas comunicações. Cada Parte procurará limitar essa reserva de modo a permitir a aplicação mais ampla possível das medidas referidas nos Artigos 20º e 21º.

Artigo 15º - Condições e salvaguardas

1. Cada Parte assegurará que o estabelecimento, a entrada em vigor e a aplicação dos poderes e procedimentos previstos na presente Secção são sujeitos às condições e salvaguardas estabelecidas pela legislação nacional, que deve assegurar uma protecção adequada dos direitos do Homem e das liberdades, designadamente estabelecidas em conformidade com as obrigações decorrentes da aplicação da Convenção do Conselho da Europa para a Protecção dos Direitos do Homem e das Liberdades Fundamentais dos Cidadãos (1950), do Pacto Internacional das Nações Unidas sobre os Direitos Cívicos e Políticos, (1966), bem como de outros instrumentos internacionais aplicáveis relativos aos Direitos do Homem e que deve integrar o princípio da proporcionalidade.
2. Quando for apropriado, tendo em conta a natureza do poder ou do procedimento em questão, as referidas condições e salvaguardas incluirão, designadamente, um controlo judicial ou outras formas de controlo

independente, os fundamentos que justificam a sua aplicação, bem como a limitação do âmbito de aplicação e a duração do poder ou procedimento em causa.

3. Na medida em que seja do interesse público, em particular da boa administração da justiça, cada Parte examinará o efeito dos poderes e dos procedimentos da presente Secção sobre os direitos, responsabilidades e interesses legítimos de terceiros.

Título 2 – Conservação expedita de dados informáticos armazenados

Artigo 16º - Conservação expedita de dados informáticos armazenados

1. Cada Parte adoptará as medidas legislativas e outras que se revelem necessárias para permitir às suas autoridades competentes exigir ou obter de uma outra forma a conservação expedita de dados informáticos 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.
2. Sempre que a Parte aplique o disposto no n.º 1, através de uma injunção ordenando a uma pessoa que conserve os dados informáticos específicos armazenados que estão na sua posse ou sob o seu controlo, esta Parte adoptará as medidas legislativas e outras que se revelem necessárias para obrigar essa pessoa a conservar e proteger a integridade dos referidos dados durante um período de tempo tão longo quanto necessário, até um máximo de 90 dias, de modo a permitir às autoridades competentes obter a sua divulgação. Uma Parte pode prever que essa injunção seja subsequentemente renovada.
3. Cada Parte adoptará as medidas legislativas e outras que se revelem necessárias para obrigar o responsável pelos dados, ou outra pessoa encarregada de os conservar a manter segredo sobre a execução dos referidos procedimentos durante o período previsto pelo seu direito interno.
4. Os poderes e procedimentos referidos no presente artigo devem estar sujeitos aos artigos 14º e 15º.

Artigo 17º - Conservação expedita e divulgação parcial de dados de tráfego

1. A fim de assegurar a conservação de dados relativos ao tráfego em aplicação do artigo 16º, cada Parte adoptará as medidas legislativas e outras que se revelem necessárias, para:
 - a) Assegurar a conservação rápida desses dados de tráfego, quer tenham participado na transmissão dessa comunicação um ou vários fornecedores de serviços; e

- b) Assegurar a divulgação rápida à autoridade competente da Parte ou a uma pessoa designada por essa autoridade, de uma quantidade de dados de tráfego, suficiente para permitir a identificação dos fornecedores de serviços e da via através do qual a comunicação foi efectuada.
2. Os poderes e procedimentos referidos no presente artigo devem estar sujeitos aos artigos 14º e 15º.

Título 3 – Injunção

Artigo 18º - Injunção

1. Cada Parte adoptará as medidas legislativas e outras que se revelem necessárias para habilitar as suas autoridades competentes para ordenar:
- a) A uma pessoa que se encontre no seu território que comunique os dados informáticos específicos, na sua posse ou sob o seu controlo e armazenados num sistema informático ou num outro suporte de armazenamento de dados informáticos; e
- b) A um fornecedor de serviços que preste serviços no território da Parte, que comunique os dados na sua posse ou sob o seu controlo, relativos aos assinantes e respeitantes a esses serviços
2. Os poderes e procedimentos referidos no presente artigo devem estar sujeitos aos artigos 14º e 15º.
3. Para os fins do presente artigo, a expressão “dados relativos aos assinantes” designa qualquer informação, contida sob a forma de dados informáticos ou sob qualquer outra forma, detida por um fornecedor de serviços e que diga respeito aos assinantes dos seus serviços, diferentes dos dados relativos ao tráfego ou ao conteúdo e que permitam determinar:
- a) O tipo de serviço de comunicação utilizado, as medidas técnicas tomadas a esse respeito e o período de serviço;
- b) A identidade, a morada postal ou geográfica e o número de telefone do assinante, e qualquer outro número de acesso, os dados respeitantes à facturação e ao pagamento, disponíveis com base num contrato ou acordo de serviços;
- c) Qualquer outra informação sobre a localização do equipamento de comunicação, disponível com base num contrato ou acordo de serviços.

Título 4 – Busca e Apreensão de dados informáticos armazenados

Artigo 19º - Busca e apreensão de dados informáticos armazenados

1. Cada Parte adoptará as medidas legislativas e outras que se revelem necessárias para habilitar as suas autoridades competentes para proceder a buscas ou aceder de modo semelhante:

- a) A um sistema informático ou a uma parte do mesmo, bem como a dados informáticos que nele se encontrem armazenados; e
 - b) A um suporte que permita armazenar dados informáticos.
2. Cada Parte adoptará as medidas legislativas e outras que se revelem necessárias para assegurar que, nos casos em que as suas autoridades procedam a buscas ou acedam de forma semelhante a um sistema informático específico ou a uma parte do mesmo, em conformidade com o disposto no n.º 1, a), e tenham razões para pensar que os dados procurados se encontram armazenados noutro sistema informático ou numa parte do mesmo situado no seu território, e que esses dados são legalmente acessíveis a partir do sistema inicial ou obteníveis a partir desse sistema inicial, as referidas autoridades estejam em condições de estender de forma expedita a busca, ou o acesso de forma semelhante ao outro sistema.
3. Cada Parte adoptará as medidas legislativas e outras que se revelem necessárias para habilitar as suas autoridades competentes para apreender ou para obter de forma semelhante os dados informáticos relativamente aos quais o acesso foi realizado em aplicação dos n.ºs 1 ou 2. Essas medidas incluem as prerrogativas seguintes:
- a) Apreender ou obter de forma semelhante um sistema informático ou uma parte deste ou um suporte de armazenamento informático;
 - b) Realizar e conservar uma cópia desses dados informáticos;
 - c) Preservar a integridade dos dados informáticos pertinentes armazenados; e
 - d) Tornar inacessíveis ou eliminar esses dados do sistema informático acedido.
4. Cada Parte adoptará as medidas legislativas e outras que se revelem necessárias para habilitar as suas autoridades competentes a ordenar a qualquer pessoa que conheça o funcionamento do sistema informático ou as medidas utilizadas para proteger os dados informáticos nele contidos, que forneça na medida do razoável as informações razoavelmente necessárias, para permitir a aplicação das medidas previstas nos n.ºs 1 e 2.
5. Os poderes e procedimentos referidos no presente artigos devem estar sujeitos aos artigos 14º e 15º.

Título 5 – Recolha em tempo real de dados informáticos

Artigo 20º - Recolha em tempo real de dados relativos ao tráfego

1. Cada Parte adoptará as medidas legislativas e outras que se revelem necessárias para habilitar as suas autoridades competentes a:
- a) Recolher ou registar, através da aplicação de meios técnicos existentes no seu território, e

- b) Obrigar um fornecedor de serviços, no âmbito da sua capacidade técnica existente, a:
 - i. Recolher ou registar por meio da aplicação de meios técnicos no seu território, ou
 - ii. Prestar às autoridades competentes o seu apoio e assistência para recolher ou registar,

em tempo real, dados de tráfego relativos a comunicações específicas no seu território transmitidas através de um sistema informático.
- 2. Quando uma Parte, em virtude dos princípios estabelecidos pela sua ordem jurídica interna, não pode adoptar as medidas descritas no nº 1, alínea a), pode, em alternativa, adoptar as medidas legislativas e outras que se revelem necessárias para assegurar a recolha ou o registo em tempo real dos dados de tráfego associados a comunicações específicas transmitidas no seu território através da aplicação de meios técnicos existentes nesse território.
- 3. Cada Parte adoptará as medidas legislativas e outras que se revelem necessárias para obrigar um fornecedor de serviços a manter secreto o facto de qualquer um dos poderes previstos ter sido executado, bem como qualquer informação a esse respeito.
- 4. Os poderes e procedimentos referidos no presente artigo devem estar sujeitos aos artigos 14º e 15º.

Artigo 21º - Intercepção de dados relativos ao conteúdo

- 1. Cada Parte adoptará as medidas legislativas e outras que se revelem necessárias para habilitar as suas autoridades competentes relativamente a um leque de infracções graves, a definir em direito interno, a:
 - a) Recolher ou registar, através da aplicação de meios técnicos existentes no seu território, e
 - b) Obrigar um fornecedor de serviços, no âmbito da sua capacidade técnica existente, a:
 - i. Recolher ou registar através da aplicação de meios técnicos no seu território, ou
 - ii. Prestar às autoridades competentes o seu apoio e a sua assistência para recolher ou registar,

em tempo real, dados relativos ao conteúdo de comunicações específicas no seu território, transmitidas através de um sistema informático.
- 2. Quando a Parte em virtude dos princípios estabelecidos pela sua ordem jurídica interna, não pode adoptar as medidas descritas no n.º 1, alínea a), pode, em alternativa, adoptar as medidas legislativas e outras que se revelem

necessárias, para assegurar a recolha ou o registo em tempo real dos dados relativos ao conteúdo associados a comunicações específicas transmitidas no seu território através da aplicação de meios técnicos existentes nesse território.

3. Cada Parte adoptará as medidas legislativas e outras que se revelem necessárias, para obrigar um fornecedor de serviços a manter secreto o facto de qualquer um dos poderes previstos no presente artigo ter sido executado, bem como qualquer informação a esse respeito.
4. Os poderes e procedimentos referidos no presente artigo devem estar sujeitos aos artigos 14º e 15º.

Secção 3 – Competência

Artigo 22º - Competência

1. Cada Parte adoptará as medidas legislativas e outras que se revelem necessárias para estabelecer a sua competência relativamente a qualquer infracção penal definida em conformidade com os artigos 2º a 11º da presente Convenção, sempre que a infracção seja cometida:
 - a) No seu território; ou
 - b) A bordo de um navio arvorando o pavilhão dessa Parte;
 - c) A bordo de uma aeronave matriculada nessa Parte e segundo as suas Leis; ou
 - d) Por um dos seus cidadãos nacionais, se a infracção for punível criminalmente onde foi cometida ou se a infracção não for da competência territorial de nenhum Estado.
2. Cada Parte pode reservar-se o direito de não aplicar ou de apenas aplicar em casos ou em condições específicas, as regras de competência definidas no n.º1, alínea b) a alínea d) do presente artigo ou em qualquer parte dessas alíneas.
3. Cada Parte adoptará as medidas que se revelem necessárias para estabelecer a sua competência relativamente a qualquer infracção referida no artigo 24º, n.º1 da presente Convenção, quando o presumível autor da infracção se encontre no seu território e não puder ser extraditado para outra Parte, apenas com base na sua nacionalidade, após um pedido de extradição.
4. A presente Convenção não exclui qualquer competência penal exercida por uma Parte em conformidade com o seu direito interno.
5. Quando mais que uma Parte reivindique a competência em relação uma presumível infracção prevista na presente Convenção, as Partes em causa, se for oportuno, consultar-se-ão a fim de determinarem qual é a jurisdição mais apropriada para o procedimento penal.

Capítulo III – Cooperação Internacional

Secção 1 – Princípios gerais

Título 1 – Princípios gerais relativos à cooperação internacional

Artigo 23º - Princípios gerais relativos à cooperação internacional

As Partes cooperarão entre si, em conformidade com as disposições do presente capítulo, em aplicação dos instrumentos internacionais pertinentes sobre a cooperação internacional em matéria penal, de acordos celebrados com base nas legislações uniformes ou recíprocas, e do seu direito nacional, na medida mais ampla possível, para efeitos de investigações ou de procedimentos relativos a infracções penais relacionadas com sistemas e dados informáticos, ou para recolher provas sob a forma electrónica de uma infracção penal.

Título 2 – Princípios relativos à extradição

Artigo 24º - Extradição

1. a) O presente artigo aplica-se à extradição entre as Partes relativamente a infracções penais definidas em conformidade com os artigos 2º a 11º da presente Convenção, desde que sejam puníveis na legislação de duas Partes envolvidas, por uma pena privativa de liberdade por um período máximo de, pelo menos um ano ou através de uma pena mais grave.

b) Quando for exigida uma pena mínima diferente, com base num tratado de extradição aplicável entre duas ou mais Partes, incluindo a Convenção Europeia de Extradição (STE N° 24), ou num acordo baseado em legislações uniformes ou recíprocas, é a pena mínima prevista por esse tratado ou acordo que se aplica.
2. As infracções penais descritas no n.º 1 do presente artigo são consideradas como infracções passíveis de extradição em qualquer tratado de extradição existente ou que venha a existir entre as Partes. As Partes comprometer-se-ão a incluir essas infracções como infracções passíveis de extradição em qualquer tratado de extradição que possa ser firmado entre as Partes.
3. Quando uma Parte condicionar a extradição à existência de um tratado e receba um pedido de extradição de outra Parte com a qual não tenha celebrado qualquer tratado de extradição, pode considerar a presente Convenção como base jurídica para a extradição relativamente a qualquer infracção penal referida no n.º 1 do presente artigo.
4. As Partes que não condicionem a extradição à existência de um tratado, reconhecerão entre si as infracções penais referidas no n.º 1 do presente artigo como infracções passíveis de extradição.
5. A extradição ficará sujeita às condições previstas pelo direito interno da Parte requerida ou pelos tratados de extradição aplicáveis, incluindo os fundamentos com base nos quais a Parte requerida pode recusar a extradição.

6. No caso de a extradição por uma infracção penal mencionada no n.º 1 do presente artigo ser recusada unicamente com base na nacionalidade da pessoa procurada, ou pelo facto de a Parte requerida se considerar competente relativamente a essa infracção, a Parte requerida remeterá o processo, a pedido da Parte requerente, às suas autoridades competentes para fins de procedimento criminal e comunicará em tempo útil o resultado do processo à Parte requerente. As autoridades em questão tomarão a sua decisão e conduzirão a investigação e o procedimento do mesmo modo que em relação a qualquer outra infracção de natureza comparável, em conformidade com a legislação desta Parte.
7.
 - a) Cada Parte comunicará ao Secretário Geral do Conselho da Europa, no momento da assinatura ou do depósito do seu instrumento de ratificação, aceitação, aprovação ou adesão, o nome e morada de cada autoridade responsável pelo envio ou pela recepção de um pedido de extradição ou de detenção preventiva, no caso de ausência de tratado.
 - b) O Secretário Geral do Conselho da Europa constituirá e manterá actualizado um registo das autoridades assim designadas pelas Partes. Cada Parte deve assegurar com permanência a exactidão dos dados que constam do registo.

Título 3 – Princípios Gerais relativos ao auxílio mútuo .

Artigo 25º - Princípios gerais relativos ao auxílio mútuo.

1. As Partes concederão entre si o auxílio mútuo mais amplo possível para efeitos de investigações ou de procedimentos relativos a infracções penais relacionadas com sistemas e dados informáticos, ou para efeitos de recolha de provas sob a forma electrónica de uma infracção penal.
2. Cada Parte adoptará igualmente as medidas legislativas e outras que se revelem necessárias para darem cumprimento às obrigações estabelecidas nos artigos 27º a 35º.
3. Em caso de urgência, cada Parte pode formular os pedidos de auxílio mútuo ou comunicações com ele relacionadas, através de meios de comunicação rápidos, tais como o fax ou o correio electrónico, desde que esses meios ofereçam condições de segurança e de autenticação (incluindo, se necessário, o uso da encriptação) com posterior confirmação oficial sempre que o Estado requerido o exigir. O Estado requerido aceitará o pedido e responderá através de qualquer desses meios de comunicação rápidos.
4. Salvo disposição em contrário expressamente prevista nos artigos do presente Capítulo, o auxílio mútuo será sujeito às condições fixadas pelo direito interno da Parte requerida ou pelos tratados de auxílio mútuo aplicáveis, incluindo os fundamentos com base nos quais a Parte requerida pode recusar a cooperação. A Parte requerida não deve exercer o seu direito de recusar o auxílio mútuo relativamente às infracções previstas nos artigos 2º a 11º apenas com fundamento em que o pedido se refere a uma infracção que considera ser de natureza fiscal.

5. Quando em conformidade com as disposições do presente capítulo, a Parte requerida estiver autorizada a subordinar o auxílio mútuo à existência de dupla incriminação, esta condição será considerada como satisfeita se o comportamento que constitui a infracção relativamente à qual foi efectuado o pedido de auxílio, for qualificado como infracção penal pelo seu direito interno, quer o direito interno classifique ou não a infracção na mesma categoria de infracções ou a designe ou não pela mesma terminologia que o direito da Parte requerente.

Artigo 26º - Informação espontânea

1. Uma Parte pode, dentro dos limites da sua legislação nacional e na ausência de pedido prévio, comunicar a outra Parte informações obtidas no quadro das suas próprias investigações, sempre que considerar que isso pode ajudar a Parte destinatária a iniciar ou a levar a cabo investigações ou procedimentos relativos a infracções penais, estabelecidas em conformidade com a presente Convenção, ou sempre que essas informações possam conduzir a um pedido formulado por essa Parte, nos termos do presente Capítulo.
2. Antes de comunicar essas informações, a Parte que as fornece pode solicitar que as mesmas permaneçam confidenciais ou apenas sejam utilizadas em determinadas condições. Caso a Parte destinatária não puder dar satisfação a esse pedido, deve informar a outra Parte desse facto que determinará se as informações devem contudo ser fornecidas. Se a Parte destinatária aceitar a informação nas condições estipuladas, fica obrigada a observar essas condições.

Título 4 – Procedimentos relativos aos pedidos de auxílio mútuo na ausência de acordos internacionais aplicáveis

Artigo 27º - Procedimentos relativos aos pedidos de auxílio mútuo na ausência de acordos internacionais aplicáveis

1. Na ausência de tratado de auxílio mútuo ou de acordo de que se baseie em legislação uniforme ou recíproca em vigor entre a Parte requerente e a Parte requerida, serão aplicáveis as disposições dos n.ºs 2 a 9 do presente artigo. Não serão aplicáveis se existir um tratado, um acordo, ou legislação deste tipo, a menos que as Partes em causa decidam aplicar em sua substituição o presente artigo no todo ou em parte.
2.
 - a) Cada Parte designará uma ou mais autoridades centrais encarregadas de enviar os pedidos de auxílio mútuo ou de lhes responder, de os executar ou de os transmitir às autoridades competentes para a sua execução;
 - b) As autoridades centrais comunicarão directamente entre si;
 - c) Cada Parte, no momento da assinatura ou do depósito dos seus instrumentos de ratificação, aceitação, aprovação ou adesão, comunicará ao Secretário Geral do Conselho da Europa os nomes e moradas das autoridades designadas em aplicação do presente parágrafo.

- d) O Secretário Geral do Conselho da Europa constituirá e manterá actualizado um registo das autoridades centrais designadas pelas Partes. Cada Parte assegurará em permanência a exactidão dos dados constantes do registo.
- 3. Os pedidos de auxílio ao abrigo do presente artigo serão executados em conformidade com os procedimentos especificados pela Parte requerente, excepto se forem incompatíveis com a legislação da Parte requerida.
 - 4. Além das condições ou fundamentos de recusa previstos no artigo 25º, n.º 4, o auxílio pode ser recusado pela Parte requerida:
 - a) Se o pedido respeitar a infracções consideradas pela Parte requerida como infracções políticas ou com elas conexas; ou
 - b) Se a Parte considerar que o cumprimento do pedido pode atentar contra a sua soberania, segurança, ordem pública ou qualquer outro interesse essencial do seu país.
 - 5. A Parte requerida pode adiar a execução de um pedido, se isso puder prejudicar as investigações criminais ou os procedimentos levados a cabo pelas suas autoridades.
 - 6. Antes de recusar ou adiar a cooperação, a Parte requerida examinará após ter consultado, se for caso disso, a Parte requerente, se pode satisfazer o pedido no todo ou em parte ou sujeitá-lo às condições que considere necessárias.
 - 7. A Parte requerida informará rapidamente a Parte requerente do seguimento que entende dar ao pedido de auxílio mútuo. Deve ser fundamentada a eventual recusa ou adiamento do pedido. A Parte requerida informará igualmente a Parte requerente de qualquer fundamento que torne impossível a execução do pedido ou que seja susceptível de o retardar significativamente.
 - 8. A Parte requerente pode solicitar que a Parte requerida mantenha confidenciais os factos e o objecto de qualquer pedido formulado ao abrigo do presente Capítulo, excepto na medida necessária à execução do referido pedido. Se a Parte requerida não puder dar satisfação a esse pedido de confidencialidade, deve informar prontamente a Parte requerente, a qual determinará então se o pedido deve contudo ser executado.
 - 9.
 - a) Em caso de urgência, as autoridades judiciárias da Parte requerente podem enviar directamente às suas homólogas da Parte requerida os pedidos de auxílio mútuo ou as comunicações que lhes digam respeito. Nesses casos, uma cópia será dirigida às autoridades centrais da Parte requerida por intermédio da autoridade central da Parte requerente.
 - c) Qualquer pedido ou comunicação ao abrigo do presente parágrafo pode ser efectuado através da Organização Internacional de Polícia Criminal (Interpol).
 - d) Quando um pedido tiver sido efectuado em aplicação da alínea a) do presente parágrafo e a autoridade não for competente para o tratar,

transmiti-lo-á à autoridade nacional competente e informará desse facto directamente a Parte requerente.

- e) Os pedidos ou comunicações efectuados em aplicação do presente parágrafo, que não impliquem uma acção coerciva, podem ser directamente transmitidos pelas autoridades competentes da Parte requerente às autoridades competentes da Parte requerida.
- f) Cada Parte pode informar o Secretário Geral do Conselho da Europa, no momento da assinatura ou do depósito do seu instrumento de ratificação, aceitação, aprovação ou adesão que, por razões de eficácia, os pedidos efectuados em conformidade com o presente número devem ser dirigidos à sua autoridade central.

Artigo 28º - Confidencialidade e restrição de utilização

1. Na ausência de tratados ou acordos de auxílio judiciário mútuo celebrados com base em legislações uniformes ou recíprocas em vigor entre a Parte requerente e a Parte requerida, serão aplicáveis as disposições do presente Artigo. Estas não serão aplicáveis quando exista um tratado, um acordo ou legislação daquele tipo, excepto se as Partes envolvidas decidirem aplicar em sua substituição o presente Artigo no todo ou em parte.
2. A Parte requerida pode sujeitar a comunicação da informação ou de material em resposta a um pedido à condição de que:
 - a) Seja mantida confidencial quando o pedido de auxílio judiciário mútuo não puder ser satisfeito na ausência dessa condição, ou
 - b) Não seja utilizada para fins de outra investigação ou de procedimento diferente dos indicados no pedido.
3. Se a Parte requerente não puder satisfazer uma das condições mencionadas no n.º 2, informará prontamente a Parte requerida, a qual determinará então se a informação deve, ainda assim, ser fornecida. Se a Parte requerente aceitar esta condição, ficará vinculada pela mesma.
4. Qualquer Parte que forneça informações ou material sujeita a uma das condições referidas no n.º 2, pode exigir à outra Parte que lhe forneça esclarecimentos relativos a essa condição, quanto à utilização dessa informação ou desse material.

Secção 2 – Disposições específicas

Título 1 – Auxílio mútuo em matéria de medidas provisórias

Artigo 29º - Conservação expedita de dados informáticos armazenados

1. Uma Parte pode pedir a outra Parte que ordene ou obtenha de outra forma a conservação rápida dos dados armazenados por meio de um sistema informático, que se encontre no território dessa outra Parte, e relativamente aos quais a Parte requerente pretenda apresentar um pedido de auxílio mútuo para

fins de busca ou de acesso similar, apreensão ou obtenção por meio similar, ou divulgação dos dados.

2. Um pedido de conservação efectuado nos termos do n.º 1 deve especificar:
 - a) A autoridade que pede a conservação;
 - b) A infracção que é objecto de investigação criminal ou de procedimento e uma breve exposição dos factos relacionados;
 - c) Os dados informáticos armazenados a conservar e a sua relação com a infracção;
 - d) Todas as informações disponíveis que permitam identificar o responsável pelos dados informáticos armazenados ou a localização do sistema informático;
 - e) A necessidade da medida de conservação; e
 - f) Que a Parte tenciona apresentar um pedido de assistência mútua com vista à busca ou outra forma de acesso, apreensão ou obtenção semelhante, ou divulgação dos dados informáticos armazenados.
3. Após ter recebido o pedido de outra Parte, a Parte requerida deve tomar as medidas apropriadas a fim de proceder, de forma expedita, à conservação dos dados especificados, em conformidade com o seu direito interno. Para poder responder a esse pedido, a dupla incriminação não é exigida como condição prévia à conservação.
4. Uma Parte que exija a dupla incriminação como condição necessária para responder a um pedido de auxílio mútuo para fins de busca ou acesso semelhante, apreensão ou obtenção por meio semelhante, ou a divulgação dos dados, pode, no que diz respeito a outras infracções diferentes das estabelecidas em conformidade com os artigos 2º a 11º da presente Convenção, reservar-se o direito de recusar o pedido de conservação ao abrigo do presente artigo, se tiver razões para crer que no momento da divulgação, a condição de dupla incriminação não pode ser preenchida.
5. Além disso, um pedido de conservação só pode ser recusado se:
 - a) O pedido respeitar a infracções consideradas pela Parte requerida como infracções políticas ou com elas conexas; ou
 - b) A Parte requerida considerar que o cumprimento do pedido pode atentar contra a sua soberania, segurança, ordem pública ou qualquer outro interesse essencial.
6. Quando a Parte requerida considerar que a simples conservação não é suficiente para garantir a disponibilidade futura dos dados, e comprometerá a confidencialidade da investigação da Parte requerente, ou prejudica de outra forma a mesma, informará prontamente disso a Parte requerente que decidirá, então, se o pedido deve, ainda assim, ser executado.

7. Qualquer conservação efectuada em resposta a um pedido referido no n.º 1 será válida por um período não inferior a 60 dias, a fim de permitir à Parte requerente apresentar um pedido para fins de busca ou acesso semelhante, apreensão ou obtenção semelhante, ou divulgação dos dados. Após a recepção desse pedido, os dados devem continuar a ser conservados até à adopção de uma decisão respeitante ao pedido.

Artigo 30º - Divulgação expedita dos dados de tráfego conservados

1. Se ao executar um pedido de conservação de dados relativos ao tráfego relacionados com uma comunicação específica efectuada em aplicação do artigo 29º, a Parte requerida descobrir que um fornecedor de serviços noutro Estado participou na transmissão dessa comunicação, a Parte requerida divulgará rapidamente à Parte requerente uma quantidade suficiente de dados relativos ao tráfego que permita identificar esse fornecedor de serviços e a via através da qual a comunicação foi transmitida.
2. A divulgação de dados de tráfego nos termos do disposto no n.º 1 apenas pode ser recusada se:
 - a) Se o pedido respeitar a uma infracção considerada pela Parte requerida como infracção de natureza política ou com ela conexa; ou
 - b) Se a Parte requerida considerar que o cumprimento do pedido pode atentar contra a sua soberania, segurança, ordem pública ou qualquer outro interesse essencial.

Título 2 – Auxílio mútuo relativamente a poderes de investigação

Artigo 31º - Auxílio mútuo relativamente ao acesso a dados informáticos armazenados

1. Uma Parte pode pedir a outra Parte para investigar ou aceder de forma semelhante, apreender, ou obter de forma semelhante, e divulgar dados armazenados por meio de sistema informático que se encontre no território dessa outra Parte, incluindo os dados conservados em conformidade com o artigo 29º.
2. A Parte requerida dará satisfação ao pedido aplicando os instrumentos internacionais, acordos e legislação referida no artigo 23º, e dando cumprimento às disposições pertinentes do presente Capítulo.
3. O pedido deve ser satisfeito o mais rapidamente possível nos casos em 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 n.º 2 prevejam uma cooperação rápida.

Artigo 32º - Acesso transfronteiriço a dados informáticos armazenados, com consentimento ou quando são acessíveis ao público

Uma Parte pode, sem autorização de outra Parte:

- a) Aceder a dados informáticos armazenados acessíveis ao público (fonte aberta), seja qual for a localização geográfica desses dados; ou
- b) aceder ou receber, através de um sistema informático situado no seu território, dados informáticos armazenados situados no território de outra Parte, se obtiver o consentimento legal e voluntário da pessoa legalmente autorizada a divulgar esses dados, através deste sistema informático.

Artigo 33º - Auxílio mútuo relativamente à recolha de dados de tráfego em tempo real

1. As Partes concederão entre si o auxílio mútuo no que diz respeito à recolha, em tempo real, de dados de tráfego associados a comunicações específicas transmitidas no seu território por meio de um sistema informático. Sem prejuízo do disposto no n.º2, esse auxílio regular-se-à pelas condições e procedimentos previstos em direito interno.
2. Cada Parte concederá o auxílio pelo menos no que diz respeito às infracções penais relativamente às quais seria possível a recolha ao nível interno a recolha em tempo real dos dados de tráfego em caso semelhante.

Artigo 34º - Auxílio mútuo em matéria de interceptação de dados de conteúdo

As Partes concederão auxílio judiciário mútuo, na medida em que é permitido pelos tratados e pelas legislações aplicáveis no que diz respeito à recolha ou ao registo, em tempo real, de dados relativos ao conteúdo de comunicações específicas transmitidas por meio de um sistema informático.

Título 3 - Rede 24/7**Artigo 35º - Rede 24/7**

1. Cada Parte designará um ponto de contacto disponível 24 horas sobre 24 horas, 7 dias por semana, a fim de assegurar a prestação de assistência imediata a investigações ou procedimentos respeitantes a infracções penais relacionadas com dados e sistemas informáticos, ou a fim de recolher provas, sob forma electrónica, de uma infracção penal. O auxílio incluirá a facilitação, ou se o direito e práticas internas o permitirem, a aplicação directa das seguintes medidas:
 - a) A prestação de aconselhamento técnico;
 - b) A conservação de dados em conformidade com os artigos 29º e 30º; e
 - c) A recolha de provas, informações de carácter jurídico e localização de suspeitos.

2. a) O ponto de contacto de uma Parte deve ter capacidade técnica para corresponder-se com o ponto de contacto de outra Parte de uma forma rápida;

b) Se o ponto de contacto designado por uma Parte não depender da autoridade ou autoridades dessa Parte responsáveis pela cooperação internacional ou extradição dessa Parte, o ponto de contacto assegurará que pode agir em coordenação com essa ou essas autoridades de forma rápida.
3. Cada Parte assegurará que pode dispor de pessoal formado e equipado a fim de facilitar o funcionamento da rede.

Capítulo IV – Disposições Finais

Artigo 36º - Assinatura e entrada em vigor

1. A presente Convenção está aberta à assinatura dos Estados membros do Conselho da Europa e dos Estados não membros que participaram na elaboração da mesma.
2. A presente Convenção é submetida a ratificação, aceitação ou aprovação. Os instrumentos de ratificação, aceitação ou aprovação serão depositados junto do Secretário Geral do Conselho da Europa.
3. A presente Convenção entrará em vigor no primeiro dia do mês seguinte ao termo de um período de três meses após a data na qual cinco Estados, incluindo pelo menos três Estados membros do Conselho da Europa, tenham manifestado o seu consentimento em ficar vinculados pela Convenção, em conformidade com as disposições dos n.ºs 1 e 2.
4. Em relação a qualquer Estado signatário que posteriormente exprima o seu consentimento em vincular-se à Convenção, esta entrará em vigor no primeiro dia do mês seguinte ao termo de um período de três meses após a data em que tenha sido expresso o seu consentimento em vincular-se à Convenção, em conformidade com as disposições dos n.ºs 1 e 2.

Artigo 37º - Adesão à Convenção

1. Após a entrada em vigor da presente Convenção, o Comité 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 Comité de Ministros.
2. Em relação a qualquer Estado aderente à Convenção, em conformidade com o n.º 1, a Convenção entrará em vigor no primeiro dia do mês seguinte ao termo de um período de três meses após a data do depósito do instrumento de adesão junto do Secretário Geral do Conselho da Europa.

Artigo 38º - Aplicação territorial

1. Qualquer Estado pode, no momento da assinatura ou no momento do depósito do seu instrumento de ratificação, aceitação, aprovação ou adesão, designar o, ou os territórios aos quais se aplicará a presente Convenção.
2. Qualquer Estado pode, em qualquer momento posterior, mediante declaração dirigida ao Secretário Geral do Conselho da Europa, tornar extensível a aplicação da presente Convenção a qualquer outro território designado na declaração. A Convenção entrará em vigor em relação a esse território no primeiro dia do mês seguinte ao termo de um período de três meses após a data de recepção da declaração pelo Secretário Geral.
3. Qualquer declaração feita nos termos dos dois parágrafos anteriores pode ser retirada, no que diz respeito a qualquer território designado na declaração, mediante notificação dirigida ao Secretário Geral do Conselho da Europa. Essa declaração produzirá efeitos no primeiro dia do mês seguinte ao termo de um período de três meses após a data de recepção da referida notificação pelo Secretário Geral.

Artigo 39º - Efeitos da Convenção

1. O objectivo da presente Convenção é complementar os tratados ou acordos multilaterais ou bilaterais aplicáveis existentes entre as Partes, incluindo as disposições:
 - Da Convenção Europeia de Extradução, aberta para assinatura em Paris a 13 de Dezembro de 1957 (STE Nº 24);
 - Da Convenção Europeia de Auxílio Mútuo em Matéria Penal, aberta para assinatura em Estrasburgo, a 20 de Abril de 1959 (STE n.º 30);
 - Do Protocolo Adicional à Convenção Europeia de Auxílio Mútuo em Matéria Penal, aberta para assinatura em Estrasburgo, a 17 de Março de 1978 (STE n.º 99).
2. Se duas ou mais Partes tiverem já celebrado um acordo ou tratado relativo às matérias tratadas pela presente Convenção ou se, de outra forma, tiverem estabelecido relações a este respeito, ou se vierem a fazê-lo no futuro, terão a possibilidade de aplicar o referido acordo ou tratado ou estabelecer essas relações em substituição da presente Convenção. Todavia, sempre que as Partes estabeleçam relações respeitantes a matérias objecto da presente Convenção de forma diferente daquela que é prevista pela mesma, fa-lo-ão de uma forma que não seja incompatível com os princípios e objectivos da presente Convenção.
3. Nada na Convenção prejudicará outros direitos, restrições, obrigações e responsabilidades de uma Parte.

Artigo 40º - Declarações

Qualquer Estado pode, mediante notificação por escrito dirigida ao Secretário Geral do Conselho da Europa no acto da assinatura ou do depósito do seu instrumento de ratificação, aceitação, aprovação ou adesão, declarar que fará uso da faculdade de exigir, se for caso disso, um ou mais elementos suplementares, tal como previsto nos artigos 2º, 3º, 6º, n.º 1, alínea b), 7º, 9º, n.º 3 e 27º, n.º 9, alínea e).

Artigo 41º - Cláusula federal

1. Um Estado federal pode reservar-se o direito de assumir as obrigações nos termos do capítulo II da presente Convenção na medida em que sejam compatíveis com os princípios fundamentais que governam as relações entre o seu Governo central e os Estados federados, ou outras entidades territoriais análogas, desde que esteja em condições de cooperar com base no Capítulo III.
2. Quando tiver feito uma reserva prevista no n.º1, não pode utilizar essa reserva para excluir ou diminuir de forma substancial as suas obrigações nos termos do Capítulo II. Em qualquer caso, dotar-se-á de meios amplos e eficazes que permitam a aplicação das medidas previstas no referido capítulo.
3. No que se refere às disposições da presente Convenção, cuja execução seja da competência legislativa dos Estados federados ou de outras entidades territoriais análogas que não são, nos termos do sistema constitucional da federação obrigados a tomar medidas legislativas, o governo federal levará com parecer favorável as referidas disposições ao conhecimento das autoridades competentes dos Estados federais incitando-os a adoptar as medidas adequadas para as executar.

Artigo 42º - Reservas

Qualquer Estado pode, mediante notificação por escrito dirigida ao Secretário Geral do Conselho da Europa no momento da assinatura ou do depósito do seu instrumento de ratificação, aceitação, aprovação ou adesão, declarar a sua intenção de fazer uso da(s) reserva(s) previstas nos artigos 4º, n.º 2, 6º, n.º 3, 9º, n.º 4, 10º, n.º 3, 11º, n.º 3, 14º, n.º 3, 22º, n.º 2, 29º, n.º 4, e 41, n.º 1. Nenhuma outra reserva poderá ser formulada.

Artigo 43º - Estatuto e levantamento das reservas

1. Uma Parte que tenha formulado uma reserva em conformidade com o artigo 42º pode retirá-la no todo ou em parte, mediante notificação dirigida ao Secretário-Geral do Conselho da Europa. A declaração produzirá efeitos na data de recepção da referida notificação pelo Secretário Geral. Se a notificação indicar que o levantamento da reserva deve produzir efeitos numa data precisa e essa data for posterior à da recepção da notificação pelo Secretário Geral, a declaração produz efeitos nessa data posterior.
2. Uma Parte que tenha formulado uma reserva nos termos do artigo 42º retirará essa reserva no todo ou em parte, logo que as circunstâncias o permitam.

3. O Secretário-Geral do Conselho da Europa pode, periodicamente, pedir às Partes que formularam uma ou mais reservas nos termos do artigo 42º, informações sobre as perspectivas de levantamento dessas reservas.

Artigo 44º - Aditamentos

1. Quaisquer aditamentos à presente Convenção podem ser propostas por qualquer uma das Partes e serão comunicadas pelo Secretário Geral do Conselho da Europa aos Estados membros do Conselho da Europa, aos Estados não membros que participaram na elaboração da presente Convenção, bem como a qualquer Estado que tenha aderido, ou sido convidado a aderir em conformidade com as disposições do artigo 37º.
2. Qualquer aditamentos proposta por uma Parte deve ser comunicada ao Comité Europeu para os Problemas Criminais (CDPC), que submeterá ao Comité de Ministros o seu parecer relativamente à alteração proposta.
3. O Comité de Ministros examinará o aditamento proposto e o parecer submetido pelo Comité Europeu para os Problemas Criminais (CDPC) e, após consulta dos Estados não membros, Partes na presente Convenção, pode adoptar o referido aditamento.
4. O texto de qualquer aditamento adoptado pelo Comité de Ministros em conformidade com o n.º 3 do presente artigo será comunicado às Partes para aceitação.
5. Qualquer aditamento adoptado em conformidade com o n.º 3 do presente artigo entrará em vigor no trigésimo dia após todas Partes terem informado o Secretário Geral acerca da sua aprovação.

Artigo 45º - Resolução de litígios

1. O Comité Europeu para os Problemas Criminais (CDPC) será mantido informado sobre a interpretação e a aplicação da presente Convenção.
2. No caso de litígio entre as Partes sobre a interpretação ou a aplicação da presente Convenção, as mesmas esforçar-se-ão por encontrar uma solução para o litígio através da negociação ou de qualquer outro meio pacífico à sua escolha, incluindo submeter o litígio ao Comité Europeu para os Problemas Criminais (CDPC), a um tribunal arbitral, cujas decisões vincularão as Partes no litígio, ou ao Tribunal Internacional de Justiça, de comum acordo entre as Partes envolvidas.

Artigo 46º - Consulta entre as Partes

1. As Partes consultar-se-ão periodicamente, se necessário, a fim de facilitar:
 - a) A utilização e a execução efectiva da presente Convenção, incluindo a identificação de qualquer problema na matéria, bem como os efeitos de qualquer declaração ou reserva feita em conformidade com a presente Convenção;

- b) A troca de informações sobre os desenvolvimentos jurídicos, políticos ou técnicos importantes verificados no domínio da cibercriminalidade e a recolha de provas sob forma electrónica;
 - c) A análise de eventuais complementos ou aditamentos à Convenção.
2. O Comité Europeu para os Problemas Criminais (CDPC) será mantido periodicamente informado do resultado da consulta referida no n.º 1.
 3. O Comité Europeu para os Problemas Criminais (CDPC) facilitará, se necessário, as consultas referidas no n.º 1 e adoptará as medidas necessárias para ajudar as Partes nos seus esforços destinados a complementar ou a fazer aditamentos à Convenção. O mais tardar no final de um prazo de três anos a contar da entrada em vigor da presente Convenção, o Comité Europeu para os Problemas Criminais (CDPC) procederá em cooperação com as Partes a um reexame de todas as disposições constantes da Convenção e, se necessário, proporá os aditamentos adequados.
 4. Salvo quando o Conselho da Europa assuma as despesas ocasionadas pela aplicação do disposto no n.º 1, as mesmas serão suportadas pelas Partes.
 5. As Partes são assistidas pelo Secretariado do Conselho da Europa no exercício das suas funções decorrentes do presente artigo.

Artigo 47º - Denúncia

1. Qualquer Parte pode, em qualquer momento, denunciar a presente Convenção através de notificação dirigida ao Secretário Geral do Conselho da Europa.
2. A denúncia produzirá efeitos no primeiro dia do mês seguinte ao termo de um período de três meses após a data de recepção da notificação pelo Secretário Geral.

Artigo 48º - Notificação

O Secretário Geral do Conselho da Europa notificará os Estados membros do Conselho da Europa, os Estados não membros que participaram na elaboração da presente Convenção, bem como qualquer Estado aderente, ou que tenha sido convidado a aderir à presente Convenção de:

- a) Todas as assinaturas;
- b) O depósito de qualquer instrumento de ratificação, aceitação, aprovação ou adesão;
- c) Todas as datas de entrada em vigor da presente Convenção, em conformidade com os artigos 36º e 37º;
- d) Todas as declarações efectuadas em aplicação do(s) artigo(s) 40º, 41º, ou as reservas formuladas em aplicação do artigo 42º;

e) Qualquer outro acto, notificação ou comunicação relacionados com a presente Convenção.

Em fé do que os abaixo assinados, devidamente autorizados para este efeito, assinaram a presente Convenção.

Feito em Budapeste, em 23 de Novembro de 2001, em francês e inglês, ambos os textos fazendo igualmente fé, num único exemplar, que será depositado nos arquivos do Conselho da Europa. O Secretário Geral do Conselho da Europa enviará cópias autenticadas a cada um dos Estados membros do Conselho da Europa, aos Estados não membros que participaram na elaboração da presente Convenção, e a qualquer Estado que tenha sido convidado a aderir à Convenção.