Gregório Edoardo Raphael Selingardi Guardia

Comunicações Eletrônicas e Dados Digitais no Processo Penal

DISSERTAÇÃO DE MESTRADO

Dissertação apresentada à Banca Examinadora da Faculdade de Direito da Universidade de São Paulo, como exigência parcial para obtenção do titulo de MESTRE em Direito, sob a orientação do Prof. Doutor José Raul Gavião de Almeida.

Área de Concentração: Direito Processual Penal.

Faculdade de Direito da Universidade de São Paulo
São Paulo
2012

Banca Examinadora

Meu profundo agradecimento,

ao Professor José Raul Gavião de Almeida, por todos os ensinamentos e preciosa orientação.

ao Professor Marcos Alexandre Coelho Zilli, mestre das primeiras lições na graduação.

aos Professores Antonio Scarance Fernandes e Gustavo Henrique Righi Ivahy Badaró, cujas valiosíssimas sugestões e críticas permitiram o aperfeiçoamento deste trabalho.

aos Funcionários das Bibliotecas da Faculdade de Direito, por sua atenta colaboração.

aos meus caros amigos. Em especial, à Bianca Leão Bertin e João Guilherme Mazzini Bruschi.

a minha família e a Deus.

"(…) di fronte ad una mondializzazione in cui la dimensione economica sembra prevalere sull'universalismo dei diritti dell'uomo, il diritto penale apre una via verso un'etica comune. Ma tale via resta per il momento tortuosa: sarà, infatti, richiesto ai giudici molto coraggio ed ostinazione, agli avvocati ed ai professori molta immaginazione per sviluppare ed inquadrare quei complessi meccanismi di integrazione verticale ed orizzontale capaci di conferire al futuro ordinamento giuridico mondiale legittimità e legalità".

(– Mireille Delmas-Marty, *Il diritto penale come etica della mondializzazione* –)

"Oh, amor, se pudéssemos conspirar com o destino, / de modo a compreender essa melancólica e íntegra estrutura das coisas! / A*c*aso não a de*s*integraríamos em pedaços / para computá-la conforme o dese*j*o do coração?".

(= Om. Kh., *Orbis Tertius*, t. XVI, n. 4, DS-V=)

Para Marília

SUMÁRIO

INTRODUÇÃO.....12

CAPÍTULO I – CIBERNÉTICA, INFORMÁTICA E DIREITO

1.1. Estudo interdisciplinar.....16

1.2. Cibernética: breves considerações.....20

1.3. Telecomunicações.....24

1.4. Informática e Direito.....27

1.4.1. Telemática e informação em rede.....30

1.4.2. Novas tecnologias e processo penal.....34

1.4.3. Uma reflexão sobre o entorno digital: interpretação em rede e liberdade como reciprocidade.....36

1.4.3.1. Entorno digital (território-tempo-estrutura).....36

1.4.3.2. Interpretação e Direito em rede.....40

1.4.3.3. Liberdade como autonomia recíproca de acesso à informação.....44

1.5. Comunicações eletrônicas.....45

CAPÍTULO II – DIREITO À INTIMIDADE E SIGILO DAS COMUNICAÇÕES NA PERSECUÇÃO PENAL

2.1. Evolução da proteção à intimidade.....50

2.1.1. Análise constitucional: inviolabilidade das comunicações, inviolabilidade do domicílio e intimidade.....51

2.1.2. Das noções de *privacy*, intimidade e *riservatezza* ao direito à proteção de dados.....55

2.1.3. Direito internacional.....58

2.2. Direito à proteção de dados (ou à autodeterminação informativa) como direito fundamental autônomo.....60

2.3. Teoria das três esferas.....65

2.4. Inviolabilidade das comunicações na Constituição de 1988.....69

2.4.1. Hermenêutica.....71

2.4.2. Divergências doutrinária e jurisprudencial.....74

2.4.3. Interpretação do art. 5º, XII.....77

2.5. Comunicações postais e telegráficas.....82

2.6. Correio eletrônico.....87

2.7. Comunicações telefônicas e de dados.....89

2.8. Sigilo das comunicações e processo penal.....94

2.9. Entorno digital e comunicação de dados.....96

CAPÍTULO III: CONCEITO E CATEGORIAS DE DADOS DIGITAIS

3.1. Conceito.....99

3.2. Categorias.....100

3.2.1. Dados pessoais: dados sensíveis, dados pessoais em sentido estrito e dados públicos.....100

3.2.2. Dados de conteúdo e dados de tráfego.....104

3.2.2.1. Dados indubitavelmente de tráfego.....107

3.2.2.2. Dados eventualmente de tráfego e dados afins.....109

3.3. Fontes de provas digitais e persecução criminal.....112

3.3.1. Aproveitamento dos dados digitais na persecução penal.....114

3.3.2. Utilidade dos dados de tráfego.....116

3.3.3. Dados digitais e modalidade delitiva.....119

3.3.4. Tese de acusação e de defesa: a garantia do contraditório.....121

3.4. Provas no ambiente digital.....123

CAPÍTULO IV – INTERVENÇÃO NAS COMUNICAÇÕES ELETRÔNICAS

4.1. Generalidades.....127

4.1.1. Intervenção e interceptação.....128

4.1.2. Comunicações em canal aberto e fechado.....132

4.1.3. Intervenção nas comunicações em canal aberto e fechado.....133

4.2. Regulação.....134

4.2.1. Ordenamento pátrio.....135

4.2.2. Convenção de Budapeste.....136

4.3. Natureza jurídica.....139

4.3.1. Medidas de investigação criminal.....139

4.3.2. Preservação das fontes de provas.....141

4.3.3. Limitação de direitos fundamentais.....142

4.3.3.1. Direito à inviolabilidade das comunicações.....143

4.3.3.2. Direito à proteção de dados de caráter pessoal.....144

4.3.3.3. Direitos à liberdade de expressão e opinião.....146

4.3.4. Finalidade e objeto.....147

4.4. Intervenção nas comunicações em canal fechado: pressupostos, requisitos e limites legais.....148

4.4.1. Pressupostos: legalidade e justificação teleológica.....149

4.4.2. Requisitos.....152

4.4.2.1. Reserva jurisdicional.....153

4.4.2.1.1. Competência.....155

4.4.2.1.2. Relevância do consentimento.....158

4.4.2.2. Motivação.....159

4.4.3. Limites objetivos, subjetivos e temporais.....163

4.5. Direito de defesa.....168

4.6. Princípio da proporcionalidade.....171

4.7. Controle.....173

4.8. Intervenção nas comunicações em canal aberto.....176

CAPÍTULO V – ACESSO AOS DADOS DIGITAIS ARMAZENADOS EM SUPORTE ELETRÔNICO

5.1. Generalidades.....179

5.1.1. Conceito.....180

5.2. Regulação.....181

5.2.1. Ordenamento pátrio.....182

5.2.2. Convenção de Budapeste.....185

5.3. Natureza Jurídica.....186

5.3.1. Medida de investigação.....187

5.3.2. Preservação das fontes de prova.....189

5.3.3. Limitação de direitos fundamentais.....191

5.3.4. Finalidade e objeto.....194

5.4. Pressupostos, requisitos e limites legais.....196

5.4.1. Pressupostos: legalidade e justificação teleológica.....197

5.4.2. Requisitos: reserva jurisdicional e motivação.....198

5.4.3. Limites objetivos, subjetivos e temporais.....200

5.5. Direito de defesa.....202

5.6. Princípio da proporcionalidade.....204

5.7. Controle.....205

CAPÍTULO VI – DADOS DIGITAIS COMO FONTE DE PROVA: NOÇÕES DE CONSERVAÇÃO, EFICÁCIA E ILICITUDE

6.1. Conservação dos dados digitais e o direito à proteção dos dados pessoais.....208

6.2. Eficácia probatória dos dados digitais.....212

6.3. Valoração da prova digital.....214

6.4. Prova científica e dados digitais.....218

6.5. Efeitos da ilicitude probatória em relação aos dados digitais.....219

6.6. Prova digital e os sistemas da *Civi Law* e *Common Law*.....222

Conclusões.....229

BIBLIOGRAFIA.....236

ABREVIATURAS.....251

Resumo / *Abstract* / *Resumen* / *Riassunto*.....253

INTRODUÇÃO

O contínuo avanço tecnológico experimentado nas últimas décadas proporcionou expressivo aperfeiçoamento das relações interpessoais. A instantaneidade dos processos comunicativos e o caráter eminentemente dinâmico das interações materializadas na chamada *sociedade da informação* constituem transformações que não podem ser ignoradas pela ciência jurídica.

Cabe ao jurista ponderar cuidadosamente os efeitos destas inovações, que transcendem os limites da técnica e alcançam também o corpo social. O desenvolvimento tecnológico não encontra razão apenas no progresso econômico, presta-se a facilitar o desenvolvimento humano e deve produzir-se em estrita observância aos direitos fundamentais historicamente reconhecidos e consagrados pelo legislador constitucional.

Em tempos correntes, importantes processos de comunicação (escrita ou verbal) e armazenamento de dados aperfeiçoam-se por intermédio dos meios eletrônicos. À medida que o acesso à rede mundial de computadores *(internet)* se intensifica em progressões geométricas, multiplicam-se também os arquivos intercambiados por internautas e emergem técnicas cada vez mais avançadas de coleta e processamento de dados.

Atividades rotineiras como a navegação e o envio de mensagens eletrônicas realizam-se apenas à custa de imenso trânsito de dados; como pegadas, os signos comutados nestas atuações permitem reconstituir os caminhos percorridos e as ações desenvolvidas na rede. A salvaguarda destas informações afigura-se imprescindível à vida privada e demanda rígida disciplina normativa. Não se trata apenas de impedir que dados de tráfego ou de conteúdo sejam empregados contrariamente ao Direito, mas de assegurar também que, nas situações excepcionais descritas pelo legislador, sirvam para corroborar investigações criminais.

Não se perca de vista que a coleta de fontes de provas no ambiente digital se perfaz no marco constitucional do devido processo legal. Destarte, de rigor o

equilíbrio entre a preservação das liberdades do cidadão e o interesse público de apurar e punir as condutas criminosas.[1] A harmonização entre preservação de direitos fundamentais e eficiência na apuração dos delitos[2] faz-se à luz do único sistema processual condizente com o Estado de Direito – o processo penal de índole acusatória.[3]

Pretende-se neste trabalho, o exame sistemático dos principais meios de busca da prova digital, com o escopo de delimitar o regime jurídico das intervenções nas comunicações eletrônicas e das medidas de apreensão de dados automatizados. Em particular, insta examinar a constitucionalidade destes meios de obtenção de prova à luz dos direitos e garantias individuais que inspiram o ordenamento jurídico brasileiro.

Neste mister, inafastável analisar a disciplina constitucional do sigilo da comunicação de dados (CF, art. 5º, inciso XII) e perscrutar o fundamento legal das autorizações judiciais para a obtenção de informações eletrônicas. Igualmente, há que responder se a inviolabilidade afeta apenas os dados de conteúdo das comunicações, ou se pode também ser estendida aos dados de tráfego.

O capítulo primeiro dedica-se à compreensão dos principais temas que integram o complexo quadro das relações entre Direito e tecnologias informativas. Sob perspectiva eminentemente interdisciplinar, cumpre discorrer objetivamente sobre noções[4]

---

[1] ROGÉRIO LAURIA TUCCI expõe, com propriedade, o duplo escopo processualístico-penal: jurisdicionalização da sanção penal e afirmação do *ius libertatis* (*Direitos e Garantias Individuais no Processo Penal Brasileiro*, 3ª ed., São Paulo, RT, 2009, pp. 28-32).

[2] Sobre as noções de eficiência e garantismo, *v.* A. S. FERNANDES, *Processo Penal Constitucional*, 6ª ed., São Paulo, RT, 2010, pp. 19-21. LUIGI FERRAJOLI aponta três significados diversos para o termo garantismo: *"Designa um modelo normativo de direito: precisamente, no que diz respeito ao direito penal, o modelo de "estrita legalidade" SG, próprio do Estado de direitos, que sob o plano epistemológico se caracteriza como um sistema cognitivo ou de poder mínimo, sob o plano político se caracteriza como uma técnica de tutela idônea a minimizar a violência e a maximizar a liberdade e, sob o plano jurídico, como um sistema de vínculos impostos à função punitiva do Estado em garantia dos direitos dos cidadãos (...). Em um segundo significado, "garantismo" designa uma teoria jurídica da "validade" e da "efetividade" como categorias distintas não só entre si mas, também pela "existência ou "vigor" das normas. (...) Segundo um terceiro significado, por fim, 'garantismo' designa uma filosofia política que requer do direito e do Estado o ônus da justificação externa com base nos bens e nos interesses dos quais a tutela ou garantia constituem a finalidade"* (*Direito e Razão: Teoria do Garantismo Penal*, trad. Ana Paula Zomer Sica (et alii), 2ª ed., São Paulo, RT, 2006, pp. 785-787). A escolha do "modelo garantista" como esquadro de uma investigação pressupõe a preservação de garantias como método de legitimação para o exercício do poder punitivo. Uma vez instituídas, representam barreiras, vínculos, obstáculos à punição indiscriminada (A. M. GOMES FILHO, *O "Modelo Garantista" de Luigi Ferrajoli*, *Boletim IBCCRIM*, n. 58, 1997, p. 6).

[3] Sobre o sistema acusatório *v.* nota 247.

[4] Conquanto não se pretenda imiscuir em questões excessivamente técnicas, pertinentes apenas aos estudos da ciência da computação, de rigor a busca de critérios técnicos para a definição dos conceitos informáticos, justamente para não se descuidar de uma exata compreensão das repercussões jurídicas do fenômeno tecnológico.

de *Cibernética*, *telecomunicações, Informática*, *liberdade como autonomia recíproca de acesso à informação* e *comunicações eletrônicas*, imprescindíveis à compreensão deste novo espaço do agir humano: o entorno digital.

Em razão das graves ingerências na vida privada que se tem produzido neste entorno, as noveis tecnologias serão apresentadas principalmente a partir dos elementos que conformam o ambiente digital. Por óbvio, há diversas maneiras de apresentar estas importantes questões atinentes à denominada *sociedade da informação*. Inclusive, há quem preferia associar esta problemática ao contexto globalizado da criminalidade cibernética, ou mesmo, tratar os direitos de *internet* como autênticos direitos de terceira geração.[5] Contudo, mais ajustado ao objeto desta Dissertação limitar o estudo aos aspectos relacionados à proteção do direito fundamental à intimidade, cuja afronta faz-se sentir na sociedade contemporânea.

No campo da hermenêutica constitucional (capítulo 2), necessário perquirir relevantes aspectos da vida privada e da proteção da intimidade – antecedentes históricos, direito à *privacy*, hodierna projeção como autodeterminação informativa, teoria das três esferas e inviolabilidade das comunicações – que permitirão opinar sobre a constitucionalidade das interceptações de dados em processos informacionais.

No capítulo terceiro, devem ser conceituados os dados digitais e suas respectivas categorias. Convém também aferir a utilidade dos dados informáticos, das técnicas de investigação penal e do resguardo de fontes de provas digitais, à luz do paradigma da atuação contraditória e isonômica dos sujeitos processuais.

Sem deixar de contribuir para o aperfeiçoamento da normativa legal vigente, imperioso o exame de duas ordens distintas de incorporação dos dados ao

[5] Para a doutrina, enquanto os direitos de primeira geração dizem respeito à liberdade, os de segunda geração concernem à igualdade. Os direitos de terceira geração apresentam-se no contexto de uma nova fundamentação, novos instrumentos de tutela e novas formas de titularidade. A. E. PÉREZ-LUÑO enumera expressões similares para o conceito: *novos direitos*, *direitos de solidariedade*, *direitos da era tecnológica*, *direitos da sociedade global* (*La tercera generación de derechos humanos*, Navarra, Thomson, 2006, p. 17). Segundo o autor: *" (...) los derechos de la tercera generación tiene como principal valor de referencia a la solidaridad. Los nuevos derechos humanos se hallan aunados entre sí por su incidencia universal en la vida de todos los hombres y exigen para su realización la comunidad de esfuerzos y responsabilidades a escala planetaria. Sólo mediante un espíritu solidario de sinergia, es decir, de cooperación y sacrificio voluntario y altruista de los intereses egoístas será posible satisfacer plenamente las necesidades y aspiraciones globales comunes relativas a la paz, a la calidad de vida, o a la libertad informática"* (Idem, pp. 34-35).

processo: a intervenção no fluxo comunicativo destinada a captar dados e a apreensão física do dispositivo informático que alberga as informações. Como meios de busca de prova, esses procedimentos devem ser estudados de maneira individualizada, a partir de aspectos como *conceito*, *regulação*, *natureza jurídica*, *finalidade*, *condicionantes legais* (*pressupostos, requisitos* e *limites*), *direito de defesa*, *juízo de proporcionalidade* e *controle*.

Por fim, tecidas as necessárias considerações sobre a conservação, eficácia probatória e valoração dos conteúdos automatizados, impõe-se indagar acerca dos efeitos decorrentes de operações ilícitas perpetradas sobre dados digitais.

Em síntese, inescusável diferenciar os meios fidedignos e necessários de investigação criminal daqueles outros que resultam na produção de provas em desacordo com o direito material. O ordenamento jurídico brasileiro não pode permanecer à margem de ingentes ofensas ao ser humano e à sua eminente dignidade facilitadas pelo progresso tecnológico.

CAPÍTULO I – CIBERNÉTICA, INFORMÁTICA E DIREITO

1.1. Estudo interdisciplinar

A vanguarda da teoria Cibernética de NORBERT WIENER, brevemente comentada a seguir (item 1.2), é inegável. Para MARIO LOSANO muito cara ao matemático estadunidense a noção de interdisciplinariedade: no contexto das ciências delimitadas e entendidas como sistemas, os campos mais fecundos para a pesquisa são aqueles que se encontram na fronteira entre as várias disciplinas. Tem-se a possibilidade de examinar o objeto de estudo ora sob o viés de um dos sistemas, ora pelo ponto de vista do outro, ora pela combinação de ambos.[6]

A autêntica interdisciplinaridade propugnada por WIENER não obriga o cientista ao domínio pleno das inúmeras searas do conhecimento, mas acentua a necessária disposição do pesquisador para a compreensão de um tema sob vários enfoques críticos.

Diante de um mesmo problema inicial se faz possível comparar o raciocínio empregado e as respectivas conclusões. No campo da diversidade de perspectivas e resultados obtidos por distintos setores do conhecimento, a ponderação guia-se pela riqueza da contraditoriedade das opiniões. Por sua vez, no plano da convergência de premissas e resultados, prevalece a complementariedade dos discursos científicos.

É verdade que o aparente abismo entre os conceitos de *justiça* (sensivelmente afeita aos valores humanos) e *informática* (abstração própria de um mundo de quantificação) pode fazer desacreditar sobre possíveis relações entre Informática e Direito.

---

[6] *"O matemático não precisará saber fazer uma experiência física ou análise fisiológica, mas deverá estar apto a compreender os resultados dela e, eventualmente, a sugerir a experiência ao colega, de tal maneira que no grupo exista uma efetiva interação, isto é, uma integração de pesquisas e não, simplesmente, uma sobreposição de pontos de vista diferentes"* (*Lições de Informática Jurídica,* São Paulo, Resenha Tributária, 1974, p. 7).

As primeiras reflexões próprias da *Informática Jurídica* problematizavam a viabilidade da computação servir a uma qualquer função judiciária acessória. Atualmente desponta a noção de Informática como instrumento a serviço da informação, em razão de possuir o computador, a capacidade de *"recolher, comparar, ordenar, associar, excluir, integrar, armazenar e difundir todo tipo de mensagens, quer de natureza alfabética, quer numérica";* atividades relevantes para o Direito.[7]

Com base nestas primeiras constatações, o desenvolvimento de uma Dissertação que envolva dados digitais e processo penal não pode ignorar as constantes interações entre ambos os setores do conhecimento envolvidos diretamente na pesquisa.

Nada obstante o enfoque aqui pretendido seja preponderantemente jurídico-dogmático (processual e técnico), permeará o enfrentamento do tema a busca pela complementariedade, sobretudo no mister de conceituar e compreender o funcionamento das ferramentas do entorno digital que diretamente se relacionam ao processo penal.

O desafio de constatar as intersecções entre Direito e Informática, bem como de propor soluções condizentes com a complexidade de tais problemas, remonta às agruras do jurista ao lidar com o sempre intrigante desafio de conhecer e descrever o novo.

O relato de um destes momentos fica por conta de MARIO LOSANO, ao mencionar uma esquecida teoria internacionalística de ANTONIO SCRIMALI. Este jurista, ao mesmo tempo que intuiu a ocorrência de uma série de transformações no Direito internacional, não conseguiu identificar a natureza das alterações. Nas palavras de LOSANO:

> *"Lendo-o, revi a cena final de um filme de culto juvenil: um grupo de rapazes, depois de uma noite plena de contratempos, tem a ideia poética de ir até a praia para assistir ao nascer do sol no mar. Sentam-se na areia e esperam. Pena que o sol tenha surgido do lado oposto. A mesma coisa aconteceu com a teoria trialista de SCRIMALI".*[8]

[7] GARCIA MARQUES, LOURENÇO MARTINS, *Direito da informática*, Lisboa, Almedina, 2000, p. 24.
[8] A teoria trialística de ANTONIO SCRIMALI foi concebida no calor das discussões entre monismo e dualismo jurídicos; para o autor, além do direito interno e do direito internacional, haveria o direito "inter-regional". No entanto, o ponto débil da teoria é a fonte deste direito "inter-regional" – ao momento em que era escrita

Ao deparar-se com a multitude de transformações políticas, sociais e jurídicas do século XX, SCRIMALI propôs uma inovadora teoria: "*pena que o sol tenha surgido do lado oposto"*.

Com efeito, enfrentar a complexidade é o sempre renovado desafio do jurista; como ensina MIGUEL REALE, admirável a capacidade humana de lidar com a complexidade (capacidade reveladora e nomotética do espírito).[9]

Ainda que falte precisão para delimitar a natureza dos noveis problemas, ainda que se incorra no risco de conclusões prematuras ou parciais, por vezes sólidos argumentos constroem-se a partir de inquietações de tempos pretéritos. Estas contribuições provisórias, resgatadas pelas vindouras gerações, deixam transparecer o aspecto diacrônico da ciência.

O jurista não pode desprezar que o convívio entre homem e aparelho eletrônico afigura-se capaz de modificar o agir humano.[10] Indispensável, pois, sensibilidade e perspicácia na constatação da influência destes novos rumos da evolução tecnológica para o indivíduo e para a vida social.

A liberdade do homem ao manejar a máquina é programada; restringe-se a um número finito de possibilidades, ambos funcionam conjuntamente.[11] Mas seria esta *reversibilidade* – o homem em função do aparelho e o aparelho em função do homem – uma constatação preocupante?

(1939) não existia um poder "inter-regional" legitimado para emanar um direito desta natureza (*Modelos teóricos, inclusive na prática: da pirâmide à rede*, in Revista do IASP, São Paulo, RT, ano 8, n. 16, jul./dez, 2005, p. 273).

[9] *Invariantes axiológicos*, in Estudos avançados, v. 15, n. 13, set./dez., São Paulo, 1991, p. 8.

[10] Para exemplificar alterações do agir humano pense-se no advento do compartilhamento simultâneo de todo tipo de informação, característica marcante da revolução cultural hodierna. Se por um lado o receptor de uma comunicação não precisa distanciar-se do espaço privado para interagir e acessar o conhecimento, por outro, sua participação não necessariamente é efetiva. A superficialidade das atitudes e escolhas no entorno digital pode ser uma consequência negativa do excedente de informações – os relatos e as imagens são muito superiores às possibilidades humanas de "processá-los".

[11] *"Pois o aparelho só faz aquilo que o homem quiser, mas o homem só pode querer aquilo de que o aparelho é capaz"* (V. FLUSSER, *O mundo codificado: por uma filosofia do design e da comunicação*, trad. Raquel Abi-Sâmara, São Paulo, Cosacnaify, 2007, pp. 40-41).

Não há como responder definitivamente esta indagação, mas se deve advertir: em grande medida os desastres tecnológicos ou usos maléficos e destrutivos das máquinas dependem imediatamente da vocação de seus titulares para utilizá-los.

A máquina, a exemplo do próprio processo[12], constitui instrumento dirigido à realização de valores humanos, meio utilizado com fundamento na postura ética.[13] Não há, pois, qualquer outra vereda a ser percorrida senão aquela da *humanização dos recursos tecnológicos*.

As conquistas tecnológicas[14] em si mesmas são neutras, o seu emprego voltado ao bem-estar de uma comunidade ou para a instituição de um modelo constritivo de liberdades individuais não é um dado pré-constituído. É responsabilidade dos cidadãos e dos juristas pensá-los como instrumentos úteis à sociedade e aos valores que orientam o Estado de Direito.[15]

O homem situa-se exatamente no ponto de inflexão entre duas realidades antagônicas: passado e futuro. Ubicados neste intervalo, os sentidos humanos voltam-se para trás à busca de autoconhecimento, e tornam para adiante, esperançosos e inquietos. Ao procurar as estradas que o levaram até ali revelam-se escolhas determinantes; ao mirar adiante o horizonte não tem limites.

---

[12] O processo judiciário tem as características de um instrumento *técnico, ético, público e político* (R. L. TUCCI, *Direitos e Garantias ...*, *op. cit.,* p. 31).

[13] Não se pretende discutir a autonomia da ética como setor específico do conhecimento, ou como discurso aplicado ao Direito. Sobre o tema, *v.* U. SCARPELLI, *Ética jurídica sin verdad*, Ciudad de México, Fontamara, 2007.

[14] A realidade no século XXI é pródiga em exemplos de aparelhos tecnológicos de acentuada complexidade (por aparelhos tecnológicos ou eletrônicos designa-se não apenas os computadores e *laptops*, mas também todas as modalidades de sistemas digitais embutidos como dispositivos móveis e *smart cards)*. Pense-se, *v.g.*, os problemas suscitados pela computação em nuvem. *A Cloud Computing* é uma forma particular de gestão da tecnologia da informação, em que a localização e a operação da nuvem não são levados ao conhecimento dos clientes.

[15] O poeta português ERNESTO M. DE MELO CASTRO, valendo-se dos ensinamentos de PAUL VIRILLO, adverte que *"para o bem ou para o mal, qualquer invento científico ou produto tecnológico pode, maniqueistamente, ser usado. (...) cada produto tecnológico contém em si a sua específica capacidade de desastre, que mais tarde ou mais cedo se manifestará"* (*Algorritmos*, São Paulo, Musa, 1998, p. 10).

Entre passado e futuro o pensamento e o conhecimento são os instrumentos de transformação. Cada novo ser humano *"inserido entre um passado infinito e um futuro infinito, deve descobri-lo e, laboriosamente, pavimentá-lo de novo"*.[16]

1.2. Cibernética[17]: breves considerações

A breve alusão que se faz à Cibernética justifica-se pelo seu caráter precursor. A partir dos primeiros estudos de WIENER, setores do conhecimento aproximados das modernas comunicações – como a Informática e a Telemática – foram rascunhados. Aliás, historicamente os aparelhos eletrônicos são o resultado de muitas tradições precedentes.[18]

O estudo da Cibernética enquanto campo científico autônomo data de meados do século XX. Das pesquisas de vanguarda pautadas pelo exame minucioso do comportamento fisiológico de animais e humanos, assim como das analogias entre a máquina de cálculo de grandes dimensões e o cérebro humano, origina-se o objeto central da Cibernética: o paralelo entre máquinas e homens.[19]

O estudo desta interação está voltado à compreensão do funcionamento do comportamento humano ou animal, com o objetivo de reproduzi-lo por meio mecânico. Em muitos casos, a habilidade específica de alguns animais serve de subsídio para estudos técnicos. Dois bons exemplos são o morcego (capaz de voar no escuro sem se chocar com

---

[16] H. ARENDT, *Entre o passado e o futuro*, trad. Mauro W. Barbosa de Almeida, São Paulo, Perspectiva, 1979.

[17] O vocábulo "cibernética" tem origem no grego, a partir do termo *"kubernetes"* (dirigir, governar). Na Grécia antiga era empregado para designar a arte de conduzir os navios. O timoneiro, constantemente corrige o trajeto do barco em razão das intempéries do tempo e das variações do vento e da água. No século XVIII, o físico e matemático A. M. AMPERE nomeou *cibernética* a ciência de governar o Estado. A interpretação do termo, no século XX, evidencia a Cibernética como *a ciência do controle*, no sentido mais amplo da palavra.

[18] Para VILÉM FLUSSER a terceira Revolução Industrial é aquela que impõe a substituição das máquinas por aparelhos eletrônicos: *"as ferramentas imitam a mão e o corpo empiricamente; as máquinas, mecanicamente, e os aparelhos neurofisiologicamente". Trata-se de 'converter' (wenden) em coisas as simulações cada vez mais perfeitas de informações genéticas, herdadas, pois os aparelhos eletrônicos consistem nos mais adequados métodos para transformar coisas para o uso"* (*O mundo codificado..., op. cit.,* p. 38).

[19] M. LOSANO, *Lições ..*, *op. cit.,* p. 10.

obstáculos) e o delfim (que possui um "sonar biológico" apto a localizar obstáculos submarinos através da emissão de ondas sonoras).[20]

A reprodução mecânica da fisiologia animal, dos eventos naturais e das ações humanas centram-se como os principais campos de estudo da Cibernética. Para esta ciência impõe compreender o autocontrole encontrado em sistemas estáveis, sejam estes biológicos, mecânicos ou elétricos, com análise profunda dos processos lógicos de transmissão, de informação e de controle de eficácia operativa, em todo tipo de sistemas naturais e artificiais.

A Cibernética assentou fundamentos para analogias antes derivadas do raciocínio geral de caráter metodológico. Os métodos matemáticos passam a descrever de um ponto de vista quantitativo os processos que ocorrem no funcionamento de dispositivos técnicos, da atividade vital dos organismos e das coletividades de seres vivos.[21]

Tema relevante no estudo da Cibernética, pois, a questão de como controlar os mecanismos que regulam determinados fenômenos. A Cibernética oferece a possibilidade do homem tornar-se sujeito ativo em eventos dos quais até hoje foi apenas espectador passivo. Nas palavras de MARIO LOSANO, o homem encontra-se em posição de maior responsabilidade; a Cibernética engrandece as responsabilidades humanas porque superada a posição de impotência frente ao mundo.[22]

O advento da Cibernética marca o estágio da evolução tecnológica em que o homem substitui em parte sua atividade intelectual. Ainda que o momento intelectual mais elevado – de criação e solução dos problemas – permaneça em suas mãos, os setores de organização e execução passam a ser operados pelas máquinas.[23]

A adequada compreensão do fenômeno tecnológico, bem como de suas consequências para o Direito, perpassa pelo conhecimento dos atributos das máquinas cibernéticas. O computador, instrumento encarregado do tratamento automatizado da

[20] *Idem,* pp. 11-12.
[21] YU. M. KORSHUNOV, *Fundamentos Matemáticos de la Cibernética*, trad. Roberto Lanier Alvarez, Moscú, Mir Moskú, s/d, p. 13.
[22] *Giuscibernetica: macchine e modelli cibernetici nel diritto*, Torino, Einaudi, 1969, p. 19.
[23] A. TARANTINO, *Elementi di Informatica Giuridica*, Milano, Giuffrè, 1998, p. 27.

informação, é utilizado no intuito de reproduzir a mais fascinante de todas as funções: o cérebro humano.[24]

Entretanto, somente o homem detém a capacidade de pensar e aprender. Para a máquina estabelecer conexões e relações entre dados e informações distantes depende em grande medida do aperfeiçoamento de soluções próprias de inteligência artificial.[25] Uma pessoa pode estabelecer analogias entre processos que no mais das vezes são inacessíveis aos computadores. Ao traçar metas, bem como estratégias para alcançá-las, a máquina é *instrumento* a serviço do agir humano.

Os precursores do estudo interdisciplinar entre Cibernética e Ciências Humanísiticas são o matemático NORBERT WIENER e o jurista LEE LOEVINGER, ambos estadunidenses.

WIENER vislumbrou em meados da década de 1950 a utilidade do estudo do controle sistemático da informação, na célebre obra "*Cybernetics: or the Control and Communication in the Animal and the Machine"*.

LEE LOEVINGER denominou jurimetria a aplicação dos métodos quantitativos de automação ao conhecimento jurídico, inclusive em relação à formulação de cálculos probabilísticos aplicados à atividade judiciária. O autor foi precursor no estudo de temas que posteriormente seriam revisitados à luz da Informática Jurídica: aplicação da teoria da comunicação e da informação à expressão jurídica; uso da lógica no Direito; recuperação de dados jurídicos por meios mecânicos e eletrônicos e cálculo das probabilidades aplicado à atividade judiciária.

---

[24] *"Para WIENER, o sistema nervoso central engendra um processo circular – 'emergindo do sistema nervoso para os músculos, e reentrando ao sistema nervoso pelos órgãos dos sentidos' – cujo princípio seria idêntico ao que havia encontrado em dispositivos de controle de máquinas"* (JOON HO KIM, *Cibernética, ciborgues e ciberespaço: notas sobre as origens da cibernética e sua reinvenção cultural*, in Horizontes Antropológicos, v. 10, n. 21, jan./jun., Porto Alegre, 2004).

[25] O aperfeiçoamento da chamada inteligência artificial é um desafio para a ciência. O computador tem a capacidade de armazenar milhares de informações sem prejudicar seus mecanismos lógicos de decisão. A automatização permite incrementar a eficiência dos processos de decisão, ao mesmo tempo, no entanto, pode revelar-se uma fonte de perigos; se a máquina não estiver apta a analisar todas as contingências referentes à complexidade do meio ambiente em estudo poderá falsear a realidade (F. MADRID CONESA, *Derecho a la Intimidad, Informática y Estado de Derecho*, Valencia, Soler, 1984, p. 16).

Em síntese são três os setores principais do pensamento jurimétrico: o processamento eletrônico dos dados jurídicos, o uso da Lógica no campo do Direito e a análise das decisões jurídicas.[26]

Os pontos de contato entre Direito e Cibernética foram investigados mais tarde por MARIO LOSANO na obra *Giuscibernetica*, para quem os objetos principais de estudo são: (1) as relações entre o subsistema do Direito e o sistema social, segundo o modelo cibernético[27]; (2) o Direito como sistema normativo, dinâmico e auto-regulador, totalidade em que se investigam não as relações externas, mas sim, as internas, *i.e.,* as que vinculam as partes entre si; (3) a formalização da linguagem jurídica, condição prévia para sua incorporação ao processo cibernético (lógica formal aplicada ao Direito, análise da linguagem jurídica e estudos de teoria geral do Direito)[28]; (4) o tratamento das normas jurídicas como informações e sua ordenação eletrônica, aplicação da tecnologia computacional ao Direito.[29]

Os inegáveis progressos da Cibernética constituem uma das etapas até o atual estágio da sociedade tecnológica. A convivência entre homem e máquina é o prenúncio da criação de um novo território. O entorno digital, oportunamente analisado (item 1.4.3), reflete a construção de um mundo artificial onde as tradicionais noções de tempo, estrutura e espaço se esvaziam.

---

[26] N. DE LUCCA, *Títulos e Contratos Eletrônicos: o advento da Informática e suas consequências para a pesquisa jurídica*, in N. de Luca e A. Simão Filho (orgs.), *Direito & Internet*: *aspectos jurídicos relevantes*, São Paulo, Quartier Latin, 2005, p. 50.

[27] A teoria Cibernética, usualmente descrita como uma superciência (a ciência das ciências) estimulou pesquisas em muitas áreas dentro dos sistemas de controle e de informação. O ponto de partida para a aplicação da teoria Cibernética aos diversos campos do conhecimento é a possibilidade de reduzir todo fenômeno ou processo em informação e sua respectiva transmissão. A informação no interior destes processos é tratada como codificação e descodificação, retroação ou realimentação *(feedback)*. *Feedback* é um princípio que a engenharia de controle utiliza para descrever a atividade de realimentar o sistema com as informações sobre o próprio desempenho realizado a fim de compensar os desvios em relação ao desempenho desejado.

[28] Acerca das consequências negativas de um enfoque eminentemente computacional na Informática Jurídica, bem como da relação dos padrões de decisão, argumentação, justificação e linguagem algorítmica, *v.* J. BARRAGÁN, *Informática y Decisión Jurídica*, México: Fontamara, 2000. Por sua vez, G. CARIDI denomina *Informática Jurídica analítica* os esforços voltados à enunciação algorítmica, porém, esclarece que no Direito os instrumentos interpretativos são incompatíveis com esta aplicação informática (*Metodologia e Tecniche Dell'Informatica Giuridica*, Milano, Giuffrè, 1989*,* p. 9).

[29] *Giuscibernetica ..., op. cit.,* p. 108.

1.3. Telecomunicações

VITTORIO FROSINI, na reflexão sobre as complexas consequências sociais do progresso tecnológico, destaca a instantaneidade do conhecimento dos fatos. Os eventos são vividos pelo homem no exato momento em que ocorrem e as mesmas emoções podem ser sentidas nos pontos mais remotos do planeta. Na relação entre próximo e distante, o progresso tecnológico revolucionou o sentido do *nosso próximo*, uma vez que a Humanidade toda (e não apenas aqueles que nos cercam) avizinham-se graças à comunicação de massa.[30]

Nesta revolução das relações interpessoais, o advento das telecomunicações constitui um dos fatores centrais para a velocidade do fluxo de informações.

O processo comunicativo objetiva a transmissão da informação. Para tanto, em razão da modalidade comunicativa, sempre haverá infraestrutura específica, na qual atuam intermediários. Este contexto, associado às telecomunicações, evidencia três características essenciais: a existência de ao menos duas pessoas ou dois entornos, o emprego de artifício técnico ou infraestrutura comunicativa, e o objetivo de eliminar as eventuais barreiras físicas.

Em sentido técnico, o conceito de *telecomunicações* pode ser extraído do Convênio Internacional de Torremolinos (1973) como *"toda transmissão, emissão ou recepção de signos, sinais, escritos ou imagens, sons ou informações de qualquer natureza por fios, radioeletricidade, meios óticos ou outros sistemas electromagnéticos"* (trad. nossa).[31]

---

[30] *Il Diritto nella Società Tecnologica*, Milano, Giuffrè, 1981, p. 204.

[31] Na Conferência de Madrid de 1932, quando fundou-se a *União Internacional de Telecomunicações (UIT)*, foi definida pela primeira vez como *"toda comunicação telegráfica ou telefônica de signos, sinais, imagens e sons de qualquer natureza, por fio, radioeletricidade ou outro sistema ou procedimento de sinalização elétrica ou visual"* (C. E. DELPIAZZO, M. J. VIEGA, *Lecciones de Derecho Informático*, Montevideo, FCU, 2004, p. 9, trad. nossa). O anexo sobre telecomunicações, aprovado junto com a ata final da rodada Uruguai do GATT, que criou a Organização Mundial do Comércio (Decreto Legislativo 30, de 15 de dezembro de 1994 e promulgado pelo Decreto 1.355, de 30 de dezembro de 1994), de maneira mais sintética definiu telecomunicações como *"a transmissão e recepção de sinais por qualquer meio eletromagnético"*.

Na referida descrição estão compreendidas muitas das comunicações de larga distância. A propagação da informação pode valer-se de aparelhagem técnica (*v.g.*, telegrafia ou telefonia por fio), como também, de artifícios técnicos específicos (hipótese da propagação por ondas luminosas e eletromagnéticas).

O Direito das Telecomunicações compreende a parcela do ordenamento desenvolvida a partir das invenções do telégrafo, telefone, rádio[32] e televisão. Excluídas deste âmbito, portanto, as comunicações orais diretas, por não utilizarem artifício técnico ou infraestrutura comunicativa. Nesta hipótese, patente a inexistência de intermediação técnica, à medida que, para a realização da comunicação, não há a participação de um terceiro alheio aos sujeitos.[33]

As comunicações postais também não integram o campo das telecomunicações, uma vez que a infraestrutura empregada por este sistema não se vale de "*fio, radioeletricidade, meios ópticos ou qualquer outro processo eletromagnético"*.[34]

As comunicações veiculadas pela *internet,* por sua vez, não constituem categoria telecomunicativa. Como se verá (*v.* item 1.5), a *internet* não é modalidade de comunicação, senão sistema que se utiliza de infraestruturas de comunicação variáveis e permite distintas formas de comunicação. Por intermédio da *internet* há duas espécies de vínculos informacionais: o intercâmbio entre dois ou mais usuários (*v.g.,* correio eletrônico, comunicações em tempo real, redes sociais e fóruns de discussão) e a busca de informação ou navegação.[35]

No Brasil, a lei geral de telecomunicações, nº 9.472, de 10 de julho de 1997[36], derrogou o antigo Código de 1962. Instituiu-se a diferenciação entre serviços

[32] Em sentido estrito, a radiodifusão é definida pela Convenção Internacional de Torremolinos (1973) como o *"serviço de radiocomunicação cujas emissões se destinam a ser recebidas pelo público em geral"*, e desse modo, *"abarca emissões sonoras, televisivas ou de outro género"* (trad. nossa).

[33] J. J. GONZÁLEZ LÓPEZ, *Utilización en el proceso penal de datos vinculados a las comunicaciones electrónicas recopilados sin indicios de comisión delictiva,* in E. Pedraz Penalva (coord.), *Protección de datos y proceso penal*, Madrid, La ley, 2010, p. 357.

[34] Segundo a definição do art. 60, § 1°, da Lei Federal 9.472/97: *"Telecomunicação é a transmissão, emissão ou recepção, por fio, radioeletricidade, meios ópticos ou qualquer outro processo eletromagnético, de símbolos, caracteres, sinais, escritos, imagens, sons ou informações de qualquer natureza"*.

[35] J. J. GONZÁLEZ LÓPEZ, *Los Datos de Tráfico de las Comunicaciones Electrónicas en el Proceso Penal*, Madrid, La ley, 2007, pp. 33-34.

[36] A Lei estabeleceu no art. 8º um novo marco regulatório para o setor a partir da criação da Agência Nacional de Telecomunicações (ANATEL), autarquia de regime especial vinculada ao Ministério das

públicos e privados, incumbida a União, por intermédio do órgão regulador e nos termos das políticas estabelecidas pelos Poderes Executivo e Legislativo, de organizar a exploração dos serviços de telecomunicações.

Segundo a redação do parágrafo único, do art. 1°, da lei, *"a organização inclui, entre outros aspectos, o disciplinamento e a fiscalização da execução, comercialização e uso dos serviços e da implantação e funcionamento de redes de telecomunicações, bem como da utilização dos recursos de órbita e espectro de radiofrequências."*

O legislador diferenciou no art. 62, a abrangência dos interesses a que atendem os serviços de telecomunicações, sejam estes de interesse coletivo ou de interesse restrito. Por sua vez, o art. 65 diferencia a modalidade de serviço que será prestada: exclusivamente no regime público, exclusivamente no regime privado, ou concomitantemente nos regimes público e privado.

O art. 2° destaca o dever do Poder Público de garantir o acesso às telecomunicações, a tarifas e preços razoáveis, em condições adequadas; de estimular a expansão do uso de redes e serviços de telecomunicações pelos serviços de interesse público, em benefício da população brasileira; de adotar medidas que promovam a competição e a diversidade dos serviços, incrementem sua oferta, propiciem padrões de qualidade compatíveis com a exigência dos usuários e fortaleçam o papel regulador do Estado; de criar oportunidades de investimento e estímulo ao desenvolvimento tecnológico e industrial, em ambiente competitivo, além de condições para que o progresso do setor seja harmônico com as metas de desenvolvimento social do País.

Tudo isto em face de um novo cenário telecomunicativo, muito distinto daquele do antigo Código de Telecomunicações de 1962. Cada vez mais, as novas tecnologias propiciam acentuada abertura de dados da vida privada para o mundo exterior. Dessa forma, sempre que ausente regulação legal para a tutela dos direitos básicos do cidadão, frontalmente atingida a liberdade de controle das informações pessoais.

---

comunicações. No art. 60 consta a definição de "serviço de telecomunicações" como *"o conjunto de atividades que possibilita a oferta de telecomunicação"*.

1.4. Informática e Direito

A exponencial relevância da Informática e da Telemática, sobretudo a partir do último quarto do século XX, instituiu significativas mudanças na vida social da atualidade. A imprescindibilidade dos sistemas destinados ao tratamento automatizado da informação para os diversos setores do conhecimento é representado pelo notório *protagonismo da tecnologia*, seu *dinamismo* e *tendência à internacionalização*.[37]

As redes de comunicação possibilitam obter, processar e veicular conteúdos em tempo real. Esta evolução repercute sensivelmente nas relações interpessoais e enseja um novo ciclo cultural no qual inexiste distância no tratamento e transmissão da informação.[38]

Ademais, como agente potencializador dos efeitos do fenômeno de internacionalização da comunicação, desponta a convergência de tecnologias voltadas ao fluxo instantâneo de informações entre sujeitos situados nos pontos mais distantes do planeta.

À medida que a tecnologia constantemente se modifica, a chamada *democracia eletrônica* fomenta uma revolução em curso, na qual incrementadas as possibilidades de participação direta dos cidadãos na política. As comunidades virtuais, agrupamentos sociais surgidos espontaneamente, dedicam-se a projetos comuns e constituem voz ativa na *res publica*. Não há se pensar no desaparecimento do sistema político representativo, mas sobretudo, no papel fiscalizatório e inovador desta intervenção social.[39]

---

[37] L. A. BALLESTEROS MOFFA acrescenta a estas características da sociedade moderna, ainda outra: a informação como fonte de poder e imposição de vontade (*La Privacidad Electrónica: internet en el centro de protección*, Valencia, Tirant lo blanch, 2005, pp. 36-37). Sobre poder e controle democrático da *internet*, *v.* R. J. MOLES PLAZA, *Derecho y control in Internet*, Barcelona, Ariel, 2004.

[38] Nas palavras de M. A. DAVARA RODRIGUEZ *"empieza a no contar el tempo ni el espacio"* (*Manual de Derecho Informático*, Navarra, Thomson Aranzadi, 2008, p. 25).

[39] A. TÉLLEZ AGUILERA, *Nuevas Tecnologías – Intimidad y Protección de Datos*, Madrid, Edisofer, 2001, pp. 23-24.

Por conseguinte, a regulação jurídica das situações próprias deste entorno situa-se igualmente em processo de aperfeiçoamento, diante das novas relações sociais, econômicas, políticas e culturais, até então desconhecidas.

Inegável o surgimento de temas e problemáticas específicas desta nova área do conhecimento, assim como sua repercussão nos distintos setores do Direito público e privado. O papel desempenhado pela Informática fomenta, cada vez mais, debates pautados pela abrangência do fenômeno tecnológico. Indaga-se, sobretudo, acerca de seu lugar nos tradicionais esquemas das disciplinas jurídicas.

Não se pode ignorar que a atividade informática, por concentrar em um mesmo entorno situações que concernem aos diversos ramos do Direito, cada vez mais acentua a conveniência da constituição de um novo campo do conhecimento jurídico. Trata-se do reconhecimento de um *Direito Informático* ou *Informática Jurídica,* não apenas como Direito (plexo de normas que constitui parcela da ordem jurídica), mas também como ciência (disciplina autônoma destinada ao estudo desta parcela do ordenamento).[40]

Impõe constatar, primeiramente, que Direito e Informática podem ser analisados sob enfoques distintos. Por um lado, a capacidade com a qual os avanços tecnológicos difundem-se no terreno jurídico – em especial, no que diz respeito às técnicas avançadas para o tratamento automatizado da informação jurídica – é objeto da *Informática Jurídica*. Por outro, o ramo dogmático voltado à aplicação da Informática em setores específicos, como atividades econômicas, financeiras e sociais, consubstancia o viés de estudo do *Direito Informático*.[41]

A respeito da Informática Jurídica, desponta seu caráter instrumental para os juristas. A utilização de avanços tecnológicos pode ser expressa na criação de bases de dados que permitam acesso rápido a legislação sempre atualizada, na possibilidade de

[40] C. E. DELPIAZZO, M. J. VIEGA, *Lecciones ...*, *op. cit.,* pp. 13-14.
[41] Como esclarece A. TARANTINO, no primeiro caso a Informática é um meio técnico e o Direito um objeto de tratamento sob vários níveis (decisão, documentação, gestão); em contrapartida, no segundo, o Direito é meio técnico para regulação do fenômeno da Informática e resolução de problemas (*Elementi ...*, *op. cit.,* p. 28).

consulta de jurisprudência, elaboração eletrônica de documentos e petições, ou emprego de determinado foro jurídico de discussão.[42]

A *Informática Jurídica*, já na obra de MARIO LOSANO (*Giuscibernetica macchine e modelli cibernetici nel diritto)*, não sob o enfoque sintético que mais tarde seria delimitada,[43] fora destinada ao estudo daqueles quatro objetos principais (*v.* item 1.2).[44] À luz destas quatro formulações, avulta seu papel como abordagem empírica do estudo interdisciplinar entre Informática e Direito.[45]

Diversamente, o Direito Informático – disciplina voltada à busca de respostas positivadas no ordenamento jurídico aos conflitos que as novas tecnologias podem gerar na sociedade – gradativamente se consolida como nova área de estudo. Trata-se, pois, de complexo de normas legislativas, decisões jurisprudenciais e de literatura jurídica em matéria de Informática.

Os conflitos oriundos da relação entre Informática e Direito apresentam acentuada variedade e complexidade. Os contatos entre ambos os setores do conhecimento são inúmeros, no Direito Civil (*v.g*., contratos, seguros, responsabilidade civil, direitos de autor); no Direito Econômico (*v.g*., automatização bancária); no Direito do Trabalho (*v.g*., contrato de trabalho); no Direito Penal (*v.g*., novas condutas típicas e diversidade de perfis de delinquência); no Direito Processual (*v.g*., informatização da justiça e fontes de provas digitais), e em temas notadamente interdisciplinares (*v.g*., direito à intimidade e proteção de dados).[46]

---

[42] A. TÉLLEZ AGUILERA, *Nuevas Tecnologías ...*, *op. cit.,* pp. 40-41.

[43] G. CARIDI destaca, em síntese, os dois objetivos fundamentais da Informática Jurídica: a documentação jurídica automática e a Informática jurídica de gestão (*Metodologia e Tecniche Dell'Informatica Giuridica*. Milano: Giuffrè, 1989, p. 11).

[44] *Giuscibernetica ...*, *op. cit.,* p. 108.

[45] N. DE LUCCA. *Títulos e Contratos ...*, *op. cit.,* p. 54.

[46] M. A. DAVARA RODRIGUEZ exemplifica conflitos característicos do Direito Informático: direitos e obrigações decorrentes da criação, distribuição, exploração e utilização de *hardware* ou *software*; direitos e obrigações dos criadores, distribuidores e usuários de bases de dados e produtos multimídia; contratação de bens e serviços informáticos; a proteção jurídica dos dados pessoais; a regulação do fluxo internacional de dados informatizados; a validade probatória dos documentos gerados por meios eletrônicos; os delitos informáticos; os direitos dos compradores e usuários, em face da posição dominante das multinacionais do setor informático; a vigência de leis de defesa da concorrência, diante dos grandes produtores e distribuidores de informática e de entidades que comercializam informações; a proteção jurídica do *software*; o desenvolvimento das telecomunicações; a comprovação ou autenticação eletrônica de documentos; o direito dos cidadãos de relacionar-se com a Administração pública por meios eletrônicos e a obrigação desta de compatibilizar-se com os meios e sistemas eletrônicos para que esse direito possa ser exercitado; a regulação

O crescimento quantitativo de problemas de Direito Informático, bem como o aperfeiçoamento qualitativo de conceitos próprios, permite vislumbrar certo grau de maturidade atingido. Contudo, se a autonomia científica de um setor do conhecimento jurídico consiste na capacidade de resposta aos questionamentos pelos seus próprios institutos, antes de recorrer a outros setores da dogmática ou princípios gerais do Direito[47], talvez seja prematuro sustentar o Direito Informático como protagonista de autonomia científica em plenitude.

Há que se reconhecer a vocação autônoma de uma disciplina voltada às novas tecnologias informativas no campo do Direito, sem se descurar do seu caráter fragmentário e ainda em formação.[48] Como se verá no item seguinte, em vista do caráter mais abrangente, pertinente a adoção da terminologia *Direito Telemático*.

1.4.1. Telemática e informação em rede

A sociedade atual se vê profundamente reestruturada pelo advento da convergência das telecomunicações com a Informática. A fusão do tratamento automatizado de dados com as técnicas de telefonia originou o que se conhece atualmente

---

jurídica do fenômeno da *internet* (*Manual de Derecho ..., op. cit.,* pp. *28-30).* C. E. DELPIAZZO, e M. J. VIEGA apontam, ainda, o tema da liberdade informática ou defesa das liberdades, em face de agressões perpetradas pelas tecnologias da informação e comunicação (*Lecciones ...*, *op. cit.,* p. 17).

[47] Segundo o ensinamento de C. A. BANDEIRA DE MELLO: *"Diz-se que há uma disciplina jurídica autônoma quando corresponde a um conjunto sistematizado de princípios e normas que lhe dão identidade, diferenciando-a das demais ramificações do Direito"* (*Curso de Direito administrativo*, 12ª ed., São Paulo, Malheiros, 2000, p. 25).

[48] TÉRCIO SAMPAIO FERRAZ JUNIOR afirma que distinções como Direito público e privado, bem como a identificação de seus ramos específicos, tem por objetivo *"criar condições para a decidibilidade com certeza e segurança"* (*Introdução ao Estudo do Direito*, 4ª ed., São Paulo, Atlas, 2003, p. 142). Segundo o autor, a especialização crescente de novos ramos significa para a dogmática a determinação de objeto e princípios próprios. Sem deixar de atentar, porém, à pertinência das discussões doutrinárias, que analisam o escasso acréscimo em operacionalidade (pertinência, viabilidade e oportunidade) de muitas destas novas especificações (Idem, pp. 144-145).

por Telemática.[49] Trata-se de alteração profunda na forma como a informação é captada, transformada, armazenada e difundida.[50]

A Comissão Europeia sobre convergência (1997) conceituou a Telemática como *"a capacidade de diferentes plataformas de rede de transportar tipos de serviços essencialmente similares ou a aproximação de dispositivos de consumo tais como o telefone, a televisão e o computador pessoal"* (trad. nossa).[51]

Na doutrina, frequente o uso do termo "cyber espaço"[52] para a designação do território ocupado pelo fluxo de comunicações telemáticas. O "cyber espaço" – que engloba tanto a *internet,* como outras redes de caráter restrito – evidencia a ideia de localização da informação, mais precisamente, o local onde pode ser encontrada.[53]

A paulatina substituição da tecnologia analógica para a digital representa autêntico marco para a viabilização da estrutura das redes de informação tal como as conhecemos atualmente. A digitalização consiste na conversão em números do conteúdo que se deseja transmitir; procedimento utilizado para os diversos tipos de informação, tais como, textos, imagens, gráficos e sons.[54] Em contrapartida, toda a informação que não é convertida em dígitos corresponde à tecnologia analógica.[55]

O intercâmbio da informação digitalizada depende, pois, da existência de redes eficazes de comunicação informática. Este fluxo constante de conteúdo conforma

---

[49] F. MORALES PRATS, *La tutela penal de la intimidad: privacy e informática*, Barcelona, Ediciones Destino, 1984, p. 36.

[50] Segundo E. MORÓN LERMA *"se trata de una revolución que nos ensarta directamente en el ser, en el conocimiento, en la información"* (*Internet y Derecho Penal: Hacking y otras Conductas Ilícitas en la Red*, Navarra, Arazandi, 2002*,* p. 101).

[51] *Cf.* Livro Verde da Comissão Europeia, UE 03/12/1997. No documento, a *internet* constitui parte do fenômeno da confluência entre Informática e telecomunicações.

[52] Optou-se nesta Dissertação pelo emprego da terminologia *entorno digital*. Conquanto "cyber espaço" não se mostre equivocado, de rigor privilegiar a noção de digitalização, por se tratar do melhor critério técnico-descritivo do conteúdo deste espaço: *digital* à medida que composto por números e algoritmos. Para esclarecer a terminologia empregada *"dá-se o nome de algoritmo ou processo ao conjunto de operações necessárias para transformar os dados iniciais nos resultados que se deseja obter num determinado trabalho"* (E. ALCALDE, M. GARCIA, S. PAÑUELAS, *Informática Básica*, trad. Sérgio Molina, São Paulo, Mc Graw-Hill, 1991, p. 3).

[53] R. J. MOLES PLAZA, *Derecho y control ..., op. cit.,* p. 15.

[54] Sobre os estudos precursores que permitiram mais tarde a digitalização de textos, imagens e sons, ou seja, conversão destes diversos conteúdos nas unidades numéricas 0 (zero) e 1 (um), *v.* a exposição de MARIO LOSANO acerca do sistema binário (*Lições de informática ...*, pp. 57-68).

[55]Algumas das vantagens do sistema digital são a extraordinária velocidade, a qualidade da comunicação e maior eficiência do sinal digital (L. A. BALLESTEROS MOFFA, *La Privacidad Electrónica ..., op. cit*., p. 106).

o lugar ocupado pelo computador, que deixa de ser unidade operacional altamente centralizada, para inserir-se no contexto de pluralidade e conexão em escala mundial.

Com respeito à abrangência de transmissão da rede, quando circunscrita a um mesmo edifício constitui a chamada *LAN (Local area network)* ou rede local, caracterizada por sua limitação geográfica e ausência de emprego de telecomunicações. As redes metropolitanas *(Metropolitan area network)* ocupam o espaço aproximado de uma cidade. No caso da conexão estender-se por um país ou continente tem-se uma rede de área ampliada *WAN* (*Wide area Network*).[56]

Um dos computadores da rede pode ser o responsável pelo controle dos principais arquivos *(servidor[57])* e os demais serão os *clientes*. Portanto, a estrutura cliente-servidor viabiliza a comunicação entre o sujeito que proporciona um serviço e aquele que o solicita.

É possível, também, que o servidor de uma rede conecte-se a outras, formando assim *redes de redes* ou *inter-redes*. Esta situação permite compreender o caráter da *internet* como representação de um hipertexto: rede que conecta inúmeras outras redes.

Originalmente, a *internet (International Network of Computers)*, surge em razão do aperfeiçoamento da tecnologia militar americana no período da guerra fria. A criação de uma rede de telecomunicações resistente inclusive a investidas nucleares se deu em meados dos anos 1970, quando o governo dos EUA promoveu a rede experimental *Advanced Research Projects Agency* (ARPANET), com o objetivo de facilitar a comunicação entre investigadores nas mais diversas partes do mundo. O objetivo principal das pesquisas era a implementação de uma ampla rede de computadores em que a

[56] A LAN interliga-se por meio de rede restrita espacialmente a uma sala, edifício ou campus. Normalmente todos os equipamentos encontram-se conectados a um mesmo cabo, perfazendo uma distância máxima de aproximadamente um quilômetro. Na MAN, a interligação entre os equipamentos ocorre por meio de fibras ópticas, rádios microondas ou linhas dedicadas, e a distância máxima entre os equipamentos de aproximadamente dez quilômetros. Na WAN, ou rede remota, os dados circulam por diferentes redes e sub-redes, estendendo-se por mais de mil quilômetros. A sub-rede pertence a um provedor de serviço de comunicação e sua função é levar mensagens de um computador para outro (M. MARÇULA, P. A. BENINI FILHO, *Informática: Conceitos e aplicações*, 2ª ed., São Paulo, Érica, 2007, pp. 243-245).

[57] O *servidor ou provedor de acesso a internet* possibilita a conexão TCP/IP ao disponibilizar ao usuário uma ou mais linhas; o *provedor de serviços de internet* vale-se de uma conexão TCP/IP permanente e de servidores continuamente conectados a *internet* para proporcionar serviços de rede (*v.g.* o armazenamento de páginas *web*, acesso a foros de debate e servidores FTP ou correio eletrônico); o *operador de telecomunicações* encarrega-se de transmitir dados entre o usuário de uma rede e o provedor de acesso a *internet*.

informação efetivamente não corresse risco e pudesse ser veiculada até mesmo em caso de ação bélica.[58]

A ideia principal desse sistema consiste na inexistência de um centro nevrálgico que controle a rede; a descentralização impede a existência de um ponto fraco do sistema. Durante os anos 1970 e 1980, a ARPANET continuou em expansão, foram incorporados serviços e agregaram-se outras redes que utilizavam a mesma linguagem, dando origem ao chamado protocolo TCP/IP *(Transmission Control Protocol/Internet Protocol).*[59]

A *internet* compõe-se, portanto, de todas as redes que utilizam o protocolo e comunicação comum IP e cooperam para formar uma rede apenas a fim de prestar serviços a usuários em geral.

Na *internet* prevalece o *livre intercâmbio de informação*, tanto com respeito à liberdade de acesso ao conteúdo, como também no plano técnico. Outros elementos constitutivos diretamente relacionados são: o caráter *aberto da rede* (qualquer pessoa pode nela ingressar por meio de um terminal de computação, desnecessária habilitação especial ou acordo prévio); *público* (franqueado o acesso às pessoas em geral); *global* (inúmeros e variados servidores abarcam todo o planeta) e *não governado centralizadamente* (não há autoridade central, mas sim, coordenações e cooperação técnica).[60]

O grau de liberdade no entorno digital pode ser dimensionado em face das tentativas de controle administrativo da *internet* por parte dos governos. Não raro, iniciativas destinadas a restringir o acesso a determinados documentos são imediatamente rechaçadas pelos internautas que, em poucos segundos, podem disseminar milhares de

[58] A tecnologia foi concebida sob a perspectiva de auto-regeneração, diante de eventuais ataques exteriores que pudessem incapacitar o sistema.
[59] O *Transmission Control Protocol/Internet Protocol* é o protocolo usado pela *internet* para a transmissão de dados. Este Protocolo é o mais difundido no mundo, tanto por sua ampla utilização na *internet,* mas também por ser um padrão aberto, independente do controle de qualquer empresa particular.
[60] C. E. DELPIAZZO, M. J. VIEGA, *Lecciones ...*, *op. cit*., p. 55.

cópias pelo mundo todo. Como saldo final, o documento em questão torna-se muito mais conhecido do que era antes da censura.[61]

Por vezes, recorre-se à representação da *internet* como uma teia de aranha. A sucessão de redes representada pela *internet* configura um sistema reticular[62] em contínua expansão, um sistema de sistemas ou labirinto móvel. Não há um plano concreto dos limites desta figura; assemelha-se a um hipertexto e tem ramificações universais.

Como já se fez referência (item 1.3), duas são as formas de comunicação por meio da *internet,* atividades tipicamente características dos seus usuários: a comunicação entre dois ou mais usuários e a busca de informação (navegação).

1.4.2. Novas tecnologias e processo penal

À medida que, com mais frequência, os dados pessoais são empregados na investigação penal, os pontos de contato entre o Direito processualístico penal e o Direito Telemático mostram-se relevantes. Tais fontes de provas[63] podem constituir

[61] Para R. J. MOLES PLAZA *"la red responde como un cuerpo vivo ante un ataque vírico"* (*Derecho y control ...*, *op. cit*., p. 18). Não se olvide, pois, que a rede foi constituída para que a informação chegue a toda parte, inclusive sob ameaça ou ataque nuclear.

[62] A noção de rede para o *Direito Telemático* tem caráter técnico, enquanto representação do local de intercâmbio da informação e dos liames infinitos entre cada uma de suas partes. É certo, todavia, que a rede também pode ser empregada para configurar um modelo teórico para o Direito. Trata-se, como afirma M. LOSANO, de metáfora arquitetônica que remete *"ao pensamento sistemático, aquele pensamento que, em campo jurídico, incitou nos Oitocentos os Pandectistas a 'konstruiren' o material romanístico e, nos Novecentos, incentivou Kelsen a pesquisar a estrutura do Direito. Todas essas teorias jurídicas contêm a metáfora arquitetônica da construção, do con-struere. Com essas teorias os juristas procuram explicar o Direito até os nossos dias"* (*Modelos teóricos ..., op. cit.,* p. 266). Os estreitos limites deste trabalho não permitem aprofundamento acerca da contínua e irregular expansão do Direito atual. Pretende-se apenas fazer referência à reflexão do cotejo entre Direito codicista, hierárquico, sistemático, piramidal, cujo expoente máximo é HANS KELSEN (*Teoria pura do direito*, trad. J. Baptista Machado, São Paulo, Marins Fontes, 2000) – em contraposição ao Direito pós-moderno, reticular, solúvel, heterárquico, policêntrico de MARIO LOSANO.

[63] Segundo ANTONIO MAGALHÃES GOMES FILHO, a expressão *fontes de prova* designa *"pessoas ou coisas das quais pode-se conseguir a prova"*. Por outro lado, os meios de prova são *"os instrumentos ou atividades por intermédio dos quais os dados probatórios (elementos de prova) são introduzidos e fixados no processo"*. Outra diferenciação pertinente se dá entre o elemento de prova e o resultado da prova. O primeiro aproxima-se da noção de *evidence* do Direito anglo-saxão, ou seja, *"cada um dos dados objetivos que confirmam ou negam uma asserção a respeito de um fato que interessa à decisão da causa"*; o resultado da prova *(proof)* constitui *"a conclusão que se extrai dos diversos elementos de provas existentes (...) procedimento intelectual do juiz que permite estabelecer se a afirmação ou negação é verdadeira ou não"* (*Notas sobre a terminologia da prova: reflexos no processo penal brasileiro*, in F. L. Yarshell, M. Z. de

elementos de convicção voltados à apuração de crimes e ao combate à criminalidade organizada, mas em razão de seu acentuado grau de intrusão na vida privada devem ser suficientemente reguladas.

Especial relevância tem demonstrado a temática da investigação informática, atinente ao aperfeiçoamento dos métodos de investigação que circundam o entorno digital. Notadamente, no cenário atual da *Common Law,* destaca-se a denominada *computer forensics,* consistente no uso de técnicas especiais de busca, autenticação e exame de dados eletrônicos voltadas a determinar se um equipamento foi utilizado para fins ilegais.

O objeto de estudo da *computer forensics* centra-se na análise das fonte de prova digital *(digital evidence)*; no desenvolvimento de instrumentos *(tool)* de busca de fonte de prova digital, balizados por um método preciso e estritamente técnico; nas novas tecnologias para a memorização e circulação das possíveis fontes de prova digital, segundo as quais, o dado é memorizado e armazenado com base em novo suporte.[64]

Em atenção ao cometimento de crimes mediante o uso de sistemas informáticos, cabe à *computer forensics* disciplinar a conservação, análise e documentação de dados. Avulta sua relevância como meio técnico para assegurar a integridade de tais elementos e dos suportes físicos que contenham informações eletrônicas, durante todas as fases de processamento, de forma a propiciar uma correta conservação das provas digitais.

Moraes (orgs.), Estudos em homenagem à Professora Ada Pellegrini Grinover, São Paulo, DPJ, 2005, pp. 307-309).

[64] No Direito italiano também conhecida como *digital forensics* ou *network forensics*, cujos primeiros trabalhos acadêmicos datam do final dos anos 80. Para G. ZICCARDI a definição técnica da *digital forensics* é: *"scienza che studia il valore che un dato correlato ad un sistema informatico o telematico può avere in un ambito sociale, giuridico, o legale che dir si voglia"*. Os cinco pontos cardeais da disciplina consistem na conservação, identificação, aquisição, documentação e interpretação da fonte digital de prova (*Investigazione Penale e Tenologia Informatica*, Milano, Giuffrè, 2007).

1.4.3. Uma reflexão sobre o entorno digital: interpretação em rede e liberdade como reciprocidade

Se os computadores e as redes de comunicação criam novos espaços de convivência, não é dado descurar das importantes repercussões jurídicas nesta relação entre homem e aparelho eletrônico. Destarte, o presente tópico parte de uma preliminar investigação sobre o sentido da expressão *entorno digital* e do seu alcance no Direito, em especial para examinar a reinvenção dos critérios territorial-temporal-estrutural.

A dogmática hermenêutica constitui um campo dotado de complexidade própria. Aos problemas tradicionais da ciência do Direito como teoria da interpretação soma-se o desafio atual de avaliar em que medida os influxos tecnológicos do século XXI repercutem neste plano. Seria possível, pois, constatar a existência de novas metodologias humanísticas na era digital com consequências no campo da hermenêutica jurídica?

Ainda se tratará brevemente da noção de Liberdade como autonomia recíproca de acesso à informação. A comunicação em rede institui sensíveis alterações nos processos comunicativos, sobretudo para abranger espaços vitais socialmente compartilhados por um sem número de sujeitos. O espaço antes delimitado como de autonomia individual passa a ser reconhecido como exercício de liberdade em comum.

1.4.3.1. Entorno digital (território-tempo-estrutura)

A tentativa de aclarar o sentido da expressão *entorno digital* é uma busca desafiante. Pressupõe excogitar a temática do agir humano na sociedade da informação. Com efeito, as tradicionais noções de *território, tempo e estrutura* no século XXI já não asseguram a compreensão espacial, cronológica e natural da fluidez e multidimensionalidade das relações jurídicas.

Preliminarmente, de grande valia deter-se em uma das mais surpreendentes criações de JORGE LUIS BORGES: a *Biblioteca de Babel.* Se por um lado, tal referência não serve propriamente para conceituar o *entorno digital*, por outro alerta para uma das acepções desta expressão: um certo fascínio representado pela superação das fronteiras do real. Se a vivência diária da evolução tecnológica pode desconcertar, igualmente o convite de BORGES "*hacia al fantástico"* intriga os sentidos. A imagem criada pelo autor constitui o primeiro passo para vencer a obscuridade do entorno digital, fator relevante para a compreensão da condição informática.

Foi na memorável obra *"Ficciones"* que BORGES formulou a misteriosa figura da *Biblioteca de Babel*. Inúmeras (talvez infinitas) galerias hexagonais compõem esta *Biblioteca*: em cada parede cinco prateleiras, em cada prateleira trinta e dois livros, em todos os livros as mesmas quatrocentos e dez páginas ... andares intermináveis, escadas, saguões e espelhos sobrepõem-se ...

Neste universo intangível, um infinito de livros onde todas as obras imagináveis já foram escritas. Na *Biblioteca de Babel* encontraríamos a presente Dissertação, sua respectiva refutação, bem como as *n* traduções possíveis para todas as línguas e dialetos. O irrealizável permeia o relato do autor; qualquer atividade humana de construção deste espaço físico sem limites estaria fadada ao permanente insucesso.

É certo que as leituras possíveis para a completude e o vazio da *Biblioteca* são inúmeras – a interpretação deste labirinto cunhado por BORGES tem fronteiras insuspeitadas –, alternam-se entre o mundo ora mágico do autor, ora idealista, ora metafísico, ora onírico. Os apaixonantes contornos dessa realidade inconsubstancial sugerem não se tratar de algo etéreo, *talvez esteja logo ali...*[65]

O conto data da década de 1970. Se à época o desenvolvimento científico não permitira vislumbrar a difusão da informação e a conexão mundial atualmente permitidas pela *internet*, também não se imaginaria que o conhecimento estaria à disposição para consulta neste entorno. A alegoria do mestre argentino cria um espaço

[65] *"Como todos los hombres de la Biblioteca, he viajado en mi juventud; he peregrinado en busca de un libro, acaso del catálogo de catálogos; ahora que mis ojos casi no pueden descifrar lo que escribo, me preparo a morir a unas pocas leguas del hexágono en que nací"* (*Ficciones*, 67ª ed., Buenos Aires, Emecé, 2006, p. 110).

onde se localizam todos os livros possíveis. O pensar rompe com a razão do território conhecido, próximo e palpável.

O exercício de imaginação proposto por BORGES desperta a curiosidade do leitor ao sugerir a apreensão de algo que não tem limites ou sequer pode ser capturado pelas mãos. Os hexágonos da *Biblioteca* são a barroca representação de um outro mundo – percorrer as estantes em busca de um livro, em busca do *livro dos livros.*

Ainda que capaz de imaginá-la, os alicerces que constituem a *Biblioteca de Babel* têm uma indecifrável composição. À sua maneira, a evolução da tecnologia e da *internet* também cria locais fisicamente inexistentes, ficções antes imaginadas pela literatura e pelo cinema.

Não são poucas as indagações que permeiam a condição informática, essencialmente virtual (lúdica). Em alguma medida, transitar pelo entorno digital seria uma experiência de busca pelo conhecimento do novo? O homem que percorre as autopistas da informação não está reinventando a si mesmo?[66]

As máquinas cada vez mais avançam no aprimoramento de técnicas de deslocalização, cujo exemplo recorrente é representado pelas redes. Embora notáveis as diferenças, a moderna ciência da computação permite o acúmulo de informações no entorno digital em níveis quantitativos de crescente expansão, cujos limites são efetivamente insuspeitados. O acervo de livros, notícias e documentação (não coisas) presentes em páginas da *World Wide Web (WWW)* prescindem do território físico e possibilitam até mesmo a ubiquidade do usuário.[67]

O tempo no entorno digital também é cronologicamente peculiar. Por vezes, impossível precisar a data de uma informação coletada através da navegação, assim como o momento de emissão da comunicação. A instantaneidade da informação é regra

[66] O portal do jornal *O Estado de São Paulo* noticiou, em 20 de junho de 2011 (Biblioteca Britânica no *google books*), a iniciativa do *site Google* de digitalizar duzentos e cinquenta mil livros do acervo da biblioteca britânica e oferecer conteúdo por seus resultados de buscas. "*O gigante das buscas na internet já digitalizou 13 milhões de livros, por meio de parcerias com mais de 40 bibliotecas em todo o mundo, e oferece acesso a esse conteúdo por meio de seus resultados de buscas."* Disponível em: *http://blogs.estadao.com.br/link/biblioteca-britanica-no-google-books/*. Acesso em 20 jun. 2011, h. 21:15.

[67] W. HASSEMER, *Oportunidades para la privacidad frente a las nuevas necesidades de control y las tecnologias de la información*, trad. A. Chirino Sánchez, in Nueva Doctrina Penal, Buenos Aires, Editores del Puerto, 1999, p. 100.

que comporta exceções, não sendo raras as falsas convicções temporais (espelhismos). A atualização dos serviços na *internet* pode ser menos frequente do que se acredita; ademais, a interconexão mundial ocorre no contexto dos distintos fusos horários dos internautas. A falsa instantaneidade tem fundamento em procedimentos técnicos involuntários ou voluntários (*v. g.,* mediante o uso de *softwares* específicos de modificação do momento de transmissão ou recepção da informação).[68]

A estrutura das relações jurídicas neste ambiente suscita novas problemáticas. Para citar dois exemplos, pense-se nas relações contratuais e na *cyber criminalidade*. Os contratos não se limitam a uma relação jurídico negocial entre duas partes, mas repercutem entre categorias sociais e consumidores. Por sua vez, os crimes atingem uma generalidade indeterminável de sujeitos passivos; também a potencialidade lesiva e o desvalor de certas condutas mostram-se sensivelmente gravosos.

Neste entorno extraterritorial[69] e extratemporal, informações podem ser empregadas para distintas finalidades. À medida que representa *longa manus* para o agir humano, inúmeros os escopos desta obtenção de informações: fonte de prova em uma investigação criminal; contratação de bens e serviços informáticos; proteção jurídica de dados pessoais; regulação do fluxo internacional de dados informatizados; validade probatória de documentos gerados por meios eletrônicos; delitos informáticos, etc.

O entorno digital, ao reinventar certas noções, impõe realidade peculiar e contrapõe-se aos padrões conhecidos de tempo-espaço-estrutura. A instantaneidade dos acontecimentos em muito difere do tempo cronológico e parcimonioso do Direito. Por sua vez, a deslocalização conflita com a noção de espaço físico, à medida que possibilita a ubiquidade e o encurtamento de distâncias: em um mesmo dia é possível trabalhar presencialmente no Brasil e virtualmente em outros países.

Nesse sentido, o entorno digital pode ser conceituado como *um espaço imaterial, construído a partir de bases numéricas (algorítmicas), onde está situada a informação*.

---

[68] Sobre a globalização e a aceleração do tempo *v.* C. LAFER, *Brasil: dilemas e desafios na política externa*, São Paulo, in Estudos Avançados, v. 14, n. 38, jan./abr., 2000, pp. 264-266.

[69] A extraterritorialidade sinaliza também a diluição das noções de soberania e competência territorial no entorno digital.

No entorno digital os marcos territoriais e temporais não podem ser mensurados segundo a somatória de unidades de tecnologia digital (*bit*, *byte*, *megabyte*, *gigabyte* e *terabyte*)[70]. Há algo mais nos horizontes do internauta, um certo desconcerto de conceber o virtual como real, um percurso de estranhamento, permeado de perigos e de descobertas.

O trajeto dos peregrinos na *Biblioteca de Babel* também é permeado pelo inapreensível. Irradiadas do conto de BORGES as veredas para um caminhar muito além do racional; pensar na *Biblioteca de Babel* é recorrer à poética para compreender este mundo virtual.[71] A partir do jogo entre real/fantástico o artista sente e enfrenta o mundo. Com BORGES o inverso também é verdadeiro: a *poeisis* faz sentir e desperta os sentidos para a delibação da realidade.

Ao mesmo tempo que existe, o homem percorre outros trajetos nas autopistas da informação; a multiplicidade do real na agoridade causa estranhamento e potencializa a diversidade da experiência[72] humana.

1.4.3.2. Interpretação e Direito em rede

A ciência do Direito como teoria da interpretação vale-se das técnicas interpretativas (gramatical, lógica, sistemática, teleológica, histórico-evolutiva e etc.) e da

[70] A menor quantidade de informação que pode ser armazenada na memória de um computador denomina-se *bit*. O agrupamento de oito *bits* constitui a unidade de informação *byte*. O *megabyte* é formado por cerca de 1.048.576 (ou 2^{20} *bits*), o gigabyte por 2^{30} *bits* e o terabyte por 2^{40} *bits*.

[71] A metáfora contribui para, a partir da experimentação de uma situação, a compreensão de outra. O poder da metáfora consiste na habilidade de capacitar a compreensão. Ainda que esta figura de linguagem não descreva precisamente uma situação, capta um sentimento palpável; a utilidade da metáfora não está em seu realismo, mas no modo como dirige a atenção para certos problemas políticos e sociais. Algumas das metáforas mais significativas da literatura ficam por conta de GEORGE ORWELL e FRANZ KAFKA. Na obra "*1984"* ORWELL elaborou o plano de um governo totalitário que tinha conhecimento sobre todos os aspectos de uma pessoa. O *Big Brother* exerce total controle dos cidadãos: o governo constrói a linguagem, reescreve a história, silencia as críticas, doutrina a população, queima livros... Em *O Processo* Kafka narra as desventuras de K., acusado judicialmente sem conseguir descobrir as razões pelas quais está sendo processado, dando início a infindáveis buscas. O livro de ORWELL anuncia com desolação um futuro de liberdade mitigada, no qual o íntimo e público não mais se diferenciam; o sentimento despertado por KAFKA paira em torno da frustração e vulnerabilidade humana.

[72] Nas palavras de CELSO LAFER: *"A experiência resulta da interação entre o sujeito que conhece e o objeto que é conhecido. Tem a dimensão de pôr a prova, de ensaiar, de testar"* (*Filosofia do direito e princípios gerais: considerações sobre a pergunta "o que é a filosofia do direito"*, in A. Caffé Alves [et alii], *O que é a Filosofia do Direito?*, Barueri, Manole, 2004, p. 42).

integração, como meios para a busca do sentido. Os recursos hermenêuticos viabilizam a compreensão dos fatos segundo uma dupla perspectiva: o reconhecimento da vontade do legislador ou da vontade da lei como sede do sentido da norma (*voluntas legis* e *voluntas legislatoris*).[73]

Os ensinamentos de FRANÇOIS OST e MICHEL VAN DE KERCHOVE permitem entrever o lugar ocupado pelo intérprete do Direito: o coração de um emaranhado de sentidos que a ele cumpre organizar. A função da interpretação não se reduz à reprodução mecânica de um sentido já dado, mas também não se amplia a ponto de constituir livre elaboração de um sentido inédito. Em linhas gerais, o espaço da interpretação estaria em posição intermediária à recitação e à invenção.[74]

As reflexões a respeito dos pontos de contato entre tecnologia e conhecimento jurídico não podem passar desapercebidas também no estudo da teoria da interpretação. O entorno digital, ao situar um emaranhado de informações à disposição do jurista, representa uma ferramenta valiosa de acesso ao conhecimento. Cumpre, assim, examinar se a Informática desempenha algum papel na busca pela composição entre os sentidos do texto normativo.

O acesso à informação no entorno digital pressupõe o funcionamento de equipamentos técnicos, por meio dos quais são visualizados na tela textos e imagens que não possuem matéria física. Na verdade, constituem algoritmos (fórmulas matemáticas) e qualquer tentativa de agarrar as informações com as mãos fracassará. Trata-se de uma modificação no modo de lidar com o mundo; não nos é dado apoderar ou interagir fisicamente com os objetos, pois estes são essencialmente virtuais:

> "Esse novo homem que nasce ao nosso redor e em nosso próprio interior carece de mãos (ist handlos). Ele não lida (behandelt) mais com as coisas, e por isso não se pode mais falar de suas ações concretas (Handlungen), de sua práxis ou mesmo de trabalho. O que lhe resta das mãos são apenas as pontas dos dedos, que pressionam o teclado para operar com os símbolos. O novo homem não é mais uma pessoa de ações concretas, mas sim um performer (Spieler): Homo ludens, e não Homo faber. Para ele, a vida deixou de ser um

[73] T. S. FERRAZ JUNIOR, *A ciência do direito*, São Paulo, Atlas, 2006, p. 70.
[74] *Interprétation*, in Archives de Philosofie du Droit, tomo 35, 1990, p. 185.

> drama e passou a ser um espetáculo. Não se trata mais de ações, e sim de sensações".[75]

A *interatividade* permite ao usuário ser espectador das informações veiculadas na *web*, sem prejuízo de efetivamente participar deste intercâmbio. O mundo dos conceitos, sustentado pela clareza e rigor da linguagem, base para a argumentação jurídica, passa a conviver com a rapidez da obtenção da informação na rede. Em particular, a noção de *interatividade* é muito elucidativa do caráter reticular da comunicação na *internet*: o recebimento e retransmissão da informação é instantâneo para todos os envolvidos neste processo.

A tecnologia oferece um avanço espetacular para o desempenho da atividade do jurista. O computador facilita o armazenamento de informações (documentos e peças processuais), possibilita a pesquisa simplificada de fontes normativas e jurisprudenciais, bem como o acesso a livros, revistas e periódicos em geral. Ademais, possível realizar audiências, participar de eventos, certificar documentos e manter correspondência eletrônica com outros profissionais, sem a necessidade de deslocamento físico.

Por outro lado, a tecnologia ainda não alcançou êxito na tarefa de desenvolver e aperfeiçoar processos confiáveis de interpretação e decidibilidade. Os esforços na criação de *softwares* para a solução de conflitos jurídicos apenas muito restritamente obtiveram êxito, limitando-se a uma gama de relações jurídicas abstratamente simples. A inteligência artificial depara-se com as dificuldades ínsitas à ciência do Direito, relativas à razão jurídica, à complexidade da argumentação e ao uso de critérios que busquem o justo, como os princípios gerais do Direito e a equidade.[76]

Alguns estudiosos da *Informática Jurídica* dedicaram-se a investigar os padrões jurídicos de decisão e argumentação, à luz da formalização algorítmica da linguagem. Sem embargo, o aperfeiçoamento de algoritmos que logrem obter a solução de problemas jurídicos mostra-se ainda muito incipiente.

---

[75] V. FLUSSER, *O mundo*..., op. cit., p. 5.

[76] MIGUEL REALE assevera duas acepções para os princípios: *"uma de natureza moral, e outra de ordem lógica"* (*Filosofia do Direito*, 6ª ed., v.1, São Paulo, Saraiva, 1972, p. 53). Sobre a expansão não apenas lógica, mas axiológica do Direito, *v.* C. LAFER, *A Constituição de 1988 e as Relações Internacionais: reflexões sobre o art. 4º,* in A internacionalização dos direitos humanos: Constituição, racismo e relações internacionais, Barueri, Manole, 2005, p. 217.

O rigor e a técnica do jurista na atividade de interpretação não podem ser sintetizados em expressões matemáticas que, com razoável sucesso, deem conta dos avanços e contingências da hermenêutica jurídica. Assim, os esforços para a elaboração de *softwares* que realizem a interpretação do Direito parecem em grande medida superados.

Se a *Informática Jurídica* não demonstrou resultados satisfatórios para a informatização dos processos decisórios, a generalização do acesso ao entorno digital franqueou uma série de informações ao jurista, sendo possível recorrer amplamente a doutrina e jurisprudência que consta na própria rede. Estas atividades repercutem no processo de escrita e de interpretação – como consequência observa-se uma ampla apropriação e reprodução dos textos encontrados na *web*.

Cada vez mais o trabalho do jurista, voltado a captar o sentido dos conceitos, convive (ou é substituído) com novos recursos da era digital que sugerem soluções cada vez mais objetivas. Hoje, o processo de escrita relaciona-se mais à ideia de ordenação de uma série de referências a outros textos, do que propriamente a análise dos fatos e a aplicação do direito. A interpretação converte-se em infindável repetição de sentidos já conhecidos, ignorado por completo o desafio de encontrar um *intermezzo* entre recitação e invenção...[77]

Por tudo isso, intolerável que a tecnologia sirva como muleta na elaboração de sentenças, peças processuais e pareceres, ou que permita a convergência em torno de soluções mecânicas ou padronizadas. O uso dos aparelhos eletrônicos e o acúmulo de informações na *internet* são instrumentos valiosos, desde que seu emprego esteja dirigido por acurada reflexão do jurista.

Imprescindível neste cenário, o rigor por parte dos órgãos estatais. As metas institucionais não podem se restringir à produtividade dos órgãos e serviços jurisdicionais, mas principalmente, devem visar a qualidade destas decisões. Ainda que se observe um crescente número de demandas a cargo do Judiciário, este argumento não serve para que se descure da justiça das decisões. Os esforços devem estar envidados em

[77] A redação do texto jurídico converte-se em *ready-made*, ou seja, limita-se a reproduzir uma série de textos pré-existentes. A somatória de citações ignora as técnicas interpretativas e constitui o abandono da busca racional pelo sentido; a apropriação descompromissada e acrítica de algo que já está feito repercute negativamente para o aperfeiçoamento das decisões judiciais.

ambos os sentidos: justiça em prazo razoável e motivação judicial compatível com o corolário democrático do *due process of law*.[78]

1.4.3.3. Liberdade como autonomia recíproca de acesso à informação

A análise dos efeitos do uso da *internet* para a esfera das liberdades do cidadão permite constatar criticamente o desenvolvimento dos direitos civis no contexto das novas tecnologias. As redes telemáticas despertam a impressão de que as fronteiras se diluíram e a possibilidade de comunicar-se com as pessoas de todas as partes do mundo, sem sair do domicílio, já é parte da vida no século XXI.

Compreender a liberdade como atributo individual carece da operacionalidade esperada para solucionar as questões jurídicas. Os modelos tradicionais oferecem o risco de desconsiderar a vida social em rede proporcionada pelo entorno digital, com a transformação da subjetividade em inter-subjetividade, pois *"há ao mesmo tempo você e o outro, no espaço virtual."*[79]

No mundo virtual a liberdade separada por espaços não mais proporciona respostas. Os processos comunicativos funcionam em liberdade generalizada de um número grandioso de pessoas. O fluxo constante de informações de todos para todos descaracteriza a noção de autonomia e coloca luz sobre o caráter da *liberdade como reciprocidade* – a informação colocada na rede é simultaneamente oferecida a todos.[80]

---

[78] Sob o pretexto de solucionar a morosidade da Justiça não se pode tolerar o afrouxamento das exigências legais de motivação suficiente e idônea. O exame da qualidade da atuação jurisdicional deve se iniciar justamente por aquelas medidas que mais sensivelmente afetam os direitos individuais, como são exemplos, os decretos de prisões provisórias e as autorizações para o uso de meios invasivos de obtenção de prova (*v.g.*, as interceptações telefônicas e as buscas e apreensões). A publicidade das decisões e a participação pública nesta discussão são essenciais para a superação de eventuais posturas corporativistas dos órgãos jurisdicionais, algumas vezes demasiados complacentes com atecnicismos, e pouco atentos ao mérito profissional, que deveria prevalecer sobre o favoritismo pessoal ao longo da carreira. As atenções devem estar voltadas a identificar todas as formas de plágio e o uso de modelos processuais em escala de repetição.

[79] T. S. FERRAZ JUNIOR, *A invenção do futuro: um debate sobre a pós-modernidade e a hipermodernidade,* in T. S. FERRAZ JUNIOR (org.), *A invenção do futuro*, São Paulo, Manole, 2005. p. 33.

[80] T. S. FERRAZ JUNIOR, *Liberdade de Informação e Privacidade ou o Paradoxo da Liberdade*, in A. de Almeida Filho (org.), *Estado de Direito e Direitos Fundamentais*, Rio de Janeiro, Forense, 2005, p. 662.

O primado Iluminista, segundo o qual a liberdade de um começa onde termina a liberdade do outro, é sucedido pelo contexto de vida em comunicação livre com o outro. Em síntese, *"a dignidade humana deve estar centrada no viver em livre comunicação com o outro. Na verdade, hoje, o que deveria ser dito é que a liberdade de um começa onde começa a liberdade do outro."*[81]

1.5. Comunicações eletrônicas

A definição de telecomunicações, apresentada pela lei nº 9.472/97 como *"a transmissão, emissão ou recepção, por fio, radioeletricidade, meios ópticos ou qualquer outro processo eletromagnético, de símbolos, caracteres, sinais, escritos, imagens, sons ou informações de qualquer natureza"*, evidencia três aspectos técnicos principais: as infraestruturas, os meios de transmissão (o modo como a informação é propagada por meio das infraestruturas) e o objeto de transmissão (o sinal).[82]

A lei nº 9.472/97 não dispõe especificamente sobre a noção de comunicação eletrônica. Ainda que uma interpretação dilatada de telecomunicações permita abranger o meio digital, os principais meios comunicativos da *internet* – *comunicação instantânea* e *navegação* – não têm suporte normativo.

O conceito de comunicações eletrônicas decorre das hodiernas inovações no âmbito das telecomunicações. A terminologia passa a ser empregada, com vanguarda, nas Diretivas comunitárias do Parlamento Europeu.

A Diretiva 2002/21/CE (Conselho da Europa) de 7 de março de 2002, institui um marco regulador comum para as redes e os serviços de comunicação eletrônica. O art. 1.1 dispõe: *"um marco harmonizado para a regulação dos serviços de*

[81] T. S. FERRAZ JUNIOR, *A Liberdade como autonomia recíproca de acesso à informação*, in M. A. Greco e I. G. da Silva Martins (coords.), *Direito e internet: relações jurídicas na sociedade informatizada*, São Paulo, RT, 2001, p. 245.
[82] Aspectos ressaltados também por J. J. GONZÁLEZ LÓPEZ, *Utilización en el proceso…*, *op. cit*., p. 360.

comunicações eletrônicas, para as redes de comunicações eletrônicas e para os recursos e serviços associados".

A combinação dos três conceitos apresentados compõe o que modernamente pode ser compreendido como comunicação eletrônica. Em síntese, as redes de comunicação eletrônica referem-se à *infraestrutura da comunicação*; aos *serviços de comunicação eletrônicas* [83], voltados à transmissão da informação por meio das infraestruturas de comunicação; e aos *recursos associados,* noveis ferramentas associadas ao fenômeno tele-comunicativo.[84]

Os instrumentos técnicos a serviço das comunicações eletrônicas, porém, apresentam um quadro mais amplo de abrangência: satélites, redes terrestres fixas e móveis, redes para a difusão sonora e televisiva e redes de televisão a cabo.[85]

A maior amplitude do conceito em relação às telecomunicações fortalece-se, ademais, com fulcro na ideia de convergência das comunicações. A digitalização, que permite converter textos, sons e imagens em números e transmiti-los conjuntamente, associada ao contexto das avançadas infraestruturas e meios de comunicação, potencializa a transmissão da informação.

---

[83] Os serviços na *internet*, em grande parte funcionam com base no modelo cliente-servidor. Os computadores dos usuários representam os clientes que, por meio de um programa de navegação, enviam pedidos de autorização a outros computadores (servidores), para que estes enviem as informações que constituem uma determinada página *web*.

[84] Segundo o art. 2º da Diretiva, *"para efeitos da presente diretiva, entende-se por: a) Rede de comunicações eletrônicas, os sistemas de transmissão e, se for o caso, os equipamentos de comutação ou encaminhamento e os demais recursos que permitem o envio de sinais por cabo, feixes hertzianos, meios ópticos, ou por outros meios eletromagnéticos, incluindo as redes de satélites, as redes terrestres fixas (com comutação de circuitos ou de pacotes, incluindo a internet) e móveis, os sistemas de cabos de eletricidade, na medida em que são utilizados para a transmissão de sinais, as redes utilizadas para a radiodifusão sonora e televisiva e as redes de televisão por cabo, independentemente do tipo de informação transmitida; (...) c) Serviço de comunicações eletrônicas, o serviço oferecido em geral mediante remuneração, que consiste total ou principalmente no envio de sinais através de redes de comunicações eletrônicas, incluindo os serviços de telecomunicações e os serviços de transmissão em redes utilizadas para a radiodifusão, excluindo os serviços que prestem ou exerçam controle editorial sobre conteúdos transmitidos através de redes e serviços de comunicações eletrônicas; excluem-se igualmente os serviços da sociedade da informação, tal como definidos no artigo 1º da Diretiva 98/34/CE que não consistam total ou principalmente no envio de sinais através de redes de comunicações eletrônicas; (...) e) Recursos conexos, os recursos associados a uma rede de comunicações eletrônicas e/ou a um serviço de comunicações eletrônicas que permitem e/ou suportam a prestação de serviços através dessa rede e/ou serviço. Incluem sistemas de acesso condicional e guias eletrônicos de programas"* (Diretiva 2002/21/CE do Parlamento Europeu e do Conselho de 7 de Março de 2002).

[85] J. J. GONZÁLEZ LÓPEZ, *Utilización en el proceso …*, *op. cit.,* p. 361.

A convergência tecnológica representa uma consequência da codificação digital; a modificação do material objeto de transmissão para a linguagem numérica, isto é, uma sequência de códigos, permite o tratamento conjunto. Traduz-se em processo de aproximação, mescla e integração dos setores de audiovisual, Informática e de telecomunicações, que permitiu a aparição de novos elementos e serviços de transmissão eletrônica.[86] [87]

A respeito das modalidades de comunicação instantânea, de início cumpre mencionar o correio eletrônico *(eletronic mail)*. Este serviço de comunicação permite que sejam enviadas mensagens escritas para outras pessoas que tenham acesso à *internet*, em qualquer localidade do mundo. Para enviar a mensagem é necessário conhecer o endereço do receptor; uma vez remetido, o conteúdo permanece armazenado no servidor à disposição do destinatário.

Em síntese, algumas características que o tornaram popular e amplamente difundido: ausência de papel; velocidade de transmissão (chega ao destino quase imediatamente); possibilidade de enviar arquivos multimídia e textos extensos; baixo custo de transmissão; opção de trabalhar diretamente sobre o texto recebido, sem necessidade de transcrevê-lo, e ausência de fronteiras físicas ou ideológicas.[88]

As comunicações em tempo real caracterizam-se pelo caráter simultâneo, a distância e multidirecional.[89] Todos os usuários de *internet* têm acesso ao conteúdo, a menos que se adote o sistema de conversação bidirecional e fechado entre os usuários próprio das modalidades IRC (*Internet Relay Chat*), ICQ e MSN.[90]

---

[86] BALLESTEROS MOFFA, *La Privacidad Eletrónica ...*, *op. cit*., p. 117.

[87] O livro verde sobre convergência dos setores de telecomunicação e tecnologias da informação, da Comissão das Comunidades Europeias, define a convergência como *"a capacidade de diferentes plataformas de rede de transportar tipos de serviços essencialmente similares, ou a aproximação de dispositivos de consumo tais como o telefone, a televisão e o computador pessoal"* (trad. nossa).

[88] Sobre a natureza jurídica do correio eletrônico como verdadeiro correio, portanto similar ao meio postal: R. D. UICICH, *El derecho a la intimidad en internet y en las comunicaciones electrónicas*, Buenos Aires, Adhoc, 2009, pp. 48-49. Em orientação oposta, como comunicação tipicamente informática, *v.* J. L. RODRÍGUEZ LAINZ, *Intervención judicial en los datos de tráfico de las comunicaciones*, Barcelona, Bosch, 2003, p. 62. O conceito será analisado no próximo capítulo (item 2.6).

[89] As redes sociais, dente as quais destacam-se no Brasil o *Facebook,* o *Orkut, o LinkedIn e o MySpace*, são comunidades virtuais criadas para que os usuários relacionem-se com outras pessoas. Organizam-se a partir da criação de perfis pessoais onde são disponibilizadas informações do usuário.

[90] O *Internet Relay Chat (IRC)* é um serviço desenvolvido na década de 80 que permite a conversação simultânea, por meio da digitação de textos, entre vários internautas. Tem caráter de troca de mensagens

O chamado sistema de *voz sobre IP (Voip)* consiste na transmissão de voz por meio da *internet*, sendo o seu maior vetor atual o *Skype.*[91]

O *File Transfer Protocol* (FTP)[92] possibilita enviar arquivos de dados por meio da *internet*, de qualquer magnitude ou formato. O uso de uma aplicação FTP permite que o usuário conecte-se a outro computador remoto para procurar em uma lista de arquivos disponíveis para esse serviço e transferir os arquivos para o seu computador (*download*).

A outra modalidade de comunicação na *internet* é a navegação[93], viabilizada través do acesso de páginas virtuais interligadas por *hyperlinks*[94], que permitem localizar variados conteúdos. A visualização de páginas *da World Wide Web*[95] foi criada em meados da década de 1980, e possibilitam a difusão de conteúdos e o intercâmbio de informações de forma ágil e descomplicada. Por meio dos *sites* é possível publicar ou acessar documentos de texto, imagens e vídeos; estas ferramentas popularizaram-se de tal maneira que o senso comum frequentemente confunde a *internet* com a própria *WWW*.

A navegação tem particulares características enquanto comunicação eletrônica. Para assim enquadrá-la, necessário entender que sua função transborda os lindes de uma ferramenta interativa de comunicação, na qual os papéis tradicionais de emissor e

---

instantâneas, no qual os usuários optam pelo canal em que desejam conversar (normalmente organizados em torno de assuntos específicos). O *Windows Live* (programa que substituiu o antigo MSN *Messenger)*, o *Google Talk*, o *Aol Instant Messenger, o Yahoo Instant Messenger* e o *ICQ*, são algumas das principais ferramentas de comunicação instantânea. Estes serviços exigem a instalação de aplicações clientes que promovem o acesso aos respectivos servidores, onde uma lista de contatos permanece associada à conta do usuário. Insta notar que a popularidade dos programas de comunicação instantânea declinou nos últimos anos, pois aplicações interativas e mais funcionais têm sido sistematicamente ofertadas pelas grandes redes sociais.

[91] O *VoIP (Voice over IP)* é a comunicação de conversação de voz que utiliza como meio de comunicação redes com endereçamento IP (protocolo *TCP/IP*). É possível por intermédio do *VoIP* realizar a comunicação diretamente com outro computador, assim como a chamada telefonia IP, ou seja, realizar ligações telefônicas com a rede pública de telefonia (fixa ou celular). O serviço apresenta-se vantajoso à medida que é possível trafegar voz e dados em uma única infra-estrutura. O programa mais utilizado para esta modalidade de comunicação é o *Skype* (M. MARÇULA, P. A. BENINI FILHO, *Informática ..., op. cit.* p. 346).

[92] O *Protocolo de transferência de arquivos* é um serviço oferecido na *internet* que permite que os usuários localizem e movam arquivos de um lugar para outro da rede. Os programas que realizam as transferências movem os arquivos entre o computador local e outro remoto.

[93] O navegador *(web browser)* é a ferramenta virtual para solicitar o acesso das páginas *web*.

[94] Os *hyperlinks* permitem que o internauta acesse sucessivos documentos disponíveis na *web*, através de simples movimentos e "cliques" de *mouse* sobre a área atrelada ao *hyperlink* na tela, em geral uma palavra ou figura.

[95] A *WWW* é um sistema de servidores *internet* que utiliza como protocolo principal o *HyperText Transfer Protocol* (HTTP). Por meio desta rede virtual é possível acessar os serviços disponíveis na *internet*, valendo-se de palavras-chave e ícones específicos.

receptor da comunicação se situam em contexto onde cada um atua sucessivamente como emissor e receptor. O internauta ao ingressar na página *web* solicita uma informação e participa ativamente da busca, do acesso e da seleção do conteúdo de interesse.

CAPÍTULO II – DIREITO À INTIMIDADE E SIGILO DAS COMUNICAÇÕES NA PERSECUÇÃO PENAL

2.1. Evolução da proteção à intimidade

A análise das Constituições pátrias anteriores fortalece a compreensão do objeto de tutela do direito consagrado no art. 5º, incisos X e XII, evidenciando um caminho de avanços e retrocessos no percurso de consolidação dos direitos e garantias fundamentais no Brasil.

Ainda que a expressa previsão de um direito à intimidade tenha sido introduzida apenas pela Lei Maior de 1988, a tutela de certos aspectos da vida privada está presente tanto nas Constituições anteriores como nos documentos internacionais de direitos. O aperfeiçoamento do tratamento constitucional dos direitos à inviolabilidade do domicílio e das comunicações constituem capítulos históricos de conquista de um espaço amplo de proteção da esfera íntima do cidadão.

A especial atenção do legislador constituinte para a preservação da intimidade há que ser contextualizada no seio da elaboração de uma Constituição democrática e cidadã. Ao lado do estudo desta liberdade pública, igualmente relevante o escorço de noções correlatas utilizadas pela doutrina estrangeira (*privacy* e *riservatezza*), assim como da reflexão sobre a localização deste direito fundamental no plano internacional.

A partir destas conceituações, proceder-se-á a análise do direito à proteção de dados, da teoria das três esferas e das disposições constitucionais de regência do sigilo das comunicações.

2.1.1. Análise constitucional: inviolabilidade das comunicações, inviolabilidade do domicílio e intimidade

A Carta imperial (1824), no art. 179, inciso XXVII, previa a inviolabilidade do segredo das cartas[96], incumbindo à administração do correio a responsabilidade por qualquer violação desta proteção.

O mesmo art. 179, em seu § 7º, tutelava a casa como asilo inviolável, diferenciando a entrada noturna da diurna: *"Todo cidadão tem em sua casa um asilo inviolável. De noite não se poderá entrar nela senão por seu consentimento, ou para defender de incêndio ou inundação; e de dia só será franqueada a sua entrada nos casos e pela maneira que a lei determinar"*.

A Constituição de 1891 (art. 72, § 18) consagrou a inviolabilidade do sigilo da correspondência. Para EDUARDO ESPÍNOLA o constituinte de 1891 declara *"a inviolabilidade do segredo da correspondência abrangendo a epistolar, postal, ou não, e a telegráfica"*.[97] Para a doutrina, a liberdade de pensamento era o valor que informava esta garantia.[98]

O art. 72, § 11, da Constituição republicana dispôs: *"A casa é o asilo inviolável do indivíduo; ninguém pode aí penetrar de noite sem o consentimento do morador, senão para acudir as vítimas de crime ou desastres, nem de dia, senão nos casos e pela forma prescritos na lei"*. Inegável a inspiração do legislador pátrio no direito inglês;

---

[96] Como observou CARLOS MAXIMILIANO, o art. 11 da Declaração de Direitos do Homem de 1789 assegurou o sigilo da correspondência, repúdio frontal às habituais práticas dos Estados absolutistas e de seus "gabinetes negros", oficinas secretas em que funcionários reais violavam o segredo das correspondências. A Declaração de Direitos, contudo, *"não impediu a abertura solene das cartas suspeitas pelas comissões revolucionárias durante a ditadura jacobina"* (C. MAXIMILIANO, *Comentários à Constituição Brasileira*, v. III, Rio de janeiro, Freitas Bastos, 1948, pp. 72-73).

[97] *Constituição dos Estados Unidos do Brasil*, v. II, Rio de Janeiro, Freitas Bastos, 1952, p. 555. Conforme JOÃO BARBALHO, à época foi proposta emenda, nos termos da Constituição suíça, para o acréscimo das expressões postal e telegráfica. A ideia foi rechaçada, porém, para que não ficassem impunes os casos de violação por particulares (*Constituição Federal Brasileira: Commentarios*, Rio de Janeiro, F. Briguet e cia. editores, 1924, p. 439).

[98] A. A. MILTON, *A Constituição do Brazil: notícia, história e texto comentado*, 2ª ed., Rio de Janeiro, Imprensa Nacional, 1898, p. 406.

a expressão *"my home is my castle"* constitui dogma em matéria de liberdades públicas no Reino Unido.[99]

A diferenciação do momento da entrada (de dia e de noite) permaneceu na Constituição seguinte. Ao contrário de Estados estrangeiros, que optaram em conceber uma garantia em branco, a fórmula brasileira seguiu a tradição liberal.[100]

Neste momento a noção de casa já englobava acepção ampla, típica do Direito público, diversa do conceito restritivo de domicílio do Direito privado. Se para a doutrina civilista se considerava domicílio a residência com ânimo definitivo (CC/16, art. 31)[101], no Direito constitucional a casa designa todos os locais de retiro da pessoa (mansão, aposento alugado, escritório, oficina, pátios, jardins, granjas, estrebarias ...), desde que não se trate de local aberto ao público.[102]

Em 1934, a nova Carta de Direitos preservou a disciplina da inviolabilidade do domicílio, exceção feita apenas para a prática criminosa e para os casos de desastres. Outrossim, a inviolabilidade do sigilo de correspondência também seguia a orientação da Constituição anterior.

A Carta constitucional de 1937, outorgada em 10 de novembro do mesmo ano pelo então Presidente Getúlio Vargas, disciplinou a inviolabilidade de correspondência associada à inviolabilidade do domicílio (art. 122, § 6º), ressalvadas "as exceções expressas em lei". A previsão mitigou a liberdade de correspondência, antes de eficácia plena e irrestrita, ao *status* de norma de eficácia limitada e restringível[103] – a opção por uma redação vaga redundou em nítida ameaça aos direitos individuais.[104]

---

[99] J. BARBALHO, *Constituição Federal ...*, *op. cit*., p. 428.
[100] F. C. PONTES DE MIRANDA, *Comentários à Constituição de 1967*, tomo V, São Paulo, RT, 1968, pp. 164-165.
[101] O art. 70 do Código Civil de 2002 manteve a mesma redação do art. 30 do código anterior: *"O domicílio da pessoa natural é o lugar onde ela estabelece a sua residência com ânimo definitivo"*.
[102] C. MAXIMILIANO, *Commentarios: Constituição Brasileira*, Rio de Janeiro, Jacinto Ribeiro dos Santos editor, 1918, p. 705. Sobre os locais públicos e o conceito de casa, atualmente é pacífico o entendimento de que o quarto de hotel habitado está protegido pela inviolabilidade do domicílio.
[103] PINTO FERREIRA, *Comentários à Constituição brasileira*, v. I, São Paulo, Saraiva, 1989, p. 85.
[104] Outro exemplo de uso de conceitos indeterminados na Carta de 1937 pode ser observado no art. 122: *"A Constituição assegura aos brasileiros e estrangeiros residentes no país o direito à liberdade, à segurança individual e à propriedade, nos termos seguintes: (...) 15. Todo cidadão tem o direito de manifestar o seu pensamento, oralmente, ou por escrito, impresso ou por imagens, mediante as condições e nos limites prescritos em lei"*.

O direito à inviolabilidade do domicílio, a exemplo da opção de outras nações europeias, passou a permitir restrição da legislação infraconstitucional. O retrocesso tem manifesta influência das ditaduras então existentes e apenas com o advento da Constituição de 1946 o equívoco seria corrigido.

A Constituição de 1946 (art. 141, § 6º) preservou a inviolabilidade do sigilo da correspondência.[105] No que toca ao domicílio a previsão é quase idêntica à Constituição de 1934: *"A casa é o asilo inviolável do indivíduo. Ninguém poderá nela penetrar à noite, sem consentimento do morador, a não ser para acudir as vítimas de crime ou desastre, nem durante o dia, fora dos casos e pela forma que a lei estabelecer"*.

Nos *comentários à Constituição de 1946*, PONTES DE MIRANDA sustenta a natureza da inviolabilidade da correspondência como uma liberdade de negação, *"liberdade de não emitir pensamento"*:

> "Assim como aos indivíduos se reconheceu a liberdade ativa de emissão do pensamento, reconheceu-se-lhe a liberdade negativa: pensar, porém não emitir; saber, porém não dizer. Quem sabe e não quer dizer é livre, como quem ignorasse".[106]

Segundo o jurista, o princípio da inviolabilidade das comunicações na Constituição de 1946 dirigia-se tanto contra abusos do Poder Público, como também contra a legislação. Neste momento, as garantias e direitos assumem maior extensão e consistência. Se em 1937 o legislador originário interrompeu a linha de evolução técnica constitucional, retomou-a na Constituição de 1946.[107]

Em 1967, a preservação do domicílio pela Constituição ganhou redação lacônica, ao limitar-se a prever sua inviolabilidade. Acrescentou-se ao sigilo de correspondência a referência às comunicações telegráficas e telefônicas, ausente qualquer

---

[105] A Carta de Direitos de 1946 fazia alusão à competência da União de *"explorar, diretamente ou mediante autorização ou concessão, os serviços de telégrafos, de radiocomunicação, de radiodifusão, de telefones interestaduais e internacionais"* (art. 5º, inc. XII).

[106] *Comentários à Constituição de 1946*, tomo IV, Rio de Janeiro, Borsoi, 1960, p. 437. O autor reitera o conceito na obra *Comentários à Constituição de 1967 ..., op. cit*. JOSÉ CRETELLA JUNIOR critica a posição de PONTES DE MIRANDA, preferindo a noção de liberdade positiva, por se tratar de uma: *"liberdade de emissão do pensamento, embora para um só, mas respeitada pelo Estado, quando protege esse tipo especial de emissão, mediante dispositivos de lei ou dispositivos constitucionais"* (*Comentários à Constituição de 1988*, v. I, Rio de Janeiro, Forense, 1997, p. 268).

[107] *Comentários à Constituição de 1967 ..., op. cit*., p. 162.

ressalva à inviolabilidade destas modalidades de comunicação (art. 150, § 9º). A Emenda constitucional 1/1969 reafirmou a disciplina que já era prevista (art. 153, §§ 9º e 10º).

Por sua vez, o legislador constituinte de 1988, antes da inviolabilidade da casa e das comunicações, tratou dos direitos fundamentais à intimidade e vida privada, resguardando-os em distintos graus, *"... invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito à indenização pelo dano material ou moral decorrente de sua violação"* (CF, art. 5º, inciso X).

Ao declará-los invioláveis, alçados estes valores à condição de direitos individuais, o legislador optou por diferenciar dois aspectos da vida: um voltado para o exterior (vida privada) e outro para o interior (intimidade). E no que diz respeito à honra e à imagem das pessoas enfatizou seu caráter como direito autônomo da personalidade.[108]

O mandamento inscrito no art. 5°, inciso XI, tutela a inviolabilidade do domicílio, vedado o ingresso sem consentimento do morador, salvo nas hipóteses de flagrante delito ou desastre, para prestar socorro, ou, durante o dia, por determinação judicial. Cuida-se do reconhecimento de direito fundamental cujo objeto de tutela diz respeito não à propriedade, mas ao respeito à esfera íntima e privativa.

ADA PELLEGRINI GRINOVER diferencia a liberdade de domicílio da liberdade de correspondência e das comunicações em vários aspetos: (i) diversidade de sujeito ativo do direito (enquanto o titular do domicílio é apenas um, a liberdade de comunicações estende-se ao remetente e ao destinatário); (ii) o domicílio é projeção espacial da pessoa, a correspondência projeção espiritual; (iii) a violação da liberdade de domicílio realiza-se por meio da invasão, a violação da liberdade de correspondência se efetiva pela suspensão, sustação ou interferência no seu curso.[109]

A segurança das comunicações, tutelada no art. 5°, inciso XII, tem objeto de tutela dúplice *"de um lado, a liberdade de manifestação do pensamento; de*

---

[108] J. A. DA SILVA, *Comentário contextual à Constituição*, 4ª ed., São Paulo, Malheiros, 2007, pp. 100-102. Até a promulgação da Carta de Direitos de 1988 não havia proteção expressa do direito à imagem, relegada a proteção deste direito à construção doutrinária e jurisprudencial (C. RIBEIRO BASTOS, *Comentários à Constituição do Brasil*, v. 2, São Paulo, Saraiva, 1989, pp. 62-63).

[109] *Liberdades públicas e Processo Penal: as interceptações telefônicas,* 2ª ed., São Paulo, RT, p. 192.

outro lado, o segredo, como expressão da intimidade".[110] As informações transmitidas devem permanecer completamente reservadas ao emissor e ao destinatário.

Em apertada síntese, a tradição constitucionalista pátria consagra a inviolabilidade de domicílio como a liberdade da pessoa, isoladamente considerada, de resguardo, recato e exercício de uma projeção espacial íntima. Por outro lado, a liberdade de comunicação diz respeito ao exercício das faculdades do próprio espírito, a autonomia e independência do pensamento perante terceiros.

2.1.2. Das noções de *privacy*[111], intimidade e *riservatezza* ao direito à proteção de dados

O curso da História evidencia que as noções de íntimo e de privado se desenvolveram a partir daquilo que antes era público. Cruciais para a demarcação destas noções, o advento do liberalismo e a cultura humanística do século das luzes: à medida que a ânsia de expansão do poder político se confronta com os ideais liberais, passa a pensar-se na realização humana como referencial.[112]

O contexto histórico que permeia a temática do reconhecimento do *right of privacy* data do final do século XIX, ocasião que o memorável estudo dos ingleses WARREN e BRANDEIS[113] já fazia referência ao direito de estar só (*"right to be let alone"*). As raízes do reconhecimento deste direito de isolamento físico encontram-se diretamente relacionadas à *Common Law*. A origem do *right of privacy* como um sentimento de

[110] Idem, p. 190.
[111] Do termo *privacy* advém a expressão *privacidade,* como ensina PAULO JOSÉ DA COSTA JUNIOR *"a expressão exata, em bom vernáculo, é privatividade, que vem de privativo. E não privacidade, que é péssimo português e bom anglicismo* (*vem de privacy*)*"* (*O direito de estar só: a tutela penal do direito à intimidade*, 3ª ed., São Paulo, Siciliano, 2004, p. 21).
[112] A. GARRIGA DOMÍNGUEZ, *Tratamiento de datos personales y derechos fundamentales*, Madrid, Dykinson, 2004, p. 18.
[113] L. BRANDEIS, S. D. WARREN, *The right to privacy*, Harvard Law Review, v. 4, n. 5, Boston, dez., 1890.

tradição jurídica anglo-saxã é parte do processo que posteriormente o reconheceu nas modernas Cartas de Direitos internacionais como valor constitutivo da pessoa humana.[114]

À época, os autores preocuparam-se em repudiar as frequentes intromissões da imprensa na vida privada. A tradição dos precedentes da *Common Law*, aos poucos, consolidava o direito de rechaçar toda invasão não consentida – *privacy*, como típico direito de não intromissão.

O direito de exclusão de qualquer ingerência estranha na vida privada tem evidente conteúdo negativo e consente a cada um o adequado isolamento moral para atingir a *peace of mind*. A noção anglo-saxônica de *privacy* cada vez mais é associada ao controle das informações, autêntica manifestação do exercício da autonomia pessoal sobre as áreas de retiro da pessoa.

Na Europa continental, por sua vez, o exame do direito à intimidade é comumente realizado à luz da doutrina dos direitos da personalidade, típica formulação do Direito Civil.[115] Sob este viés, a intimidade ocupa lugar no rol dos direitos essenciais, invioláveis e em contínuo movimento. Tem como alicerce a própria essência humana, portanto, adaptável às novas circunstâncias sociais e necessidades.[116]

Hodiernamente, impõe constatar o caráter multidimensional deste direito. A partir da conceituação como direito de conteúdo eminentemente negativo, cada vez mais se pensa a *privacy* não apenas como faceta do *direito de estar só*, mas também,

---

[114] Aprofundando-se na conjugação da tradição jurídica anglo-saxã e da filosofia fenomenológica (F. MORALES PRATS, *La tutela penal ..., op. cit.*). O autor destaca que a noção de *privacy,* em meados do século XIX, deixa de ser vista como um privilégio para representar um valor de toda comunidade: *"el derecho que todo individuo tiene a ser resguardado de intrusiones"*. A expressão, paradoxalmente, não é elaborada no Reino Unido – onde a industrialização e os ideais burgueses primeiro se consolidaram –, mas sim nos EUA, na obra de WARREN e BRANDEIS (*Idem,* p. 20).

[115] No Direito italiano, o *diritto a la riservatezza* tem notáveis semelhanças com a *privacy* e refere-se ao modo de ser da pessoa que exclui do conhecimento de outros os fatos relativos ao desenvolvimento da vida. A tradição do reconhecimento da *riservatezza* enquanto direito da personalidade é muito presente na Itália; assevera A. SCALISI que a sentença proferida pela Suprema Corte de Cassação, em 27 de maio de 1975, pela primeira vez reconhece a *riservatezza* como um aspecto do direito unitário da personalidade, previsto no artigo 2º, da Constituição (*Il diritto ala riservatezza*, Milano, Giuffrè, 2002, p. 388). Outras expressões empregadas no Direito italiano *(diritto ala vita privata* e *diritto ala segretezza)* não exprimem com tanta exatidão a noção de *privacy*.

[116] Como assevera HERRÁN ORTIZ, os direitos da personalidade preservam os bens que garantem a faculdade de cada qual desfrutar de suas próprias faculdades físicas, morais e intelectuais, sem as quais o ser humano estaria desprovido das principais garantias para assegurar o pleno desenvolvimento da pessoa (*La violación de la intimidad en la protección de datos personales*, Madrid, Dykinson, 1998, p. 34).

sob o aspecto positivo do controle direto de informações e da capacidade de comunicá-las e mantê-las para si mesmo.

Podemos falar, portanto, de uma aspiração a não circulação de informações pessoais; pretensão que consiste no interesse de afastar do domínio público fatos desabonadores, e filtrar a realidade por meio da revelação seletiva de fatos que concernem ao próprio indivíduo.

Costuma-se elencar uma série de princípios relevantes em matéria de proteção de dados.

Em primeiro lugar, o consentimento deve ser livre e inequívoco. É necessário definir claramente as informações que se pretende obter e manter, bem como, muito concretamente, o que será utilizado (*v.g.* o uso de *opt-out* na *internet*),[117] vedadas as fórmulas abertas de consentimento que descaracterizem o objeto.

O consentimento deve existir para o registro, recepção e posterior cessão dos dados a terceiros.[118] Ademais, informações sensíveis (*v. g.,* origem racial ou étnica, crenças religiosas e opiniões políticas, dentre outras) não podem ser tratadas, salvo em hipóteses excepcionais e com a devida fundamentação legal.

A obrigação de apenas usar dados pessoais para *finalidade* específica e legal constitui princípio, segundo o qual, o momento de coleta dos dados deve estar voltado aos fins para os quais são armazenados, vedada a utilização para qualquer outro

---

[117] Acerca da diferenciação entre *opt-in* e *opt-out*, CATARINA SARMENTO E CASTRO esclarece: *"Na solução de opt-in deve entender-se que o receptor das mensagens deve, antes mesmo da sua remessa, dar o seu consentimento ao remetente para envio da mensagem, optando por constar da mailing list deste, ao contrário da solução opt-out, segundo a qual o receptor, depois de recebida a mensagem, poderá então pedir ao remetente para não constar na mailing list respectiva, solicitando a remoção dela."* (*Privacidade e proteção de dados em rede*, in V Curso de Verão sobre Sociedade da Informação, Faculdade de Direito de Lisboa e Associação Portuguesa de Direito Intelectual, 2006, p. 104).

[118] Excepcionalmente o consentimento pode ser dispensado, como ocorre no caso de armazenamento temporário de dados para assegurar a própria realização da comunicação ou para sua faturação, desde que se operem de maneira leal e transparente, conforme previsão legal. A única maneira de gerir o custo econômico dos serviços realizados por empresas provedoras de serviços de telecomunicação e comunicações eletrônicas é mediante o armazenamento dos dados de tráfego úteis para avaliar economicamente as prestações realizadas. A gestão dos dados de tráfego (origem, destino, duração de uma comunicação) possibilita o cômputo dos custos pelo uso de um serviço.

desiderato.[119] Resta proibida a coleta de dados para fins não concretos, ou por qualquer forma fraudulenta, desleal ou ilícita.

Conforme o princípio do *equilíbrio* ou *da justificação social,* os dados pessoais detidos devem ser adequados, pertinentes e não excessivos. A coleta da informação e o armazenamento compatibilizam-se com o razoavelmente necessário para o cumprimento do objetivo.

O princípio da *veracidade* impõe ao responsável por um banco de dados zelar pela exatidão das informações no momento da coleta e mantê-las atualizadas. Os deveres de cancelamento, retificação ou adição conformam a imposição de que os dados sejam conformes à realidade atual.

Outros princípios frequentemente indicados no Direito Comunitário Europeu: lealdade (a informação deve ser exata, completa e atual); temporalidade (o armazenamento há que ser feito por tempo não superior ao estritamente necessário); participação individual e acesso (obrigação de responder pedidos escritos dos titulares para a descrição dos dados armazenados); segurança (proteção contra perdas, destruições ou acessos não autorizados); política de abertura (garantia de transparência da ação da administração pública e privada no processamento de dados), e controle (elaboração de instrumentos de controle voltados à efetividade do sistema de proteção).[120] [121]

2.1.3. Direito internacional

No âmbito internacional, expressa a proteção da *privacy* em inúmeros diplomas: art. 12 da Declaração Universal dos Direitos Humanos (1948)[122], art. 8º da

[119] R. HERRERA BRAVO, A. NUÑEZ ROMERO, *Derecho Informático*, San Martín, La ley, 1999, p. 148.
[120] S. STAINES, *Data Protection Act Guidelines – a Practical Summary*, in United Kingdom Law Articles in English, Pictons Solicitors LLP, May 2004, *http://vlex.com/vid/29346721* (acesso em 30 set. 2010, h. 18:20).
[121] Ao lado do direito-garantia ao *habeas data,* possível elencar os seguintes direitos em matéria de proteção de dados: direito à informação; direito ao consentimento; direito à oposição; direito à proteção especial dos dados sensíveis; direitos de acesso, retificação e cancelamento dos dados; direito ao esquecimento; tutela dos direitos do afetado e direito de indenização; direito à impugnação dos atos ou decisões baseados unicamente no tratamento de dados destinados a valorar a personalidade; direito a conhecer a cessão de dados.
[122] Proclamada pela resolução 217 A (III), da Assembleia Geral das Nações Unidas, em 10 de dezembro de 1948.

Convenção Europeia de direitos do Homem (1950)[123], art. 17 do Pacto Internacional sobre Direitos Civis e Políticos (1966)[124], art. 11, n. 2, do Pacto de São José da Costa Rica (1969)[125] e art. 16 da Convenção sobre os direitos da criança.[126]

Os diplomas internacionais expressam a opção pela terminologia *vida privada* para assegurar o resguardo da *privacy*, tal como na redação do artigo 12 da Declaração de 1948:

> "Ninguém será sujeito a interferências na sua vida privada, na sua família, no seu lar ou na sua correspondência, nem a ataques à sua honra e reputação. Toda pessoa tem direito à proteção da lei contra tais interferências ou ataques."

Sobre o direito à proteção de dados no cenário internacional, a evolução deste tema tem precedentes em diplomas como a Convenção nº 108 do Conselho da Europa para a proteção de pessoas a respeito do tratamento automatizado dos dados de caráter pessoal (1981), a Diretiva 95/46/CE do Parlamento Europeu e do Conselho (1995), relativa a proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados.

Com efeito, o art. 8º da Carta dos Direitos Fundamentais da União Europeia (2007), de 7 de dezembro de 2000, com as adaptações que lhe foram introduzidas em 12 de dezembro de 2007, recepcionado em 2010 pelo Tratado de Lisboa (art. 6º), assentou:

> "Art. 8.
> 1. Toda pessoa tem direito à proteção dos dados de caráter pessoal que lhe diga respeito.
> 2. Estes dados serão tratados de modo leal, para fins concretos e sobre a base do consentimento da pessoa afetada ou com outro fundamento legítimo previsto por lei. Todas as pessoas têm o direito de aceder aos dados coligidos que lhes digam respeito e de obter a respectiva

[123] Adotada em Roma, na data de 4 de Novembro de 1950.
[124] Adotado pela XXI sessão da Assembleia geral da Organização das Nações Unidas (ONU), em 16 de dezembro de 1966; promulgado no Brasil pelo Decreto 592 (art. 17), de 6 de julho de 1966.
[125] A Convenção Americana sobre Direitos Humanos ("Pacto de São José da Costa Rica") foi adotada no âmbito da Organização dos Estados Americanos (OEA), na data de 22 de novembro de 1969, em vigor no plano internacional desde 18 de julho de 1978, e promulgada no Brasil por meio do Decreto 678 (art. 11), de 6 de novembro de 1992.
[126] Adotada pela Assembleia Geral nas Nações Unidas em 20 de Novembro de 1989.

retificação.
3. O cumprimento destas regras fica sujeito a fiscalização por parte de uma autoridade independente."

O referido artigo situa, portanto, o direito à proteção de dados como direito fundamental autônomo ao lado de outros direitos fundamentais. A recomendação geral n. 16 (1998), do Comitê de Direitos Humanos da Organização das Nações Unidas (ONU), assegura que seja regulado por lei a coleta e o armazenamento de informações pessoais em computadores, bancos de dados e outros dispositivos, seja por parte de autoridades públicas, indivíduos ou empresas.[127]

Este regime jurídico de proteção de dados assenta uma série de direitos em âmbito internacional, dentre os quais: (i) o conhecimento das informações armazenadas em bancos de dados; (ii) a verificação da finalidade do armazenamento; (iii) o detalhamento das autoridades públicas ou indivíduos autorizados a controlar os arquivos; (iv) a faculdade de solicitar a retificação ou a eliminação do dado.

Na sequência desta Dissertação, à medida do necessário, se fará referência a julgados do Tribunal Europeu de Direitos Humanos, sobretudo para mencionar alguns posicionamentos de vanguarda da Corte.

2.2. Direito à proteção de dados (ou à autodeterminação informativa) como direito fundamental

A proteção jurídica da intimidade cresceu sensivelmente, em razão da multiplicação dos procedimentos suscetíveis de vulnerá-la. Para tanto, basta mencionar os meios técnicos de captação e transmissão de imagem e som, assim como a acumulação e o

[127] Segundo a recomendação geral nº 16: *"10. Medidas eficazes devem ser tomadas pelo Estado para assegurar que informações a respeito da vida privada de uma pessoa não estejam ao alcance de pessoas que não são autorizadas por lei para receber, processar ou usar tais informações, assim como para que nunca sejam usadas para finalidades incompatíveis com o Pacto"* (trad. nossa).

processamento de informação em geral e de dados pessoais, em particular, por meios tecnológicos.[128]

Com base nas modernas tecnologias, a obtenção de dados que permitam delinear o perfil dos indivíduos evidencia o potencial lesivo do meio informático. Assim, a somatória de determinadas características (desunião familiar, fracasso escolar, estilo de vida, hábitos de consumo) poderia comprometer a participação de uma pessoa em sua vida social, seja para entrevista de emprego, obtenção de crédito ou oportunidade de promoção na carreira.

A faculdade da pessoa humana de determinar e controlar como e em que medida deve haver comunicação de informações suas a terceiros é garantia indispensável para a tutela da liberdade, do direito a não ser discriminado, e da plena realização da personalidade.

No Direito europeu, notável a consagração do direito à autodeterminação informativa.[129] Tal postura desvela a busca por soluções específicas para o tratamento automatizado da informação pessoal. Ou seja, procura-se uma resposta mais eficaz e adequada por meio do reconhecimento de um direito que assegure novas formas de garantias complementares àquelas já previstas no ordenamento jurídico.[130] Não se pretende excluir por completo os dados da vida privada do conhecimento público, mas sim, municiar o indivíduo com os meios necessários para o controle da informação.[131]

---

[128] C. M. ROMEO CASABONA, *La intimidad y los datos de carácter personal como derechos fundamentales y como bienes jurídicos penalmente protegidos*, in Revista de direito da Universidade Estácio de Sá, n. 6, v. 7, Rio de Janeiro, 2004, p. 139.

[129] Como sinônimo, há referência doutrinária ao conceito de *direito de liberdade informática* (F. MORALES PRATS, *La tutela penal..., op. cit.,* p. 45) ou *direito à proteção de dados pessoais* (M. ARENAS RAMIRO, *El derecho fundamental a la protección de datos personales en Europa*, Valencia, Tirant lo Blanch, 2006).

[130] Jamais se olvide o caráter permeável e aberto dos Direitos Humanos à incorporação de novos valores e direitos, bem como a possibilidade de constante reformulação dos direitos fundamentais reconhecidos.

[131] Na vanguarda, a Constituição portuguesa de 1976 dispõe *"1. Todos os cidadãos têm o direito de acesso aos dados informatizados que lhes digam respeito, podendo exigir a sua rectificação e actualização, e o direito de conhecer a finalidade a que se destinam, nos termos da lei. 2. A lei define o conceito de dados pessoais, bem como as condições aplicáveis ao seu tratamento automatizado, conexão, transmissão e utilização, e garante a sua protecção, designadamente através de entidade administrativa independente. 3. A informática não pode ser utilizada para tratamento de dados referentes a convicções filosóficas ou políticas, filiação partidária ou sindical, fé religiosa, vida privada e origem étnica, salvo mediante consentimento expresso do titular, autorização prevista por lei com garantias de não discriminação ou para processamento de dados estatísticos não individualmente identificáveis. 4. É proibido o acesso a dados pessoais de terceiros, salvo em casos excepcionais previstos na lei. 5. É proibida a atribuição de um número nacional único aos cidadãos. 6. A todos é garantido livre acesso às redes informáticas de uso público, definindo a lei*

O direito à autodeterminação informativa tem sua gênese na doutrina e na jurisprudência alemãs, que reconhecem a liberdade individual de estabelecer as condições para o conhecimento de informações referentes à própria pessoa, contidas em arquivos públicos ou privados. Este direito encerra uma dimensão positiva – relacionada ao controle das informações públicas ou privadas referentes a cada indivíduo – e outra negativa, que se traduz na prerrogativa de repelir intromissões alheias na vida privada.

O Tribunal Constitucional alemão, em sentença de 15 de dezembro de 1983, assim reconheceu o direito fundamental à autodeterminação informativa (*Recht auf informationelle Selbstbestimmung*): *"faculdade do indivíduo, derivada da ideia de autodeterminação, de decidir basicamente por si mesmo quando e dentro de quais limites procede revelar situações referentes à própria vida"* (trad. nossa).[132]

O direito do cidadão à tutela e ao tratamento de dados pessoais irradia efeitos tanto na vertente negativa, quanto na positiva. Sob o viés menos abrangente, trata-se de direito de defesa do cidadão diante de eventuais ataques e intromissões; indispensável impedir a estranhos, o acesso e publicização das informações sobre a vida privada e familiar.[133]

A noção de intimidade como simples vedação da intromissão por parte de terceiros, desacompanhada do reconhecimento dos efeitos relacionados à liberdade de atuação para a tutela de outros direitos, é típica das primeiras formulações deste direito. Naquele momento, o exercício do direito fundamental redundava exclusivamente o aspecto negativo reconhecido a seu titular de exigir a não ingerência na vida íntima e privada.[134]

---

o regime aplicável aos fluxos de dados transfronteiras e as formas adequadas de protecção de dados pessoais e de outros cuja salvaguarda se justifique por razões de interesse nacional. 7. Os dados pessoais constantes de ficheiros manuais gozam de protecção idêntica à prevista nos números anteriores, nos termos da lei".

[132] Não é imune a discordâncias a defesa da autodeterminação informativa como direito fundamental. A. I. HERRÁN ORTIZ ressalta o argumento de que este direito remete a outros já formulados; portanto, estéril o esforço de configuração de um novo direito fundamental que nada acrescente à defesa dos direitos fundamentais (*La violación ...*, *op. cit.,* p. 116).

[133] S. COSTA, *A Proteção de Dados Pessoais na Internet,* in Revista Jurídica, n. 6, Universidade Eduardo Mondlane, set., 2004, p. 287.

[134] C. M. ROMEO CASABONA, *La intimidad y los datos ...*, *op. cit*., p. 141.

Por outro giro, o exercício de controle dos dados pessoais representa um direito fundamental positivo. Nas palavras de WINFRIED HASSEMER, cuida-se de autêntico *direito de participação*.[135]

O titular das informações tem o poder de conhecer o conteúdo dos registros informáticos de dados pessoais, além das respectivas condições, finalidades e identidade dos responsáveis. Igualmente, há que ser preservada a faculdade de retificá-los e atualizá-los.

O atual desafio de estabelecer o regime jurídico pátrio de proteção de dados, não se restringe à defesa contra o aparelhamento estatal voltado ao processamento da informação. Nesse sentido, cumpre atentar ao tratamento de dados por parte das grandes empresas da iniciativa privada, em razão da intensificação do potencial de ameaça decorrente da interconexão de informações e descentralização do processamento.

A enunciação genérica, nos moldes do inciso X, do art. 5º, da Constituição, não tutela satisfatoriamente os noveis componentes da esfera pessoal, especificamente protegidos pela autodeterminação informativa. Ainda que intimidade e vida privada possam ser afetadas não apenas no entorno digital, a excessiva ampliação do âmbito de proteção do direito redunda um uma série de riscos inerentes ao uso de terminologia imprecisa – sobretudo, a perda da capacidade efetiva como objeto de proteção jurídica.[136]

O legislador infraconstitucional, na lei n º 7.232/80, que rege a Política Nacional de Informática, tão somente dispôs no art. 2º, inciso IX, o *"estabelecimento de mecanismos e instrumentos para assegurar a todo cidadão o direito ao acesso e à retificação de informações sobre ele existentes em bases de dados públicas ou privadas",* sem, contudo, ir mais além e detalhar um direito fundamental à autodeterminação informativa.

Na lição de TÉRCIO SAMPAIO FERRAZ JUNIOR, a estrutura básica dos direitos fundamentais subdivide-se em três elementos: sujeito, objeto e conteúdo. O sujeito

---

[135] W. HASSEMER, *Oportunidades para la …*, *op. cit*., p. 112.
[136] C. M. ROMEO CASABONA, *Tendencias actuales sobre las formas de protección jurídica ante las nuevas tecnologías*, in Poder Judicial, n. 31, set., 1993, p. 170.

é o titular do direito, que em consonância com o art. 5º, *caput*, da Carta Federal, inclui toda e qualquer pessoa, física ou jurídica, brasileira ou estrangeira, residente ou transeunte. O *objeto* é o bem protegido. Destarte, tanto o direito à privacidade, como a autodeterminação informativa, têm como *objeto* a integridade moral do sujeito. O *conteúdo*, faculdade específica atribuída ao sujeito, evidencia porém, a diferenciação entre esses direitos. O conteúdo da privacidade circunscreve-se à noção apontada por SAMPAIO FERRAZ de:

> *"constranger os outros ao respeito e de resistir à violação do que lhe é próprio, isto é, das situações vitais, que, por dizerem a ele só respeito, deseja manter para si, ao abrigo de sua única e discricionária decisão".*[137]

A base axiológica da proteção de dados, reconhecida nas faculdades do titular de dados informáticos – relacionadas ao consentimento, controle, retificação e destruição dos dados –, evidencia o *conteúdo* da autodeterminação informativa como direito humano vocacionado à autonomia.

A proteção da esfera privada nos meandros da *internet* restringe-se, sobremaneira, ao continente europeu. Entretanto, em alguns Estados o reconhecimento do direito à autodeterminação informativa tem recebido disciplina mais extensa e pormenorizada.

No Brasil são ainda incipientes as normas específicas destinadas a disciplinar este direito. Embora intimidade e vida privada tenham sido consagradas pelo legislador constitucional de 1988, não há que se falar em normativa exclusiva, como desde muito se reclama. Notadamente, veem-se os operadores do Direito obrigados a recorrer à Lei Civil, ao Código do Consumidor ou ao conjunto de preceitos que regem as liberdades de imprensa e as atividades relacionadas às telecomunicações. Esta omissão normativa gera não apenas manifesta imprecisão conceitual, mas autêntica barafunda jurisprudencial que coloca em risco os direitos da pessoa humana.[138]

---

[137] *Sigilo de dados: o direito à privacidade e os limites à função fiscalizadora do Estado*, in Reinaldo Pizolio, Jayr Viégas Gavalcão Jr. (coords.), *Sigilo fiscal e bancário*, São Paulo, Quartier Latin, 2005, pp. 17-18.

[138] Questão controversa diz respeito ao *status* da pessoa jurídica como sujeito ativo do direito à autodeterminação informativa. Se por um lado alguns direitos da personalidade atingem reflexamente às pessoas jurídicas (*v.g.* o direito à honra, reconhecido em contextos mais alargados que o individual) e ampliam a eficácia da proteção de direitos fundamentais; por outro, a ausência de uma existência física motiva a controvérsia.

As violações ao direito à proteção e controle dos dados pessoais podem ser tuteladas por meio das garantias constitucionais do mandado de segurança (CF, art. 5°, inciso LXIX) e *habeas data* (CF, art. 5°, inciso LXXII).[139] Ainda que se possa pleitear em juízo, de maneira genérica, a preservação do direito líquido e certo à intimidade, a autonomia do âmbito de proteção do direito à autodeterminação informativa exige que seja demandado diretamente.

Por consequência, imperioso o reconhecimento expresso do direito à autodeterminação informativa, dado imprescindível ao pleno desenvolvimento da pessoa; garantia individual do poder de controle sobre os dados pessoais, cuja garantia de efetividade depende também da imposição a terceiros de deveres específicos.[140]

2.3. Teoria das três esferas

Amplamente consagrada na doutrina, a teoria das três esferas (*Spharentheorie*)[141] volta-se à delimitação do âmbito de proteção do *right of privacy*. Segundo esta corrente, a vida particular ou privada poderia ser dividida em esferas concêntricas, progressivamente menores em razão do maior grau de intimidade a ser preservado.[142]

A esfera de maior extensão compreende a vida social, setor em que os acontecimentos envolvem não apenas as pessoas do círculo íntimo do titular. Há interesse na preservação dos fatos veiculados nesse âmbito, como os dados referentes à índole

[139] Ausente ameaça direta ou indireta ao direito de locomoção, inadequado do uso do *habeas corpus* para preservação da intimidade, *v.* HC 4536/RJ, rel. Ministro Luiz Vicente Cernicchiaro, sexta turma, j. 27.03.1996.
[140] O projeto de lei 2126, de 2011, em trâmite na Câmara dos Deputados, dispõe sobre a proteção, o tratamento e o uso dos dados pessoais. No projeto não há expressa referência ao direito à autodeterminação informativa; a opção do legislador foi pela expressão *proteção de dados*, atualmente em voga nas principais normas protetivas internacionais.
[141] A teoria das esferas, atribuída inicialmente HEINRICH HUBBMANN (*Intimsphäre*, *Privatsphäre,* e *Individualsphäre)*, foi mais tarde aperfeiçoada por HEINRICH HENKEL e SCHMIDT, *v.* P. J. COSTA JUNIOR, *O direito de estar...*, *op. cit*., pp. 34-35; F. MORALES PRATS, *La tutela penal ...*, *op. cit*., pp. 128-133; A. TÉLLEZ AGUILERA, *Nuevas Tecnologías ..., op. cit*., pp. 62-65.
[142] P. J. DA COSTA JÚNIOR, *O direito de estar ..., op. cit.* , p. 34.

profissional[143], ao nome, à reputação e estima social. Aqui, a preocupação com a proteção do segredo é pouco abrangente.

No interior da vida social situa-se a vida privada, cujo objeto de proteção é a tranquilidade espiritual ou paz psíquica. A participação compete somente às pessoas em que o titular confia, notadamente, familiares e amigos com os quais mantém certa intimidade. Desta categoria estará excluído, tanto o público em geral, como também os indivíduos cujo relacionamento não é dotado de estritos vínculos pessoais.

Na porção mais exclusiva do âmago encontram-se todas as informações da vida particular conservadas em segredo, das quais ninguém tem conhecimento, ou de que compartilham somente pessoas muito próximas a (intimidade em sentido estrito). A proteção nesta esfera se faz sentir de forma mais intensa, pois ninguém pode ser forçado a revelar o que não pretende sem a violação da dignidade da pessoa humana.[144] A intimidade configura a máxima interioridade humana, a relação consigo mesmo, necessidade de autoconhecimento e resguardo de um mundo íntimo próprio que a ninguém é dado invadir.[145]

A proteção constitucional no ordenamento pátrio baliza-se pela tutela da intimidade e da vida privada, como expressamente dispõe a Constituição da República no art. 5º, inciso X: *"são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas (...)"*.

---

[143] A. SCARANCE FERNANDES, *O sigilo financeiro e a prova criminal,* in J. de Faria Costa, M. A. Marques da Silva (coords.), *Direito penal especial, processo penal e direitos fundamentais*, São Paulo, Quartier Latin, 2006, p. 458.

[144] JOSÉ RAUL GAVIÃO DE ALMEIDA conceitua uma quarta esfera, ainda mais restrita, a da *intimidade oculta "que abarca todos os segredos que não se quer compartilhar, mas reservar à própria consciência. É em decorrência deste mais íntimo direito à privacidade, que integra o âmbito de conhecimento protegido pela 'reserva da própria mente' e a ninguém revelado, que não se admite a submissão a métodos que eliminam a capacidade volitiva da pessoa, tal como o soro da verdade e a hipnose. Tais métodos de obtenção de conhecimento, se utilizados sem prévio conhecimento, violam a própria personalidade do indivíduo."* (*Anotações acerca do direito à privacidade*, in J. Miranda, M. A. Marques da Silva [orgs.], *Tratado Luso-Brasileiro da Dignidade Humana*, 2ª ed., São Paulo, Quartier Latin, 2009, p. 720). Tal como apresentada, esta noção aproxima-se da esfera mais íntima, sobre a qual discorre HENRICH HENKEL, denominada *Vertrauenshäre* ou *Vertralichkeutssphäre*, onde se tem a exclusão completa de terceiros (A. TÉLLEZ AGUILERA. *Nuevas Tecnologías ..., op. cit.,* p. 63).

[145] A. I. HERRÁN ORTIZ, *La violación ...*, *op. cit*., p. 12.

A Carta de 1988 erigiu a *intimidade,* a *vida privada*[146]*,* a *honra* e a *imagem* das pessoas à categoria de direitos individuais. Embora não sejam poucas as discordâncias quanto à precisão da terminologia, parece mais adequado o uso amplo e genérico da expressão *direito à intimidade* para fazer referência a todo o espectro de proteção do art. 5º, inciso X.[147]

Entretanto, o dispositivo constitucional, ao assegurar a inviolabilidade deste valor humano, aponta para a existência de distintos graus de proteção instituídos pelo legislador.

A intimidade em sentido estrito, setor mais recôndito e sobre o qual se tem o direito de manter reserva da ingerência de terceiros, caracteriza-se pelo segredo e pela autonomia. Memórias pessoais, confissões amorosas, aspectos da vida conjugal, particularidade associadas às relações familiares, segredo sob juramento, as confidências escritas em um diário, bem exemplificam a intimidade em acepção restrita.

A vida privada, por outro lado, pressupõe a convivência com o outro, estabelece-se por meio da comunicação ou de opções pessoais que podem repercutir para terceiros.[148] O legislador constitucional considerou que a vida das pessoas engloba um aspecto voltado para o interior, circunscrito aos membros da família e amigos, inviolável segundo a Constituição.[149]

A honra e a imagem, direitos da personalidade, também repercutem socialmente, porque dotadas de inegável sentido comunicacional.[150] A honra projeta-se como um plexo de qualidades que compõem a dignidade da pessoa ou consideração pessoal, tais como o nome e a reputação; se ocorrer lesão surge imediatamente o direito de

---

[146] No Direito interno a expressão *vida privada* consta não apenas no inciso XII, art. 5º, da Constituição Federal, mas também como direito da personalidade previsto no art. 21 do Código Civil e como direito do ofendido no art. 201, § 6º do Código de Processo Penal (redação dada pela Lei 11.690, de 9 de junho de 2008).

[147] ADA PELLEGRINI GRINOVER atesta preferência pela noção de *direito à intimidade*, *v. Liberdades Públicas ..., op. cit*, p. 72. Distinta a solução preconizada por JOSÉ AFONSO DA SILVA que, para designar as distintas esferas, prefere a expressão *direito à privacidade* (*Curso de Direito Constitucional Positivo*, 25ª ed., São Paulo, Malheiros, 2005, p. 206).

[148] T. SAMPAIO FERRAZ JUNIOR, *Sigilo Fiscal ..., op. cit*., pp. 20-21.

[149] JOSÉ AFONSO DA SILVA, *Curso de Direito ..., op. cit.,* p. 208.

[150] T. SAMPAIO FERRAZ JUNIOR, *Sigilo Fiscal ..., op. cit.*, p. 21.

defesa. O direito à imagem consiste na reserva do aspecto físico, a preservação da pessoa frente à reprodução visivelmente perceptível de suas compleições físicas.[151]

Advirta-se, porém, que as teorias jurídicas baseiam-se em premissas voltadas a descrever os fenômenos ocorridos no mundo e possibilitam a identificação de similitudes ou diferenças frente a certas situações. Os critérios escolhidos para solucionar os casos concretos não buscam a forma mais conveniente ou verdadeira para a interpretação da realidade, mas sim o rigor de um modelo científico formal.[152]

A teoria das três esferas, tanto pelo caráter didático como pela significativa operacionalidade, favorece ao intérprete do direito diferenciar os variados níveis de gravidade das intrusões à intimidade. Contudo, há que ser aplicada sempre com parcimônia à medida que algumas informações analisadas individualmente não apresentam relevância, mas associadas a outras podem revelar um retrato amplo da personalidade individual.

Diferenciar a natureza das informações pessoais no que concerne ao grau de resguardo da intimidade é atividade complexa, de difícil consecução.[153] Transposta ao ordenamento jurídico, a inviolabilidade do setor mais reservado da consciência humana não é capaz, por si só, de assegurar o respeito à intimidade; a salvaguarda dos traços mais

---

[151] Nos dizeres de CELSO RIBEIRO BASTOS o *"direito de ninguém ver o seu retrato exposto em público sem o seu consentimento"* (*Comentários à Constituição do Brasil*, v. 2, São Paulo, Saraiva, 1989, p. 62).

[152] Reflexão de grande valia acerca da teoria das três esferas se dá em razão de sua aplicação para superar situações complexas. Não se despreze, contudo, a pertinência de outros modelos, como é o caso da teoria dos mosaicos e da teoria da comunicação social. A primeira, criação do Tribunal Superior Alemão (BGH), pressupõe a relatividade dos conceitos de público e privado, em razão da relação informativa que se estabelece entre dois sujeitos. Temos dados *a priori* irrelevantes sob o ponto de vista do direito à intimidade; todavia, relacionados a outros, podem revelar a personalidade de um indivíduo. Assim como as pequenas pedras que formam os mosaicos, o valor individual é escasso, mas unidas formam conjuntos plenos de significados (A. TÉLLEZ AGUILERA, *Nuevas Tecnologías ...*, *op. cit.,* pp. 64-65). A teoria da comunicação social foi desenvolvida pela Suprema Corte americana a partir do direito de estar só (*"right to withhold" como corolário do "right to be alone"*). Como afirmam G. E. ABOSO e M. F. ZAPATA, a pessoa cumpre uma diversidade de papéis na vida social, e as distintas informações que recebe ou transmite não necessariamente ingressam na esfera privada (*Cibercriminalidad y Derecho Penal*, Montevideo-Buenos Aires, Julio César Faira, 2006, p. 133).

[153] A tutela dos chamados dados sensíveis (*v.* item 3.2.1), ou seja, a elaboração de uma classe de informações que não pode transcender do conhecimento da pessoa ou de seu núcleo familiar, seria suficiente para instituir um regime proteção dos dados individuais? Em verdade, se faz necessário reconhecer a convivência dos dados sensíveis com a noção mais ampla de *dados pessoais*, igualmente dignos de proteção. Há um legítimo interesse do titular em proteger o nome, número de telefone, informações relativas a seu trabalho e preferências pessoais, muito embora estas informações não se situem no setor mais recôndito da personalidade.

caros à personalidade depende não apenas dos conceitos ínsitos na norma posta, mas, sobretudo, da garantia efetiva da proteção de dados.

A simples noção de inviolabilidade transposta ao setor mais reservado da personalidade não se perfaz instrumento concreto de proteção do direito à intimidade; impõe também assegurar o controle e a proteção dos dados.

O direito subjetivo de administrar os próprios dados repercute nos três círculos concêntricos. Pensar a teoria das três esferas para proteger o titular de dados no entorno digital não pode significar descurar das informações que não estejam no setor mais exclusivo, pois todos os dados pessoais veiculados na *web* são dignos de proteção.

Exatamente para que não se esvazie o âmbito de proteção do direito à proteção de dados, a aplicação da teoria das três esferas à tutela das informações veiculadas no entorno digital deve compatibilizar-se com outros preceitos a seguir expostos: a impossibilidade do tratamento de dados sensíveis (ressalvadas as hipóteses legais de exceção, *v.* item 3.2.1) e a necessidade de consentimento do titular dos dados (*v.* itens 4.4.2.1.2 e 6.1).

2.4. Inviolabilidade das comunicações na Constituição de 1988

O grau de exclusividade da comunicação (postal, telegráfica, de dados e telefônica) enquadra-se na esfera da vida privada, inserida pois não no âmbito do segredo, mas sim no espaço de convivência. Por sua vez, a intimidade em sentido estrito, setor exclusivo da vida pessoal, pressupõe segredo e autonomia. Informações relativas ao núcleo da personalidade pertencem ao titular (e/ou àqueles que lhe são próximos) e, *a priori,* não se compartilham em processos comunicativos.[154]

Sobre a inviolabilidade das comunicações dispõe especificamente o art. 5º, inciso XII, da Carta da República, *"... inviolável o sigilo da correspondência e das*

[154] Na mesma direção o posicionamento de T. SAMPAIO FERRAZ JUNIOR, *Sigilo Fiscal ..., op. cit*., p. 20.

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."

Por sua vez, o parágrafo único, do art. 1º, da lei nº 9.296/96, em redação de controversa constitucionalidade, estabelece: *"O disposto nesta Lei aplica-se à interceptação do fluxo de comunicações em sistemas de informática e telemática."*[155]

Em particular, a interpretação da última parte do art. 5º, inciso XII, da Carta, suscita ao menos três posicionamentos distintos sobre a tutela do objeto do direito.[156] Sob um primeiro viés, argumenta-se que a expressão *último caso* refere-se somente à inviolabilidade das comunicações telefônicas.[157] Outra corrente sustenta a abrangência da comunicação de dados e telefônica.[158] Por sua vez, ainda se pode pensar na extensão da possibilidade de intromissão à correspondência, às comunicações telegráficas e telefônicas e aos dados.[159]

---

[155] A constitucionalidade do dispositivo foi questionada na ADI 1.488 (rel. Ministro Néri da Silveira, j. 7.11.96), mas a ação foi obstada por ilegitimidade ativa *ad causam*.

[156] O objeto do direito subjetivo à inviolabilidade das comunicações consiste na liberdade de não comunicação do pensamento. O conteúdo, a faculdade de manter o sigilo da informação veiculada (T. SAMPAIO FERRAZ JUNIOR, *Sigilo Fiscal ...*, *op. cit*., p. 22).

[157] A. PELLEGRINI GRINOVER, A. SCARANCE FERNANDES, A. M. GOMES FILHO, *As Nulidades no Processo Penal*, 10ª ed., São Paulo, RT, 2007, p. 210; V. GRECO FILHO, *Interceptação Telefônica*, São Paulo, Saraiva, 1996, pp. 9-13; A. PELLEGRINI GRINOVER, *Novas Tendências*, Rio de Janeiro, Forense, 1990; N. NERY JUNIOR, R. M. DE ANDRADE NERY, *Constituição Federal Comentada*, 2ª ed., São Paulo, RT, 2009, p. 176.

[158] G. BANDEIRA, *A interceptação do fluxo de comunicações por sistemas de informática e sua constitucionalidade*, in Revista de Direito do TJ/RJ, n. 55, 2003; A. A. MENDES MACHADO, A. P. DE ANDRADE KEHDI, *Sigilo das comunicações e de dados*, in A. S. Fernandes, J. R. Gavião de Almeida, M. Zanoide de Moraes, *Sigilo no Processo Penal: Eficiência e Garantismo*, São Paulo, RT, 2008, pp. 243-245; G. H. BADARÓ, *Interceptação de comunicações telefônicas e telemáticas: limites ante o avanço da tecnologia*, in J. Corrêa de Lima, Rubens R. R. Casara (coords.), *Temas para uma Perspectiva Crítica do Direito: Homenagem ao Professor Geraldo Prado*, Rio de Janeiro, *Lumen Juris*, 2010. JOSÉ AFONSO DA SILVA acompanhava os autores da corrente restritiva (*v. Curso de Direito ...*, *op. cit*., p. 438), mas modificou o entendimento para incluir a possibilidade de interceptação da comunicação de dados (*Comentário contextual ...*, *op. cit.,* p. 105).

[159] É a posição de M. A. DE BARROS, *A Busca da Verdade no Processo Penal*, São Paulo, RT, 2002, pp. 227-229. Para UADI LAMMÊGO BULOS o juiz pode determinar a quebra para qualquer uma das modalidades de comunicação: *"nas situações determinadas por leis constitucionais, para evitar a tutela oblíqua de condutas ilícitas ou práticas contra legem"* (*Constituição Federal anotada*, 7ª ed., São Paulo, RT, 2007, p. 158); para ALEXANDRE DE MORAES a lei ou a decisão judicial podem, excepcionalmente, *"estabelecer hipóteses de quebra das inviolabilidades da correspondência, das comunicações telegráficas e de dados, sempre visando salvaguardar o interesse público e impedir que a consagração de certas liberdades públicas possa servir de incentivo à prática de atividades ilícitas"* (*Constituição do Brasil interpretada*, 6ª ed., São Paulo, Atlas, 2006, p. 241). A. SCARANCE FERNANDES restringe a quebra do sigilo às comunicações telefônicas, mas ressalta a aplicação da ponderação de interesses para o sigilo das demais comunicações: *"aceitação do princípio da proporcionalidade, que a justificaria para preservar outro valor amparado constitucionalmente e de maior relevância"* (*Processo Penal ...*, *op. cit*., p. 92).

Previamente ao enfrentamento do tema do uso dos dados informáticos na investigação criminal, imprescindível, portanto, perquirir se a proteção constitucional da inviolabilidade da comunicação de dados compatibiliza-se com os meios de obtenção destas fontes de prova.

Para este mister se faz oportuna, de início, uma breve exposição dos critérios hermenêuticos envolvidos e a busca da convergência entre os sentidos. Em seguida, há que se deter no exame das principais linhas de argumentação, divergências doutrinárias e jurisprudenciais, ressaltada a linha interpretativa constitucionalmente mais adequada.

2.4.1. Hermenêutica

Para que a seleção de métodos e princípios hermenêuticos por parte do intérprete não ocorra *"ao sabor de sentimentos e intuições, critérios que talvez lhe pacifiquem a consciência, mas certamente nada nos dirão sobre a racionalidade dessas opções"*,[160] ora apresentadas algumas premissas utilizadas para o esclarecimento do texto do art. 5º, inciso XII, da Constituição Federal.

Neste mister, de grande valia os escritos de FRANÇOIS OST e MICHEL VAN DE KERCHOVE para a determinação de critérios interpretativos norteadores na compreensão do âmbito de proteção do direito à inviolabilidade das comunicações de dados.

Como observam os juristas belgas, a análise histórico-comparativa das teorias da interpretação na França e na Bélgica desde o século XIX evidencia o conflito entre dois modelos tradicionais: o *exegético* e o *evolucionista* (ou funcionalista). Em apertado resumo, o primeiro volta-se à desconstituição do papel criador da interpretação. Por outro lado, o modelo *evolucionista* constitui a recusa da busca de um sentido originário

[160] G. FERREIRA MENDES, I. MÁRTIRES COELHO, P. G. GONET BRANCO, *Curso de Direito Constitucional*, 4ª ed., São Paulo, Saraiva, 2009, p. 120.

segundo a vontade do legislador, à medida que a descoberta de soluções deve harmonizar-se com as necessidades práticas (em detrimento da perspectiva histórica, privilegia-se um sentido próprio e evolutivo).[161]

Os autores, porém, com veemência referendam a insuficiência de tais modelos. Perfaz-se necessária a busca por outra solução que concilie dois dados essenciais: estabilidade e evolução (vontade do legislador e necessidades sociais presentes). Isto, sem incorrer na busca por um único sentido verdadeiro do texto normativo, escopo absolutamente irrealizável.[162]

O reconhecimento da relação dialética entre o texto e o sentido da norma obtido no processo interpretativo é parte da proposta por um modelo intermediário de interpretação jurídica que compatibilize continuidade e inovação.

Em verdade, o intérprete situa-se no coração de um emaranhado de sentidos que a ele toca organizar. Diante da complexidade do texto, o desafio interpretativo compreende ainda o risco a que aludem FRANÇOIS OST e MICHEL VAN DE KERCHOVE, da transformação do sentido, ou seja, a *interpretação como traição.* À medida que frequentes os deslocamentos, reformulações, desconstruções e reconstruções, a interpretação opera-se como ato intelectivo de produção de sentido necessariamente cotejado entre múltiplas tensões e polos opostos.

A função da interpretação não se reduz à reprodução mecânica de um sentido já dado, mas também não se amplia a ponto de constituir livre elaboração de um sentido inédito. Em linhas gerais, o espaço da interpretação estaria em posição intermediária à recitação e à invenção (*v.* item 1.4.3.2):

> *"L'interprétation comme revitalisation, réactivation du sens, ou du moins d'un sens, inscrit dans le texte, comme actualisation d'une signification virtuelle qui sommeillait en lui. Interprétation comme poursuite du travail infini de signifiance, tâche aussi éloignée de la croyance en la possibilité de découvrir un sens vrai et unique qu'il*

[161] *Interprétation ...*, *op. cit.*, p. 185.
[162] Para T. S. FERRAZ JUNIOR a dupla perspectiva é representada pelas doutrinas *subjetivista* e *objetivista*. Em síntese, a primeira corrente volta-se ao reconhecimento da vontade do legislador, análise genética *ex tunc* do texto de lei. Para o segundo viés a norma tem sentido próprio (vontade da lei) e a compreensão rege-se por aspectos estruturais ao tempo que a norma vige (*ex nunc*) (*A ciência do direito ...*, *op. cit*., pp. 70-71).

> *importerait seulement de dire et de redire, que de l'illusion opposée d`une production de sens totalement autonome, complètement affranchie de la tradition et du système de référence."*[163]

As técnicas interpretativas desempenham um papel relevante para a compreensão do sentido. Fala-se principalmente em interpretação *gramatical*, *lógica*, *sistemática, histórico-evolutiva*, critérios complementares e não excludentes entre si.

Ademais, o objeto interpretado pode ser conhecido segundo fontes ou setores específicos do conhecimento jurídico. Como representação da variação dos critérios hermenêuticos, em razão da diversidade técnico-operativa, pense-se em dicotomias como Direito *público ou privado*, *penal ou não penal*, *interno ou internacional*. Em atenção aos princípios norteadores de cada campo dogmático, a interpretação pode variar entre *restritiva*, *extensiva* e *especificadora*.

Contudo, não há falar em prevalência entre operações intelectuais, sobretudo em virtude de sua natureza complementar. Há que se adotar, portanto, uma concepção maximalista da interpretação, correspondente ao conjunto desses processos intelectivos:

> *"Si, comme nous inclinons à le penser, une telle conception reflète bien la pratique interprétative effectivement suivie par les juristes, on pourrait alors demander si, au terme d'un retournement paradoxal, l'interprétation porte bien encore sur des textes et non plutôt sur d'autres interprétations. Non que l'interprétation soit affranchie des textes ou étrangère à ceux-ci, mais que ces textes eux-mêmes sont l'interprétation d'autres textes et n'existent qu'au travers des interprétations qu'on en a données et qu'on en donnera".*[164]

---

[163] *"A interpretação como revitalização, reativação do sentido, ou ao menos de um sentido, inscrito nesse texto, como atualização de um significado virtual que estava adormecido nele. Interpretação como a perseguição de um trabalho infinito de significação, tarefa também afastada da crença na possibilidade de descobrir um sentido verdadeiro e único que implicaria somente em dizer e redizer, ou à ilusão oposta de uma produção de sentido totalmente autônoma, completamente liberada da tradição e do sistema de referência"* (*Interprétation ...*, *op. cit*., p. 167, trad. nossa).

[164] "*Se, como nos inclinamos a pensar, uma concepção tal reflita bem a prática interpretativa efetivamente seguida pelos juristas, poderíamos então nos perguntar se, ao cabo de uma virada paradoxal, a interpretação se faz sobre os textos e não mais especificamente sobre outras interpretações. Não que a interpretação seja liberada dos textos ou estranha a eles, mas que os próprios textos são interpretações de*

As divergentes interpretações doutrinárias e jurisprudenciais resultam da busca por compreensão e ordenação da plurivocidade das normas jurídicas. Tais possibilidades de sentido, no entanto, sujeitam-se a limites jurídico-dogmáticos.

Advertidos dos riscos de desconstrução e transformação de sentido que permeiam a atividade intelectiva, o norte será a busca pela convergência e o entrelaçamento dos sentidos. Nos itens seguintes, à exposição das diretivas interpretativas usualmente empregadas e às respectivas conclusões, seguir-se-á o enfrentamento dos conflitos gerados pelos posicionamentos opostos.

2.4.2. Divergências doutrinária e jurisprudencial

A corrente de interpretação *restritiva* da inviolabilidade do sigilo das comunicações apresenta duas ordens de argumentos. Em primeiro lugar, afirma-se a prevalência de uma interpretação teleológica do dispositivo, pois o legislador constituinte, ao empregar a expressão "*no último caso*", referia-se tão somente à comunicação telefônica, única a não deixar vestígios. Nesse sentido, imprescindível proceder à interceptação no momento em que a comunicação ocorre, sob pena de jamais se ter acesso ao seu conteúdo.[165]

Sob esta perspectiva, costuma-se ressaltar também o caráter excepcional das interceptações, de sorte que a exegese do dispositivo há que ser restritiva (*exceptiora non sunt amplianda*). Toda relativização de um direito fundamental não pode se estender além das estritas hipóteses legais; em todos os casos priorizada a interpretação que menos restrinja o direito em questão.[166]

---

outros textos e não existem senão através das interpretações que lhes damos e daremos" (*Interprétation*, *op. cit.,* p. 176, trad. nossa).

[165] *Cf.* a opinião do Ministro Sepúlveda Pertence (MS 21729-4/DF).

[166] LÊNIO LUIZ STRECK adota a posição restritiva com algumas particularidades. Para o autor, a expressão comunicações telefônicas estende-se a todos os meios de comunicação que, de algum modo, utilizem como suporte o sistema telefônico, tal como ocorre com o *fax-modem* (*As interceptações telefônicas e os direitos fundamentais*, 2ª ed., Porto Alegre, Livraria do Advogado, 2001, p. 48). RAUL CERVINI e LUIZ FLÁVIO

A interpretação, por assim dizer, *intermediária*, vale-se também de dois argumentos principais. A análise gramatical do art. 5º, inciso XII, da Carta, permite constatar duas conjunções aditivas "*e*" seguidas de uma vírgula, a evidenciar não quatro grupos de comunicações distintos, mas na verdade dois (o sigilo da correspondência e o sigilo das comunicações telegráficas no primeiro grupo; o sigilo de dados e o sigilo das comunicações telefônicas, no segundo).

Por sua vez, a hermenêutica histórica do dispositivo pauta-se pela análise das sucessivas alterações na sua redação. ADA PELLEGRINI GRINOVER[167] narra que à época, as Mesas de Processo Penal e a Comissão de Estudos e Assessoramento Constitucional para Assuntos Municipais de São Paulo sugeriram à Assembleia Constituinte fosse adotada a redação do art. 32, § 6º, da Constituição Portuguesa de 1976: *"É inviolável o sigilo da correspondência, das comunicações e dos arquivos particulares, salvo por ordem judicial, nos casos e na forma que a lei estabelecer, para fins de instrução processual."*

Na tramitação do projeto na Comissão, duas redações prosperaram. Em primeiro lugar: *"É inviolável o sigilo da correspondência e das comunicações telegráficas ou telefônicas, salvo por ordem judicial, nos casos e na forma que a lei estabelecer, para fins de instrução processual."* A segunda redação acrescentou a expressão *"e de dados"*: *"É inviolável o sigilo da correspondência e das comunicações telegráficas, telefônicas e de dados, salvo por ordem judicial, nos casos e na forma que a lei estabelecer, para fins de investigação criminal e de instrução processual."*

Em seguida, a redação aprovada em primeiro turno pelo Plenário da Constituinte incluiu a expressão "*último caso*": *"É inviolável o sigilo da correspondência e das comunicações telegráficas, de dados e telefônicas, salvo neste último caso, por ordem judicial, nas hipóteses e na forma que a lei estabelecer, para fins de investigação criminal e instrução criminal e instrução processual."*

GOMES ampliam a noção de comunicação telefônica ao *status* de gênero, do qual a comunicação informática seria espécie, permitindo-se, pois, de acordo com o texto constitucional, a quebra do sigilo de ambas (*Interceptação telefônica: Lei 9.296, de 24.07.96*, São Paulo, RT, 1997, pp. 167-171). Todavia, as distintas noções de comunicação telefônica e de dados não permitem sustentar uma relação gênero-espécie (*v.* item, 2.8).

[167] *Novas Tendências do direito processual*, Rio de Janeiro, Forense Universitária, 1990, pp. 79-80.

Os dois primeiros textos eram suficientemente claros ao prescrever que a ressalva se aplicava a todas as formas de transmissão de informações. O outro, igualmente imune a controvérsias, permitia apenas a quebra do sigilo das comunicações telefônicas.

No entanto, a disposição foi novamente alterada, permanecendo como redação final: *"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."*

A inserção dos termos *"das comunicações"* antes de *"telefônicas"* instituiria, pois, duas modalidades protegidas, visto que para uma interpretação diversa o legislador não haveria modificado o texto da lei.

Uma interpretação ampliativa, de modo a estender a possibilidade de intromissão à correspondência, às comunicações telegráficas e telefônicas e aos dados, é defendida por MARCO ANTONIO DE BARROS. Para o autor, mediante autorização judicial a inviolabilidade destas comunicações pode ser relativizada, uma vez que sustentar o caráter absoluto da norma redundaria na impunidade dos delinquentes, sobretudo, no âmbito das organizações criminosas. A permissão para a violação do sigilo, mesmo conflitante com a letra da lei, pode ser acolhida como *"admissão ao princípio da ponderação de interesses"*.[168]

ANTONIO SCARANCE FERNANDES leciona que, exceção feita ao telefone, a proteção absoluta das demais fontes de comunicação, jamais se permitindo divulgar o segredo nelas contido, não respeita *"a necessidade de equilíbrio entre os bens protegidos constitucionalmente"*. Para o jurista, a quebra do sigilo restringe-se às comunicações telefônicas, mas há necessidade da aplicação da ponderação de interesses para o sigilo das demais comunicações: *"a utilização como prova do dado protegido pelo sigilo depende da*

[168] *A busca da verdade ...*, *op. cit*., pp. 226-230.

aceitação do princípio da proporcionalidade, que a justificaria para preservar outro valor amparado constitucionalmente e de maior relevância."[169]

2.4.3. Interpretação do art. 5º, XII

As observações dos itens anteriores têm como escopo indicar os critérios possíveis para a interpretação jurídica e assim esclarecer o raciocínio ora empreendido. Como visto, a função da interpretação não se reduz à reprodução mecânica de um sentido já dado, mas também não se amplia a ponto de constituir livre elaboração de um sentido inédito; orienta-se, na verdade, pela ponderação e dialética das interpretações possíveis.

Toda intenção de apresentar uma única interpretação verdadeira, que revele sentido unívoco para o conteúdo normativo, representa:

> *"*no máximo uma proposta política que se esconde sob a capa de uma pretensa cientificidade. (...) daí para frente, o que se faz realmente é política, é tentativa de persuadir alguém de que esta e não aquela é a melhor saída, a mais favorável, dentro de um contexto ideológico, para uma estrutura de poder*"*.[170]

Superada qualquer pretensão de apresentar a interpretação verdadeira, o desafio de composição dos sentidos perpassa pela busca da justa medida entre a *mens legislatoris* e as inegáveis mudanças sociais. É mister do intérprete esclarecer as razões que o fizeram optar por determinados argumentos, em detrimento de outros – em vários níveis, o jurista tem inclusive o dever de observância fiel à garantia de motivação das decisões judicias.

No art. 5º, inciso XII, da Carta da República, vem prevista a inviolabilidade de quatro formas distintas de comunicação: postal, telegráfica, de dados e

[169] *Processo Penal ..., op. cit.,* pp. 91-92.
[170] T. S. FERRAZ JUNIOR, *Introdução ao Estudo ...*, *op. cit*., p. 263.

telefônica. Erigida à condição de garantia fundamental do cidadão, além de cláusula pétrea, nos termos do art. 60, § 4º, inciso IV, do ordenamento constitucional.[171]

Ao referir-se a *dados,* o legislador constituinte alude às informações transmitidas pelas tecnologias informativas, cujo objeto específico de tutela é a liberdade de comunicação entre os indivíduos.[172] Diversamente, outros dados não armazenados em suporte informático (*v.g.,* diário pessoal ou agenda) encontram proteção específica na regra do art. 5º, inciso X, da Magna Carta.

A interpretação gramatical do dispositivo não deixa dúvidas de que o legislador quis diferenciar duas situações: de um lado, o sigilo das correspondências e das comunicações telegráficas; de outro, o sigilo de dados e das comunicações telefônicas. Cada um dos grupos está unido internamente pela conjunção aditiva *e*, mas separados externamente por uma vírgula e pela repetição do termo *comunicações*.

A exemplo da análise gramatical do dispositivo, o estudo das sucessivas alterações realizadas pelo constituinte – exame histórico-reconstrutivo – evidencia a inclusão dos vocábulos *"das comunicações"* antes de *"telefônicas",* tal como descrito no item anterior. A intenção do legislador, critério usualmente privilegiado pela Escola da *exegese* (*v.* item 2.4.1), não poderia ser outra senão a de acrescentar a quebra do sigilo das comunicações de dados para fins de investigação criminal.

Como assevera TÉRCIO SAMPAIO FERRAZ JUNIOR, na investigação teleológica do art. 5º, inciso XII, da Constituição, dentre as quatro modalidades de comunicação, apenas a telefônica tem como característica a *instantaneidade*. Por não deixar vestígios do conteúdo da conversação, diferencia-se do envio de correspondência, telegrama ou fluxo de dados por sistemas informáticos, pois nestes casos os elementos de

[171] Os métodos hermenêuticos apresentados – gramatical, lógico, histórico e sistemático – seguem a tradição sistematizadora de FRIEDRICH CARL VON SAVIGNY. Não se fará referência expressa aos princípios e métodos interpretativos de matiz estritamente constitucional, ainda que uma visão sob tal perspectiva possa ter caráter complementar ao esforço ora realizado. Os métodos de interpretação constitucional (hermenêutico clássico, tópico-problemático, científico-realista, hermenêutico-concretizador), em grande medida dialogam com os próprios cânones propugnados por SAVIGNY. Para uma visão crítica sobre os métodos de interpretação constitucional, *v.* V. AFONSO DA SILVA, *Interpretação constitucional e sincretismo metodológico*, in V. Afonso da Silva (org.), *Interpretação constitucional*, São Paulo, Malheiros, 2007, p. 134.

[172] O legislador constituinte preocupava-se naquele momento com um campo ainda restrito de dados, em especial com a *"possibilidade das empresas, sobretudo financeiras, fazerem uso de satélites artificiais para a comunicação de dados contábeis"* (C. RIBEIRO BASTOS, *Comentários à Constituição ...*, *op. cit*., p. 73); gradativamente surgiram outras modalidades de dados a serem incluídos neste rol.

tais comunicações são perenes e podem ser posteriormente apreendidos. Desse modo, a interceptação da comunicação apenas se justifica nas hipóteses em que seu conteúdo não possa ser obtido por outro modo.[173]

Contudo, a premissa de que toda comunicação de dados por sistemas de informática e telemática permanece armazenada nos respectivos discos rígidos dos computadores atualmente não se mostra plenamente condizente com os avanços tecnológicos. A interceptação da comunicação constitui o único meio de obtenção das fontes de provas para comunicações em certos sistemas de telemática (como o *Voip*). Nesses casos, a busca e apreensão do computador não seria apta a obter os mesmos resultados, justamente porque os dados não constam armazenados.[174]

Acrescente-se que o legislador constitucional não poderia supor a evolução social e tecnológica futura, especialmente, o advento de novas formas de comunicação eletrônica.

Em 1988, a preocupação centrava-se em viabilizar a interceptação telefônica – que naquele momento representava o meio de comunicação mais utilizado pela criminalidade – como modo de obtenção de prova. Em comparação à comunicação postal, ao telégrafo e aos dados, certamente o telefone dispunha de melhores condições para servir como fonte de prova na investigação e instrução criminais.

Ao tutelar a liberdade de comunicação e pensamento não se poderia prever a atual substituição da comunicação telefônica pelos programas de computadores que permitem troca de vozes de maneira idêntica àquela realizada por linha telefônica convencional.[175]

É evidente o progresso tecnológico experimentado pela telefonia nas últimas décadas, atualmente não se concebe esta modalidade de comunicação dissociada da própria noção de dados. De forma análoga à evolução dos sistemas postais

[173] T. S. FERRAZ JUNIOR, *Sigilo Fiscal ...*, *op. cit*., p. 27.
[174] G. H. BADARÓ, *Interceptação de comunicações ...*, *op. cit*., p. 490. No mesmo sentido a decisão da Suprema Corte Constitucional, *v.* ADIN 14889/DF, rel. Ministro Neri da Silva, pleno, j. 07.11.1996.
[175] G. H. BADARÓ, *Interceptação de comunicações ...*, *op. cit.,* p. 489.

impulsionada pelo *e-mail*, a telefonia gradativamente tem sido substituída pela comunicação eletrônica.

As condutas criminosas realizam-se frequentemente com emprego de ferramentas próprias do entorno digital, tanto em razão da celeridade no fluxo de informações, como à vista das possibilidades de ocultação dos meios utilizados. Dessa forma, imprescindível uma leitura teleológica do direito à inviolabilidade das comunicações, que não ignore que o único meio de acessar o conteúdo de certas comunicações é efetivamente interceptá-las enquanto estejam em curso.

Indispensável, portanto, seja acrescentado o avanço tecnológico como dado significativo no processo interpretativo. A adequação dos conceitos existentes ao contexto atual (à realidade prática) remete ao ideal propugnado pela Escola de interpretação denominada por OST e VAN DE KERCHOVE, *evolucionista* ou *funcionalista*. Sem que se venha a incorrer em riscos da interpretação como desconstrução ou traição; mas na verdade, concentrando-se na sincronia entre Direito e evolução social.[176]

Por sua vez, o uso da interpretação restritiva das medidas penais segue a linha da estrita legalidade e do princípio da intervenção penal mínima. A gravidade das medidas que envolvem restrição de direitos exige que estejam previstas em lei, com suficiente justificação constitucional. Todavia, diante da convergência dos critérios interpretativos (gramatical, histórico e teleológico), não há se falar em obscuridade ou incongruência do texto normativo que autorize a aplicação deste critério. Torna-se claro o sentido da norma, com fulcro tanto na *mens legis,* quanto na *mens legislatoris*; aliás, o brocardo latino não permite esquecer que *in claris cessat interpretatio*.

A respeito dos argumentos da corrente ampliativa não se pode concordar com a posição de MARCO ANTONIO DE BARROS que, ao iniciar o exame do sigilo das comunicações, assevera:

> *"*entendo ser manifesta a falha de redação na qual incorreu o legislador, pois a exceção autorizada por via judicial

[176] Acerca da capacidade do sistema constitucional de acompanhar as transformações naturais ocorridas na sociedade, *v.* C. RIBEIRO BASTOS, S. MEYER-PFLUG, *A interpretação como fator de desenvolvimento e atualização das normas constitucionais*, in V. Afonso da Silva (org.), *Interpretação constitucional*, São Paulo, Malheiros, 2007, pp. 145-164.

> deveria abranger todas as hipóteses de sigilo enunciadas no dispositivo e não apenas limitar-se à quebra das comunicações telefônicas. Melhor seria se o constituinte brasileiro tivesse buscado inspiração na experiência do Direito português (...)".[177]

É certo que o legislador constitucional poderia ter primado pela clareza ao prescrever a inviolabilidade das comunicações, seguindo o exemplo do art. 32, § 6º, da Constituição Portuguesa. Contudo, se não decidiu assim fazer, supõe-se haja uma qualquer justificativa para a opção. O postulado do legislador racional, premissa metodológica para a interpretação, não nos permitiria raciocinar de outra maneira.

Há razões para crer que a justificativa está na acentuada preocupação de assegurar as liberdades individuais, característica marcante do processo de redemocratização do Estado brasileiro pós-ditadura. O primado de afirmação dos direitos da pessoa humana, marco da superação de arbítrios ainda tão recentes em nossa História, sustenta todo o texto da Carta Maior e prevê um avançado modelo de Estado de Direito.

Destarte, é evidente que o legislador pátrio quis dizer mais que o legislador português. E assim o fez. A postura garantista em matéria de inviolabilidade da correspondência e do telégrafo – em nenhum caso sujeita à relativização[178] – não permite instituir situação menos favorável ao cidadão.

A preocupação em apresentar sucintamente a tensão própria da hermenêutica jurídica entre intenção do legislador e evolução (recitação e invenção) baseia-se na tentativa de esclarecer quais os motivos de fundo que norteiam a interpretação. Igualmente, a exposição dos critérios interpretativos, sobre não se limitar a apontar aquele que nos pareça mais conveniente, tem justificativa na tarefa do jurista de nortear-se pela busca de clareza e coerência.

Uma vez mais afirme-se: o postulado sobre o qual repousa toda a atividade hermenêutica consiste na *racionalidade do legislador*; prescindir de sua presumida coerência leva-nos ao abandono do rigor formal e da técnica.

---

[177] *A busca da verdade ..., op. cit*., pp. 225-226.
[178] A assertiva será objeto de discussão no próximo item.

Diante da complexidade do texto normativo, a reação esperada é a busca por critérios dogmáticos de decidibilidade. Ainda que se mostrem insuficientes, sempre poderão ser aperfeiçoados. Aferir que a interpretação gramatical, histórica ou teleológica é indesejável, e escolher argumentos próprios e apartados do texto normativo, é incorrer na retórica persuasiva que, no mais das vezes, esconde interesses políticos.

Se a lei diferenciou o tratamento entre *comunicações postais e telegráficas* e *comunicações de dados e telefônicas* com o objetivo de instituir um maior grau de proteção, não se pode tolerar que na prática a proteção reste inócua. Ou seja, o legislador prescreveu a necessidade de autorização judicial para a interceptação da comunicação de dados, mas nem por isso autorizou que os dados em si, quando não veiculados por uma comunicação, possam ser utilizados na persecução penal, prescindíveis de autorização judicial. Como se verá, a reserva de jurisdição é requisito inseparável da busca por elementos armazenados em bancos de dados.[179]

A Excelsa Corte constitucional, em reiteradas ocasiões decidiu que a proteção do art. 5°, inciso XII da Constituição refere-se à *comunicação de dados e não aos dados em si mesmos, ainda quando armazenados em computador"*.[180] No entanto, a proteção do art. 5°, inciso XII tem necessariamente caráter mais amplo (*v.* itens 2.5 e 2.6). Uma vez concluída a comunicação, os dados digitais poderão ser apreendidos apenas por meio de autorização judicial motivada.

2.5. Comunicações postais e telegráficas

Segundo a definição do art. 7º, da lei nº 6.538/78, constitui serviço postal, o recebimento, expedição, transporte e entrega de objetos de correspondência, valores e encomendas, conforme definição regulamentar. O art. 47 da mesma lei consigna

[179] Situação preocupante diz respeito à prática da expedição de ofícios à Receita Federal e a outros órgãos visando obter informações, sobretudo, quando se pensa nos riscos de tornar-se *"ato rotineiro para impulsionar os processos em sua fase cognitiva e/ou executória."* (J. L. ARAUJO, *Intimidade*, *Vida Privada e Direito Penal*, São Paulo, Habeas, s/d, p. 111).
[180] *Cf.* R. Ext . 418416/SC, rel. ministro Sepúlveda Pertence, pleno, j. 10.05.2006.

que a correspondência é toda comunicação de pessoa a pessoa, por meio de carta, via postal, ou telegrama. Em acepção ampla, pois, a noção de correspondência engloba também o telégrafo.[181]

A comunicação telegráfica consiste na mensagem transmitida por sinal elétrico ou radioelétrico, ou qualquer forma equivalente, a ser convertida em comunicação escrita para entrega ao destinatário.[182]

Nesses termos, é possível afirmar que a expressão correspondência, em sentido abrangente, designa troca de mensagens escritas entre pessoas com conteúdo que interessa aos sujeitos comunicantes, transportadas pelo serviço postal e telegráfico nos termos da lei nº 6.538/1978. Como objeto da correspondência e da telegrafia, respectivamente, tem-se a carta e o telegrama.

Nos termos do parágrafo único do art. 69 da lei de Telecomunicações, a telegrafia constitui forma de telecomunicação, ou seja, forma específica de transmitir informações. Este fato, porém, não descaracteriza a idêntica proteção assegurada para as comunicações postal e telegráfica, vedada a aplicação da restrição prevista na parte final do art. 5°, inc XII, da Carta de Direitos.[183]

Na linha do item anterior, o tema da inviolabilidade das comunicações postal e telegráfica suscita divergências doutrinárias. De um lado, autores que sustentam a

---

[181] Anteriormente à lei nº 6.538/78 o critério de correspondência era dado pelo art. 36, do Decreto nº 29.151/51 (Regulamento dos serviços postais e de telecomunicações) que definia *"correspondência postal com caráter de mensagem"* como *"objeto que contém comunicação ou nota atual e pessoal, dirigida a outrem"*. O parágrafo único do mesmo dispositivo conceitua carta como *"todo papel, mesmo sem envoltório, com endereço e comunicação ou nota de caráter atual e pessoal"*, assim como *"todo objeto de correspondência com endereço, cujo conteúdo só possa ser desvendado por violação"*.

[182] Por sua vez, o Decreto nº 29.151/57 prescrevia no art. 142 que a correspondência de telecomunicação é *"a que se faz por meio de telegrama, rádio, telefonema, rádio telefonema e demais modalidades de comunicação a distância"*. Conforme o Decreto, o telegrama era a *"mensagem transmitida por sinalização elétrica ou radioelétrica, a ser convertida em recado escrito para entrega ao destinatário"*.

[183] O Código brasileiro de Telecomunicações diferenciou dois grupos de comunicações: a correspondência, composta basicamente pelas cartas; e as telecomunicações, que englobam comunicações de dados, telefonia e telegrafia. Este fato não altera, porém, o sistema de inviolabilidade do telégrafo. A proteção especial justifica-se pela grande semelhança da carta e do telegrama, ambos transmissores de mensagem escrita entre duas ou mais pessoas por intermédio dos correios. Um posicionamento que pretendesse separar as comunicações do art. 5º, inciso XII, segundo a natureza destas enquanto comunicação por correspondência e telecomunicações (telegrafia, dados e telefonia) não poderia prosperar porque a interpretação do dispositivo impede tal conclusão (R. B. C. MESQUITA, *A proteção da privacidade nas comunicações eletrônicas no Brasil*, São Paulo, Dissertação de Mestrado, 2009, p. 147).

possibilidade de restrição deste direito fundamental; de outro, o regime de defesa absoluta do direito.

Simplesmente propalar a relatividade de todo direito fundamental, para em seguida constatar a possibilidade de restrição quando em conflito com outro, certamente não dá conta da complexidade da questão. Esta postura institucionaliza a aplicação *a priori* do princípio da proporcionalidade como meio hábil para a restrição de qualquer direito fundamental.

Ao permitir apenas a interceptação das comunicações telefônicas e de dados na investigação ou instrução criminal, a Lei Maior instituiu dois níveis distintos de proteção. Com fulcro no mandamento constitucional, coube ao legislador ordinário regulá-las na Lei 9.296/96, com a previsão dos requisitos e limites destes meios de obtenção de prova.

Por sua vez, quanto ao sigilo da correspondência e do telégrafo, não foi estabelecida qualquer reserva de lei para disciplinar a matéria. Neste caso, não há negar que a preservação da liberdade de comunicação e privacidade dos sujeitos de direitos detém aqui caráter mais abrangente de proteção.[184]

Não se nega a possibilidade de restrição de um direito fundamental em face da necessidade de resguardar outro direito de mesma estatura constitucional. No entanto, o argumento de que a inviolabilidade das comunicações (CF, art. 5°, inciso XII) cede em favor da defesa da segurança social (CF, art. 5°, *caput*) e da incolumidade das pessoas (CF, art. 144) para permitir a interceptação da correspondência, não é correto.

A restrição a um direito fundamental[185] podem ser enquadrada em duas hipóteses: expressa ou tácita.

---

[184] Em caráter excepcional, o sigilo das comunicações postais e telegráficas pode ser suspenso durante o estado de sítio e de defesa (CF, art. 136, § 1º, alíneas *"b"* e *"c"*).

[185] Segundo a teoria dos princípios, as medidas restritivas de direitos fundamentais violam *prima facie* o âmbito de proteção; tais limitações necessitam de justificação constitucional e conformidade ao princípio da proporcionalidade. ROBERT ALEXY diferencia duas situações: quando o direito já contém a indicação de seus próprios limites ou restrições e aquela outra em que não estão previstos. Os instrumentos de controle destas atuações estatais lesivas de direito são a reserva de lei orgânica; a garantia do conteúdo essencial dos direitos fundamentais; a motivação da limitação do direito e o princípio da proporcionalidade. A posição privilegiada

Em primeiro lugar, a própria Constituição prevê situações em que um direito poderá ser limitado, tal como disposto na parte final dos incisos XI e XII, do art. 5°, da Carta Federal. Nesses casos o direito comporta a indicação de seus limites ou restrições. Esta *restrição expressa* (por meio de reserva legal[186]), relativa à área de proteção do direito fundamental, ocorre sem descurar da máxima preservação do direito intervindo.

A limitação pode também advir da finalidade de compatibilizar um direito individual a outros bens coletivos, em dada situação não estipulada previamente pelo constituinte. Tem-se, pois, a *restrição tácita* do direito fundamental. Em face da ausência de reserva legal que autorize a limitação do direito, a restrição se dá com base na colisão entre direitos fundamentais.

A colisão entre princípios constitucionais há que ser excepcional, de modo que *"a própria cláusula de imutabilidade de determinados princípios há de servir de baliza para evitar que, mediante esforço hermenêutico, se reduza, de forma drástica, o âmbito de proteção de determinados direitos."* [187] O juiz buscará a interpretação sistemática e a proporcionalidade para cumprir o mister do art. 93, inciso IX da Lei Maior, em respeito à garantia de motivação das decisões.

No entanto, as restrições expressa e implícita a um mesmo direito não podem coexistir em um caso concreto. Presente a reserva legal (simples ou qualificada), a única limitação possível será aquela decorrente de sua correta aplicação. Isto porque a natureza destes limites é alternativa; ou seja, o direito constitucional de colisão será possível tão somente nos casos dos direitos fundamentais sem reserva.[188]

O legislador constitucional, na parte final do art. 5°, inciso XII, previu a possibilidade da interceptação telefônica e de dados, mas apenas para a investigação e

---

ocupada pelos direitos fundamentais restringe o alcance de normas limitadoras que atuam sobre eles. Os limites devem ser interpretados segundo o sentido mais favorável à eficácia e essência dos direitos. O caráter de princípio da norma de direito fundamental reafirma sua natureza como mandado de ponderação (*Teoría de los Derechos Fundamentales*, 2ª ed., trad. Carlos Bernal Pulido, Madrid, Centro de Estudios Políticos y Constitucionales, 2008).

[186] As reservas legais expressas apresentam duas subespécies: na reserva simples a Constituição indica que o exercício de um direito será na forma ou nos termos da lei (são exemplos os incisos XV e XVIII do art. 5º, da CF); na reserva qualificada o constituinte aponta o tipo, a finalidade ou meio de intervenção autorizados, como no art. 5º, XII, da CF (D. DIMOULIS, L. MARTINS, *Teoria Geral dos Direitos Fundamentais*, São Paulo, RT, 2006, p. 153).

[187] G. FERRERA MENDES, I. MÁRTIRES COELHO, P. G. GONET BRANCO, *Curso de Direito ...*, *op. cit*., p. 379.

[188] D. DIMOULIS, L. MARTINS, *Teoria Geral ...*, *op. cit*., p. 162.

instrução penal. A esta restrição expressa da lei não será lícito cumular outras de natureza implícita.

A diferenciação entre os modos de restrição de um direito fundamental – reservas legais simples, reservas legais qualificadas e direitos fundamentais sem reserva – expressa a intenção do legislador de atribuir maior ou menor grau de tutela a um direito. Se nas hipóteses de restrição expressa o legislador de antemão vislumbrou eventuais colisões entre direitos fundamentais, em outros casos, a consagração de um direito sem reservas assegura o maior grau de proteção ao direito.[189]

No presente caso, diante de limitação expressa do legislador, não há como sustentar a cumulação de restrições.[190] A assertiva constitucional sobre a inviolabilidade das comunicações postais e telegráficas é clara e pretende abarcar a totalidade das situações. Com maior razão os autores que inadmitem restrição à inviolabilidade destas modalidades de comunicação.

A harmonia e a complementariedade entre os princípios constitucionais norteiam a interpretação sistemática do texto constitucional. Antes de propugnar a relativização de qualquer princípio constitucional, há que se buscar atender ao máximo o mandado de otimização neles contido. O jurista deve avaliar se efetivamente está presente situação fática de conflitância entre direitos fundamentais, tão somente recorrendo ao exame da colisão entre mandamentos constitucionais em situações limite.[191]

---

[189] Há uma gradação, em ordem crescente, de proteção do direito: cláusulas expressas simples, cláusulas expressas qualificadas e cláusulas implícitas, *v.* D. DIMOULIS, L. MARTINS, *Teoria Geral* ..., p. 164.

[190] O Supremo Tribunal Federal, em caso referente à interceptação da correspondência do preso, entendeu possível a cumulação de restrições constitucionais para: *"proceder à interceptação da correspondência remetida pelos sentenciados, eis que a cláusula tutelar da inviolabilidade do sigilo epistolar não pode constituir instrumento de salvaguarda de práticas ilícitas"* HC. 70.814-5/SP, rel. Ministro Celso de Mello, j. 01.03.1999. A respeito do uso da proporcionalidade de forma parcimoniosa: *"a afirmação de que as proteções são absolutas foi abalada por situações concretas em que houve necessidade de resguardar valores maiores do que o sigilo das comunicações, assim, há de se concluir que é inevitável a utilização do princípio da proporcionalidade ou invocação da existência de justa causa para amenizar a rigidez das proibições constantes do inciso XII, do art. 5º, da CF"* (A. SCARANCE FERNANDES, *O polêmico inciso XII do artigo 5º da Constituição Federal*, Justitia, 64 (197), jul./dez., 2007, p. 21). Também L. F. TORQUATO AVOLIO partilha deste entendimento *" (...) diante de um problema a ser resolvido, pode-se lançar mão do princípio da proporcionalidade, legitimando-se, eventualmente – nos casos mais graves – a intrusão nos meios de comunicação diversos da conversa telefônica"* (*Provas ilícitas ...*, *op. cit*., p. 216).

[191] Não se analisará detidamente a questão dos direitos já conterem em si a definição de seu próprio conteúdo e extensão. Sobre os pressupostos das teorias interna e externa e a distinção entre suporte fático amplo e restrito, *v.* V. AFONSO DA SILVA, *Direitos Fundamentais*, 2ª ed., São Paulo, Malheiros, 2010; M. ZANOIDE DE

Advirta-se que o legislador constitucional vedou peremptoriamente a interrupção da comunicação postal e telegráfica entre os sujeitos comunicantes, mas permanece lícita a apreensão da comunicação já concluída. O texto da Lei refere-se ao "sigilo da correspondência", que é aquele próprio da comunicação por meio de cartas. Não está, portanto, vedada a medida de busca e apreensão das cartas e telegramas as quais o respectivo destinatário já tenha realizado a leitura.[192]

2.6. Correio eletrônico

O correio eletrônico, como já afirmado (*v.* item 1.5), caracteriza-se pela imaterialidade; velocidade e baixo custo de transmissão; possibilidade de enviar extensos conteúdos, e ausência de fronteiras físicas ou lógicas.

Na definição da Diretiva 2002/58/CE, o correio eletrônico é *"toda mensagem de texto, voz, sonora ou imagem enviada por meio de uma rede de comunicações pública que possa ser armazenada na rede ou no mesmo terminal do receptor até que este acesse o mesmo."*

A correspondência virtual poderá ser bidirecional (aquela em que temos apenas um emissor e um destinatário), ou multidirecional (dirigida a um grupo de pessoas), sendo que a primeira tem caráter acentuadamente íntimo.

Tanto a carta como o correio eletrônico são meios de difusão de ideias e pensamentos em que se empregam principalmente caracteres escritos (letras e palavras). No entanto, no primeiro caso, o suporte empregado para a comunicação é físico, enquanto no outro, eletrônico ou magnético.

MORAES, *Presunção de inocência no processo penal brasileiro: análise de sua estrutura normativa para a elaboração legislativa e para a decisão judicial*, São Paulo, Tese de Livre Docência, 2008, pp. 308-344.

192 Neste sentido *v.* A. SCARANCE FERNANDES, *O polêmico inciso ...*, *op. cit*., p. 17; G. DE S. NUCCI, *Código de Processo Penal comentado*, 9ª ed., São Paulo, RT, 2009, p. 533. Sobre a inviolabilidade absoluta da correspondência *v.* C. B. PITOMBO, *Da busca e apreensão no Processo Penal*, 2ª ed., São Paulo, RT, 2005, p. 256; J. F. MIRABETE, *Processo Penal*, 18ª ed., São Paulo, Atlas, 2007, p. 346; F. DA C. TOURINHO FILHO, *Manual de Processo Penal*, 9ª ed., São Paulo, Saraiva, 2007, p. 583.

Diverso também o canal de circulação da comunicação, ou seja, a forma de atuação dos operadores ou prestadores dos respectivos serviços. A transmissão física do envelope ou pacote difere sensivelmente da intervenção dos prestadores de serviço ou servidores. Estes responsabilizam-se pelo destino e êxito da comunicação, principalmente, pela viabilização dos meios tecnológicos para a entrega da correspondência e a conservação da comunicação do destinatário.

Conquanto distintas, correspondência física e correio eletrônico detém o mesmo objeto de proteção do direito. O caráter íntimo desta comunicação escrita, destinada a um receptor determinado, exige um regime de total reserva do conhecimento de terceiras pessoas.

Ainda que a Lei Maior não faça referência às mensagens de correio eletrônico, não há duvidar que constituam forma de correspondência e mereçam o mesmo grau de proteção. Consequentemente, a disciplina de regência da inviolabilidade das comunicações postais de igual modo se aplica às interceptações ou acessos a mensagens de correio eletrônico.[193]

Assim como a correspondência interceptada, o *e-mail* captado com base em monitoramento virtual não pode ser utilizado como prova processual. Nem mesmo a autorização judicial permitirá a restrição do sigilo das comunicações para esta finalidade, em razão da expressa vedação constitucional. A retenção das informações veiculadas por correio eletrônico não está autorizada; permitida apenas a sua apreensão no momento em que se encontre armazenada no computador do destinatário, desde que já tenha sido aberta.

Os *e-mails* colhidos em respeito ao direito material são fonte lícita de prova, admitida no processo criminal. A busca por fontes de provas em *e-mails* pessoais, especialmente nos casos de busca e apreensão (*v.* capítulo V), se faz necessária à medida

[193] Na tradição constitucional pátria a correspondência não se limitou a designar a carta. Lembre-se que as Constituições de 1891, 1934, 1937 e 1946 apenas genericamente previam o sigilo da correspondência, mas a doutrina sempre estendeu certa permeabilidade ao conceito: *"a correspondência que se protege é a postal, a telegráfica, e qualquer outra, epistolar, bem que não-postal"* (F. C. PONTES DE MIRANDA, *Comentários à Constituição de 1946 ...*, *op. cit*., p. 436). Com supedâneo na inviolabilidade da correspondência chegou-se a afirmar até o *"segredo da correspondência telefônica"* (Idem, p. 441).

que o correio digital pode ser utilizado como base de armazenamento de dados por parte de seu usuário.[194]

A respeito das mensagens de telefonia SMS, sujeitam-se ao mesmo regime próprio da inviolabilidade das comunicações telefônicas e de dados. Isto porque as mensagens de SMS transmitem-se segundo os mesmos padrões da comunicação telefônica (*v.* item 2.7), o que caracteriza diversidade de suportes técnicos se comparado ao correio eletrônico. Ademais, o caráter conciso e limitado das mensagens enviadas pelo sistema de telefonia, não autoriza inclui-las no regime mais protetivo instituído em favor da correspondência e do *e-mail*.[195]

2.7. Comunicações telefônicas e de dados

Neste momento, além de conceituar a comunicação de dados e a comunicação telefônica, impõe abordar duas questões controversas. A inviolabilidade dos dados diz respeito apenas à comunicação enquanto esteja em curso, ou também aos dados em si mesmos? E quanto aos dados de tráfego das comunicações, é lícita sua obtenção?

Como se viu, a expressão "no último caso" do art. 5°, inciso XII, da Carta Maior refere-se tanto à interceptação das comunicações de dados, como das comunicações telefônicas.

---

[194] Imprescindível a correta preparação profissional da perícia técnica para a coleta apenas das fontes de prova admitidas.

[195] Por outro lado, J. J. GONZÁLEZ LÓPEZ entende que os mesmo argumentos referentes aos *e-mails* são aplicados às mensagens de telefonia emitidas por meio do serviço SMS (*short message service*). Para o autor é possível diferenciar quatro situações a respeito da tutela da comunicação por *e-mails* e mensagens SMS associada ao respectivo direito em que estão amparadas: (a) aos correios e mensagens escritas mas não enviadas incide o direito à intimidade; (b) aos correios ou mensagens enviados mas não recebidos incide o direito à inviolabilidade das comunicações; (c) aos correios ou mensagens recebidos mas não abertos incide o direito à inviolabilidade das comunicações; (d) aos correios ou mensagens abertos e armazenados no computador (seja o servidor ou destinatário) incide o direito à intimidade (*Los Datos de Tráfico...*, *op. cit.* pp. 135-163). Nada obstante a classificação do autor auxilie a compreender a diversidade de situações, parece-nos que em alguns casos deve se falar na cumulação da incidência do direito à intimidade e à inviolabilidade das comunicações. Acrescentaríamos, portanto, à formulação de GONZÁLEZ LÓPEZ, que em cada um destes momentos incide preponderantemente o direito por ele destacado, mas sem prejuízo da tutela do outro direito.

O regulamento geral aprovado pelo decreto nº 97.057, de 10 de novembro de 1988, que reformulou o Código brasileiro de Telecomunicações de 1962 (lei nº 4.417/62) definiu como telefonia a *"forma de telecomunicação caracterizada pela transmissão da voz e de outros sons audíveis"* (art. 6 º, 145 º).

Em sentido mais amplo, a comunicação telefônica designa a forma telecomunicativa de transmissão, emissão, receptação e decodificação de sinais linguísticos, caracteres escritos, imagens, sons, símbolos de quaisquer natureza veiculados pelo telefone estático ou móvel.[196]

A *comunicação de dados* pode ser definida como o processo de fluxo de informações entre dois ou mais comunicantes por intermédio de um aparelho capacitado. Os *dados* referem-se a todas as informações que indicam atributos específicos de pessoas, coisas ou eventos.[197]

Sobre o conceito de dados já se aludiu que não se faz referência a quaisquer dados pessoais (protegidos pelo CF, art. 5°, inciso X), mas apenas aos dados constantes em aparelhos eletrônicos.

O constituinte originário optou por tutelar a inviolabilidade da *comunicação* por correspondência e telegrafia, bem como a *comunicação* telefônica e os dados. Conforme entendimento da Excelsa Corte, esta proteção refere-se à comunicação de dados e não aos dados em si mesmos.[198]

No entanto, concluída a comunicação não cessa a necessidade de tutela jurisdicional para o conhecimento de seu conteúdo. Por esta razão, não há que diferenciar a proteção das comunicações e a proteção dos dados em si mesmos.

---

[196] U. LAMMÊGO BULOS, *Constituição Federal ...*, *op. cit*., p. 163.

[197] A lei nº 4.117/62, antigo código brasileiro de telecomunicações previa no artigo 6º, número 5, dados como *" (...) sinais, especiais, portadores de informações destinadas à execução automática de controles ou estudos de diversas espécies, veiculados através de linhas ou circuitos de telecomunicações"*. O regulamento geral aprovado pelo Decreto 97.057/88 substituiu o conceito anterior para classificar transmissão de dados como *"forma de telecomunicação caracterizada pela especialização na transferência de dados de um ponto a outro"*. A lei 9.472/97 ao impor novo regulamento não definiu especificamente as comunicações telefônicas e de dados, mas somente telecomunicações, opção que se coaduna com a intenção de não inviabilizar a inclusão de novas tecnologias.

[198] R. Ext., nº 418416/SC, rel. Ministro Sepúlveda Pertence, pleno, j. 10.05.2006.

Na análise do direito subjetivo à liberdade de comunicações (item 2.1.1) buscou-se refletir sobre o escopo de proteção na tradição constitucionalista brasileira. Como aferiu PONTES DE MIRANDA trata-se de uma *liberdade de não emitir pensamento* – direito exigível *erga omnes* de que não se tenha conhecimento das opiniões de uma pessoa.

Lembre-se que as Constituições anteriores a 1988 não previam genericamente a tutela da intimidade e da vida privada, tal como consta no art. 5°, inciso X, da Carta de Direitos. Até este momento não se falava que a Constituição, ao consagrar a inviolabilidade das comunicações, buscasse proteger apenas a comunicação enquanto não chegasse ao conhecimento do destinatário.

Com o advento da Constituição cidadã de 1988 não há razões para crer que a previsão constitucional dos incisos X e XII incida sempre autonomamente, prescrevendo direitos independentes entre si. Na verdade, a ampliação do rol de garantias consolida um acréscimo no espaço de defesa do cidadão.

A preservação das liberdades públicas depende diretamente da existência de meios eficazes para sua preservação. Ao elaborar distinção entre inviolabilidade das comunicações e inviolabilidade dos dados em si mesmos, para em seguida optar pela primeira, indubitavelmente esvazia-se a disposição constitucional, à medida que preservado *"somente o momento da comunicação contra qualquer tipo de violação, não o próprio sigilo da comunicação"*.[199]

Aliás, onde a lei não faz distinções, forçoso não as estabeleça o intérprete; concluída a comunicação não cessa a necessidade de tutela jurisdicional para o conhecimento de seu conteúdo. Por esta razão, não há que diferenciar a proteção das comunicações e a proteção dos dados em si mesmos.

Em face da liberdade de não emissão do pensamento é inadmissível que reste alguma hipótese em que possa o Poder Público obter informações da vida do cidadão sem a reserva de jurisdição. A harmonia e o equilíbrio entre os três Poderes não permite concordar com tal situação.

---

[199] A. SCARANCE FERNANDES, *O polêmico inciso ...*, *op. cit*., p. 19.

Para a obtenção dos dados, em respeito ao princípio democrático insculpido no art. 1º da Constituição Federal, se faz imprescindível a determinação judicial, não podendo quedar ao livre alvedrio do Poder Executivo ou de outros órgãos institucionais, a decisão sobre o conhecimento de informações caras à vida pessoal.

Para responder àquela outra questão, relativa aos dados de tráfego, é necessário fazer referência ao art. 1º, *caput*, da lei nº 9.296/96: *"A interceptação de comunicações telefônicas, de qualquer natureza, para prova em investigação criminal e em instrução penal, observará o disposto nesta lei e dependerá de ordem do juiz competente da ação principal, sob segredo de justiça"*.

Como se depreende, a quebra do sigilo pode ser tanto do conteúdo da comunicação, como dos respectivos dados de tráfego. A própria redação do dispositivo não permite outra conclusão ao utilizar a expressão *interceptação de comunicações telefônicas de qualquer natureza.*

Destarte, lícita a quebra de sigilo da comunicação referente aos dados em poder da operadora (data e horário da chamada, número de telefone chamado, duração do uso, valor da chamada, localização geográfica do aparelho).

E não se sustente a impossibilidade desta extensão com o argumento de se tratar de exceção a uma garantia de direito fundamental, pois os dados externos constituem parte integrante do processo comunicativo. O conhecimento daquele com quem se comunica, a duração da comunicação e a frequência com que é realizada são informações inseparáveis do objeto de proteção do direito.[200]

Em favor do segredo dos dados de tráfego das comunicações telefônicas em curso e dos dados de comunicações concluídas incide preponderantemente o art. 5°, inciso XII, que prevê que apenas por intermédio de autorização judicial será possível a quebra do sigilo. A obtenção dos registros telefônicos (assim como da

[200] Nada obstante a lei permita a obtenção dos dados externos da comunicação mediante a autorização judicial, o dispositivo não esclarece em quais hipóteses e condições isto ocorrerá.

correspondência, telégrafo e dados de comunicações concluídas) é possível desde que haja ordem judicial.[201]

Pensando-se no exemplo dos dados de comunicações eletrônicas, a pertinência deste posicionamento fica evidente. Em uma sociedade que se comunica interativamente, travando no entorno digital incontáveis comunicações cotidianas, é inimaginável que todas estas informações possam ser obtidas dispensada a autorização judicial.

A violação do sigilo da comunicação telefônica pode ocorrer por meio da interceptação, escuta ou gravação clandestina. As hipóteses serão vistas com a devida atenção no capítulo 4, estudadas juntamente às modalidades de intervenção nas comunicações eletrônicas. Diante da necessidade de quebrar o sigilo de dados ou telefônico, não é qualquer autorização judicial que viabiliza a obtenção desta modalidade de prova. O magistrado deve demonstrar que nenhum meio de obtenção de prova seria hábil para lograr o mesmo resultado, inclusive asseverando a ineficácia de outras diligências investigativas.

A decisão judicial, como se verá nos próximos capítulos, deve atender uma série de condições legais: pressupostos, requisitos, limites, a exigência de que a prova não possa ser obtida por outros meios disponíveis, devidamente motivada.

Tenha-se em consideração que a interceptação telefônica e de dados ocorre justamente nas situações limite, em que os fatos e o direito apontem para a acentuada probabilidade da prática delitiva grave e irreparável (*v.g.* nos casos de criminalidade organizada). É inconcebível que se torne meio de obtenção de prova diuturno. Assim, a decisão judicial que autorizar a obtenção de prova por este meio padecerá de ilicitude se não realizado minucioso escrutínio da legalidade e proporcionalidade da medida.

---

[201] *Cf.* V. GRECO FILHO, *Interceptação telefônica ...*, *op. cit*., pp. 9-10. Sobre a exigência de quebra por ordem judicial, *v.* HC 70.814-5/SP, rel. Ministro Celso de Mello, primeira turma, j. 24.06.1994. Há posicionamentos também em sentido contrário, *v.* L. F. TORQUATO AVOLIO, *Provas ilícitas: interceptações telefônicas, ambientais e gravações clandestinas*, 4ª ed., São Paulo, RT, 2010; G. H. BADARÓ, *Direito Processual Penal*, tomo I, Rio de Janeiro, Elsevier, 2008, pp. 279-280.

2.8. Sigilo das comunicações e processo penal

A inviolabilidade das comunicações constitui direito subjetivo que não se submete a modulações ou graus de atuação. A simples ingerência não consentida de terceiro no âmbito do direito constitui violação a um direito de natureza constitucional. Não há que se avaliar a relevância da informação como reflexo da vida pessoal, ou sopesar a existência de prejuízo para o titular do direito; a este cidadão confere-se direito de reação e tutela.

Malgrado o direito à inviolabilidade das comunicações reste consignado na generalidade das Constituições, inconteste que os meios de intrusão na esfera pessoal se fazem cada vez mais efetivos. O progresso tecnológico potencializa os riscos da devassa da vida particular por inúmeros meios: grampos telefônicos, micro-câmeras, micro-gravadores, veiculação de informações na imprensa, geo-localização, serviços de mensagens de telefonia instantânea (SMS), dentre outros.

Ademais, é certo que na atual sociedade industrializada[202], uma pessoa convive em inúmeras agremiações: de cunho profissional, familiar, religioso, esportivo e educacional. Não resta dúvida acerca da legitimidade da pretensão de controlar as informações referentes a si próprio, a fim de preservar a exclusividade dos informes que o titular pretende manter restritos a si ou a um determinado círculo social.

O sigilo constitui instrumento hábil de proteção da confidencialidade da informação; diferentemente do segredo, conteúdo da informação. Em tal contexto, para que venha caracterizada a violação do sigilo deve haver conhecimento e divulgação do segredo, sem a respectiva autorização.[203]

ANTONIO SCARANCE FERNANDES adverte sobre os muitos percalços na busca pelo equilíbrio entre segurança e preservação de direitos no processo penal, neste passo árdua a tarefa da quebra do sigilo, que depende de uma:

---

[202] Sobre a transformação da sociedade rural em sociedade industrializada e a variedade de ambientes sobre os quais transita o indivíduo, *v.* L. G. CASTANHO DE CARVALHO, *Processo Penal e Constituição: Princípios Constitucionais do Processo Penal*, 4ª ed., Rio de Janeiro, *Lumen Juris*, 2006, pp. 47-50.
[203] A. SCARANCE FERNANDES, *Processo Penal ...*, *op. cit*., p. 91.

> *"justa ponderação entre o interesse público na realização da quebra para a consecução de prova e o interesse privado de quem é submetido à investigação ou ao processo criminal"*.[204]

Com efeito, qualquer posicionamento fervoroso de ampla permissividade para a quebra dos sigilos pessoais, com o escopo de coibir práticas criminosas, há que ser veementemente refutado pela exigência de proteção contra as invasões nas esferas pessoais, toleradas apenas em hipóteses de grande excepcionalidade. [205] Imprescindível, enfim, reconhecer o equilíbrio entre eficiência e garantismo na persecução penal, como medida para o tratamento do sigilo.[206]

Em matéria de interceptação admite-se o uso de prova obtida mediante quebra de sigilo das comunicações de outro processo. Nos processos de natureza criminal em que haja crime punido com reclusão não se questiona o uso da prova emprestada, pois a própria lei nº 9.296 (art. 2º, inciso II) autoriza a interceptação nos casos de ilícitos apenados com esta modalidade de pena. Ainda que para os delitos sujeitos à cominação de sanção de detenção ou prisão simples o mesmo argumento não se aplique, tem prevalecido o entendimento de que após a produção da prova inexiste tutela do sigilo das comunicações. Como o direito constitucional à vida privada já fora violado de forma lícita, não haveria razão para sustentar o desrespeito da Constituição Federal por via reflexa.[207]

Ao estabelecer a reserva legal o legislador não se limitou a exigir que a restrição ao âmbito de proteção do direito fosse prevista em lei (reserva legal simples), mas também descreveu as condições especiais e os fins a serem perseguidos ou os meios a serem utilizados (reserva legal qualificada). Destarte, o texto constitucional admitiu apenas a obtenção da prova para fins de investigação criminal e instrução processual penal, vedada a utilização para autorizar interceptação em investigações de caráter administrativo-disciplinar ou associada a propositura de ações de improbidade.[208]

---

[204] *O Sigilo Financeiro ...*, *op. cit*., p. 457.
[205] Idem, p. 457.
[206] *Cf.* A. SCARANCE FERNANDES, *Reflexões sobre as noções de eficiência e de garantismo no processo penal*, in A. Scarance Fernandes, J. R. Gavião de Almeida, M. Zanoide de Moraes (coords.), *Sigilo No Processo Penal*, São Paulo, RT, 2008.
[207] O mesmo argumento tem embasado o uso da prova emprestada também em processos de natureza não criminal (A. SCARANCE FERNANDES, *O polêmico inciso..., op. cit.*, pp. 16-17).
[208] Idêntico o posicionamento dos autores G. FERREIRA MENDES, I. MÁRTIRES COELHO, P. G. GONET BRANCO, *Direito Constitucional ...*, pp. 343-344.

2.9. Entorno digital e comunicação de dados

Ao transitar pela rede mundial de computadores, de uma página a outra, o internauta pode imbuir-se da sensação de intimidade, segredo e absoluta solidão – como se de fato ninguém fosse testemunha do seu rastro virtual *(clickstream)*. A falsidade desta impressão, no entanto, é patente.

A utilização da comunicação eletrônica pressupõe uma legítima expectativa de intimidade; ou seja, a faculdade do cidadão de usar pacificamente os sistemas informáticos, resguardado das invasões não autorizadas de terceiros.[209] No entanto, as atividades cotidianas na *web*, ainda que digam respeito aos setores mais restritos da vida privada, não estão livres da intromissão de terceiros. Isto porque, uma tal expectativa de solidão não se compatibiliza plenamente com os inúmeros instrumentos de monitoramento[210], filtros e ferramentas interativas que são realidade na *web*.

O usuário dificilmente tem conhecimento da imensa quantidade de informações compartilhadas diuturnamente no entorno digital, pois são frequentes operações de tratamento automático e invisível, realizadas geralmente com o emprego de *cookies*[211] e *spywares*[212]. Por óbvio, a facilidade com que estes recursos digitais franqueiam acesso a conteúdos do usuário, sem seu conhecimento, não se coaduna com o direito à proteção de dados.

---

[209] E. STERN, *El sentido de la privacidad, la intimidad y la seguridad en el mundo digital: ámbitos y limites*, in Cuaderno del Instituto Vasco de Criminología, n. 21, San Sebastián, 2007, p. 186.

[210] As técnicas de cessão, compartilhamento ou cruzamento de dados são também conhecidas como *profiling* ou *dataminig*.

[211] O *cookie* é um arquivo de texto pelo qual os servidores fazem com que o navegador grave no *hardware* do computador informações sobre os acessos virtuais. Quando o usuário acessa novamente um site da *web*, os dados são reenviados ao servidor, proporcionando informação atualizada sobre o computador. Os servidores, por meio deste expediente, gravam dados do usuário relativos a suas preferências para a visualização de páginas, nome, senha, produtos de interesse, tempo dedicado a cada tema, assim como as transações realizadas. A preservação da autodeterminação informativa reclama tutela ainda ausente na legislação pátria, sobretudo, a exigência de que as empresas sejam claras e transparentes com o usuário para que este tenha conhecimento e possa optar clara e conscientemente sobre instalação de um *cookie* em seu aparato eletrônico. É aceitável que o *cookie* seja espécie de contraprestação aos serviços oferecidos, sendo a aceitação do usuário o requisito necessário para o compartilhamento destas informações com o prestador de serviços.

[212] Programas espiões que, uma vez instalados, permitem angariar informações e rastrear as atividades do usuário. O emprego destes expedientes facilita o controle discreto de atividades rotineiras como a navegação e a troca de correspondência eletrônica.

O internauta deve estar ciente de que a *internet* supera a distinção existente entre os habituais modelos de comunicação. Usualmente, a natureza destes é de dois tipos: privados ou de comunicação bidirecional-interpessoal (*v.g.*, telefone ou *fax*) e meios de comunicação de massa ou de comunicação unidirecional (entre um centro emissor inteligente e uma variedade de receptores passivos). Na *internet*, a tradicional diferenciação entre sistemas de comunicação social e meios de comunicação social dilui-se à medida que os usuários podem ser simultaneamente emissores e receptores da informação.[213]

TREJO DELARBE sustenta a existência de ao menos três grandes diferenças em relação à comunicação tradicional. A *interatividade*, que permite ao usuário ser espectador das informações veiculadas na *web*, sem prejuízo de efetivamente participar deste intercâmbio. Em segundo lugar, a *diversidade de localização* das fontes de propagação das mensagens veiculadas, pois, diferentemente de outros meios de comunicação, os emissores não se concentram em umas poucas empresas ou instituições. Por fim, a *acessibilidade*, exemplificada pelos baixos custos de participação na *internet*, em comparação a outros meios de informação como o rádio ou a televisão.[214]

Em especial, a noção de *interatividade* é muito elucidativa do caráter reticular da comunicação na *internet*: o recebimento e retransmissão da informação é, por vezes, instantâneo para todos os envolvidos neste processo.

Não se pretende sustentar que a extrema dificuldade de oferecer níveis irrepreensíveis de segurança no intercâmbio de informações na *internet* justifique tolerância ou permissividade no uso de dados pessoais sem o consentimento do titular. Indispensável, por óbvio, a observância de todos os princípios já expostos anteriormente (*v.* item 2.1.2).

O que se quer realçar é a natureza interativa e multidimensional da rede; características que reduzem as atividades próprias do agir mais íntimo do ser humano. O internauta, apenas em situações específicas – visita a *sites* que evidenciem

[213] Como assevera E. MORÓN LERMA, usuários de *internet* podem falar ou escutar de maneira intercambiável. É possível que um receptor torne-se emissor e produtor de conteúdos, espontaneamente, ou mediante o reenvio de conteúdo de terceiros (*Internet y Derecho..., op. cit*., p. 117).
[214] *Apud* E. MORÓN LERMA, *Internet y Derecho..., op. cit*., p. 118.

opções políticas, sexuais, ideológicas, crenças ou saúde pessoal – o fará como exercício da *intimidade* em sentido estrito.

Em outros casos, aquele que consente em divulgar informações a um terceiro – seja um *site* de relacionamento, cadastro ou troca de mensagens –, afirma não se tratar mais de objeto digno de absoluto e completo segredo. Não se está mais na esfera da intimidade (*Intimsphäre*), pois o compartilhamento pressupõe o conhecimento do outro.

Os usuários necessitam conhecer os riscos a que se sujeitam na *internet*, para assim resguardar a segurança pessoal no ambiente digital. Como ferramenta de defesa, o internauta dispõe atualmente da criptografia – método que consiste na descaracterização do código comunicativo por meio de algoritmos, de modo que apenas aqueles que conheçam a técnica utilizada (ou a senha) possam decodificar o texto. As principais vantagens da criptografia são o incremento da confidencialidade, integridade e autenticidade da informação.[215]

Outra forma de autoproteção consiste na navegação anônima. A falta de confiança do titular em relação à destinação de seus dados pessoais legitima o interesse de valer-se desta técnica. O cenário virtual, propício a violações da confidencialidade das informações, obriga a adoção de posturas que ocultem hábitos de navegação e pautas de comportamento do internauta.

[215] Os sistemas de segurança na *internet* cada vez mais se mostram eficientes. Os *programas de encriptação* permitem a modificação da linguagem natural (o significante) para uma linguagem chave que impossibilita a transcrição por quem desconhece a chave. Os *filtros* são programas seletivos que bloqueiam o acesso a certos documentos e permitem ao próprio usuário escolher os critérios para o conteúdo visitado na *internet*. As *firewalls*, sistema de segurança que impede a transferência de imagens ou dados da *internet* a um computador, estabelecem serviços previamente escolhidos e excluem os demais. Os *certificados digitais* estão voltados a identificar as partes intervenientes em uma transação comercial na *internet* com a máxima rapidez e segurança. As chamadas *cyiberpolícias* são equipes de especialistas em localização de pirataria informática e planejamento de programas de defesa, em face da criminalidade informática. Alguns países, como o Brasil, possuem estas unidades especiais. No segundo semestre de 2010, as Forças Armadas inauguraram seu primeiro Centro de Defesa Cibernética (CDCiber), que reúne cerca de cem oficiais do Exército. A atuação se faz em dois níveis: defesa nacional (no qual as Forças Armadas têm papel preponderante) e segurança nacional (como força auxiliar). O Centro visa proteger primordialmente as redes militares e governamentais, mas também pode contribuir para preservar as infraestruturas de informação como um todo. (http://www.estadao.com.br/noticias/nacional,exercito-se-arma-para-defender-o-espaco-cibernetico brasileiro,729291,0.htm?p=2, acesso em 18 jun. 2011, h. 20:40).

CAPÍTULO III: CONCEITO E CATEGORIAS DE DADOS DIGITAIS

3.1. Conceito

O *dado digital* constitui a informação[216] de estrutura numérica e imaterial, processada por sistemas computacionais, voltada a desempenhar uma função e representada em diversos formatos informativos (textos, imagens, áudio e vídeo). Denomina-se documento eletrônico o agrupamento de dados digitais gerados, transmitidos ou conservados por meio de computador ou rede telemática.[217]

Segundo o art. 1º, *b*, da Convenção sobre *cyber* criminalidade, do Conselho da Europa, em vigor desde 1º de julho de 2004, dado informático é *"qualquer representação de fatos, informações ou conceitos em forma suscetível de processamento em um sistema informático, incluindo um programa capaz de permitir um sistema informático de desenvolver uma função."*

Ainda que à luz da Ciência Informática o conceito de dado informático não seja idêntico ao de dado digital, para os fins desta Dissertação os termos serão

[216] Os conceitos de *dado* e *informação*, embora não sejam idênticos, serão tratados nos limites deste trabalho como sinônimos. O caráter mais abrangente da noção de dado consiste no fato de ser uma informação em potencial: apenas quando o dado é comunicado torna-se informação. No Direito europeu a expressão *'personal data'* é preferida no lugar de *'personal information'* porque constantes ameaças à privacidade originam-se a partir da acumulação de dados antes mesmo que sejam transformados em informação (I. WALDEN, *Computer crimes and digital investigation*, New York, Oxford University Press, 2007, p. 14). Ademais, a informação é o objeto de estudo de ramo autônomo do conhecimento – a *Tecnologia da Informação* – consistente na administração, manutenção e gestão da informação, através de dispositivos e equipamentos para o acesso, operação e armazenamento dos dados, de forma a gerar informações para tomada de decisão. Há também um sentido sociológico de estudo, segundo o qual a revolução tecnológica iniciada pelo computador privilegia a ideia de transferência da fonte de poder do proprietário de terras, indústrias ou empresas, para o controle de informação.

[217] A lei nº 11.419, de 19 de dezembro de 2006, que dispõe sobre a informatização do processo judicial assegura no art. 11: *"Os documentos produzidos eletronicamente e juntados aos processos eletrônicos com garantia da origem e de seu signatário, na forma estabelecida nesta Lei, serão considerados originais para todos os efeitos legais"*.

empregados como sinônimos. Não se faz oportuno adentrar na problemática específica deste tema.[218]

3.2. Categorias

Esclarecida a noção de dados digitais, insta conceituar suas principais modalidades.

Em atenção ao nível de reserva da informação, há três modalidades distintas: *dados sensíveis*, *dados pessoais em sentido estrito* e *dados públicos*. Esta classificação situa-se no contexto dos dados pessoais em geral, independentemente do suporte em que sejam veiculados.

No âmbito das novas tecnologias da informação, especificamente quanto à natureza dos dados comunicados, é possível diferenciá-los em *dados de conteúdo* e *dados de tráfego*. Estes últimos, também denominados dados externos das comunicações, subdividem-se em *dados indubitavelmente de tráfego*, *dados eventualmente* de tráfego e *dados afins*.

3.2.1. Dados pessoais: dados sensíveis, dados pessoais em sentido estrito e dados públicos

Os dados pessoais correspondem "*a qualquer referência ou descrição objetiva que diga respeito a uma pessoa singular e que submetidos a tratamento permitam alcançar informações acerca da sua vida.*"[219]

[218] Apenas a título elucidativo, observe-se que a noção de dado digital tem uma abrangência maior ao remeter diretamente à noção de suporte digital (numérico) como unidade constitutiva da informação veiculada. Dado digital é uma noção mais técnica para todos aqueles dados que não têm suporte em um computador (como os dados informáticos), caso das mensagens de SMS, dados do aparelho de GPS, entre outros.

Toda informação numérica, alfabética, gráfica, fotográfica ou acústica suscetível de apreciação por uma pessoa, e que seja capaz de identificar outra pessoa se consubstanciará em dado pessoal. A perfeita coincidência entre um dado e uma pessoa não é exigível, mas sim que a identificação possa ser alcançada a partir de esforços razoáveis.

Como exemplos pense-se no nome, sobrenome, número de telefone, número do documento de identidade (RG), número do cadastro pessoal de pessoa física (CPF), domicílio, profissão, afiliação a grupos políticos ou associações e etc.[220]

Nos arquivos ou bancos de dados informáticos, deve sujeitar-se a controle (ingresso e manutenção) a informação privada de um titular, consistente no exame da pertinência dos informes solicitados, em face do objetivo perseguido.[221]

Desde já, ressalte-se que os dados relativos à intimidade em sentido estrito constituem dados sensíveis ou supersensíveis, concernentes à origem racial, às opiniões políticas, preferências partidárias, convicções religiosas, saúde e orientação sexual.

É certo que uma tal conceituação ampla não diferencia a multiplicidade de dados existentes, à medida que nem todos são dignos da mesma proteção. Para tanto, oportuno diferenciar, segundo a teoria das três esferas, a conexão entre os dados e as esferas íntima, privada e da vida social. Em consonância com a teoria, os dados pessoais classificam-se em dados sensíveis (ou personalíssimos), dados pessoais em sentido estrito (ou não sensíveis) e dados públicos.

As informações sensíveis são aquelas ligadas ao núcleo mais íntimo e secreto da personalidade, conhecida no Direito alemão como *Intimsphäre* ou *Intimacy* no Direito anglo-saxão.[222] Os dados pessoais em sentido estrito situam-se na *Privatsphäre*

---

[219] S. COSTA, *A Proteção de Dados ...*, *op. cit.,* p. 281.

[220] A este rol acrescente-se todas as informações relativas a um internauta: endereço de *e-mail*, dados disponibilizados nos *sites* de relacionamento, a direção de IP e os dados de tráfego.

[221] Como esclarece ROMEO CASABONA, a chamada intimidade informática subdivide-se em dois aspectos que, embora individualizados, são também convergentes: liberdade e identidade informáticas. O controle quanto à exatidão, pertinência, atualização, destino e uso dos dados pessoais por parte do interessado individualiza a esfera de proteção da identidade informática (*Tendencias actuales ...*, *op. cit.*, p. 170).

[222] Aos dados habitualmente apontados como sensíveis (religiosos, étnicos, políticos) forçoso incluir os dados genéticos, como é o caso do DNA (ácido desoxirribonucleico). Atente-se que alguns Estados europeus (*v.g.* Reino Unido, Áustria, Alemanha, Suécia, Suiça e Espanha) recentemente editaram leis instituindo bancos

(esfera privada), noção próxima à de vida privada, que delimita as relações familiares e pessoais.[223] Os dados públicos seriam expressão da *Individualsphäre* (esfera individual), que afeta aspectos como a honra e a imagem da pessoa, elementos constitutivos da personalidade e vida social do indivíduo.[224]

Como desdobramento do direito à autodeterminação informativa tem-se firmado o entendimento doutrinário voltado ao *não tratamento informatizado de dados sensíveis*. Assim, a problemática situa-se nas controvérsias sobre a viabilidade do consentimento expresso do titular dos dados permitir o armazenamento de informações referentes a convicções filosóficas ou políticas, filiação partidária ou sindical, fé religiosa, vida privada, origem étnica, saúde e vida sexual.

Há autores que entendem que diante do consentimento do titular, a tutela dos dados sensíveis como parcela da intimidade perde sua justificação. À vista da aquiescência do titular, os dados referentes à esfera da intimidade (*Intimsphäre)* transitam

---

públicos de dados genéticos, com vistas a um futuro arquivo genético europeu. A finalidade principal dos bancos de dados é identificar os autores de crimes particularmente graves. A reflexão sobre a necessária tutela do direito à intimidade retorna a ordem do dia, sobretudo para impedir que tais informações sejam sucessivamente utilizadas para controlar a microcriminalidade (C. FANUELE, *Dati genetici e procedimento penale*, Milano, Cedam, 2009).

[223] Exemplo de dados pessoais em sentido estrito, os dados bancários, financeiros ou fiscais, têm assegurado o sigilo nos termos da lei Complementar nº 105/2001. A respeito do *status* constitucional deste sigilo a jurisprudência não é unânime, *v.* MS 21729/DF, rel. ministro Marco Aurério, pleno, j. 05.10.1995. No STJ, por sua vez, reconhecido que o sigilo bancário, decorrente do art. 5º, inciso X, da CF, ainda que não seja direito absoluto, deve ser relativizado apenas mediante autorização judicial com fundadas razões (*v.* Rec. ord. em MS 8716/GO, rel. ministro Milton Luiz Pereira, primeira turma, j. 31.03.1998; Rec. ord. em MS 9880/PR, rel. ministro Vicente Leal, sexta turma, j. 25.04.2000; HC 25560/PB, rel. ministro Gilson Dipp, j. 18.11.2003). No STF, no julgamento do recurso extraordinário 215301/CE, rel. Ministro Carlos Velloso, segunda turma, j. 13.4.1999, prevaleceu que o Ministério Público não pode quebrar por si próprio sem interferência de autoridade judiciaria o sigilo bancário. A nosso ver, o art. 6º, da LC nº 105/01 padece de inconstitucionalidade, em face da impossibilidade de quebra do sigilo bancário pelo legislador infraconstitucional, sob pena de ofensa ao princípio do Estado Democrático de Direito (CF, art. 1º, *caput*) e em obediência ao princípio da harmonia entre os poderes do Estado. Nos dizeres de NELSON NERY JUNIOR e ROSA MARIA DE ANDRADE NERY: *"O que se poderia tolerar, em homenagem aos princípios constitucionais da proporcionalidade e da razoabilidade, é a quebra do sigilo bancário por ordem judicial, mas nunca por decisão administrativa do Poder Público"* (*Constituição Federal Comentada ...*, *op. cit*., p. 176). Atribuir à Receita Federal o livre acesso às contas dos contribuintes é violar a distribuição de competências entre os órgãos do poder: *"(...) não é o Estado-Administração que diz o direito, que garante as liberdades públicas. A tutela dos direitos do homem, aqui amplamente tomada, é missão conferida ao Judiciário, ainda mais no que tange ao controle dos atos ligados à privacidade"* (U. LAMMÊGO BULOS, *Constituição Federal ...*, *op. cit*. p. 161).

[224] J. MARTÍNEZ DE PISÓN CAVERO, *El derecho a la intimidad en la jurisprudencia constitucional*, Madrid, Civitas, 1992, p. 30.

para o setor da vida privada (*Privatsphäre).* Para tanto, não bastaria a tácita manifestação da vontade, devendo o consentimento mostrar-se expresso e inequívoco.[225]

Nesse sentido, se por um lado o consentimento do titular provoca alteração da esfera onde situados os dados, qualquer veiculação de tais informações por intermédio da navegação ou atividades de comunicação (bate-papo, *Voip*, *Messenger*...), situa estes informes fora da zona restrita da intimidade. Portanto, aquele que navega em páginas para consultar o tratamento de uma doença, ou compartilha informações pelos serviços de conversa instantânea, não estaria no exercício de atividades próprias do mais completo isolamento (*v.* item 2.3).[226]

No entanto, mais acertado o posicionamento que defende como regra geral serem os dados sensíveis objeto do mais acentuado nível de resguardo, subsistindo a proibição de armazenamento destas informações.

O titular dos dados poderá impedir a sujeição dos dados personalíssimos a tratamento informatizado, sendo necessário para tanto autorização legal, resguardadas as garantias de não discriminação. O âmbito de extensão do poder do legislador infraconstitucional para prever tais hipóteses persiste, porém, como uma das questões mais problemáticas a ser enfrentadas.

E não pode vingar o entendimento de que dados sensíveis tornados públicos perdem a justificação para a tutela do direito. A publicação não desobriga o consentimento expresso. Ademais, não se ignore que a partir da publicação são incrementados os riscos da interconexão de um banco de dados[227] com outros, situação que

---

[225] Segundo a teoria das três esferas, existe comunicação entre as distintas esferas concêntricas. Ilustrativamente, possível pensá-las constituídas por uma espiral, de forma que, por meio do consentimento do titular os componentes de uma zona podem passar a integrar outra. Há que atentar, também, a extensão das esferas não é idêntica de um sujeito para outro; tem caráter relativo, que obedece à categoria ou estrato social ao qual pertence um indivíduo, em atenção à popularidade ou notoriedade de que dispõe nos ambientes sociais, *v.* F. MORALES PRATS, *La tutela penal..., op. cit.,* p. 129.

[226] Conforme este entendimento os dados pessoais informatizados pertencem à seara da intimidade, *(i)* enquanto representem informações do mais absoluto segredo; *(ii)* desde que seu titular não haja permitido o tratamento informatizado de tal conteúdo, e que *(iii)* não sejam objeto de qualquer comunicação ou veiculação na *web* por parte do titular.

[227] Por *bancos de dados* entende-se o conjunto de informações relacionadas entre si que contem registros caracterizados por um contexto comum, ou seja, referindo-se todas às mesmas pessoas, coisas ou eventos.

pode trazer ao titular prejuízos ainda superiores se comparados à veiculação em suportes não informáticos.[228]

O legislador constitucional prescreveu ação específica para o conhecimento das informações pessoais presentes em certos bancos de dados – o *habeas data* – conforme o art. 5º, inciso LXXII, da Constituição Federal. O impetrante tem o direito de conhecer dados pessoais presentes em registros ou bancos de dados públicos ou governamentais, com o escopo de retificá-los, explicá-los ou contestá-los. As hipóteses de cabimento da ação constitucional constam no art. 7º, incisos I a III da lei nº 9.507/97.[229]

3.2.2. Dados de conteúdo e dados de tráfego

As comunicações eletrônicas pressupõem a transmissão de um sinal que veicula variadas informações, com o objetivo de fazer chegar ao receptor um conteúdo determinado. Nesse fluxo de informações por meio do entorno digital, desponta um aspecto que acresce complexidade ao processo comunicativo: não apenas os dados que o emissor pretende fazer chegar ao receptor são enviados, mas outros também, usualmente denominados *dados de tráfego*.[230]

A comunicação eletrônica depende do artifício técnico da intermediação, processo que demanda a colaboração de terceiros alheios aos interlocutores. Os operadores de comunicações eletrônicas, ou os servidores de *internet*, necessitam de uma série de dados para encaminhar a comunicação ao seu destino, assim como para identificar a procedência ou adequar a transmissão à qualidade do sinal.

---

[228] S. COSTA é veemente ao atestar a violação do direito à autodeterminação informacional sempre que se aproveitar do fato de dados tornados públicos para inferir o consentimento do tratamento informático de dados sensíveis (*A Proteção de Dados ...*, *op. cit*., p. 299).

[229] Sobre o tríplice aspecto do *habeas data* como remédio jurídico-processual de natureza constitucional que se destina a garantir: (a) o direito de acesso aos registros; (b) direito de retificação dos registros; (c) direito de complementação dos registros, *v.* Rec. ord. em *Habeas Data*, rel. Ministro Marco Aurélio, pleno, j. 19.09.1991.

[230] J. J. GONZÁLEZ LÓPEZ, *Los Datos de Tráfico..., op. cit.,* p. 48.

No contexto do processo comunicativo, os dados de tráfego representam, portanto, elementos acessórios ou externos das telecomunicações, ou comunicações eletrônicas, que permitem – independentemente do conteúdo veiculado – identificar sua origem, destino, momento e duração.[231]

No ordenamento pátrio ainda se encontra em estágio de aperfeiçoamento o tratamento legal do tema. Com este desiderato, o legislador deverá atentar ao provedor de serviços de transmissão eletrônica que, dispondo de acesso aos dados de tráfego e de localização, pode, sem a devida autorização, observar o comportamento do usuário (hábitos e preferências pessoais).[232]

A Convenção nº 185, do Conselho da Europa sobre *cyber* criminalidade, consagrou no art. 1º, alínea "*d",* a seguinte definição para os dados de tráfego: *"quaisquer dados informáticos relativos a uma comunicação por meio de um sistema informático como elemento de cadeia de comunicação, que indiquem origem, destino, rota, hora, data, tamanho e duração da comunicação ou o tipo de serviço subjacente"* (trad. nossa).[233]

Sublinhe-se que a definição fez referência somente às comunicações viabilizadas por meio de sistemas informáticos; excluídas, assim, as comunicações telefônicas.

A noção formulada pelo Conselho da Europa fomentou o debate sobre a pertinência do aprimoramento terminológico. A análise do elemento volitivo do emissor da comunicação representa um primeiro referencial para a reformulação do tema: o conteúdo refere-se àquilo que o emissor quis veicular (conteúdo material, em contraposição ao conteúdo formal).

---

[231] O Tribunal Europeu de Direitos Humanos, na decisão do caso *Malone* (j. 2 de agosto de 1984), reconheceu os dados externos da comunicação como componentes do conteúdo da comunicação *lato sensu* e, portanto, dignos de tutela do direito à inviolabilidade das comunicações. A decisão irradia as bases para o entendimento de que o processo de comunicação representa um plexo de informações que circulam junto da informação, razão pela qual estendido o âmbito de proteção do direito ao segredo das comunicações para incluir os dados de tráfego.

[232] Como os dados de tráfego apontam com exatidão as páginas da *web* visitadas, dados sensíveis podem ser revelados, tais como crenças religiosas, ideologias políticas e aspectos da saúde ou vida pessoal.

[233] O Projeto de Convênio do Conselho da Europa sobre crimes cibernéticos de 1997, aprovado em Budapeste no dia 23 de novembro de 2001, consolidou algumas alterações que resultaram na atual redação do art. 1º, alínea *"d"*.

Todavia, como será visto, três situações apresentam particulares dificuldades: quando os dados de tráfego adquirem *status* de parte material da mensagem (como nos serviços de valor adicionado)[234]; nos casos em que os dados de tráfego se refiram indiretamente ao conteúdo das informações; e diante da dificuldade de delimitar aquilo que o emissor realmente quis transmitir.[235]

Estas reflexões motivaram o Conselho da Europa, na redação da Diretiva 2002/58, a conceituar dados de tráfego de modo menos estrito: *"quaisquer dados tratados para efeitos do envio de uma comunicação através de uma rede de comunicações eletrônicas ou para efeitos da faturação da mesma."*

Além de acessórios e destituídos de conteúdo, outra característica que diferencia os dados de tráfego dos demais refere-se à sua funcionalidade. É possível apontar três critérios que orientam a tarefa de identificar a finalidade destes dados: *as externalidades* (envolvem a identidade subjetiva dos interlocutores – momento, duração e destino); *dependência temporal e funcional* (dados indicativos da origem, destino, rota, tempo, data, volume, duração ou tipo de serviço), e *monitoramento da comunicação* (percurso das comunicações telemáticas e dados de localização[236] da telefonia móvel).[237]

A adequada conceituação dos dados de tráfego perpassa pela compatibilização dos três elementos essenciais já referidos: conteúdo formal, funcionalidade e acessoriedade. Para tanto, ainda que se incorra no risco de uma definição em demasia abrangente, inevitável certa flexibilidade frente ao fenômeno tecnológico, vetor constante de transformações e desenvolvimento.

---

[234] O art. 2º, *"g"*, da Diretiva 2002/58, do Conselho da Europa, dispõe: *"Serviço de valor adicionado é qualquer serviço que requeira o tratamento de dados de tráfego ou dados de localização que não seja dado de tráfego, para além do necessário à transmissão de uma comunicação ou à faturação da mesma."* Segundo o considerando 18, da mesma Diretiva, *"constituem serviços de valor adicionado, por exemplo, os conselhos sobre as tarifas menos dispendiosas, a orientação rodoviária, as informações sobre o trânsito, as previsões meteorológicas e a informação turística."* Esclareça-se que por dados de faturação temos um conjunto de dados de tráfego voltados à finalidade de cobrar determinado serviço por parte de prestadores de serviços de comunicações eletrônicas.

[235] J. J. GONZÁLEZ LÓPEZ, *Los Datos de Tráfico..., op. cit.,* p. 52.

[236] Com base na Diretiva 2002/58, do Conselho da Europa, art. 2º, *"c"*, dado de localização é *"Qualquer dado tratado em uma rede de comunicações eletrônicas que indique a posição geográfica do equipamento de um usuário de um serviço de comunicações disponível para o público."*

[237] J. J. GONZÁLEZ LÓPEZ, *Los Datos de Tráfico..., op. cit.,* p. 52.

Cumpre transcrever a precisa definição de JUAN JOSÉ GONZÁLEZ LÓPEZ:

> *"os dados gerados ou tratados no curso de uma comunicação e que diferem do conteúdo material, entendido como tal aquela informação cuja transmissão voluntária do emissor ao receptor motiva a comunicação"* (trad. nossa).[238]

A proposição acima incorpora não apenas os componentes referentes ao trinômio *momento-duração-destino*, mas também, toda a variedade de informações que se destinem a facilitar o trânsito da comunicação e assegurar seu recebimento.

Em geral, as informações contidas nos dados de tráfego possuem caráter menos íntimo se comparadas aos dados de conteúdo material. Desse modo, os requisitos que satisfazem a adoção destas fontes de prova variam segundo a finalidade perseguida. Daí porque, pertinente aferir a proporcionalidade de uma e de outra medida diante do delito investigado.

Os dados de tráfego apresentam potencialidade informativa acentuada, capazes de revelar uma ampla gama de relações pessoais. A interconexão de informações de origem diversa pode conduzir a investigação a importantes conclusões relacionadas à localização do suposto autor e a relação deste com outros autores. Por tudo isso, é patente que os dados de tráfego incluem-se no âmbito de proteção do direito à proteção de dados pessoais.

3.2.2.1. Dados indubitavelmente de tráfego

Com o escopo de reconhecer os dados que dispõem de características semelhantes, em atenção às particularidades de cada modalidade, é possível apresentar a

[238] *Idem.,* p. 62.

seguinte diferenciação: *dados indubitavelmente de tráfego*, *dados eventualmente de tráfego* e *dados afins*.

Situam-se na primeira categoria os dados que constituem um artifício técnico do qual depende o processo comunicativo. Referem-se, em especial, aos caracteres acerca da *origem*, *destino*, *rota*, *momento*, *duração*, *volume* e *modalidade* da comunicação.

O significativo referencial representado por estes caracteres, como se viu, consta na própria definição adotada pela Convenção nº 185 sobre *cyber* criminalidade, bem como na Diretiva 2002/58/CE, do Conselho da Europa.

Cada modalidade de comunicação eletrônica tem suas especificidades quanto à *origem*. O número de telefone corresponde ao dado de *origem* da telefonia de rede móvel ou fixa. Para o acesso à *internet*, o *correio eletrônico* e o *Voip*, o dado de origem é a identificação do usuário. Em outros casos, como a navegação[239], será a direção de protocolo de *internet* (IP), ou identificação similar de uma habilitação de comunicações para a qual um provedor presta serviços.

O *destino,* o *momento* e a *duração* da comunicação, a exemplo da *origem*, dependem da respectiva modalidade comunicativa. Os números escolhidos pelo emissor e aqueles para os quais as chamadas são transmitidas nas hipóteses de desvio ou transferência correspondem ao *destino* da telefonia de rede fixa ou móvel; para o correio eletrônico e para o *Voip* será a identificação do usuário ou o número de telefone do destinatário de uma chamada pela *internet*, respectivamente. O momento e a duração podem ser conhecidos pela data e hora do início e do final da comunicação para a telefonia; a hora de conexão e desconexão para o correio eletrônico e serviço de *Voip*; e a identificação e direção de IP do usuário armazenada pelo provedor de acesso quando se tratar de navegação na *internet*.

[239] Sobre o caráter da navegação como modalidade de comunicação eletrônica, *v.* item 1.5.

3.2.2.2. Dados eventualmente de tráfego e dados afins

Apenas ocasionalmente os dados de localização terão natureza de dados de tráfego, pois também é possível que sejam o próprio conteúdo material da comunicação.

Segundo a Diretiva 2002/58/CE, consideram-se dados de localização os tratados pelos operadores de comunicações eletrônicas a fim de encontrar, dentro do espectro radioelétrico, os equipamentos de telefonia móvel, ainda que não esteja em curso uma comunicação.[240]

O sistema de telefonia móvel permite determinar a localização de um telefone ligado, mesmo que não utilizado para a finalidade de comunicação.[241] Como ressalta PÉREZ GIL os dados de localização são pressupostos para a comunicação mediante telefonia móvel, sem eles seria impossível realizá-la; mas a localização não deriva necessariamente de uma ato de comunicação.[242]

Assim, em uma acepção mais alargada constituem dados de localização aqueles *dados pessoais que informam a posição espacial de um objeto ou sujeito a que se encontrem vinculados, a partir dos quais é possível traçar todos seus deslocamentos*.

O GPS constitui um sistema de navegação que engloba toda a superfície terrestre. Trata-se de um recurso amplamente utilizado nos serviços de telefonia

---

[240] O considerando 14, da Diretiva 2002/58/CE, esclarece: *"Os dados de localização podem incidir sobre a latitude, a longitude e a altitude do equipamento terminal do utilizador, sobre a direção de deslocação, o nível de precisão da informação de localização, a identificação da célula de rede em que o equipamento terminal está localizado em determinado momento e sobre a hora de registo da informação de localização."* Aparelhos eletrônicos móveis podem identificar a localização de vítimas e de suspeitos de crimes.

[241] A terminologia dados de localização, contudo, não é exclusiva da telefonia móvel.

[242] *Los datos sobre localización geográfica en la investigación penal*, in E. Pedraz Penalva (coord.), *Protección de datos y proceso penal*, Madrid, La ley, 2010, pp. 346. O autor também ressalta que o uso generalizado da telefonia móvel permite enormes possibilidades de controle sobre os portadores de telefones. A maior capacidade de acúmulo de informações do sistema GSM favorece a criação de dados permanentemente atualizados por meio do chamado *Call Data Record* (CDR). Por meio do sistema cada uma das comunicações realizadas é registrada, preservados os números de telefone de origem e destino, os dados técnicos da comunicação e o tempo e modalidade de serviço. Há o registro também das coordenadas geográficas de onde se originou a comunicação e do respectivo destinatário. Mesmo sem a realização de uma chamada é possível conhecer a localização do usuário de telefone celular por meio da base de dados VLR (*Visitor Location Register*), precisando inclusive o deslocamento físico da pessoa (Idem, pp. 343-344).

móvel. Ao acompanhar a comunicação em curso, os dados do sistema de posicionamento global apresentam natureza de dados de localização.[243]

Em face da necessidade do conhecimento de certas informações por parte dos operadores de comunicação eletrônica, os dados de localização podem estar voltados a viabilizar o processo comunicativo. Nesse caso os dados de localização produzidos em decorrência da chamada serão dados de tráfego, uma vez que acessórios ao conteúdo material da comunicação.[244]

Por outro lado, o enquadramento dos dados de localização poderá ser como dados distintos dos de tráfego. É o caso dos chamados dados de *stand by,* informações que poderiam viabilizar uma comunicação se assim desejasse um determinado emissor, mas que não se encontram em processo de transmissão. Basta mencionar um telefone celular que simplesmente por estar ligado deixa rastro digital que pode permitir a individualização do usuário. Assim, os dados decorrem não de uma comunicação, mas sim do funcionamento normal do aparelho, que uma vez ligado permite a localização do portador.

As operadoras poderão oferecer ao consumidor produto derivado do tratamento de certos dados, técnica que cria outra modalidade de dados de localização, usualmente denominada *serviços de valor acrescentado*. Estes serviços, que podem ter por finalidade realizar localização (*Location based services, LBS*), são capazes de situar com precisão um aparelho geograficamente.

Nesse caso, é indispensável o inequívoco consentimento do usuário, bem como a disponibilização de um meio simples e gratuito de recusar temporariamente o

[243] O GPS representa o principal artefato para a localização geográfica na atualidade, sem prejuízo de outros aparelhos que em um futuro próximo possam se tornar mais frequentes, como é o caso do leitor facial. Outro instrumento útil para a investigação dos delitos é o dispositivo que permite a leitura e registro automatizado das matrículas dos veículos. A partir da imagem de uma câmera e com o auxílio de um *software* é possível ler e interpretar as letras e números da placa, armazenando e registrando as informações. Estes dados podem ser contrastados automaticamente com outras bases de dados, como por exemplo relativa a veículos de interesse policial.

[244] Os dados tratados por operadoras de comunicações com o fim de localizar no espectro radioelétrico os terminais de telefonia móvel denominam-se também dados de cobertura.

tratamento de dados de localização. Além disso, a medida deve ser realizada apenas durante o tempo necessário para a prestação do serviço.[245]

Os dados referentes aos serviços de valor acrescentado podem dizer respeito à localização de um sujeito comunicante ou outra modalidade de prestação de serviço. Não resta dúvidas, porém, que independentemente da finalidade destas informações, serão classificadas como dados de tráfego ou dados de conteúdo, a depender da intenção do emissor de pretender transmitir ao receptor seu conteúdo.

Durante o lapso temporal de uma comunicação telefônica, os dados de localização integram a chamada, razão pela qual a eles é estendida a aplicação do âmbito de proteção do direito à proteção de dados e do direito à inviolabilidade das comunicações. Tratando-se de dados de localização em *stand by* há que se falar na incidência dos direitos à intimidade (CF, art. 5º, X) e à proteção de dados pessoais.

Os *dados afins* integram categoria diversa de dados digitais, cujo principal exemplo diz respeito aos dados de inscrição. Cuida-se da informação pessoal do usuário coletada no intuito de contratar a prestação de quaisquer serviços de comunicação. A conexão telefônica ou de *internet* dependem da celebração de um contrato com o operador de comunicações eletrônicas ou provedor de *internet*, segundo a qual serão disponibilizados dados como o número de identidade e o número da conta do assinante.[246]

Os dados deste modo confiados ao receptor não são comunicação transmitida em tempo real. Se tomadas por base as definições expostas anteriormente, com relação aos dados de tráfego e eventualmente de tráfego, notaremos não estar presente fluxo constante de informações entre emissor e receptor, mas apenas prévia veiculação de dados, requisitos para que se estabeleça a prestação do serviço de comunicações eletrônicas. Esta circunstância faz com que os dados de inscrição não se caracterizem como externos à comunicação.

---

[245] J. PÉREZ GIL, *Los datos sobre…, op. cit.*, p. 352.

[246] No memorando explicativo da Convenção de Budapeste os dados de inscrição são classificados como: *"qualquer informação contida em formato informático ou em qualquer outra forma, mantida pelo provedor de serviços, relativa a usuários de seus serviços, distintos dos de tráfego ou de conteúdo, segundo os quais se pode estabelecer: o tipo de serviço de comunicação usado, as previsões técnicas adotadas para ele e o período do serviço; a identidade do usuário, direção postal ou geográfica, telefone ou outro número de acesso, informação sobre contas correntes e pagamento, disponível com base em um contrato de serviço ou acordo; qualquer outra informação sobre o lugar de instalação de equipamentos de comunicação disponíveis com base em contrato de serviços ou de um acordo"* (trad. nossa).

3.3. Fontes de provas digitais e persecução penal

As novas técnicas informáticas de investigação devem ser implementadas em consonância ao modelo acusatório[247] propugnado pela Carta de Direitos de 1988. O processo penal constitucional, voltado à observância de direitos fundamentais, não se sujeita a eventuais tecnicismos de uma novel *forensic Science*. A presumida autonomia sistemática dessas operações é resultado de um viés descontrolado de introdução de ciência no processo, que se aproveita da recepção acrítica das fontes de provas digitais por parte dos órgãos judicias, com o objetivo da imposição de argumentos de autoridade.[248]

Qualquer áurea de infalibilidade dos instrumentos digitais não se compatibiliza com o primado do livre convencimento motivado do julgador. Por este viés, inoportuna a comparação do processo com laboratório científico, com vistas à obtenção de uma assim propugnada verdade material.[249]

É certo que os temas concernentes à *computer forensic* (*v.* item 1.4.2) suscitam inéditos questionamentos, mas também são numerosos aqueles que resgatam discussões antigas sob uma nova roupagem. Para estes casos em que o ineditismo limita-se ao emprego do entorno digital, uma vez que a situação envolve direitos e deveres já

---

[247] Como características do sistema inquisitório, GIULIO UBERTIS enumera: intervenção judicial *ex officio*; liberdade do juiz na coleta da prova; sigilo de todo o processo (interno e externo); evidente disparidade entre os poderes do juízo-acusador e do imputado; prática de encarceramento provisório do imputado. Por outro giro, no sistema acusatório: liberdade de acusação reconhecida ao ofendido pelo crime, aos seus parentes ou mesmo *"quivis de populo"*; exclusão da liberdade do juiz na colheita de provas; publicidade de todo o processo; paridade de posições entre as partes, enquanto o juiz atua como moderador impassível e individualizador das questões relevantes objeto de decisão; liberdade do imputado como princípio até a sentença irrevogável de condenação (*Argomenti di Procedura Penale*, Milano, Giuffrè, 2002, pp. 6-13). Sobre os traços principais dos sistemas inquisitório e acusatório, *v.* M. A. C. ZILLI, *A Iniciativa Instrutória do Juiz no Processo Penal*, São Paulo, RT, 2003, pp. 38-40.

[248] Na linha da assim denominada *junk Science*.

[249] A inoportuna dicotomia entre verdade formal e material apenas afasta a sensibilidade do jurista para a única verdade possível: aquela atingível, contingente e construída à luz das autênticas garantias de verdade, quais sejam, o contraditório e a imparcialidade do julgador (N. GUZMÁN, *La Verdad en el Proceso Penal*, Buenos Aires, Editores del Puerto, 2006). Nesse sentido, GIULIO UBERTIS propugna como característica do sistema processual inquisitório, a busca pela verdade real, pois *"non vingono, (...) limiti all' attività euristica del giudice."* (*Argomenti di Procedura ...*, *op. cit.,* pp. 6-7). O mesmo autor assinala que no modelo acusatório há uma complexa rede de regras de exclusão porque certos tipos de aquisição probatória são *"ritenute inammissibili* (...) *l'accertamento della verità può essere perseguito solo attraverso un'opera di bilanciamento con gli altri valori che entrano in gioco nel compimento delle attività processuali"* (*Idem*, pp. 10-11).

previstos no ordenamento, o Direito estadunidense consagrou a expressão *"old wines in new bottles"*[250].

Pense-se que o investigado não estará obrigado a fornecer à autoridade policial o *password* específico de acesso do computador pessoal ou as chaves para a decodificação dos arquivos sujeitos à criptografia. Outra conclusão não seria possível, pois a Carta Maior preserva ao investigado o direito de permanecer em silêncio (art. 5º, inc. LXIII), fundamento legal que também assegura não ser o réu obrigado a favorecer a própria incriminação (*nemo tenentur se detegere*).[251]

A polícia judiciária e o Ministério Público também não poderão obter coativamente a senha. Aliás, antes de qualquer sugestão ao investigado para que forneça espontaneamente o código, imprescindível a informação do seu direito de não responder. Da ofensa a este direito material resultará a ilicitude da prova coletada, bem como, a ilicitude por derivação de todo o plexo probatório obtido em decorrência da violação.

Uma relevante diferenciação do direito anglo-saxão diz respeito às noções de *computer-derived evidence* e *computer-generated evidence*. No primeiro conceito – alvo de atenção específica nos próximos dois capítulos – o computador é objeto da atividade probatória, ou seja, os dados presentes em seu interior serão analisados para a apuração do delito. No outro caso, temos o instrumento informático como objeto de uma operação demonstrativa, na qual o suporte eletrônico é empregado para realizar a simulação de fatos[252] que incorporam acentuada complexidade.[253]

A busca por dados digitais de caráter pessoal que sirvam à investigação criminal cresce à medida que as condutas delitivas são frequentemente perpetradas por intermédio do entorno digital. Os desafios para o Direito Processual Penal contemporâneo são inúmeros, dentre os quais: a regulação da atuação da polícia judiciária na investigação,

---

[250] *Cf.* S. W. BRENNER, *Cybercrime Metrics: Old wine, new bottles?*, Virginia Journal of Law & Technology Association, v. 9, n. 13, University of Virginia, 2004, in www.vjolt.net/vol9/issue4/v9i4_a13-Brenner (acesso em 17.03.2012, h. 14:40).

[251] L. LUPÁRIA, *Investigazione Penale e Tecnologia Informatica*, Milano, Giuffrè, 2007, pp. 159-160. No direito estadunidense, a mesma solução foi apontada pela doutrina especializada, com fundamento na quinta emenda à Constituição que consagra o *"privilege against self incrimination"* (E. CASEY, *Digital evidence and computer crime: forensic science, computers and the internet*, New York, Elsevier, 2011, p. 115).

[252] A reconstituição do crime por meio de computador não tem previsão normativa no ordenamento pátrio; trata-se de meio atípico de produção de prova.

[253] L. LUPÁRIA, *Investigazione Penale ..., op. cit.,* p. 146.

a apuração de crimes perpetrados por organizações criminosas, o combate ao terrorismo e o tratamento dos dados de tráfego.

3.3.1. Aproveitamento dos dados digitais na persecução criminal

As novas tecnologias têm favorecido a automatização da informação e a criação de bancos de dados pessoais, cuja função tem aporte investigativo, mas também escopo de prevenção de futuros ilícitos. Esta estrutura voltada à obtenção de informações foi associada pela doutrina especializada a uma modificação de postura na investigação criminal. Sob uma pretensa atuação repressiva contra a criminalidade institui-se a chamada investigação proativa – frente de atuação preventiva –, de alcance muito superior aos meios tradicionais e desacompanhada de normativa específica.[254]

Em face da necessidade de adaptação para o combate de novos fenômenos criminológicos, as técnicas de investigação multiplicam-se sensivelmente nos ordenamentos de muitos Estados. Expedientes como vídeo-vigilância, controle de comunicações eletrônicas, processamento de dados, análise de DNA e vigilância eletrônica, passaram a ser incorporados.[255]

Por outro lado, os modernos sistemas eletrônicos de captação e armazenamento de informações representam riscos de um protagonismo acentuado da polícia, incompatível com a atribuição diretora da autoridade judicial no curso das investigações. Um paradigma pré-processual de supremacia da autoridade policial, baseado no emprego clandestino das novas técnicas de investigação, compromete tanto o direito constitucional de defesa como a licitude na coleta da fonte de prova.

---

[254] J. PÉREZ GIL, *Investigación Penal y nuevas tecnologías: algunos de los retos pendientes,* in Revista Jurídica de Castilla y León, n. 7, out., 2005, p. 216.

[255] A Corte europeia de Direitos do Homem, no julgamento do caso *Klass* (1978), pacificou o entendimento sobre a necessidade do sigilo na obtenção da prova criminal, afinal a natureza e a lógica de providências como a vigilância secreta demandam realização sem o prévio conhecimento do interessado (j. 6 de set. de 1978).

Conforme afirmado anteriormente, as novas tecnologias coadunam-se ao modelo processual acusatório, único de índole autenticamente democrática, no qual impera a divisão das tarefas de julgar e acusar, proscritos os amplos poderes instrutórios do magistrado e preservada a estrita legalidade dos meios de obtenção de prova. O devido processo legal, tradicional corolário de respeito a garantias constitucionais, não se compatibiliza com a mitigação do papel dos órgãos judiciais na investigação e com a falta de transparência das técnicas investigativas.

Inegável o interesse de toda a sociedade voltado à atuação da autoridade policial segundo os ditames da lei, justamente para que os elementos informativos coletados possam servir à instrução probatória. De rigor, portanto, o adequado aparelhamento e aperfeiçoamento científico da polícia para a superação de obstáculos criados pela tecnologia.

O rótulo de luta contra a criminalidade organizada[256] e contra o terrorismo[257], com frequência fundamenta restrições a direitos fundamentais e incrementa os riscos de invasão dos íntimos setores da vida pessoal. Particular atenção merece o emprego indiscriminado destas medidas à generalidades de delitos, inegável ameaça às liberdades individuais.

---

[256] A Colômbia é exemplo de recrudescimento legislativo no combate ao crime organizado em matéria de recuperação de informações na *internet* ou meios semelhantes. A apreensão de equipamentos destinados ao armazenamento físico de dados informatizados pressupõe: ordem emanada pela *Fiscalia*, sendo desnecessária a prévia autorização judicial; motivos razoavelmente fundados acerca da utilidade da diligência; apreensão pelo tempo necessário à captura dos dados e controle de legalidade a *posteriori* feito pelo juiz de garantias, no prazo de 24 horas (A. A. MENDES DE MACHADO, D. F. M. LEÃO DE SOUZA, O *Crime Organizado na Colômbia*, in A. Scarance Fernandes, J. R. Gavião de Almeida, M. Zanoide de Moraes (orgs.), *Crime organizado: aspectos processuais*, São Paulo, RT, 2009, p. 108).

[257] No panorama internacional, o *USA Patriot Act*, assinado pelo presidente George W. Bush é o exemplo mais conhecido de normativa contra o terrorismo. Dentre o rol de medidas restritivas de direitos fundamentais encontram-se: incursão no segredo das comunicações; violação do segredo de dados; vigilância e uso de informações e agentes secretos; diligências secretas; regras probatórias extraordinárias; detenção em massa de estrangeiros; detenção de combatentes inimigos, e uso da tortura na aquisição de informações (F. R. BECHARA, L. F. DE MORAES MANZANO, *Crime Organizado e Terrorismo nos Estados Unidos da América,* in *Crime organizado...*, *op. cit*., pp. 178-182). No Reino Unido, o *Human Rights Act* de 1998 assegurou maiores efeitos às disposições da Convenção Europeia de Direitos do Homem. No entanto, o Ato de Poderes Investigativos de 2000 institucionalizou as modalidades de vigilância invasiva, a pretexto, como se sabe, de combater o terrorismo. O critério frequentemente apontado pelas Cortes inglesas de que a vigilância, com base na Convenção Europeia de Direitos do Homem, deve ser *"proporcional àquilo que busca encontrar"*, revela-se insuficiente e viola as garantias do investigado. Ademais, a própria redação do *Act* não se mostra clara e inequívoca em suas prescrições. Sobre a condenação do Reino Unido por práticas policiais de vigilância violadoras dos artigos 8º e 13, da CEDH, notadamente, o uso de aparelhagens de escuta e gravação em residências, *v.* Armstrong *vs.* U. K. (j. 16 /07/2002), Elahi *vs.* U. K. (j. 20/09/1996), Chalkley *vs.* U. K. (j. 12/09/2003) e Wood *vs.* U. K. (j. 16/02/2005).

No combate à criminalidade organizada e ao terrorismo é recorrente o tema da interceptação preventiva de dados digitais como meio de investigação. Trata-se de um meio de obtenção de provas anterior ao conhecimento da *notitia criminis,* usualmente respaldado em argumentos voltados à defesa social e à prevenção da atividade criminosa. A interceptação das comunicações eletrônicas depende, no entanto, da materialidade do delito, desarrazoada qualquer justificativa baseada em possíveis comportamentos futuros do investigado. Não se pode confundir a prevenção do delito ou asseguramento de eventuais fontes futuras de provas com uma indesejada "guerra preventiva" ou "tutela antecipatória".

A necessidade de harmonizar os novos meios de investigação com o *due process of law* é desafiadora nos planos interno e internacional. A discordância entre os valores *liberdade* e *segurança*, mais uma vez na ordem do dia, exige o estudo detido das diligências de investigação destinadas à obtenção e ao armazenamento dos dados digitais, à luz do cotejo entre preservação de garantias constitucionais e eficiência da persecução.

O desenvolvimento de novas tecnologias não deve ser convertido em justificativa para a manutenção de deficiências no sistema penal ou para comprometer garantias historicamente afirmadas. O entorno tecnológico não altera a lógica processual penal: toda restrição a direitos fundamentais depende de previsão normativa e autorização judicial, vedadas invocações de caráter genérico.[258]

3.3.2. Utilidade dos dados de tráfego

Os dados de origem e destino podem ser de grande valia para a apuração do delito. A análise destes dados de tráfego serve como indício para aferir se o emissor da informação, seu receptor, ou ainda terceiros, mantêm relação com os infratores.

[258] Nas palavras de J. PÉREZ GIL, *"la irrupción de las nuevas tecnologías en la investigación penal no debe ser convertida, consciente o inconscientemente, en excusa o en coartada para acentuar hiperestésicamente carencias y deficiencias del sistema, abriendo peligrosos portillos" (Investigación Penal …*, *op. cit*., p. 214).

Desse modo, os dados referentes a um suspeito podem indicar outros, favorecendo inclusive a elucidação de uma complexa trama de relações pessoais entre os envolvidos.[259]

No entanto, a possibilidade de identificação do responsável por meio dos dados de tráfego é limitada. A direção de *IP*, *v.g.*, permite apenas revelar o computador utilizado, fator que pode não se mostrar suficientemente elucidativo se consideradas possíveis variações no uso de um número de IP (denominado IP dinâmico) ou o uso de ferramentas de navegação anônima. Ademais, se o identificado for parte integrante de uma rede de acesso à *internet*, que pode ser tanto empresa como organismo público, imprescindível a obtenção dos dados das pessoas que utilizam a rede local.

As dificuldades de identificação dos sujeitos envolvidos em uma comunicação telemática são complexas. É certo que não são raros os casos de uso de um computador por um número indeterminado de pessoas, como nos *cybercafés*, *lan-houses* e centros de informática. Ademais, a pessoa que utiliza o terminal pode ser outra diferente do seu titular, como na hipótese de alguém se valer do computador de outrem, prática frequente no ambiente profissional.

A identificação do usuário que acessa à *internet* pode ser inviabilizada também em razão da informação necessária não estar armazenada, ou no caso de ser falseada. O provedor de *internet*, ao contratar diretamente com o cliente, pode prescindir de dados relativos à conexão telefônica, não comprovando as informações fornecidas. Se os dados não forem autênticos ocorrerá acesso praticamente anônimo.[260]

O emprego de correio eletrônico anônimo é ainda mais frequente, tendo em visto que a revelação da identidade do emissor não é requisito para a criação do endereço eletrônico e para o exercício da comunicação.

Os dados de origem e destino unicamente considerados não permitem a localização geográfica do computador, mas somente a identificação do código de *IP*. A

[259] J. J. GONZÁLEZ LÓPEZ, *Los Datos de Tráfico..., op. cit.,* p. 84.
[260] Idem, p. 87.

partir deste número, no entanto, é possível descobrir o local em que se encontra o computador por meio de ferramentas específicas.[261]

A localização geográfica constitui etapa do processo de identificação de um sujeito, em alguns casos sucedida de diligências investigativas, tal como a vigilância do lugar em que se encontra o computador identificado.

Dados de tráfego que indiquem o volume, momento ou duração de comunicação são de menor valia para a identificação do agente ativo de uma conduta. Serão úteis se entrecruzados com outros dados pessoais, quando da combinação de informações resultar um significado particular.

A obrigação dos operadores de comunicações de arquivar dados de tráfego durante determinado lapso temporal (temporalidade), obedecidos critérios de necessidade e finalidade, não representa medida de investigação senão instrumento preventivo de asseguramento de eventuais fontes de prova. Todavia, não há justificativa para a conservação indefinida e apartada da existência de indícios delitivos.

Igualmente essenciais para as investigações penais os objetos que permitam localizar geograficamente seus portadores. A utilidade consiste na credibilidade de atestar o posicionamento exato de pessoas e objetos, as respectiva trajetórias, a frequência com que se encontravam em determinado âmbito espacial e os sujeitos que se situavam concomitantemente em um mesmo lugar. Estes indícios são dotados de acentuada precisão e, somados a outros elementos probatórios, favorecem a formação da convicção judicial.[262]

Os dispositivos de localização geográfica apresentam uma série de vantagens: possibilitam o acúmulo de vasto volume de informações, incomparavelmente superior à capacidade humana; recebem informações mesmo a distâncias consideráveis do objeto ou pessoa investigada; a observação da trajetória ocorre de maneira absolutamente oculta, sendo desnecessária presença física de agentes na operação.

---

[261] Há inclusive *sites* que realizam gratuitamente este serviço na *internet*, como é o caso do *IP Location Finder* (*http:* www.*iplocationfinder.com)*.
[262] J. PÉREZ GIL, *Los datos sobre ....*, *op. cit*., p. 308.

Os dados de localização poderão ser obtidos pela polícia no curso das investigações, ou por particulares que pretendam colaborar com a investigação ou que estejam obrigados por lei a colaborar com a justiça.

3.3.3. Dados digitais e modalidade delitiva

Impõe diferenciar duas modalidades delitivas distintas no entorno digital. Em primeiro lugar, os crimes em que o computador é utilizado como *longa manus* do criminoso, ou seja, instrumento para a própria consecução do delito. Este rol de condutas engloba, dentre outros, os furtos realizados com o uso do computador, os crimes sexuais contra crianças ou adolescentes, o uso de tecnologias avançadas por parte de organizações criminosas e a coação ou ameaça cometida com uso de comunicações eletrônicas.

Por sua vez, outros casos podem revelar que o computador não está diretamente vinculado ao cometimento do injusto penal, mas contém dados que refletem a atividade criminosa e podem ser úteis à elucidação dos fatos. A obtenção dos dados digitais será relevante também nesta hipótese, sobretudo, para vincular autor e vítima, bem como coautores e cúmplices, com base em comunicações eletrônicas. Trata-se de providência especialmente pertinente em crimes que atentem contra a integridade física (*v.g.,* homicídios, lesões corporais), onde a linha investigava se pautará pela busca de informações que demonstrem a atividade delituosa dos envolvidos.

Além da Informática constituir meio para a execução do delito, também é possível que o entorno digital seja suporte de informação para o cometimento do crime. Desse modo, com base em uma noção ampla de delito informático, todos os ilícitos poderiam constituir delinquência informática, desde que os dados digitais servissem para a obtenção de informação relevante por parte do criminoso.

Há casos em que a tecnologia constitui suporte para a prática do injusto, tanto em relação ao modo de cometimento específico do crime, como também para sua

difusão. Os delitos contra a liberdade sexual, a exemplo do que ocorre com a pornografia infantil na rede, ilustram bem estas situações.[263]

A pertinência do uso de novas tecnologias na investigação criminal é observável na quase totalidade dos ilícitos. Porém, mostra-se ainda mais proveitosa em certos delitos, como tráfico de drogas, oferta de conteúdos ilícitos através da *internet*, atentados contra a propriedade intelectual, crimes contra crianças e adolescentes, *cyberstalking*[264] e terrorismo. Isto principalmente em razão das peculiaridades da delinquência informática: celeridade e distanciamento para o cometimento do crime, com ampla possibilidade de ocultação e dificuldade probatória.

Para a elaboração de uma noção técnica de delito informático é necessário um enquadramento nos limites do critério restritivo. Assim, incluídas devem ser unicamente as hipóteses em que os sistemas informáticos aparecem como meio específico de execução do injusto, porque somente nestas hipóteses estão presentes as características que dotam de ineditismo os delitos vinculados à Informática.[265]

Os países que aderiram à Convenção de Budapeste sobre *cyber* criminalidade incorporaram um significativo rol de crimes informáticos. Não é o caso do Brasil, cuja legislação, no entanto, prevê alguns tipos penais com estas características: *(a)* divulgação na *internet* de fotografias pornográficas envolvendo menores de idade (ECA, lei nº 8.069/90, art. 241, *caput*); *(b)* interceptação informática ou telemática não autorizada (lei nº 9.296/96, art. 10); *(c)* violação de direitos de autor de programa de computador (lei nº 9.609/98, art. 12); *(d)* inserção de dados falsos em sistemas de informações (CP, art. 313-A); *(e)* modificação ou alteração não autorizada de informações (CP, art. 313-B); *(f)* divulgação de segredo, consistente em informações sigilosas ou reservadas, contidas ou não nos sistemas de informações ou bancos de dados da Administração Pública (CP, art.

[263] Em razão do bem jurídico lesionado, há casos em que as comunicações eletrônicas serão tanto objeto do delito como meio específico de cometimento. Nas violações contra os direitos à intimidade e à honra, as condutas variam entre a interceptação de comunicações, o apoderamento de correio eletrônico, a revelação de segredos, calúnias e injúrias. Neste sentido, os dados informáticos são essenciais para identificar e localizar os respectivos agentes ativos.

[264] *Cyberstalking* designa o comportamento repetitivo de perseguição e assédio via *internet*, baseado em ameaças que tenham o potencial de causar danos físicos ou morais à vítima.

[265] Os delitos informáticos podem ser classificados também sob a perspectiva de uma criminalidade em rede: *(a)* delitos de divulgação específica na *internet*; *(b)* delitos em que a *internet* é empregada como meio para a comunicação dos infratores (*v.g. e-mail*, *VoIP,* redes sociais); *(c)* delitos em que a *internet* serve como ferramenta delitiva virtual, por meio da qual se faz possível a prática de crimes fora da rede (sabotagem de dados, espionagem e furto de dados, dentre outros).

153, § 1-A); *(g)* utilização ou divulgação de programa de processamento de dados que permita ao sujeito passivo da obrigação tributária possuir informação contábil diversa daquela que é, por lei, fornecida à Fazenda Pública (lei nº 8.137/90, art. 2º, inciso V); *(h)* os crimes eletrônicos de natureza eleitoral (lei nº 9.504/97).[266]

3.3.4. Tese de acusação e de defesa: a garantia do contraditório

O contraditório, segundo um viés técnico-processual, está estruturalmente relacionado à noção de contraste bilateral entre tese e antítese. Como requisito para a substancial igualdade entre as partes processuais – a chamada paridade de armas – imprescindível, pois, a exposição das próprias razões e a sua refutação. Tais oportunidades de manifestação devem ser sempre efetivas, nunca limitadas a possibilidades mediatas ou puramente hipotéticas.

A produção de provas no marco do justo processo pressupõe como etapa prévia à sentença judicial a observância do contraditório assertivo e argumentativo, consistente na possibilidade de dizer e contradizer os fatos.[267]

Segundo uma perspectiva jurídico-política a garantia constitucional do contraditório (CF, art. 5º, inciso LV) consubstancia o método por excelência voltado ao descobrimento da verdade, não em forma unidirecional, mas por meio do confronto de hipóteses contrárias entre si que tentam prevalecer. Os escopos desta dialética processual voltam-se à consecução da justiça substancial e ao controle bilateral e recíproco dos riscos de abuso dos instrumentos processuais à disposição das partes.[268]

Ao mesmo tempo que se submete à prova a tese de acusação, oferece-se também o direito de refutá-la. Este método não é constituído sob a prerrogativa de

---

[266] *Cf.* M. A. DE BARROS, *Processo Penal Impulsionado pela Tecnologia: A Investigação Criminal Realizada com Novos Meios Tecnológicos e a Iminente Semi-Informatização do Procedimento Penal Anunciada pela Lei 11.419/2006*, São Paulo, Tese, 2008, pp. 58-59.
[267] M. CHIAVARIO, *Diritto Processuale Penale*, 5ª ed., Milano, UTET, 2012, pp. 27-28.
[268] L. P. COMOGLIO, C. FERRI, M. TARUFFO, *Lezioni sul processo civile*, 5ª ed., Bologna, Mulino, 2011, p. 70.

favorecer uma das partes em seu direito de defesa, vai além, à medida que se constitui como instrumento para o conhecimento dos fatos.[269]

A atividade investigativa realizada pela autoridade policial tem como escopo a descoberta de fontes de provas. Trata-se de reunir indícios que permitam aferir se determinadas condutas constituem atos típicos e qual o grau de culpabilidade do agente ativo. Posteriormente ao contraditório e à imediação judicial, as fontes de provas recolhidas constituirão elementos de convicção para a apuração dos fatos.

A identificação dos autores e das vítimas das condutas na rede mundial depende, em grande medida, da obtenção dos dados informáticos no ambiente digital. O mesmo será possível dizer das informações relativas ao crime quando usadas as comunicações eletrônicas como instrumento para tais práticas.

Nos delitos em que empregado o computador como suporte para a perpetração, inegável o interesse em utilizá-lo como fonte de prova. Da mesma forma, tais informações serão úteis para sustentar teses favoráveis ao investigado, na linha de uma assim denominada investigação defensiva.

A produção do elemento de prova se dá à luz da contraditoriedade de opiniões dos atores processuais na instrução processual. Se o contraditório assegura a igualdade entre os sujeitos processuais, é certo que a estes é assegurado o contato com a prova obtida pela via eletrônica.[270]

A fonte de prova deve estar acessível completa ou parcialmente, conforme sua relevância, mas sempre preservada a integridade do material obtido (em formato de documento digital ou devidamente transcrita). Faz-se necessário disponibilizar

---

[269] NICOLÁS GUZMÁN constata que o contraditório não é simples condição do direito de defesa, mas na verdade, estrutura do processo, autêntico sistema lógico de conhecimento para o descobrimento da verdade: *"(...) el mecanismo del contradictorio fue por mucho tiempo concebido simplemente como una garantía individual establecida en tutela del imputado, pero se hay olvidado lo que hoy ya no parece posible negar: que el contradictorio constituye el mejor medio para el conocimiento de la verdad"* (*La verdad...*, *op. cit*., p. 157).

[270] Sobre a participação das partes J. L. RODRÍGUEZ LAINZ sustenta três orientações: (i) a necessidade de um ato formal de conformação contraditória do material probatório; (ii) a efetiva colocação à disposição das partes da informação recolhida, com oferecimento da possibilidade de fazerem valer seus pontos de vista, e (iii) oportunidade às partes do exercício de iniciativas processuais (*Intervención judicial ...*, *op. cit*., pp. 359-360).

às partes a comunicação, em formato inteligível, dos dados objeto de tratamento, assim como de toda a informação relativa à origem dos dados.[271]

Tão logo cesse a necessidade de sigilo sobre a fonte de prova obtida, deverá ser franqueada às partes para que dela tenham conhecimento. A participação em igualdade de condições pressupõe a possibilidade de apresentar dúvidas sobre a licitude da medida e a credibilidade da prova.

O questionamento da veracidade ou integridade do documento eletrônico incumbe às partes. Por sua vez, o respectivo ônus probatório de demonstração da genuinidade (*v.g.* o fato de pertencer aquela voz a uma determinada pessoa) e da autenticidade (integridade do conteúdo da conversação atribuída a um dado sujeito) pertence ao órgão acusador.[272] Suscitada a dúvida razoável da defesa em relação a fiabilidade da fonte de prova, a realização da perícia esclarecerá a controvérsia.

A eficácia processual dos dados depende diretamente de procedimentos de autenticidade, integridade e inalterabilidade, sob responsabilidade do órgão responsável pelo tratamento dos dados (polícia, prestadoras de serviços e etc.). O contraste entre as teses poderá abordar questões como nível de segurança dos bancos em que situados os dados de localização, o registro dos operadores que tenham acessado aqueles dados e as respectivas operações técnicas realizadas.

3.4. Provas no ambiente digital

Elucidativa a classificação de GIOVANNI ZICCARDI em cinco características principais da fonte de prova digital,[273] particularidades que evidenciam sua

[271] Em caráter inédito a Convenção nº 108 do Conselho da Europa (1981) previu no *art. 8º b)*: *"Obter, em intervalos razoáveis e sem demoras excessivas ou altas custa, informações sobre os dados pessoais que lhe digam respeito, armazenados em arquivo automatizado de dados, bem como a comunicação desses dados de forma inteligível"* (trad. nossa).

[272] A paridade de armas não significa que os direitos e deveres das partes sejam idênticos. A disponibilidade a favor do órgão acusador de um aparato público voltado à realização do processo exige, em algumas situações, um balanceamento que reestabeleça o equilíbrio

[273] Nos países de *Common Law* consagrada a expressão *digital evidence*, que diz respeito a *"qualquer dado armazenado ou transmitido por meio de computador, que seja capaz de corroborar ou refutar uma tese*

natureza tanto sobre o aspecto estático (dados armazenadas no computador), como também sob o viés dinâmico (dados em rede).[274]

Em primeiro lugar, a busca da fonte de prova digital ocorre no contexto de *anonimato do autor*. Os indícios deixados em um computador podem ser extraviados ou modificados com facilidade, sendo numerosa a quantidade de suspeitos potenciais no ambiente digital.[275]

Há uma particular *dificuldade de identificação do crime,* em razão de ser menos evidente a natureza do evento criminoso, muitas vezes não percebido nem mesmo pela vítima. Um exemplo contundente deste desconhecimento é o chamado furto de informação dos dados relativos a um cartão de crédito *(account password)*. Ainda com a identificação de um equipamento como o utilizado para a prática do crime, frequentemente não se consegue apontar seu autor, ou seja, embora constatada a existência do crime não se poderá atribuí-lo a uma pessoa em concreto.[276]

A *filtragem e determinação das fontes de provas relevantes* mostram-se desafiadoras para o investigador, uma vez que as áreas geográfica e lógica do cometimento do crime são extremamente incertas, a evidenciar muitas provas em potencial.

A *vulnerabilidade das fontes de provas digitais* é acentuada, não raros os casos em que ocorre a contaminação do material probatório, tanto pelo mal uso dos

---

sobre a prática de um crime, ou que esclareça elementos determinantes do crime como a intenção do agente e o álibi" (E. CASEY, *Digital evidence ...*, *op. cit*., p. 7, trad. nossa).

[274] G. ZICCARDI, *Investigazione Penale ..., op. cit.,* p. 49.

[275] Quase todas as investigações informáticas se iniciam com a operação conhecida por *tracing*, técnica consistente em rastrear as atividades anteriores para individuar um dado que possa relacionar um fato a uma pessoa (*v.g.*, obter, a partir do endereço *IP,* o respectivo número de telefone fixo).

[276] Acrescente-se que para o cometimento do crime é desnecessária a presença física, sendo possível permanecer todo o tempo muito distante dos locais onde repercutem as consequências delitivas. O *iter criminis* pode ser executado em tempo muito breve, instantâneo, e longe do alcance ou controle do titular do computador. A facilidade com que os fatos podem ser encobertos também é acentuada: com o uso de *softwares* específicos modifica-se um programa para que realize uma atividade ilícita em benefício do autor e depois retorna-se ao estado anterior (L. REBOLLO DELGADO, *Derechos Fundamentales y Protección de Datos*, Madrid, Dykinson, 2004, pp. 187-188).

instrumentos digitais, quanto pelo insuficiente conhecimento do sistema e de suas funções próprias.[277]

Por fim, em função da fonte de prova digital ser solidamente constituída num sistema sequencial *(step by step)*, sua contaminação invalida todos os elementos de convicção dela oriundos.

Diante de um crime cometido em meio eletrônico não se pode recorrer à busca de provas físicas; a conduta virtual impossibilita, pois, a obtenção de um elemento tangível de prova. Desta maneira, em grande medida podem restar inviabilizadas estratégias tradicionais de obtenção de prova, como a oitiva de testemunhas, inspeções e buscas. O trajeto investigativo percorre os arquivos e dados digitais, com vistas à reconstrução dos fatos ocorridos.

A *computer forensics* exige, com frequência, a demanda ao administrador do sistema eletrônico de todas as informações correlatas a um determinado fato para que se possa obter o *clickstream* (*v.g.*, conta em servidor, ou endereço de *IP)*; em seguida, percorrido ao reverso o *iter criminis* no intuito de identificar-se o criminoso.

Os três passos principais da estratégia investigativa consistem em *(i)* colher as provas memorizadas no servidor de terceiros; *(ii)* buscar a identificação de onde provém o ataque; *(iii)* por último, a análise do computador do suspeito.[278]

Aspecto relevante concerne à irrepetibilidade da atividade de busca de fonte de prova digital, própria da *computer forensics*. A possibilidade de modificação dos dados digitais comporta decisivas consequências processuais, especialmente, quanto à

---

[277] O acompanhamento do procedimento *standard* de investigação segue a chamada continuidade probatória, sujeita a uma completa descrição das vária etapas, desde o momento da apreensão do dado até a sucessiva fase de conservação.

[278] G. ZICCARDI, *Investigazione Penale e Tecnologia ..., op. cit.,* p. 59. Com maior detalhamento, o processo de identificação de um criminoso no entorno digital pode ser dividido em quatro etapas: (i) identificação do endereço de IP, realizada por meio dos *arquivos de log* gerados pelo suspeito; (ii) relação entre o número de IP e o respectivo servidor, que se faz mediante *softwares* específicos que identificam a procedência do usuário; (iii) se o número de IP pertencer a uma empresa ou qualquer outro órgão onde haja muitos usuários compartilhando o mesmo número de IP, serão necessárias outras providências investigativas; (iv) por fim obtém-se dados pessoais do usuário armazenados no servidor de *internet*. É notável a importância dos *arquivos de log* para a identificação do usuário, autênticos rastros virtuais, fator que desencadeou a preocupação de diversos ordenamentos com a previsão legal de resguardo destes dados por prazos determinados.

necessidade de comunicação prévia à defesa para a designação de assistente técnico que acompanhe a produção do elemento de prova.

Impõe, contudo, afastar de plano um entendimento peremptório que sustente a irrepetibilidade da prova digital em todos os casos. Indispensável que a apreensão do dado digital e sua sucessiva análise não comportem alguma modificação dos arquivos originais. Por esta razão, sugere a doutrina especializada a realização da chamada cópia-clone (*legal imaging* ou *bit stream image*) do conteúdo presente no computador.[279]

Dois procedimentos igualmente importantes são a documentação e a autenticação.

A documentação permite o conhecimento da origem do dado e do respectivo tratamento. Do ponto de vista técnico, a aquisição de um dado deve modificá-lo o mínimo possível, sendo que toda alteração deve estar devidamente descrita. A autenticação é o processo de determinação da autenticidade de uma prova, segundo o qual se atesta que um documento eletrônico: (i) permaneceu inalterado; (ii) que a informação armazenada realmente é oriunda de determinada fonte; (iii) que informações relevantes como a data do documento são precisas.[280]

[279] A cópia-clone consiste em uma "fotografia digital", cuja credibilidade depende da idoneidade da operação de *computer forensics*, especialmente, no que respeita ao uso de *softwares* reconhecidos (como exemplo, o *"Encase"* da empresa *Guidance Software Inc*., utilizado pela maior parte das forças policiais na Europa e nos Estados Unidos da América) que garantam a adequação do procedimento técnico (L. LUPÁRIA, *Investigazione Penale ..., op. cit.,* p. 152). No Direito inglês fala-se na elaboração de três cópias: uma cópia para ser apresentada intacta como *evidence in court*, outra onde será realizada a análise e uma última oferecida ao investigado para que faça sua própria verificação. As imagens são aceitas como representação fidedigna do original, de forma que o uso das cópias-clone nunca foi questionado com sucesso nas cortes do Reino Unido. É vantajoso o fato desta técnica permitir que o aparato eletrônico seja devolvido ao seu proprietário, de forma a não prejudicar à vítima ou terceiros envolvidos (I. WALDEN, *Computer crimes ...*, *op. cit*., p. 213).

[280] E. CASEY, *Digital evidence ..., op. cit.*, p. 21.

CAPÍTULO IV – INTERVENÇÃO NAS COMUNICAÇÕES ELETRÔNICAS

4.1. Generalidades

A regulação da *internet* no Brasil tem como principal protagonista o Comitê Gestor da Internet no Brasil (CGI.br). A implementação dos projetos fica a cargo de órgão interno – o Núcleo de Informação e Coordenação do Ponto br – associação civil sem fins lucrativos, pessoa jurídica de direito privado. Como objetivos do NIC.br constam o registro de nomes de domínio sob o domínio de primeiro nível (DPN) ".br", a distribuição, promoção e manutenção dos endereços IP, bem como a gestão dos servidores e da rede para garantir boa operacionalidade de registro e manutenção dos domínios ".br".

O registro de domínios para a *internet* do Brasil ("Registro.br") constitui serviço que atribui um endereço ou bloco de endereço IP por periodicidade de doze meses. A partir do fornecimento de dados pessoais (nome, número de CPF, entre outros) e de pagamento, ao usuário (pessoa física ou jurídica) é atribuído um número IP e um nome de domínio registrado.

O titular de um domínio na *internet*, diante de qualquer conduta ilícita, tem condições técnicas de identificar o número de IP do usuário que acessou seu domínio. Este número poderá ser fixo ou aleatório; nesta última hipótese faz-se particularmente difícil a identificação do internauta responsável.

A lei não exige dos requerentes a domínio ".br", a elaboração e manutenção de um cadastro de usuários dos endereços *IP*. Também não há obrigação legal para os provedores em relação ao armazenamento dos registros de conexão ou *logs*, de modo que cada provedor decide por quanto tempo mantém as informações.

Observe-se que a ANATEL não pode ser considerada um órgão regulador da *internet*, pois, segundo a lei nº 9.472/97 (art. 60), a agência tem a

incumbência somente de regular as condições de acesso dos interessados ao uso das redes de comunicação para a prestação de serviços de valor adicionado (como o acesso à *internet*), não considerados de telecomunicação.[281]

De longa data reclama-se a elaboração de novo marco legislativo, por vir constatada verdadeira lacuna em matéria de comunicações eletrônicas, especialmente, quanto ao tempo em que os dados digitais deverão ser armazenados pelos prestadores de serviço.[282]

4.1.1. Intervenção e interceptação

Como já firmado, o âmbito de proteção do direito à inviolabilidade das comunicações comporta tanto a comunicação enviada ao destinatário, sem que tenha sido concluída, como também, a comunicação já concluída e armazenada em suporte físico ou eletrônico. Assim, o modo de obtenção da prova depende da situação fática: em se tratando de comunicação em curso é necessária sua interceptação; no caso de comunicação concluída, a medida de busca e apreensão.

Interceptar consiste no ato de apoderar-se de algo antes que logre alcançar o respectivo destinatário. Como ensina ADA PELLEGRINI GRINOVER, da etimologia do termo extrai-se a noção de *"deter na passagem e, consequentemente impedir que algo chegue ao lugar que se dirigia"*.[283]

---

[281] Conforme o art. 22, do Regulamento dos Serviços de Telecomunicações, aprovado pela Resolução nº 73, de 25 de novembro de 1998, não compete à agência a regulação da tecnologia do *VoIP*, mas apenas do serviço, desde que haja atribuição conferida por lei.

[282] O armazenamento diz respeito aos dados de tráfego e não ao conteúdo das comunicações. O Anteprojeto da comissão de juristas (Projeto de Lei da Câmara nº 84/1999) obrigava as prestadoras de serviço de telefonia à conservação das informações, por cinco anos; porém, no último substitutivo (PL 2126/2011), consignado o prazo de um ano. O armazenamento de comunicações representa não apenas uma medida economicamente custosa, como também, de questionável constitucionalidade. A Diretiva 2006/24/CE, da União Europeia, impõe prazo de seis meses a dois anos para o armazenamento dos dados de tráfego apenas, vedado o acúmulo de dados de conteúdo das comunicações. A gravação prévia e permanente das comunicações visando permaneçam à disposição da Justiça, não se compatibiliza com o marco do devido processo legal.

[283] *Liberdades públicas ...*, *op. cit*., p. 198.

A interceptação das comunicações eletrônicas designa, assim, a interferência realizada por terceiros nos processos comunicativos que tenham suporte informático. Em sentido amplo, interceptar significa imiscuir-se na comunicação em canal fechado, com o propósito de conhecer ou desviar os dados transmitidos, sem o consentimento do emissor e/ou do receptor.

O termo denomina tanto a diligência de investigação executada no curso da persecução penal, como também, refere-se ao ato típico e antijurídico de interceptação informática ou telemática não autorizada (lei nº 9.296/96, art.10). No processo penal, a relevância da interceptação consiste na obstrução da via comunicativa com o escopo da obtenção de prova.[284]

A intervenção, por outro vértice, tem um caráter menos específico e refere-se a toda ingerência em processo comunicativo, realizada tanto em canal aberto como fechado. Possível depreender que a relação entre intervenção e interceptação é de gênero e espécie.

Nesse sentido, a intervenção será utilizada, preferencialmente, para referir-se às buscas por fontes de provas de comunicações em canal aberto, enquanto para as comunicações em canal fechado mais adequado falar em interceptação.

O rigor técnico necessário para a definição da interceptação é inegável, pois não se confunde com outros conceitos. Em linhas gerais, o *impedimento* designa a intervenção para que a comunicação não chegue ao seu destino; a *interrupção,* a obstrução da comunicação em determinado momento; a *escuta,* a interceptação feita com o conhecimento de um dos interlocutores; a *gravação,* a operação realizada por um dos próprios sujeitos comunicantes.[285]

---

[284] O Projeto de lei nº 3.272, em trâmite no Senado Federal, cujo objeto é a regulamentação da parte final do inciso XII, do art. 5º, da Constituição Federal, dá preferência à expressão mais ampla "quebra de sigilo", em lugar de interceptação: *"(...) considera-se quebra do sigilo das comunicações telefônicas de qualquer natureza todo ato que intervém no curso dessas comunicações com a finalidade de conhecer as informações que estão sendo transmitidas, incluindo interceptação, escuta e gravação"* (art. 1º, § 1º).

[285] As noções foram apresentadas em consonância com a exposição do Anteprojeto de lei da comissão ministerial, apresentada pelos juristas Ada Pellegrini Grinover, Antônio Carlos de Almeida Castro, Antônio Magalhães Gomes Filho, Antônio Scarance Fernandes e Luiz Guilherme Vieira.

A evolução dos estudos em matéria de interceptações aponta para as principais diferenças entre as modalidades de intervenção na comunicação telefônica: (i) a interceptação telefônica caracteriza-se pela interferência intencional na comunicação de terceiros, sem o conhecimento dos interlocutores;[286] (ii) a escuta telefônica consiste na interferência provocada na comunicação de terceiros, com o conhecimento de um dos interlocutores;[287] (iii) a gravação clandestina é a interferência realizada por um dos interlocutores, sem o conhecimento do outro.[288]

A gravação clandestina constitui o modo sub-reptício de captar a conversa entre pessoas, sem que estas tenham conhecimento, executada por um dos presentes dentro do ambiente onde se situam os interlocutores. Prevalece no Supremo Tribunal Federal o entendimento da inexistência de ilegalidade no uso deste meio probatório.

A gravação ambiental consiste na conversa entre presentes, registrada por um dos interlocutores sem o conhecimento do outro.[289] Não encontra respaldo no

---

[286] A exemplo do que ocorre com a comunicação telefônica, é possível a interceptação da comunicação de dados a partir da atuação de um terceiro, sem o conhecimento dos interlocutores.

[287] Ainda que a escuta telefônica possa gerar casos complexos, pacífico que não constituirá ilícito penal quando realizada no curso de ato criminoso, e respectivamente autorizada por um dos interlocutores (a vítima).

[288] Havendo justa causa, a obtenção sem consentimento não resulta ilicitude probatória. O Pretório Excelso reiteradas vezes decidiu pela ausência de sigilo de gravação clandestina feita por um dos interlocutores sem o conhecimento do outro, *v.* RE 402717/PR, rel. Ministro Cezar Peluso, segunda turma, j. 02.12.2008; HC 75.338-RJ, rel. Ministro Nelson Jobim, segunda turma, j. 25.09.1998; RE 232.001-SC, rel. Ministro Carlos Velloso, j. 05.03.1999; RE 271.707-RJ, rel. Ministro Sydney Sanches, j. 06.12.2000; HC 949-RJ, rel. Ministro Sepúlveda Pertence, primeira turma, j. 14.12.2001; RE 226.644-SP, rel. Ministra Ellen Gracie, j. 08.08.2002; RE 345.568-PE, rel. Ministro Nelson Jobim, j. 01.08.2002; RE 271.707-RJ, rel. Ministro Sydney Sanches, j. 06.12.2000; HC 75338/RJ, rel. Ministro Nelson Jobim, pleno, j. 11.03.1998, e HC 75261/MG**,** rel. Ministro Octavio Gallotti, primeira turma, j. 24.06.1997. Posicionamento idêntico ao do Superior Tribunal de Justiça, *v.* Rec. Ord. em HC 14041/PA, rel. Ministro José Arnaldo da Fonseca, quinta turma, j. 20.11.03; HC 33110/SP, rel. Ministro José Arnaldo da Fonseca, quinta turma, j. 27.04.2004. Sustentada no julgamento do HC 57961/SP, rel. Ministro Félix Fischer, quinta turma, j. 21.06.07, a impossibilidade de regra geral sobre a licitude da gravação de conversa própria, cuja análise deve ser realizada caso a caso. A gravação clandestina pode ocorrer também nas comunicações eletrônicas, hipótese que seguirá a mesma diretriz apontada pela Excelsa Corte.

[289] Como esclarece G. H. BADARÓ, a grav*a*ção ambiental é distinta da interceptação ambiental, porque nesta a conversa entre presentes é interceptada por um terceiro não participante, sem o conhecimento dos interlocutores (*Direito Processual ..., op. cit.,* p. 279). Parece-nos acertada a posição de L. F. TORQUATO AVOLIO, que sustenta, à falta de previsão legal, a impossibilidade da interceptação ambiental *"em locais onde se possa inferir uma expectativa de privacidade"*. O autor faz ressalva, contudo, às investigações de crime organizado, em razão dos procedimentos probatórios (captação e interceptação ambiental) incluídos pelos incisos IV e V, do art. 2º, da lei nº 10.217/01 (*Provas ilícitas ..., op. cit*., p. 273). Para M. G. B. ARANTES FILHO, *"o regime instituído na lei nº 9.034, de 1995 não possibilita a observância das exigências para a restrição de comunicações entre presentes por meio de interceptação: a reserva de lei, reserva de jurisdição e a proporcionalidade. Interceptação de comunicação entre pessoas presentes que seja operada, sob o regime previsto na lei nº 9.034, de 1995, ou fora deste regime, é ilícita. (...) não é possível a aplicação,*

regime do art. 5º, inciso XII, da Carta Federal, nem na disciplina da Lei de interceptações telefônicas. Na verdade, a partir da criteriosa ponderação de interesses em cada hipótese, aplica-se o disposto do art. 5º, inciso X, da Constituição.[290]

As providências de interceptação nas comunicações telefônicas e de intervenção nas comunicações eletrônicas guardam acentuada similitude em razão dos meios técnicos empregados e da natureza das informações recolhidas. Enquanto para as primeiras a informação é obtida de uma conversa telefônica, no segundo caso será interrompida a comunicação viabilizada por aparelho eletrônico ou similar. Se por sua natureza, a interceptação telefônica capta dados de conteúdo e de tráfego transmitidos a partir do início do procedimento de coleta de prova, no meio eletrônico será possível ter conhecimento não apenas de conteúdos que integrem o processo comunicativo, como também dados que se encontrem na *web*.

Ambas apresentam viés particularmente invasivo, principalmente nos casos em que a medida esteja associada à obtenção de outras informações além daquelas oriundas do conteúdo em si da comunicação. Lembre-se que tanto a interceptação da comunicação eletrônica, como da telefônica, fatalmente redundam no conhecimento dos locais onde se encontra o sujeito passivo da medida, bem como de seus respectivos deslocamentos.

---

por analogia, à interceptação de comunicação entre pessoas presentes do procedimento probatório previsto, para a interceptação de telecomunicações, na lei nº 9.296, de 1996. Além de a interceptação de comunicação entre pessoas presentes integrar os meios de investigação de prova, para os quais não se admite a aplicação de procedimento probatório por analogia, há evidentes incompatibilidades entre o procedimento previsto na lei nº 9.296 e o instituto da interceptação de comunicação entre presentes" (*A interceptação de comunicação entre pessoas presentes como meio de investigação de prova no Direito Processual Penal brasileiro*, São Paulo, Dissertação de Mestrado, 2011, p. 290).

[290] Atente-se para a observação de L. F. TORQUATO AVOLIO de que a admissão da gravação ambiental clandestina depende da demonstração da justa causa: *"deve existir, portanto, um interesse superior, que se contraponha ao valor intimidade, a ser sopesado no caso concreto (...) impõe-se que o exame da validade da gravação clandestina seja feito caso a caso, não se podendo de antemão acolher ou rejeitar indiscriminadamente esse meio de prova"* (*Provas ilícitas ...*, *op. cit.*, p. 267). Em busca de critérios para o tema da instalação de escuta ambiental, inclusive, aludindo aos limites característicos do regime das escutas telefônicas, *v.* Caso *Vetter* vs. França, j. 31 mai. 2005. O Tribunal de Estrasburgo decidiu que tal procedimento viola o art. 8º, da CEDH, no que toca à intimidade e vida privada, sendo incompatível este meio de busca de prova com o convívio em uma sociedade democrática.

4.1.2. Comunicações em canal aberto e fechado

O caráter aberto ou fechado das comunicações eletrônicas varia em razão da privacidade que se pretende atribuir ao seu conteúdo. Se em alguns casos a modalidade de transmissão eletrônica de informações abarca um coletivo indeterminado de pessoas, em outros prevalecem a exclusividade e a reserva dos sujeitos comunicantes.

O próprio meio de comunicação pode dispor de vocação para a difusão pública, como é o caso do rádio e da televisão. O mesmo vale para as conversas via *chat,* as redes sociais e *blogs*, quando não restritos a interlocutores determinados, e para os conteúdos livremente disponibilizados na *internet*.

Em contrapartida, como ocorre nas comunicações telefônicas e telegráficas, o intercâmbio de informações em canal fechado particulariza-se pela transferência de dados a destinatários bem definidos. No entorno digital, o correio eletrônico, o *VoIP*, os grupos de notícias e as informações restritas de redes sociais estão limitados a um rol específico de usuários.

Alguns serviços oferecidos na *internet* exigem um processo de registro que não descaracteriza necessariamente o caráter aberto dessas comunicações. Ainda que haja individualização do usuário, não se realiza a verificação da informação pessoal e consequente determinação precisa do sujeito em questão. Destarte, o ponto central consiste no grau de êxito com que se poderá alcançar a identificação do grupo de pessoas envolvidas na conexão.[291]

Em relação à comunicação realizada em canal fechado, incide tanto a tutela do direito ao sigilo da comunicação de dados, como também, do direito à autodeterminação informativa. Para as comunicações em canal aberto, se de um lado não há segredo sobre o conteúdo, de outro persiste o dever de preservar o direito à proteção dos dados pessoais por parte daquele que detém a informação.

[291] J. J. GONZÁLEZ LÓPEZ, *Los Datos de Tráfico...*, *op. cit.,* p. 114.

4.1.3. Intervenção nas comunicações em canal aberto e interceptação nas comunicações em canal fechado

O termo intervenção expressa ingerência, intromissão, ato de acessar ou obter algo por meio de um agir específico. No processo penal, pode ser empregado para designar a violação do sigilo das comunicações, por meio da qual se toma conhecimento de um conteúdo veiculado por terceiro distinto dos operadores e provedores de serviços de comunicação, independentemente da finalidade da intromissão.

A intervenção nos dados de comunicações em canal fechado, diligência de natureza investigativa que preferimos designar *interceptação*, tem como finalidade a obtenção de fontes de provas, ou seja, a coleta de informações úteis à persecução penal. Trata-se de medida restritiva do direito fundamental à inviolabilidade das comunicações e, como tal, condicionada a observância dos pressupostos, requisitos e limites legais, sob pena de infringir o corolário do devido processo penal.

Para as comunicações em canal aberto, destinadas a um coletivo indeterminado de pessoas, a intervenção em tempo real nos dados veiculados tem também a natureza jurídica de diligência investigativa, com a diferença, neste caso, que os dados encontram-se amplamente acessíveis no entorno digital.

A intervenção tem suporte legal, já se afirmou, no art. 1º, § 1º, da lei nº 9.296/96, e pode representar tanto a busca de dados digitais de conteúdo, como de dados externos à comunicação (de tráfego).[292] Por seu caráter invasivo, cumpre a observância de um estrito rol de garantias processuais: reserva de jurisdição; motivação da resolução judicial; controle judicial enquanto perdurar a medida; resguardo do direito de defesa do investigado e direito à proteção dos dados pessoais relativos à informação de terceiros afetados.

[292] A Convenção de Budapeste sobre crimes cibernéticos diferencia, nos artigos 20 e 21, a *interceptação do conteúdo dos dados informáticos (real-time interception)* da *obtenção em tempo real dos dados de tráfego da comunicação (real-time collection)*.

4.2. Regulação

A previsão de um meio de obtenção de provas sobremaneira invasivo, como a intervenção na comunicação de dados, pressupõe a existência de lei específica que discipline sua implementação[293], bem como, das condicionantes legais que mais adiante serão analisadas (pressupostos, requisitos e limites).

Impossível negar que o fundamento constitucional desta medida está na preservação da liberdade, da segurança e do bem-estar social. Trata-se da necessidade de apurar injustos perpetrados no contexto de uma sociedade que se comunica frequentemente por meio de novas e complexas tecnologias. Contudo, a contrapartida para a sensível limitação imposta pela intervenção na comunicação de dados consiste na fiel observância do juízo de legalidade e jurisdicionalidade da medida.

Sem embargo, intoleráveis argumentos genéricos que, a pretexto da gravidade dos delitos e do combate à criminalidade, sustentem uma reação meramente simbólica[294] dos intérpretes do Direito. Recrudescer a persecução criminal como resposta à insegurança social gerada pelo crime é valer-se de retórica persuasiva característica de regimes arbitrários. Em um Estado de Direito, não há outra alternativa ao exegeta senão atuar conforme os padrões da legalidade em senso estrito – compromisso técnico-formal com o rigor na decretação das medidas restritivas de direitos fundamentais.

À medida que ameaçam as liberdades cívicas, inquietante o incremento dos meios estatais invasivos de segurança. Cada vez mais aprimorados, os sistemas de intervenção nas comunicações podem exercer controle simultâneo de todas as comunicações eletrônicas de uma pessoa por meio de estações de interceptação.

Neste contexto, aperfeiçoam-se modelos de espionagem em escala internacional, onde a colaboração e interação de vários Estados permitem a convergência de iniciativas e de recursos técnicos. Com caráter igualmente intrusivo, os meios

[293] Sobre o posicionamento de ADA PELLGRINI GRINOVER a respeito da existência de previsão normativa para o emprego da interceptação telefônica mesmo antes da vigência da lei nº 9.296/96, e da constitucionalidade desta medida de busca de prova antes da Constituição de 1988, *v. Liberdades Públicas*, *op. cit.,* pp. 247-274.
[294] L. L. STRECK, *As Interceptações telefônicas ...*, *op. cit.,* pp. 30-32.

destinados à localização e rastreio das comunicações de um usuário na *internet*. A invasão ocorre em ponto estratégico do provedor de serviços de *internet*, de maneira que todas as palavras escritas pelos internautas são recolhidas.[295]

Os macrossistemas de vigilância na *internet* vulneram as garantias penais próprias de uma sociedade democrática, independente qualquer apreciação prévia sobre a materialidade e autoria delitivas. Fundada exclusivamente na suposta gravidade dos crimes, esta política de persecução criminal preventiva atenta contra a presunção de inocência.[296] Vulnera-se, ainda, a garantia básica da legalidade, pois ignorado o caráter prévio da lei *(lex previa)* e a necessária clareza dos pressupostos fáticos da medida *(lex manifesta)*.[297]

4.2.1. Ordenamento pátrio

Segundo o art. 1º, § 1º, da lei nº 9.296/96, as disposições acerca da interceptação das comunicações telefônicas aplicam-se ao fluxo de informações nos sistemas de informática e telemática.

A normativa de regência das interceptações de comunicações de dados mostra-se, porém, insuficiente. Não há diferenciação de uma série de situações complexas que envolvem a coleta, o processamento e o armazenamento dos chamados dados de

[295] Um exemplo de programa de interceptação de comunicações em escala global é o *Echelon*, adotado pelos Estados Unidos da América, Reino Unido, Canadá, Austrália e Nova Zelândia. O programa aparentemente surgiu após a segunda grande guerra para monitorar as comunicações da União Soviética e Estados aliados; com o término da guerra fria o sistema continuou em operação para investigar atividades terroristas. A colaboração dos Estados permite a vigilância, no âmbito mundial, de todas as mensagens enviadas por *fax*, telefone, *internet* ou *e-mail,* que podem ser captadas independentemente do remetente. Em 2001, o *Echelon* foi objeto de investigação por um comitê temporário do Parlamento Europeu, firmadas as bases da Resolução de 21.03.2002, que condenou formalmente este sistema por ser incompatível com a Convenção Europeia de Direitos do Homem (I. WALDEN, *Computer crimes ...*, *op. cit*., p. 226). Por outro lado, o programa *Carnivore,* adotado pelo *Federal Bureau of Investigation* (FBI), é exemplo de captação de modalidades de comunicação instantâneas através da rede (A. E. PÉREZ-LUÑO, *La tercera generación ..., op. cit*., pp. 97-98).

[296] *V.* R. BERKOVITZ, *Packet Sniffers and Privacy: Why the No-Suspicion-Required Standard in the USA Patriot Act is Unconstitutional*, Computer Law Review and Technology Journal*,* v. 7, in studentorgs.law.smu.edu/Science-and-Technology-Law.../Berkowitz.aspx (acesso em 10 mai. 2011, h. 20:40).

[297] A. E. PÉREZ-LUÑO, *La tercera generación ...*, *op. cit*., p. 100.

conteúdo e dados de tráfego, e entre comunicações em canal aberto e fechado. O tratamento de dados pessoais no entorno digital parece ter sido desestimado pelo legislador; é de se refletir, pois, sobre as bases para o aperfeiçoamento da disciplina normativa nacional.

Um regime jurídico compatível com os novos desafios proporcionados pela tecnologia deve prever mecanismos impeditivos da continuidade delitiva e voltados à minoração de seus efeitos lesivos. De rigor atentar a uma série de novas situações, como o aperfeiçoamento de ferramentas para a investigação dos fatos, da respectiva autoria, a preservação das fontes de prova e a fixação de foro competente para o julgamento das condutas.

4.2.2. Convenção de Budapeste

O estudo das comunicações eletrônicas e de dados digitais no processo penal não pode prescindir de alusão à disciplina da Convenção de Budapeste sobre *cyber* crime, apresentada pelo Conselho da Europa em 18 de novembro de 2001, que passou a vigorar após a ratificação de cinco Estados.[298]

O documento internacional, vigente desde 1º de julho de 2004, harmoniza o Direito Penal e o Direito Processual Penal de inúmeros Estados, delineando os instrumentos necessários para a investigação e repressão da criminalidade informática. Um dos marcos deste sistema supranacional diz respeito a veloz, instrumentalizada e eficaz cooperação entre os Estados signatários, assim como entre os Estados e o setor privado.

[298] Após mais de quatro anos dedicados a elaboração, formuladas quase trinta versões diferentes, o Tratado foi aprovado pelo Comitê de Ministros do Conselho da Europa na 109ª sessão, realizada em 8 de novembro de 2001. Aberto para assinatura na cidade de Budapeste, em 23 de novembro de 2001, foi imediatamente subscrito por um total de 30 países (inclusive Estados não membros do Conselhos da Europa: Japão, Canadá, Estados Unidos e África do Sul).

O paradigma propugnado pelos Estados membros do Conselho da Europa[299] baseia-se em uma política comum, voltada à proteção da sociedade contra a delinquência cibernética, em face do risco iminente de que as redes informáticas convertam-se em expediente úteis à prática delitiva, e que as respectivas provas sejam armazenadas e transmitidas pela rede de mundial de computadores. Segundo o preâmbulo da Convenção:

> " (...) the present Convention is necessary to deter action directed against the confidentiality, integrity and availability of computer systems, networks and computer data as well as the misuse of such systems, networks and data by providing for the criminalisation of such conduct, as described in this Convention, and the adoption of powers sufficient for effectively combating such criminal offences, by facilitating their detection, investigation and prosecution at both the domestic and international levels and by providing arrangements for fast and reliable international co-operation".[300]

Consta expressamente no preâmbulo da Convenção de Budapeste, o compromisso com o devido equilíbrio entre a tutela penal e o respeito aos direitos humanos fundamentais consagrados nos diplomas internacionais[301], reafirmados os direitos à liberdade de expressão, intimidade e proteção de dados.

Os Estados signatários aderiram à obrigação de criminalizar alguns grupos de condutas: as infrações contra a confidencialidade, integridade e disponibilidade dos dados e sistemas informáticos (acesso doloso e ilegal a um sistema de informática, interceptação ilegal de dados ou comunicações informáticas e atentado à integridade dos dados); produção, obtenção, comercialização ou posse de aplicativos ou códigos de acesso que permitam a prática dos crimes anteriores; infrações informáticas (falsificação de dados

[299] O Conselho da Europa (*Council of Europe*), organização internacional fundada em 5 de maio de 1949, objetiva a defesa dos Direitos Humanos, o desenvolvimento democrático e a estabilidade político-social na Europa. No âmbito do Conselho da Europa estão a Convenção Europeia dos Direitos Humanos e o Tribunal Europeu dos Direitos Humanos.

[300] *"(...) a presente Convenção resulta necessária para prevenir as ações dirigidas contra a confidencialidade, a integridade e a disponibilidade dos sistemas informáticos, redes e dados informáticos, assim como o abuso de ditos sistemas, redes e dados, mediante a criminalização dessas condutas, tal e como se definem na presente Convenção, e a assunção de poderes suficientes para lutar de forma efetiva contra tais delitos, facilitando sua detenção, investigação e sanção, tanto nacional como internacionalmente, e estabelecendo disposições que permitam uma cooperação rápida e confiável"* (trad. nossa).

[301] Com expressa referência à Convenção do Conselho da Europa para a Proteção dos Direitos Humanos e Liberdades Fundamentais (1950) e ao Pacto Internacional de Direitos Civis e Políticos das Nações Unidas (1966).

e estelionato eletrônico e infrações relativas ao conteúdo); infrações relativas ao conteúdo (pornografia infantil, racismo e xenofobia), e atentados à propriedade intelectual e aos bens que lhe são conexos.

As disposições da Convenção favorecem a assistência mútua dos Estados na coleta de dados telemáticos, a cooperação entre os signatários segue as condições e procedimentos previstos nas respectivas legislações nacionais.

Sobre os dados informáticos, o art. 16, da Convenção, dispõe acerca da conservação, também, dos dados de tráfego, sempre que haja razões para crer que estes são suscetíveis de perda ou modificação. O art. 17, prevê as seguintes medidas: (i) assegurar a conservação expedita dos dados de tráfego, independentemente do envolvimento de um ou mais fornecedores de serviços na transmissão da comunicação; (ii) assegurar a divulgação à autoridade competente, ou pessoa designada por essa autoridade, de uma quantidade suficiente de dados de tráfego para permitir a identificação pelo Estado parte, dos fornecedores de serviço e da via pela qual a comunicação foi transmitida.

Os artigos 33 e 34, da Convenção, disciplinam a assistência mútua entre os Estados para a obtenção de dados de tráfego e de conteúdo em tempo real. Nesse caso, a norma processual aplicável será aquela do Estado requerido, respeitada a respectiva legislação e os Tratados eventualmente subscritos.[302]

Em matéria de interceptação da comunicação telefônica, a Corte Europeia de Direitos Humanos[303] referendou a obrigação dos Estados, nas respectivas leis, da disciplina suficiente das restrições. Os objetivos e meios de realização da intervenção devem estar descritos, com previsões, dentre outras, do rol de crimes sujeitos à medida; do lapso temporal; das regras sobre a destruição e o armazenamento das comunicações, e dos legitimados legais ao acesso das informações.

---

[302] Segundo os arts. 33 e 34, da Convenção: *"art. 33. 1. Os Estados partes devem prestar assistência mútua na coleta de dados de tráfego em tempo real associados a comunicações específicas no seu território transmitidas por meio de um sistema de computador. Sem prejuízo do disposto no § 2 º, este auxílio deve ser regido pelas condições e procedimentos previstos no direito interno. 2. Cada Parte deverá prover auxílio ao menos com relação às infrações penais segundo as quais a coleta de dados de tráfego em tempo real esteja disponível de maneira similar em âmbito nacional. Art. 34. As Partes devem prestar assistência mútua na obtenção em tempo real ou gravação de dados de conteúdo de comunicações transmitidas por meio de um sistema informático até o limite permitido pelos tratados e leis domésticas".*

[303] Caso *Valenzuela Contreras vs.* Espanha, j. 30 jul. de 1998.

Por força do art. 37 da Convenção, o Comitê de Ministros do Conselho da Europa, respeitado o consentimento de todos os seus membros, poderá convidar qualquer Estado que não tenha acompanhado a elaboração do texto. Nestes termos, o debate dirigido à pertinência da adesão do Brasil à Convenção é inciativa urgente, primeiro passo para a regulação interna da matéria. Ainda que se possa questionar a adesão ao conteúdo integral do texto, o combate à criminalidade cibernética depende da eficácia dos instrumentos de cooperação e do aperfeiçoamento do processo de integração – participação da qual não pode o Estado brasileiro descurar. Uma vez signatário, ainda será possível complementar as disposições da Convenção mediante atos normativos internos.

4.3. Natureza Jurídica

A intervenção no fluxo das comunicações de dados (de conteúdo ou de tráfego), seja em canal aberto ou fechado, constitui diligência com dúplice finalidade: a investigação dos atos ilícitos e a preservação de possíveis fontes de provas. Não se ignore, porém, o caráter restritivo de direitos fundamentais da medida que, por afrontar diretamente o direito à inviolabilidade das comunicações (*v.* item 2.4), exige criteriosa análise.

4.3.1. Medida de investigação criminal

De rigor diferenciar as medidas de investigação de sistemas informáticos (continente) das medidas dirigidas à obtenção de dados (conteúdo). Quando se pensa em sistema informático, tem-se algo tangível, como um computador ou *notebook,* objeto de busca e apreensão, conforme será visto no próximo capítulo. Por outro lado, a obtenção dos dados digitais se perfaz por meio das intervenções policiais ou dos próprios

servidores, assegurado o conteúdo apreendido de múltiplas formas, *v.g*. mediante uma cópia clone (*v.* item 3.4).[304]

A respeito da obtenção de dados, há que atentar ao modo de proceder em face das distintas modalidades, sejam de conteúdo ou externos à comunicação, dados sensíveis, pessoais em sentido estrito ou públicos, uma vez que o grau de proteção será tanto maior quanto mais significativa a ingerência no direito à intimidade.

A existência de uma criminalidade informática que faz uso das distintas formas de comunicação viabilizadas pela *internet* exige o aperfeiçoamento técnico da investigação criminal. Contudo, não há pensar que as modernas tecnologias instituam o primado da proliferação dos meios de obtenção de provas ao desaviso da previsão normativa. A restrição de direitos facilitada por medidas como a interceptação das comunicações e as buscas e apreensões, reclama observância a um rol de garantias expressas.

As diligências de intervenção nas comunicações eletrônicas, voltadas à elucidação de ilícitos e identificação de seus responsáveis, podem resultar em variadas situações. Em primeiro lugar, a autoridade policial poderá, como consequência de uma descoberta casual, aclarar a materialidade e a autoria de uma conduta delituosa. É de avaliar a licitude desta fonte de prova, uma vez que não inserida na autorização judicial.[305]

O descobrimento de fatos relevantes pode ocorrer também em razão de buscas realizadas nas redes de comunicação eletrônica de caráter aberto. O rastreamento de dados é realizado com o fito de encontrar indícios do cometimento de um ato delitivo, no exercício das funções policiais preventivas (*v.* item 3.3).

---

[304] J. PÉREZ GIL, *Investigacion Penal y nuevas..., op. cit.,* p. 224.

[305] LÊNIO LUIS STRECK distingue duas situações para as provas fortuitas oriundas da interceptação telefônica: aquela em que o crime descoberto se encontra dentro de uma cadeia de fatos atribuídos ao sujeito cujas comunicações foram interceptadas, e aquela outra em que não há nexo causal ou liame entre os atos ilícitos. No primeiro caso, não há dificuldade na utilização da fonte de prova:*"Há que se ter claro* (...) *que na investigação de grandes quadrilhas é impossível que todas as situações concretas sejam especificadas no pedido de escuta. O mesmo se diga a respeito da investigação de grandes fraudes fiscais, em que outros delitos como corrupção, falsidade etc., poderão ser descobertos mediante os dados recolhidos na escuta. Por isso, como já dito, o juiz autorizará a interceptação depois de aferir a devida proporcionalidade."* Para o autor, no segundo caso a fonte de prova não será imediatamente inquinada como ilícita, porque poderá servir como indício para fundamentar a *noticia criminis* e para que assim seja instaurado inquérito (*As interceptações telefônicas ...*, *op. cit*., p. 126).

Ainda uma terceira possibilidade decorre do conhecimento de fontes de prova a partir de dados digitais levados a polícia por particulares, que poderá ensejar a *noticia criminis* e o início da persecução criminal.

4.3.2. Preservação das fontes de provas

Um dos alegados riscos do crescente surgimento de novas tecnologias para o processo penal é a possibilidade de restringir o papel do juiz, convertendo sua atuação em mero instrumento de convalidação. A existência de medidas investigativas que fujam ao seu controle sinaliza a perda do papel diretor da autoridade judicial.

O alto grau de complexidade técnica requerido em algumas investigações favorece a especialização dos corpos policiais. Ainda que a participação de peritos seja completamente imprescindível para elucidar os fatos, os limites de sua atuação devem ser bem delineados, para que a polícia, em nenhuma circunstância, se veja liberada do controle exercido pelo Judiciário e pelo Ministério Público.

Ou seja, a complexidade técnica da investigação ou a urgência para assegurar fontes de prova não podem justificar a delegação à polícia de funções ligadas a faculdades judiciárias instrutoras.[306] A pré-constituição probatória figura como intolerável fonte de fragilização da via judicial que converte o juiz em mero agente de convalidação de decisões previamente tomadas.

A reflexão sobre o caráter de prova pré-constituída da interceptação das comunicações, voltada a antecipar a coleta das fontes de prova, constitui questão controvertida. Por uma perspectiva menos refletida, possível aventar que a obtenção destas informações consolidaria em si um ato probatório antecipado.

No entanto, tais medidas devem ser entendidas como atos de preservação das fontes de prova, no qual a fonte não é a comunicação em si, mas

[306] J. PÉREZ GIL, *Investigación Penal y nuevas..., op. cit.,* p. 230.

justamente o conteúdo da conversação gravada ou os dados apreendidos. O caráter irrepetível não decorre do meio de prova que incorporará tais informações ao processo (documental), mas do conteúdo sonoro ou visual, ou seja, a irrepetibilidade consiste na própria comunicação.[307]

Não se está diante de um meio de prova irrepetível, mas em face da impossibilidade de obter a fonte de prova em outro momento. Portanto, não cabe falar em pré-constituição probatória, nem em violação do princípio da imediação.

Em contrapeso à necessidade de limitar o conhecimento do inculpado sobre a obtenção da prova, estará garantido o contraditório diferido sobre a fonte probatória, de modo a assegurar uma oportunidade adequada e suficiente para a apresentação dos questionamentos da defesa.

4.3.3. Limitação de direitos fundamentais

Assim como todo meio de obtenção de provas, a interceptação das comunicações de dados caracteriza-se pela limitação de direitos fundamentais. Em particular, necessário analisar brevemente os direitos à inviolabilidade das comunicações, à proteção de dados pessoais e à liberdade de pensamento e expressão.

A restrição dos referidos direitos pode ocorrer tanto pela interceptação direta da comunicação por parte dos órgãos policiais, como por intermédio do auxílio das operadores de serviços contratados na cessão das informações, sempre observadas as condições legais para cada caso.

[307] J. J. GONZÁLEZ LÓPEZ, *Los Datos de Tráfico ..., op. cit*., pp. 154-155.

4.3.3.1. Direito à inviolabilidade das comunicações

O direito ao segredo das comunicações, preserva setores íntimos da personalidade, e situa-se no plano da inviolabilidade da vida privada (*v.* item 2.3). Com relação ao resguardo dos dados digitais, cumpre indagar quais os sujeitos ativo e passivo, objeto e categorias que se encontram no âmbito de proteção do direito.

O sujeito ativo deste direito será tanto o emissor como o destinatário da comunicação, pois, a faculdade de manutenção do segredo compete a ambos os envolvidos no processo comunicativo. Por outro lado, a inviolabilidade da comunicação será exercida *erga omnes*, em face do Estado e dos particulares (sujeitos passivos).

Imperioso constatar, não apenas a confidencialidade da comunicação constitui objeto do direito, mas também, a divulgação do respectivo conteúdo e das circunstâncias ou dados externos.

O segredo das comunicações tutela justamente a razoável expectativa de intimidade que seu titular deseja resguardar da ingerência arbitrária de terceiros. Por esta razão, o âmbito de proteção do direito limita-se às comunicações em canal fechado, aquelas cuja configuração técnica esteja voltada ao intercâmbio de informações entre pessoas determinadas. As comunicações em canal aberto não impõem condições específicas para o acesso; daí porque, descabe falar em proteção do segredo destas comunicações.

Em consonância com o exposto (*v.* item 1.5), o campo protetivo compreende o correio eletrônico, as comunicações em tempo real, o *VoIP*, os grupos de notícia e consulta de informações, sempre que não se estiver diante de uma comunicação em canal aberto.[308] Poderão ser incluídas neste rol outras modernas formas de comunicação eletrônica que venham a surgir, desde que realizadas à distância, por meio de aparato técnico, e entre pessoas determinadas ou determináveis.

[308] J. J. GONZÁLEZ LÓPEZ, *Infiltración Policial en Internet*: Algunas Consideraciones, in Revista del Poder Judicial, Consejo General del Poder Judicial, n. 85, 2007.

O segredo não se limita temporalmente apenas ao momento em que a comunicação está em curso. Antes de iniciada, realizados certos atos preparatórios, a tentativa de comunicação também resta protegida, à medida que impedir alguém de realizar a comunicação constitui ingerência no exercício do direito.

Demonstrada a intenção do emissor de se comunicar, os motivos do insucesso da comunicação podem se dar por razões técnicas ou fatores externos, mas não por ato voluntário de terceiros. Outro posicionamento redundaria em esvaziar a proteção do direito, olvidando dados vinculados à transmissão da informação (chamadas perdidas, notificação de frustração do envio de correio eletrônico).[309]

Por sua vez, as comunicações já concluídas estão protegidas não apenas pelo sigilo das comunicações previsto no art. 5º, inciso XII, da Constituição Federal, mas também, pela inviolabilidade da vida privada, conforme o inciso X, da norma constitucional.

À primeira vista, os provedores e as operadoras de serviços responsáveis pelo fluxo da informação interferem diretamente na comunicação, mediante o uso de instrumento técnico específico. Por óbvio, o mero gerenciamento das informações não constitui violação do segredo das comunicações: o aparato técnico envolvido é condição inerente ao exercício da comunicação. Neste caso, o terceiro alheio ao emissor e ao receptor age como intermediário e colaborador da comunicação.[310]

4.3.3.2. Direito à proteção de dados de caráter pessoal

A proteção de dados não representa apenas a reserva com a qual certas informações devem ser tratadas, mas principalmente, o reconhecimento de que todos os cidadãos detêm poder de contínuo controle sobre os próprios dados (*v.* item 2.2).

---

[309] J. J. GONZÁLEZ LÓPEZ, *Los Datos de Tráfico ..., op. cit*., p. 146.

[310] O armazenamento de dados pelo prestador de serviços deve restringir-se àqueles essenciais para a viabilização da comunicação. O tratamento de toda informação que exceda o estritamente necessário à prestação do serviço deve ser expressamente consentida pelo contratante do serviço.

Voltado à defesa da privacidade do cidadão, o direito à proteção de dados ou autodeterminação informativa, compatibiliza-se com os fins processualísticos-penais. Afinal, os escopos da imposição de uma sanção ao término do processo e da preservação de direitos e garantias fundamentais não são finalidades apartadas ou contraditórias, mas sim, harmônicas.

A complexidade da questão situa-se, porém, no plano da efetividade do direito à proteção de dados. Seria este direito fundamental um novo filtro para a ponderação das providências adotadas na investigação? Em que medida considerado necessário em uma sociedade democrática?

O enfrentamento da questão esbarra no aparente conflito entre *proteção de dados pessoais* e *investigação penal,* sobretudo, se entendida a persecução como a busca do maior número de elementos informativos sobre os eventos e sobre as pessoas relacionadas ao delito. Ainda que aparentemente controversos, ambos os objetivos devem ser compatibilizados.

Os dados divulgados publicamente por seu titular no entorno digital persistem objeto de tutela da proteção de dados. Ao revelar o endereço eletrônico seu titular não autoriza o uso para todo e qualquer fim, como *v.g.,* publicidade eletrônica, armazenamento dos dados ou análise cruzada de informações. Destarte, para o respectivo uso em sede de investigação criminal, imprescindível a observância de previsão normativa, autorização jurisdicional, motivação e proporcionalidade.

A crescente preocupação em proteger os dados pessoais no entorno digital fomentou o crescimento das políticas de segurança e anonimato na *internet*. Inúmeros *softwares* possibilitam a ocultação dos hábitos de navegação do internauta por meio de ferramentas de autenticação (firma eletrônica), encriptação[311] e o emprego de servidores seguros (VPN) que filtram os dados pessoais e permitem a navegação anônima.

[311] O termo advém dos vocábulos gregos *"kryptós"* (escondido) e de *"gráphein"* (escrever) e designa o estudo de escritos secretos. A criptologia subdivide-se em criptografia, que inclui o estudo dos mecanismos para garantir a confidencialidade, e criptoanálise, que visa decodificar o texto. Esta técnica garante a segurança do armazenamento e transmissão de dados, privilegiando a confidencialidade, a autenticação e o controle da integridade dos escritos (M. QUÉMÉNER, Y. CHARPENEL, *Cybercriminalité: Droit pénal appliqué*, Paris, Economica, 2010, p. 81).

À medida que se multiplicam as técnicas de ocultação dos usuários, propagam-se também possíveis espaços de impunidade por onde circulam todo tipo de informação constitutiva de delitos. Assim, frequentes as situações de conflito entre o legítimo interesse de garantir o anonimato durante a navegação nas redes eletrônicas e o interesse público de impedir que a ocultação seja empregada para a prática criminosa.

Diante desta difícil controvérsia, com maior razão a postura tendente a admitir a navegação anônima; afinal, são realmente escassos os recursos eficazes para o internauta proteger os dados oriundos de navegação na rede. Nos últimos anos proliferaram soluções relativamente práticas e baratas que permitem a qualquer usuário, independente de conhecimentos avançados, manter-se incógnito na rede (*v.g., Anonimyzer* e *Safeweb*).[312]

Convém notar que tão importante quanto assegurar a cada internauta o direito de valer-se destas importantes ferramentas de proteção, é normatizar o uso destes serviços para que a encriptação e a reserva do IP não se convertam deliberadamente em expedientes úteis à prática delitiva. Embora premente, a disciplina normativa do serviços de navegação anônima deve estruturar-se em âmbito internacional, pois a possibilidade de utilizar servidores localizados nas mais variadas partes do mundo, recomenda a adoção de critérios homogêneos.

4.3.3.3. Direitos à liberdade de expressão e opinião

O segredo das comunicações, como autêntico direito de liberdade, pressupõe comunicar-se com sujeito certo. Por sua vez, as liberdade de expressão e de opinião têm destinatário genérico.

Entre liberdade de expressão e liberdade das comunicações observa-se relação de gênero e espécie. Segundo a lição de ADA PELLEGRINI GRINOVER, o primeiro

[312] Como assevera J. L. RODRÍGUEZ LAINZ, para os usuários há um legítimo interesse de valer-se do anonimato, em razão da falta de confiança sobre a destinação dos dados pessoais, informações e parâmetros de comportamento que possam ser extraídos de seus hábitos de navegação (*Intervención judicial…*, *op. cit*., pp. 121-123).

direito caracteriza-se como a difusão de informação que não tem destinatário certo, ao passo que o segundo diz respeito à transmissão de uma informação em relação a determinado sujeito:

> "o que existe não é uma diferença conceitual entre liberdade das comunicações e liberdade de manifestação do pensamento; mas sim, um aspeto diverso que não é atinente à liberdade, mas sim ao segredo. Assim, a liberdade das comunicações distingue-se da liberdade de expressão de pensamento, como espécie que é, não pela diferença entre duas liberdades, mas sim pelo aspecto de sigilo que acresce à liberdade das comunicações."[313]

Cada vez mais a *internet* representa valioso meio de difusão pública de ideias e participação cidadã. Não há perder de vista, as autoridades encarregadas da investigação com frequência se valem de informações veiculadas neste canal aberto de comunicações.

No entanto, informações que constam publicamente da rede, por vezes revelam dados pessoais dos usuários, veiculados sem o seu consentimento. Especial atenção merecem os dados individualizadores, sem muita dificuldade encontrados na rede (*v.g.*, número de RG e CPF). As medidas de vigilância e busca de fontes de provas na *internet* devem ser pensadas à luz de um juízo de proporcionalidade, justamente para que não se incorra em excesso violador do direito à proteção de dados pessoais e dos direitos à informação e à liberdade de expressão.

4.3.4. Finalidade e objeto

As intervenções eletrônicas constituem operações técnicas voltadas a captar o conteúdo comunicativo presente em textos, imagens, sons, ou outro conteúdo digital. O caráter preponderante da medida é sua natureza jurídica de meio de busca de prova, cujo conteúdo apreendido será materializado na respectiva fonte de prova.

[313] *Liberdades Públicas ..., op. cit.,* pp. 192-193.

Estas intervenções restringem os direitos fundamentais à inviolabilidade das comunicações e à proteção dos dados pessoais, com o objetivo de obter elementos de prova úteis aos sucessivos atos de investigação. A *intervenção* é a medida destinada a coletar dados digitais amplamente disponíveis na rede; por outro lado, a interceptação serve para captar o conteúdo de uma comunicação em canal fechado.

Em síntese, a finalidade da medida é a obtenção de fontes de prova durante a investigação criminal ou no curso do processo. Após a regular ciência das partes sobre estas fontes e a efetiva oportunidade de manifestação contraditória sobre os fatos demonstrados, o material coletado passará ao *status* de elemento de prova e poderá influenciar na formação da convicção judicial.

A exemplo da interceptação telefônica, a apreensão do conteúdo próprio da comunicação eletrônica é alcançada com a detenção das comunicações em tempo real, por meio da técnica de monitoração dos fluxos comunicativos. A partir de uma operação técnica os dados digitais são colhidos, gravados e registrados, sem que haja obstrução da relação comunicativa entre emissor e receptor.[314]

O conteúdo gravado e incorporado em suporte material possui natureza de prova documental, que poderá resultar em documentação escrita ou sonora. O aparato técnico que corporifica as informações coletadas será o *meio de prova* específico. A gravação eletrônica poderá ser materializada em CD *(compact disk)*, *pen drive* ou meio similar.

4.4. Intervenção nas comunicações em canal fechado: pressupostos, requisitos e limites legais

Em primeiro lugar, a análise estará centrada nas condições específicas para a obtenção de fontes de provas em comunicações de canal fechado. Justamente pelo

[314] B. S. RODRIGUES, *A monitorização dos fluxos informacionais e comunicacionais*, v. II, Coimbra, Dissertação de Mestrado, 2009, p. 88.

caráter restringente de direitos fundamentais, inescusável a observância dos *pressupostos essenciais* (legalidade e justificação teleológica), dos *requisitos* (autorização judicial, motivação) e *limites* (objetivos, subjetivos e temporais).

À luz do corolário do devido processo legal não se pode deixar de analisar o direito do investigado a uma ampla defesa. Os contornos desta garantia constitucional não se restringem à mera possibilidade de defender-se no curso do processo, mas consolidam a substancial faculdade de conhecer e exercer a autodefesa e a defesa técnica.

Ademais, de rigor esclarecer o papel do princípio da proporcionalidade ou proibição do excesso como vetor para o justo equilíbrio das decisões judiciais.

Há que ressaltar a maior proteção dispensada aos dados digitais de conteúdo, em comparação com os dados de tráfego. Conquanto pressupostos, requisitos e limites vigorem para ambas as hipóteses, é certo que em relação aos dados externos a menor gravidade da ingerência resulta em tratamento menos restritivo.[315]

4.4.1. Pressupostos: legalidade e justificação teleológica

A noção de legalidade pressupõe, primeiramente, o caráter formal ou legal do critério de definição do desvio, que jamais será conhecido na casuística e por meio de características intrínsecas ou ontológicas que indiquem aquilo que é socialmente lesivo ou imoral.

[315] Imbuído do mesmo esforço sistematizador dos limites para as intervenções nas comunicações eletrônicas – a partir do texto da Convenção Europeia de Direitos do Homem e do caso paradigmático *Valenzuela Contreras vs*. Espanha (j. 30 de jul. 1998) – PÉREZ GIL aponta os seguintes critérios para tolher os excessos: (1) a definição de categorias e sujeitos suscetíveis às intervenções; (2) a natureza das infrações que possam dar lugar à medida; (3) a fixação de limites para a duração e execução da medida; (4) as condições de elaboração dos processos verbais de síntese consignados nas conversações interceptadas; (5) as precauções para comunicar os registros realizados, com o fim de controle eventual por parte do juiz e da defesa; (6) as circunstâncias que podem ou devem apagar-se ou destruir o material que consigne os dados pessoais (*Medidas de investigación y de aseguramiento de la prueba en el Convenio sobre el Cibercrimen*, in Actualidad penal: Revista semanal técnico-jurídica de derecho penal, n. 36, Madrid, La ley, 2003, p. 926).

Na verdade, o princípio consagra o desvio como a expressão da prescrição formalmente definida em lei como pressuposto necessário para a aplicação de uma pena. Dessa maneira é de se pensar na submissão do juiz à lei, em adstrita convergência à fórmula *nulla poena et nullum crimen sine lege*.

O mesmo princípio abrange, em um segundo momento, o caráter empírico dos desvios legalmente definidos, que não preconiza referências a figuras subjetivas de *status* ou de autor, mas apenas a figuras empíricas e objetivas de comportamento. Há, pois, a imprescindibilidade de referências empíricas e fáticas precisas e exaustivas, convergentes com a máxima *nulla poena sine crimine et sine culpa.*[316]

O convencionalismo relaciona-se à legalidade estrita, em razão da preocupação da manutenção nominalista e empírica do desvio punível, extirpando-se qualquer configuração extralegal das hipóteses cabíveis. Não se admite sejam criadas situações de desvio sem nada prescrever, cujo conteúdo possa transitar por mais de uma possibilidade de ação – a proibição, enquanto modalidade deôntica, há que ser aplicável a todos indistintamente, não podendo referir-se a diferenciações políticas, sociais ou antropológicas.

De modo semelhante, é possível falar em legalidade das disposições relativas aos meios de obtenção de prova. As diligências voltadas à busca de prova devem ser nominadas e o procedimento cabível estar previsto. A exemplo da pena e da figura típica, coerente que toda medida a resultar em limitação de direitos fundamentais conte com lei anterior que a discipline.[317]

É possível que as previsões legais de tais medidas apresentem alguma abertura ao desenvolvimento tecnológico, de modo a autorizar acessos a novos sistemas conectados em rede, a instalação de programas rastreadores, dispositivos de localização geográfica e de busca cruzada de dados, dentre outros. Contudo, as habilitações para a

---

[316] L. FERRAJOLI, *Direito e Razão ...*, *op. cit.,* pp. 38-39.

[317] No caso *P. G.* e *J. H. vs*. Reino Unido (j. 25 set. 2001), o Tribunal de Estrasburgo consagrou a necessidade do meio usado para a obtenção da prova contar com fundamento legal no Direito interno. Entretanto, as condenações de Estados europeus em razão da ausência de previsão legal para o uso de meios de busca de prova não são frequentes; o problema situa-se mais no âmbito qualitativo, à medida que as leis existem, mas não são completas e específicas. Os termos da lei devem ser suficientemente claros para apontar de maneira eficaz as circunstâncias concretas que autorizam o Poder Público a valer-se destes meios, *v. Kruslin vs.* França, j. 24 abr. 1990.

implantação destas medidas são expressas invariavelmente por força de lei e devem buscar o rigor e a clareza das respectivas proposições.

A disciplina normativa acerca da interceptação das comunicações eletrônicas é insuficiente e requer imediata readequação. Não é condizente com a relevância atual das comunicações telemáticas que sua autorização permaneça restrita ao § 1º, do art. 1º, da Lei 9.296/96. As diversas formas de ingerência e os problemas suscitados variam em consonância com as modalidades de comunicações eletrônicas.[318]

Algumas das mais sensíveis deficiências envolvem a ausência de distinção entre as intervenções nos dados de conteúdo material e nos dados de tráfego, e de normativa para o tratamento e armazenamento dos dados, bem como questões próprias das comunicações em canal fechado ou aberto.

Outro pressuposto igualmente relevante concerne à justificação teleológica ou finalidade legítima. A doutrina frequentemente associa este preceito ao princípio da proporcionalidade (ou proibição do excesso). Cuida-se, na verdade, de pressuposto material de tal princípio.[319]

A necessária justificação teleológica consubstancia a noção de justo no processo. A imposição de uma medida gravosa ao investigado não pode dissociar-se do valor justiça. Assim, o escopo constitucionalmente legítimo é aquele que mais se aproxima da realização da segurança nacional, da segurança pública, do bem estar econômico do Estado, da defesa da ordem e da prevenção das infrações penais, da defesa da saúde e das liberdades públicas, e sobretudo da dignidade do homem.

A intervenção nas comunicações eletrônicas, medida restritiva de direitos, pauta-se por finalidade constitucionalmente legítima. A autorização judicial deve ser concedida com finalidade específica que tem clara afinidade com o objetivo constitucionalmente perseguido. Nesse sentido, não há maiores dificuldades para

[318] A Resolução nº 59, de 9 de setembro de 2009, do Conselho Nacional de Justiça (CNJ), regula e uniformiza o procedimento de interceptação das comunicações telefônicas e de sistemas de informática e telemática nos órgãos jurisdicionais do Poder Judiciário, iniciativa salutar para o aperfeiçoamento técnico.
[319] *Cf.* A. SCARANCE FERNANDES, *Processo Penal ...*, *op. cit.*, p. 52.

compreendê-la à luz do desígnio constitucional de investigação dos delitos e de preservação da segurança social (CF, art. 5º, *caput*).

Absolutamente vedada a intervenção voltada a investigações genéricas de possíveis infrações, medida própria do sistema inquisitivo e incompatível com as garantias do processo segundo os ditames do *due process of law*. A quebra do sigilo das comunicações não se presta ao desiderato de prevenir ou descobrir delitos sem que haja base fática concreta.[320]

A atividade investigativa impõe a realização da busca de relevantes fontes de prova relacionadas a um delito específico. A finalidade constitucional da medida será desvirtuada se a ingerência nos direitos fundamentais voltar-se à prevenção de crimes. O marco do devido processo legal exige que a intervenção nas comunicações seja uma medida processual destinada exclusivamente à investigação de delitos cuja prática venha conhecida no início do processo, com base em *noticia criminis*.

Contudo, no caso de comunicações em canal aberto, de conteúdo publicamente acessível para diversos fins, a atuação investigativa como polícia de segurança justifica o desempenho da função preventiva de delitos.

4.4.2. Requisitos

A observação dos fatos públicos por qualquer pessoa pode ser levada aos autos tanto pelo meio testemunhal, como documental. No entanto, há casos que rompem as barreiras naturais que separam a vida privada da vida pública. Sempre que houver ingerência na normal expectativa de resguardo da intimidade, justifica-se a necessidade de autorização judicial para o conhecimento desses fatos.

[320] A interceptação preventiva das comunicações eletrônicas confronta a aspiração de igualdade do devido processo legal. Se o processo com garantias é aquele que se harmoniza com os ditames constitucionais, não se pode tolerar a limitação de direitos fundamentais que tenha como base decisões judiciais carecedoras de descrição objetiva e subjetiva. A insuficiência de determinação do crime cometido, do sujeito passivo da medida e dos indícios de autoria são fatores que contaminam a justiça da decisão.

Os meios de obtenção de prova sempre se relacionam à restrição de direitos fundamentais. Indispensável sejam nominados, respectivamente disciplinados quanto ao procedimento cabível e suficientemente motivados pela autoridade judicial competente.

Apenas quando atendidas as condições legais e jurisdicionais estará presente a justificação constitucional para a limitação do direito. Sempre que inobservadas, restará configurada a violação do direito.

4.4.2.1. Reserva Jurisdicional

A jurisdicionalidade, enfocada sob a perspectiva do cognitivismo processual na determinação do desvio punível, concerne às motivações, às razões de fato e de direito acolhidas para sua justificação. Condição indispensável da pena não é somente a lei, mas também, hipótese de acusação que contenha prova, consoante a fórmula *nulla poena et nulla culpa sine judicio*. FERRAJOLI ainda prevê a necessidade de verificações expostas à refutação – apresentadas provas e contraprovas –, conforme a máxima *nullum judicium sine probatione.*[321]

Mas não é apenas a imposição de uma sanção por parte do Estado-juiz que exige a apreciação judicial, como também, as medidas que signifiquem restrição de direitos fundamentais. A apreciação e o controle dos meios de obtenção de prova pelo Poder Judiciário é exigência do primado do *due processo of law* – o processo com garantias se perfaz como o único instrumento legítimo para a imposição de situações desfavoráveis ao cidadão.

Na Constituição Federal, o inciso XII, do art. 5º, consagra a reserva de jurisdição para a limitação do segredo das comunicações. Este inciso configura, assim, regra de legitimação que investe a autoridade judiciária de legitimidade e exige que se proceda sempre por ato motivado.

[321] *Direito e razão ...*, *op. cit.,* pp. 40-41.

Portanto, a determinação da monitoração das comunicações eletrônicas compete ao juiz, inadmitido o decreto por parte de qualquer outra autoridade administrativa ou governamental.[322] É atribuição do Poder Judiciário, órgão legitimado a exercer com independência e imparcialidade a função jurisdicional,[323] assegurar a defesa dos cidadãos, combater as ilegalidades e dirimir os conflitos de interesses públicos e privados. Assim, o mandado judicial é o instrumento adequado para examinar a restrição dos direitos ao segredo das comunicações e à autodeterminação informativa.

A permissão para a continuidade da intervenção nas comunicações eletrônicas depende da apreciação e do controle do juiz criminal, que fundamentará eventuais ampliações objetivas e subjetivas da medida. Ainda que persistam as razões apresentadas anteriormente esta motivação deve ser conhecida de nova feita e de maneira autônoma.

Para a medida de intervenção nas comunicações em canal fechado a judicialidade é indispensável em todos os casos; contudo, para as comunicações em canal aberto inocorre tal imposição (*v.* item 4.8).

[322] Nem todos os Estados adotam esta diretriz. No Reino Unido, a intervenção nas comunicações é regulada pelo *Interception of Communications Act* (1985), que atribui ao Ministro do Interior a prerrogativa de autorizar a gravação. O propósito da medida é o de prevenir ou detectar crimes graves, não sendo admissível no processo o uso das informações obtidas. A polícia, munida do mandado, pode realizar a interceptação em quatro casos: (a) quando detectado risco à segurança nacional; (b) para evitar o cometimento de "sérios crimes" (ofensa que possa acarretar sentença de três anos de prisão, ou infração que envolva importantes interesses financeiros, ou praticada por um grande número de pessoas com um propósito comum); (c) se a segurança econômica do país estiver envolvida; e (d) se as autoridades do Reino Unido forem solicitadas com base em acordo de cooperação mútua para auxiliar na solução de sérios crimes ocorridos no exterior. As hipóteses (a), (b) e (c) são também previstas para o emprego do agente infiltrado e da vigilância invasiva, dois meios de obtenção de provas que constam no *Investigatory Powers Act* (2000).

[323] A doutrina italiana consagrou a noção de *'terzietà'* para indicar a posição de equidistância do magistrado em relação às partes, *status* característico para assegurar a independência das funções de acusação e de defesa. GIULIO UBERTIS destaca os aspectos objetivo e subjetivo da imparcialidade: no primeiro sentido, comporta o foro interior do juiz (até prova em contrário, presume-se que o magistrado não atue para favorecer ou prejudicar as partes); em uma segunda perspectiva, corporifica a necessária ausência de situações funcionais que obriguem manifestação do próprio convencimento antes do momento da sentença (*Argomenti di procedura penale*, v. III, Milano, Giuffrè, 2011, pp. 4-5).

4.4.2.1.1. Competência

A determinação da jurisdição competente para o julgamento de determinados crimes, como é o caso dos delitos informáticos, mostra-se particularmente difícil. A definição do lugar de cometimento do injusto suscita inúmeras dificuldades, sem que se possa desprezar o risco de sobre um mesmo fato confluírem distintas linhas de investigação. Daí porque, o conflito pode ocorrer em relação às frentes de investigação e aos órgão jurisdicionais intervenientes.

O caráter transfronteiriço da criminalidade informática cria situações sensíveis em que a apreciação jurisdicional de mais de um Estado pode estar em questão. Uma conduta pode iniciar-se em um Estado e completar-se em outro.

No caso do Brasil, não signatário da Convenção de Budapeste sobre crimes cibernéticos, a cooperação internacional para a investigação de crimes desta natureza põe-se em termos ainda pouco desenvolvidos.[324]

Cumpre aludir à solução proposta no relatório de motivos da Convenção de Budapeste (apartado 239). Para evitar uma duplicação desnecessária de esforços ou competição entre os corpos policiais dos Estados afetados, em certos casos a solução mais adequada pode ser a escolha de apenas um Estado para o processamento da medida; em outros, um Estado pode processar alguns dos investigados, enquanto um ou vários Estados perseguem outros.[325]

---

[324] Sobre a ausência de normativa no Direito pátrio e por um modelo normativo de cooperação judicial em matéria penal, *v.* F. R. BECHARA, *Cooperação Jurídica Internacional em material penal: eficácia da prova produzida no exterior*, São Paulo, Tese de Doutorado, 2009.

[325] Segundo o art. 22.5: *"Quando mais de uma Parte reivindique a competência em relação a uma presumível infração prevista na presente Convenção, as partes em causa, se for oportuno, consultar-se-ão a fim de determinar qual é a jurisdição mais apropriada para o procedimento penal"*. Dispõe o apartado 239*:"No caso de crimes cometidos com o uso de sistemas de computador, haverá ocasiões em que mais de um Estado parte terá jurisdição sobre alguns ou todos os participantes do crime. Os ataques de vírus, as fraudes e as violações de direitos autorais cometidos por meio da internet são exemplos em que atingidas vítimas situadas em muitos Estados. A fim de evitar duplicação de esforços, inconveniente desnecessário para as testemunhas, ou competição entre os agentes policiais dos Estados interessados, ou de outra forma facilitar a eficiência ou a equidade do processo, as partes afetadas devem proceder a consulta a fim de determinar o local adequado para acusação. Em alguns casos, será mais eficaz para os Estados interessados escolher um local único para a acusação; em outros, melhor que um Estado processe alguns*

A presença de frentes de investigação em Estados distintos, quando desvinculadas do compromisso de coordenação de esforços, ou ao menos, de interação recíproca entre as linhas investigativas, nada favorece a eficiência da prestação jurisdicional.

A Convenção de Budapeste, ao aludir ao *locus delicti* para os crimes informáticos, favorece o caminho do diálogo e da busca pela comunhão de interesses entre os Estados. Esta solução, de caráter internacionalístico, figura como uma via interessante voltada à eficiência na apuração de delitos.[326]

O combate desta modalidade de criminalidade transfronteiriça exige a união de esforços. Ainda que o ordenamento jurídico e os instrumentos legais dos Estados signatários da Convenção de Budapeste não possuam contornos idênticos, as inúmeras semelhanças prestigiam a eficiência no combate dos delitos cibernéticos.[327]

Ademais, a opção por um critério legal que não exclua *a priori* a jurisdição penal de um Estado não descuida da esperada eficiência da persecução, bem como possibilita o permanente contato com as novas formas de criminalidade virtual.[328]

Segundo o artigo 6º, do Código Penal, considera-se praticado o crime *"no lugar em que ocorreu a ação ou omissão, no todo ou em parte, bem como onde se*

---

participantes, enquanto um ou mais Estados persigam outros. Ambos os casos são permitidos nos termos do presente parágrafo. Finalmente, a obrigação de consultar não é absoluta, mas deve ter lugar "quando apropriado". Assim, por exemplo, se uma das partes sabe que a consulta não é necessária (por exemplo, recebeu a confirmação de que a outra parte não está planejando tomar medidas), ou se uma parte é de opinião que a consulta pode prejudicar a investigação ou o processo, poderá adiar ou recusar consulta" (trad. nossa).

[326] Tratados e Convenções que instituam regime jurídico uniforme para a determinação do *locus delicti* apresentam maior efetividade se comparados com a opção dos Estados por critérios próprios, como a adoção da teoria da ação (segundo a qual, o delito se consuma quando produzida a ação típica) ou da teoria do resultado (a consumação do delito no mesmo instante do resultado jurídico). Pense-se que um Estado que adota a teoria da ação não pode julgar um crime cibernético cometido por seu cidadão no exterior, mesmo que os efeitos do ilícito repercutam neste Estado. Igualmente, um estrangeiro que perpetrar crime no exterior, cujos efeitos atinjam o Estado adotante da teoria da ação, não será processado neste local mesmo que ali permaneça após a consumação do delito.

[327] Concordamos com M. OLINET e K. MARTHIN-CHENUT, no sentido de que a teoria da ação (para a determinação da lei aplicável considera-se praticado o crime no momento da ação ou omissão do agente ativo) mostra-se insuficiente para fazer frente a uma criminalidade sem fronteiras. Ainda que nem todos os ordenamentos se pautem pela teoria da ubiquidade, necessário caminhar nesta direção (*La preuve Cybernétique,* in *Les transformations de l'administration de la preuve pénale,* Genevève Giudicelli-Delage (org), Paris, Société de Législation Comparé, 2006, p. 234).

[328] E. CASEY, *Digital investigation …*, *op. cit.,* p. 186.

produziu ou deveria produzir-se o resultado" (teoria intermediária ou da ubiquidade).[329] Dessa forma, os ilícitos praticados no território nacional e os que aqui realizaram ou deveriam ter realizado seu resultado, estarão afetos à jurisdição pátria.[330]

Dentro do território nacional o poder da autoridade judicial para o ato que autorize ou ordene *ex officio* a ingerência sobre o sigilo das comunicações emana da legitimidade apontada pelo legislador constituinte na reserva jurisdicional do art. 5º, inciso XII, da Carta Federal, observadas as disposições dos artigos 69 a 91 do Código de Processo Penal.

Há que se buscar o foro que direta e definitivamente seja competente para a completa instrução da causa, em respeito ao princípio da unidade da investigação. Entretanto, é possível que as primeiras diligências judiciais estejam a cargo de juiz relativamente competente para a causa. Esta responsabilidade para autorizar e controlar as intervenções será possível desde que não decorra de manipulação tendente a escolher um juiz mais inclinado à adoção de medidas restritivas de direitos fundamentais.

Para determinação do foro competente deve ser identificado o lugar da infração (CPP, art. 70), sem prejuízo dos demais critérios dispostos no art. 69, do Código de processo penal. O art. 70, do estatuto processual, determina como regra a competência do lugar da consumação da infração e, no caso de tentativa, o lugar em que praticado o último ato de execução.[331]

A investigação criminal pode iniciar-se com base no lugar de onde se tenha notícias do cometimento de um delito, do domicílio do suposto réu ou do lugar de sua prisão, ou do lugar em que descobertas as primeiras evidências da prática criminosa.

---

[329] Segundo a teoria da ação, o delito se consuma quando produzida a ação típica; para a teoria do resultado, a consumação do delito ocorre no momento em que se produz o resultado antijurídico; para a teoria intermediária ou da ubiquidade, qualquer um dos anteriores conceitos é apto para entender consumado o delito.

[330] Sublinhe-se o caráter dúplice ou misto (material e processual) do preceito que rege o *locus delicti* nos crimes informáticos (CP, art. 6º).

[331] Segundo os parágrafos do art. 70, do Código de Processo Penal: *"§ 1º Se, iniciada a execução no território nacional, a infração se consumar fora dele, a competência será determinada pelo lugar em que tiver sido praticado, no Brasil, o último ato de execução. § 2º Quando o último ato de execução for praticado fora do território nacional, será competente o juiz do lugar em que o crime, embora parcialmente, tenha produzido ou devia produzir seu resultado.§ 3º Quando incerto o limite territorial entre duas ou mais jurisdições, ou quando incerta a jurisdição por ter sido a infração consumada ou tentada nas divisas de duas ou mais jurisdições, a competência firmar-se-á pela prevenção"*.

Porém, sempre que possível a competência para a autorização de uma intervenção nas comunicações está diretamente associada ao lugar em que se entenda como de cometimento do delito.

A Resolução nº 59, do Conselho Nacional de Justiça, de 9 de setembro de 2008, assegurou aos juízes de plantão, competência para a autorizar a medida de interceptação da comunicação telefônica e de dados, mas vedou a possibilidade de prolongamento da providência em plantão judiciário.[332]

4.4.2.1.2. Relevância do consentimento

Nas comunicações eletrônicas em canal fechado o consentimento cobra particular interesse, especialmente quando um dos interlocutores autoriza o conhecimento de seu conteúdo, ou utiliza esta fonte de prova no curso do processo. A apreensão de dados digitais pode ocorrer por meio das memórias de telefones celulares, diretórios que armazenam as mensagens de correio eletrônico, históricos de navegação, dentre outros.

Neste caso, ainda que ausente a autorização de um dos comunicantes para o acesso ao conteúdo, não há falar em ilicitude probatória. A jurisprudência pátria enfrentou questão idêntica ao tratar das comunicações telefônicas, diferenciando os casos de interceptação daqueles de gravação clandestina, no qual um dos interlocutores registra a conversa sem o conhecimento do outro.[333]

O crime previsto no art. 10, da Lei 9.296/96, trata da interceptação realizada por terceira pessoa em comunicação telefônica, telemática ou de informática

---

[332] *"Art. 13. Durante o Plantão Judiciário as medidas cautelares sigilosas apreciadas, deferidas ou indeferidas, deverão ser encaminhadas ao Serviço de Distribuição da respectiva comarca, devidamente lacradas. § 1. Não será admitido pedido de prorrogação de prazo de medida cautelar de interceptação de comunicação telefônica, telemática ou de informática durante o plantão judiciário, ressalvada a hipótese de risco iminente e grave à integridade ou à vida de terceiros, bem como durante o Plantão de Recesso previsto artigo 62 da lei nº 5.010/66. § 2º Na Ata do Plantão Judiciário constará, apenas, a existência da distribuição de "medida cautelar sigilosa", sem qualquer outra referência, não sendo arquivado no Plantão Judiciário nenhum ato referente à medida".*

[333] *V.* nota de rodapé 288.

(grampeamento). Contudo, a gravação clandestina não viola o sigilo das comunicações e também não constitui conduta ilícita, porque o direito ao segredo das comunicações não existe em relação ao seu destinatário.[334]

Situação distinta é aquela em que a pedido de um dos interlocutores, terceiro interfere para gravar a conversa. A violação do segredo das comunicações restará patente nesta hipótese se não houver autorização judicial que permita a intervenção.

Atente-se que a Lei 9.472/97 assegura ao usuário o direito de não ter divulgados os dados de tráfego referentes às comunicações telefônicas (números discados e recebidos e o tempo de ligação). A vedação da divulgação do código de acesso (art. 3º, inciso VI), o sigilo sobre os dados pessoais (art. 3º, inciso IX) e a anuência expressa e específica (art. 72, § 1º) são direitos do usuário.

4.4.2.2. Motivação

A atividade judicial permite conceber a atuação do juiz sob duas perspectivas distintas: a primeira, voltada ao contexto da descoberta (decisão), ou seja, a escolha de solução que se apresente como a melhor para o deslinde do caso (procedimento que conduz à resolução de um problema). Em seguida, o magistrado haverá de demonstrar a validade de sua solução por meio da *motivação*; argumentos serão relacionados com vistas à elaboração de discurso justificativo da decisão tomada.[335]

O dever de motivação das medidas restritivas de direitos fundamentais tem fundamento na genérica obrigação prevista no art. 93, inciso IX, da Constituição Federal. A exteriorização dos argumentos da decisão constitui o meio concreto de conhecer

---

[334] Como leciona ADA PELLEGINI GRINOVER: *"Aquele que grava suas próprias conversas não é terceiro, com relação às mesmas nem toma conhecimento de notícias que de outra forma desconheceria: limita-se a documentar fatos já conhecidos*" (*Liberdades Públicas ...*, *op. cit*., p 199). Por configurar possível afronta à intimidade, a divulgação da conversa pode caracterizar o crime de violação de segredo, descrito no art. 153, do Código Penal (A. P. GRINOVER, A. S. FERNANDES, A. M. GOMES FILHO, *As nulidades ...*, *op. cit*., p. 234).

[335] A. M. GOMES FILHO, *A motivação das decisões penais*, São Paulo, RT, 2001, p. 112.

o direito aplicado, pressuposto do exercício pleno do direito de defesa, que impede sejam prolatadas decisões arbitrárias.

Por outro viés, constitui também requisito formal do princípio da proporcionalidade, segundo o qual, nas decisões limitativas de direitos fundamentais o órgão jurisdicional deve realizar a ponderação entre o direito fundamental afetado e o interesse constitucionalmente protegido. Nestes casos, a ausência de fundamentação vulnera o próprio direito fundamental substantivo.[336]

Conclui-se, portanto, que ingerências nas comunicações em canal fechado não podem ser decretadas por qualquer tipo de decisão judicial; necessário que a resolução monocrática ou colegiada justifique-se. A motivação constitui garantia jurisdicional inafastável de todo Estado de Direito, que possibilita aos destinatários do *decisum* o conhecimento das razões e interesses que envolvem o sacrifício de suas liberdades. Neste contexto, considera-se imotivada a autorização que se limita a repetir fundamentos legais da medida sem pormenorizá-los.

A decisão judicial deve indicar claramente o objeto da investigação; identificar e qualificar os investigados (salvo impossibilidade manifesta devidamente justificada); demonstrar a importância da medida restritiva para a apuração da infração penal e indicar os meios que serão empregados para executá-la.

Em regra, o ato decisório terá forma escrita, apenas excepcionalmente permitido que o pedido seja formulado verbalmente. Nestas situações, faz-se obrigatório atentar não apenas à existência de condições que autorizem a interceptação, mas reduzi-la integralmente a termo.

A excepcionalidade da interceptação das comunicações eletrônicas, autêntica forma de coação processual, requer a caracterização do chamado *fumus boni iuris* que, sob a égide do processo penal, é costumeiramente previsto como *fumus delicti comissi*. Desse modo, ao juiz cabe demonstrar por meio de argumento objetivo e concreto, os elementos presentes nos autos que sejam aptos a revelar a existência de crime, bem como o nexo entre este e a participação do agente (lei nº 9.296, art. 2º, inciso I).

[336] M. M. DE MORALES ROMERO, *La intervención judicial de las comunicaciones telefónicas y electrónicas*, in A. S. Hermida (org.), *Investigación y prueba en el proceso penal*, Madrid, Colex, 2006, p. 164.

A materialidade e a autoria delitiva são critérios a ser explicitados pelo magistrado, de forma que, quanto mais restritiva for a medida, maior deverá ser a convicção judicial. Portanto, a aplicação da mais gravosa das providências não poderá se pautar por simples presunções ou conjecturas, mas unicamente por um alto grau de probabilidade passível de demonstração.

Indispensável individualizar o sujeito, ou seja, identificar plenamente a pessoa (ou pessoas) cuja atividade delitiva se investiga por meio da interceptação das comunicações eletrônicas. Apenas quando a intervenção indiciária evidenciar um computador e estando o aparelho vinculado a um sujeito concreto será possível entender cumprida a exigência de especificação pessoal.

Os indícios aptos a sustentar a decretação da intervenção nas comunicações são relativos ao fato típico atribuído ao sujeito, não se prestam a tal finalidade informações que apenas genericamente atestem a gravidade do delito ou a prática de outros crimes. Isto porque, a argumentação deve coadunar-se com o direito do fato e jamais com o chamado direito do autor.[337]

Também, imperioso considerar o denominado *periculum in mora*, cujo conceito filia-se à probabilidade de perigo concreto de insatisfação de um direito, em face da demora na prestação jurisdicional definitiva.[338]

O *fumus boni iuris* e o *periculum in mora,* pressupostos legais da decretação de medidas cautelares, delimitam os aspectos sobre os quais deve versar a motivação judicial: os indícios de existência do crime e da possível autoria, bem como, a necessária tutela de urgência.

---

[337] As ciências criminais informam-se por princípios basilares, como a legalidade estrita, a materialidade e lesividade dos delitos, a responsabilidade pessoal, o contraditório e a presunção de inocência. Na determinação abstrata do que é punível observa-se *"o caráter formal ou legal do critério de definição do desvio e caráter empírico ou fático das hipóteses de desvio legalmente definidas"* (L. FERRAJOLI, *Direito e razão ...*, *op. cit*., p. 38). Por outro lado, o chamado direito do autor é prática de governos autoritários onde *"o objeto de conhecimento e de tratamento penal não é apenas o delito enquanto formalmente previsto na lei, mas o desvio criminal enquanto em si mesmo imoral ou antissocial e, para além dele, a pessoa do delinquente, de cuja maldade ou antissociabilidade o delito é visto como uma manifestação contingente, suficiente, mas nem sempre necessária para justificar a punição"* (Idem, pp. 44-45).

[338] A. P. GRINOVER, A. S. FERNANDES, A. M. GOMES FILHO, *As Nulidades no Processo Penal*, 10ª ed., São Paulo, RT, 2007, p. 332.

Os indícios constituem elementos indiretos de convicção que servem para convalidar a ocorrência dos fatos. Ainda que não se possa falar no caráter de plenitude probatória dos indícios, é certo que possibilitam suspeita fundada e razoável, com base em regras de experiência e postulados lógicos. A partir de uma operação mental de inferência é possível vincular mediatamente certas informações à existência de fatos delitivos.[339]

Segundo o preciso ensinamento de MARIA THEREZA ROCHA DE ASSIS MOURA: *"indício é todo rastro, vestígio, sinal e, em geral, todo fato conhecido, devidamente provado, suscetível de conduzir ao conhecimento de um fato desconhecido, a ele relacionado, por meio de um raciocínio indutivo-dedutivo".*[340]

Aos indícios não pode ser atribuída a segurança característica de um elemento de prova, mas possibilitam a suspeita fundada – razoável, lógica e segundo as regras da experiência – da relação entre a ocorrência do delito e a pessoa investigada, a quem se faz possível imputar responsabilidade.

A intervenção nas comunicações eletrônicas exige apreciação jurisdicional com suporte indiciário. Meras suspeitas ou investigações preventivas com caráter prospectivo não podem ser toleradas para justificar a quebra do sigilo das comunicações e a violação da proteção de dados. Exige-se a observância dos elementos de existência jurídica do indício: (i) conexão lógica entre o indício e o fato a ser provado; (ii) certeza do fato indiciante; (iii) relação de causalidade entre o fato indicador e o fato indicado.

Muito embora o grau indiciário exigido para a interceptação do conteúdo das comunicações seja mais acentuado, não se ignore que a obtenção de dados de tráfego também requer indícios, proscritas as ingerências de caráter genérico voltadas a prevenir ou descobrir delitos.[341]

Os dados externos ou de tráfego têm caráter indiciário, em razão da possibilidade de sustentar uma fundada suspeita. Associados a outros elementos de

[339] M. M. DE MORALES ROMERO, *La intervención judicial ..., op. cit.,* pp. 165-166.
[340] M. T. R. DE ASSIS MOURA, *A Prova por indícios no Processo Penal*, Rio de Janeiro, *Lumen Juris*, 2009, p. 41.
[341] J. J. GONZÁLEZ LÓPEZ, *Los Datos de Tráfico..., op. cit.,* p. 248.

convicção diretos possibilitam construir uma tese coerente. Os fatos que constem em desfavor do investigado devem ter um mínimo de concreção e plausibilidade, de modo que a partir deles se possa inferir que o crime foi ou será praticado.

4.4.3. Limites objetivos, subjetivos e temporais

Indissociável da análise de qualquer medida de coerção faz-se o exame da incidência dos limites de natureza material e processual. A valoração destas restrições obsta eventuais arbitrariedades judiciais e instaura nexo de legalidade a legitimar a atuação estatal.[342]

Em atenção ao parâmetro objetivo, importa averiguar primeiramente a natureza do crime. Deve tratar-se de conduta apenada com reclusão, vedada a intervenção nas comunicações de dados e telefônica em delitos que tenham cominadas penas de detenção ou multa, e nas contravenções. Segundo a letra do art. 2º, inciso III, da lei nº 9.296/96:

> *"Art. 2º. Não será admitida a interceptação de comunicações telefônicas quando ocorrer qualquer das seguintes hipóteses:*
> *(...) III – o fato investigado constituir infração penal punida, no máximo, com pena de detenção."*

Com caráter extraordinário, entretanto, a medida pode ser autorizada na hipótese de crimes não apenados com reclusão, mas que sejam conexos a um injusto para o qual cominada sanção desta natureza.

Sobre a possibilidade de interceptação em todos os crimes apenados com reclusão, parece-nos discordar do caráter de excepcionalidade da medida. Com efeito, nem mesmo o inciso II, do mesmo artigo, que inadmite a interceptação quando a prova

[342] No estudo dos limites da prisão provisória, ANTONIO SCARANCE FERNANDES propõe diferenciação sob os aspectos objetivos, subjetivos e temporais. Formulação que, por sua clareza e adequação, é também adotada neste trabalho (*Funções e limites da prisão processual*, in Revista Brasileira de Ciências Criminais, n. 64, São Paulo, RT, 2007, p. 245).

puder ser obtida por outros meios, é suficiente para afastar o uso desta medida nos ilícitos de menor gravidade.[343]

A opção pelo regime de cumprimento de pena mostra-se generalizadora ao englobar todo o rol de condutas apenadas com reclusão. A previsão legal multiplica as interceptações, em discordância com o critério de proibição do excesso, quando deveria reservar-se aos crimes de maior gravidade, que envolvam lesões ao bens jurídicos mais caros (*v.g.,* vida e a saúde pública), e as condutas que afetam um grande contingente de pessoas.[344]

Por certo, como parâmetro objetivo há também a exigência de que os fatos justificadores da interceptação tratem de conduta delitiva; ou seja, que a determinação judicial esteja no bojo do processo penal. O art. 5º, inciso XII, da Constituição Federal, é expresso ao limitar a medida às investigações criminais.

Os limites subjetivos, por sua vez, delineiam a atuação dos sujeitos processuais envolvidos na intervenção das comunicações: o juiz, o acusado ou investigado e o Ministério Publico.

---

[343] Atente-se à solução do legislador italiano que autorizou a medida apenas para os crimes cuja pena privativa de liberdade seja superior a cinco anos: art. 266 (*Codice di procedura penale) "1. A intercepção de conversas telefónicas ou de comunicações e outras formas de telecomunicação é permitida em ações para as seguintes infrações: a) crimes não culposos para os quais prevista pena de prisão perpétua ou pena de reclusão superior a um máximo de cinco anos determinados de acordo com o artigo 4; b) crimes contra a administração pública para os quais a pena de prisão não seja inferior a cinco anos como previsto no artigo 4; c) infrações relacionadas com estupefacientes ou substâncias psicotrópicas; d) os crimes relativos a armas e substâncias explosivas; e) os crimes de contrabando; f) os crimes de injúria, ameaça, usura, atividades financeiras abusivas, abuso de informação privilegiada, manipulação de mercado, o assédio ou distúrbio a pessoas por meio do telefone; f-bis) crimes previstos no artigo 600-ter, terceiro parágrafo do Código Penal, também se relacionados a material pornográfico referido no artigo 600-quater do mesmo código. 2. Nos mesmos casos, é permitida a intercepção de comunicações entre estes. No entanto, caso venham a ocorrer nos locais especificados no artigo 614 do Código Penal, a interceptação só é permitida se houver fundada razão para acreditar que há uma atividade criminosa ocorrendo* (trad. nossa).

[344] Se a permissão para o emprego da medida em todos os crimes apenados com reclusão não se coaduna com a proporcionalidade em sentido estrito, por outro lado, alguns delitos apenados com detenção são perpetrados por meio dessas modalidades de comunicação e a quebra do sigilo se apresenta como o meio mais adequado de investigação. O Projeto de lei nº 3.272/08 *"estende esse mecanismo de investigação/prova aos delitos apenados com detenção quando a conduta delituosa tiver sido cometida através de meios de comunicação instantânea. Assim, crimes como ameaça e estelionato, quando praticados pelo telefone, não ficarão fora da possível quebra do sigilo de comunicações telefônicas, o que facilitará de forma significativa a apuração e elucidação do caso, em respeito ao princípio da proporcionalidade"* (Exposição de Motivos do Projeto).

Caberá ao juiz decretar a medida, por meio de ordem fundamentada, no início da persecução penal (inquérito policial), ou durante a instrução criminal[345], nos exatos termos do art. 5°, inciso LXI, da Carta Federal.[346]

O decreto será abusivo se não respeitar os casos previstos na lei ou se evidenciada a utilização de argumento legal para encobrir outra motivação. Portanto, a mera repetição da fundamentação legal nos autos, desprovida de suportes fáticos e eivada de hipóteses e suposições, claramente extrapola os limites de atuação fidedigna do magistrado.

O Ministério Público, órgão incumbido de zelar pelas instituições democráticas, está legitimado a requerer a medida na investigação criminal e durante a instrução processual (lei nº 9.296/96, art. 3°, inciso II). Possível, também, seja decretada de ofício pelo magistrado (art. 3°, *caput*), ou mediante requerimento da autoridade policial (art. 3°, inciso I).

Nada obstante a previsão da decretação de ofício (art. 3°, *caput*), de rigor a oitiva do *parquet* para a imposição da medida, por se tratar de órgão constitucional cuja missão é assegurar os direitos individuais e coletivos da sociedade. Sem que seja possível reconhecer adequada a opção do legislador de não lhe dar vista do requerimento da diligência pela autoridade policial.

A manifestação do Ministério Público se dá em nome da defesa das garantias constitucionais do cidadão. Daí porque, a adoção da providência, com a devida intervenção do órgão público acusador, apresenta-se em consonância com o processo penal de índole acusatória.[347]

---

[345] Para o Superior Tribunal de Justiça, o pedido de interceptação prescinde até da instauração de inquérito, por se tratar de providência com natureza de medida cautelar preparatória (HC 85968/SP, rel. Ministro Napoleão Nunes Maia Filho, quinta turma, j. 19.06.08).

[346] Apenas o juiz tem atribuição para impor a medida. Sobre o poder de determinação de interceptação por parte das comissões parlamentares de inquérito (CPI), cuja constituição investiu *"poderes de investigação próprios das autoridades judiciais"* (art. 58, § 3º), a questão encontra-se há muito superada. A Excelsa Corte sustenta a impossibilidade da quebra do sigilo das comunicações em razão da inexistência de poder instrutório ou investigatório para fins penais (MS 23.452-1, rel. Ministro Celso de Melo, pleno, j. 16.09.1999). Para a quebra do sigilo bancário, a melhor exegese do texto constitucional impõe a decisão judicial motivada, *v.* nota 223.

[347] Sobre a determinação judicial de interceptação telefônica de ofício na fase pré-processual, em março de 2005, o Procurador Geral da República ajuizou a ADIN 3450/DF, visando a declaração da

O sujeito passivo da interceptação pode ser tanto o imputado como, também, outras pessoas contra as quais constem indícios de responsabilidade criminal. De qualquer modo, o sujeito afetado pela medida – seja interceptação das comunicações eletrônicas ou intervenção nos dados de tráfego – é aquele sobre quem recaem as suspeitas do cometimento do ato ilícito.[348] Portanto, quem não guarda relação com a conduta típica investigada não pode figurar nos autos como sujeito passivo.[349]

A execução da interceptação realiza-se pela Polícia Civil, federal ou estadual. Recentemente, a discussão assumiu maior complexidade ao se cogitar a realização da diligência pelo órgão ministerial.

Tanto em relação ao plano objetivo, quanto ao subjetivo, pertinente enfrentar a questão da possível ampliação do âmbito da intervenção em razão dos chamados encontros fortuitos. Avaliam-se, aqui, os conhecimentos adquiridos mediante uma intervenção nas comunicações eletrônicas, legitimamente ordenada e executada, que evidencie a prática de outro delito, ou a atuação de sujeito passivo diverso do investigado, situações que não correspondem à finalidade imediata da investigação.[350]

Caso reste evidente que a comunicação se refere a uma conduta criminosa, mais acertado informar de imediato o juiz da causa (ou juiz de plantão) para que avalie a legalidade da instauração consecutiva de inquérito policial para investigar o ilícito.

---

inconstitucionalidade parcial, sem redução de texto, do art. 3º, da lei nº 9.296/96. Ademais, na Ação Direta de Inconstitucionalidade 4112/DF, ajuizada em julho de 2008, sustenta-se a inconstitucionalidade do referido dispositivo legal, com base no comprometimento da imparcialidade do julgador e do processo acusatório. A ADIN 4112/DF contesta, também, a legalidade do art. 3º, inciso II, da lei nº 9.296/96, no que diz respeito à possibilidade de requisição da interceptação pelo Ministério Público durante a instrução penal. Atualmente em trâmite no Supremo Tribunal Federal, as duas ações têm como relator o Ministro Gilmar Mendes.

[348] Situação particularmente difícil refere-se aos casos em que o investigado se vale de computadores públicos (*v.g.* nas *lan houses*) para perpetrar delitos. É necessário, aqui, observar a maior gravidade da intervenção nas comunicações – seja a interceptação da comunicação eletrônica, seja a busca e apreensão do aparelho –, em razão de ingerência potencialmente capaz de ferir direitos de outros usuários de um mesmo terminal. Trata-se, então, de optar com ainda maior cuidado por este meio de obtenção de prova, certificando-se da inexistência de outros igualmente aptos.

[349] A interceptação é dirigida a um sujeito passivo determinado ou determinável, vedada a escuta em desfavor de um grupo de pessoas. Sobre a ilicitude das provas resultantes de interceptação telefônica em que a qualificação e identificação do investigado não conste do requerimento da autoridade policial e nem da decisão do juízo de autorização do monitoramento, *v.* HC 89023/MS, Superior Tribunal de Justiça, rel. Ministra Jane Silva, sexta turma, j. 07.10.08. A Resolução 59, da Corte Superior de Justiça, obriga o magistrado a identificar, expressamente na autorização *"os números de telefone ou nome de usuário, e-mail ou outro identificador em caso de interceptação de dados"*.

[350] A doutrina diferencia o *encontro fortuito* do chamado *encontro inevitável*. Este último refere-se à inevitável aparição de atividades criminosas a respeito das quais se tinha mera suspeita, mas as circunstâncias eram suficientemente claras para aferir que a atividade seria conhecida de qualquer maneira (J. L. R. LAINZ, *Intervención judicial ...* , *op. cit*., p. 288).

Assim, não se despreza a nova prova, mas também não se prescinde da autorização judicial.[351]

Identificada a participação de outro agente na conduta delitiva por meio da intervenção, o conhecimento das comunicações deste com terceiros dependerá inarredavelmente de autorização judicial. O sujeito passivo da medida é sempre individualizado; ou seja, configura séria ameaça às garantias constitucionais, a defesa da tese, segundo a qual, a ingerência possa dar cobertura à invasão do sigilo das comunicações de uma terceira pessoa.

Esta solução impõe que não se renuncie a investigar a *notitia criminis* incidentalmente descoberta em intervenção dirigida a outro fim, desde que haja uma nova e específica autorização.

Deve-se atentar, ainda, à gravidade do delito necessariamente apenado com reclusão; ou seja, inserido no rol de injustos que poderiam ser objeto de uma intervenção telefônica independente.

No âmbito dos limites, ainda outro aspecto – de ordem temporal – deve ser conhecido. Em matéria de restrição de direitos individuais, nenhuma medida poderá perpetuar-se além do lapso temporal estritamente necessário, sob pena de vilipêndio à proporcionalidade da atuação estatal no tratamento da pessoa, com o risco de arbitrariedades. O prazo previsto em lei é de quinze dias, sendo possível a renovação por igual período (lei nº 9.296/96, art. 5°).[352]

[351] O encontro fortuito de crimes conexos ao investigado poderá compor a mesma investigação, não se tratando de ampliação objetiva indevida. Na descoberta de nova prova de crime, por meio de interceptação telefônica cuja autorização judicial não mencione o nome de terceiro (ampliação subjetiva), imprescindível que as informações se relacionem ao fato criminoso objeto da investigação (HC 33553/CE, Superior Tribunal de Justiça, rel. Ministra Laurita Vaz, quinta turma, j. 17.03.2005). Se das comunicações entre o investigado e um terceiro são obtidas fontes de provas que, por si sós, permitiriam a ingerência nas comunicações deste, será necessária autorização judicial ampliadora do âmbito subjetivo para legitimar a intervenção.

[352] Firmado entendimento majoritário no Supremo Tribunal Federal e no Superior Tribunal de Justiça sobre a possibilidade da renovação do prazo, por períodos de até quinze dias, quantos necessários; e ainda, da viabilidade da investigação de crimes conexos descobertos durante a medida, *v.* STF, HC 83515/RS, Ministro Nelson Jobim, pleno, j. 16.09.2004; STJ, Recurso Ordinário em HC 13274/RS, rel. Ministro Gilson Dipp, quinta turma, j. 19.08.2003.

Este entendimento, contudo, foi mitigado pelos tribunais superiores. Caberá ao magistrado avaliar as situações fáticas da investigação e sopesar as circunstâncias que determinaram a requisição da medida.[353]

A motivação da decisão que prorroga a intervenção deve possuir fundamentação autônoma daquela que permitiu o início da medida. A resolução não pode simplesmente reiterar, abstrata ou tautologicamente, as razões anteriores. Nada impede sejam feitas referências às circunstâncias originariamente determinantes da providência, desde que, acrescentados novos motivos ou explicada a razão de não ter alcançado pleno êxito até então.

Há que se demonstrar um sério prognóstico das circunstâncias concretas do caso e da necessidade da medida, justamente para evitar riscos de automatismo no deferimento de prorrogações, com inobservância do esperado juízo de proporcionalidade.

4.5. Direito de defesa

Entre os dez axiomas do garantismo penal encontra-se o postulado *nulla probatio sine defensione*;[354] a defesa representa direito inviolável em todos os atos e graus do procedimento penal.

Sob pena de se comprometer a validade das fontes de prova obtidas por meio de interceptações telemáticas, indispensável a efetiva oportunidade do exercício da

[353] Sobre as interceptações telefônicas, a Excelsa Corte pronunciou-se pela licitude das prorrogações no caso de crimes graves e complexidade da causa (envolvimento com organização criminosa; conexão criminosa com o exterior, número relevante de autos), *v.* Inq. 2424/RJ, rel. Ministro Cezar Peluso, pleno, j. 26.11.2008; RHC 88371/SP, rel. Ministro Gilmar Mendes, segunda turma, j. 14.11.2006; RHC 85575/SP, rel. Ministro Joaquim Barbosa, segunda turma, j. 28.03.2006; HC 84.301/SP, rel. Ministro Joaquim Barbosa, segunda turma, j. 24.03.2006; HC 83.515/RS, rel. Ministro Nelson Jobim, pleno, j. 04.03.2005, e HC 83515/RS, rel. Ministro Nelson Jobim, pleno, j. 16.09.2004.

[354] L. FERRAJOLLI, *Direito e razão* ..., *op. cit*., p. 152.

ampla defesa por parte do inculpado. Afinal, para que a tecnologia atue em favor do processo, *"não poderá subtrair nem diminuir o direito de defesa"*.[355]

Necessário, portanto, tenha conhecimento e acesso ao plexo probatório apresentado pela acusação (sejam os elementos coligidos em seu favor ou desfavor), com o objetivo de acompanhar a produção dos elementos de prova e oferecer argumentos em contrário durante a instrução processual.

O devido processo penal exige o conhecimento pelo acusado da prova produzida pela parte oposta. O ideal de igualdade, representado no processo pela paridade de armas, faz concluir pela possibilidade de controle da prova digital. A defesa técnica efetiva e a autodefesa mostram-se indispensáveis durante a produção probatória.

Nas diligências de investigação realizadas na etapa pré-processual, igualmente deve ser assegurada a participação do investigado e de seu advogado. Neste momento, ainda que não incumba ao poder estatal o dever de cientificar o investigado sobre a realização do ato, inadequado vedar, também, o respectivo acompanhamento.

Em alguma medida, porém, a própria eficiência na obtenção da prova pode depender do sigilo. A hipótese diz respeito a todos os casos em que qualquer advertência sobre a realização da providência comprometa o êxito da operação. Para evitar seja frustrada sua finalidade, admite-se que o poder jurisdicional se furte à informação do investigado quando suficientes as razões de tal limitação do direito de defesa.

A interceptação das comunicações eletrônicas – pela natureza de intromissão instantânea no processo comunicativo – depende do conhecimento do afetado, sob pena do comprometimento da própria dinâmica e eficácia da medida de investigação.

Como desdobramento do exercício da defesa, o direito de informação acerca da realização das intervenção nas comunicações constitui aspecto pouco debatido na doutrina e jurisprudência. Ainda que em momento posterior, a faculdade de ter

[355] J. R. GAVIÃO DE ALMEIDA, *O interrogatório à distância*, São Paulo, Tese de Doutorado, 2000, p. 154.

conhecimento da realização de medidas restritivas de direitos fundamentais decorre diretamente do reconhecimento de um direito fundamental à proteção de dados.[356]

Incumbe ao juiz não permitir que o investigado permaneça indefeso. Se a este não pode ser dado conhecimento prévio da atuação sobre o segredo de suas comunicações, resguarda-se a tutela para o posterior exercício do direito de defesa. Assim, imprescindível disponibilizar às partes, de maneira integral, a comunicação originalmente captada.

O acesso a toda comunicação eletrônica coligida possibilita à defesa colher relevantes elementos probatórios. Afigura-se indispensável contraditório não apenas para facilitar a juntada aos autos dos elementos de prova pertinentes, mas também para contrastar a integridade do material.

O objeto de proteção do direito, em relação às informações de conteúdo pessoal, não se esvai após a realização da intervenção. Remanesce, portanto, a obrigação estatal de dar ciência ao investigado da realização pretérita de medidas investigativas, sejam de interceptação das comunicações eletrônicas, como também, de obtenção de dados de tráfego.[357]

Não é razoável invocar a menor potencialidade lesiva da intervenção nos dados externos da comunicação como justificativa para elidir a obrigação de informar o investigado da realização desta medida. Como é sabido, nem sempre a obtenção de dados de tráfego será providência menos lesiva aos direitos fundamentais, em razão do acentuado

[356] Precedente deste posicionamento, a sentença do Tribunal Europeu de Direitos Humanos, de 6 de setembro de 1978 (caso *Klass vs.* Alemanha), sustentou que depois da conclusão da ingerência no sigilo das comunicações, o sujeito passivo da medida tem o direito de informar-se sobre todas as intervenções realizadas sem o seu conhecimento, exatamente para que possa averiguar a legalidade da atuação. Após a ciência da medida, o cidadão poderá fazer uso dos remédios legais para questionar o procedimento do Poder Público. É de se ressalvar, no entanto, os casos em que a revelação, mesmo posterior ao término da intervenção, possa comprometer outras linhas investigativas que estejam em curso ou a eficácia do método investigativo. A referida hipótese é excepcional, destinada especialmente à criminalidade organizada, hipótese em que o referido investigado disseminaria a notícia da investigação prontamente e ocultaria eventuais fontes de prova da prática delitiva. A lei pátria não disciplinou esta situação, mas já é chegado o momento de fazê-lo. Especial atenção merece a circunstância do tratamento de dados sensíveis por partes dos órgãos policiais, armazenadas por vezes informações atinentes à ideologia, filiação partidária, religião, saúde e vida sexual, em frontal restrição do direito à autodeterminação informativa.

[357] O legislador pátrio ainda não se ocupou desta previsão legal. Caberá à norma determinar o marco temporal para a disponibilização da informação ao investigado; por óbvio, sempre posterior ao término da manutenção do sigilo da medida.

perigo representado pelo cruzamento de informações geralmente destinado a elaborar perfis pessoais.

Em caráter excepcional pode ser adiada a comunicação da realização da medida ao inculpado, com o objetivo de não revelar outras investigações em curso ou para não evidenciar métodos policiais, linhas investigativas, e de não inviabilizar futura diligência policial. O controle judicial é imprescindível no curso desta dilação temporal.[358]

As possibilidades de exercício de investigação defensiva ampliam-se rapidamente, franqueando ao investigado o emprego de meios técnicos, gráficos, fotográficos ou audiovisuais.

4.6. Princípio da proporcionalidade

O princípio da proporcionalidade tem *status* de postulado constitucional autônomo, ainda que não conste expressamente na Carta Maior. A sede material de sua formulação deita raízes no corolário constitucional do devido processo legal (CF, art. 5°, inciso LIV).[359]

A proporcionalidade, técnica jurídica a nortear o juízo do magistrado, pode ser desdobrada em três subprincípios: a *idoneidade* da medida para o alcance do fim almejado; a *necessidade* de sua adoção e a *proporcionalidade em sentido estrito* (ponderabilidade dos interesses em conflito).

---

[358] B. S. RODRIGUES, *A monitorização dos fluxos*..., *op. cit*., p. 232.

[359] Sobre o caráter jurídico da proporcionalidade como instrumento de defesa de direitos fundamentais e o vínculo jurídico deste princípio com o *due processo of law, v.* W. S. GUERRA FILHO, *Princípio da proporcionalidade e devido processo legal*, in V. Afonso da Silva (org.), *Interpretação constitucional*, São Paulo, Malheiros, 2007, pp. 255-269; W. S. GUERRA FILHO, *Ensaios de Teoria Constitucional*, Fortaleza-Ceará, Universidade do Ceará, 1989, pp. 69-86. A. SCARANCE FERNANDES ressalta a íntima ligação entre o princípio da proporcionalidade e o princípio da isonomia: *"(...) embora tenham objetos e fins próprios, tangenciam-se principalmente no fato de que, para haver igualdade, devem ser superadas as desigualdades dos indivíduos e especificados os critérios para determinar em que medida as distinções entre eles podem ser admitidas"* (*Processo Penal* ..., *op. cit*., p. 51).

Em linhas gerais, a idoneidade corresponde à adequação qualitativa, quantitativa e subjetiva da medida, em atenção à viabilidade de concretização do respectivo escopo. Dificilmente se sustentará uma intervenção operada durante lapso temporal prolongado ou contra diversos sujeitos passivos que não produza resultados concretos; o excesso desqualifica a legitimidade pretérita.

A necessidade relaciona-se diretamente ao juízo de intervenção mínima, característico do Direito Penal: a limitação do direito opera-se somente quando razoavelmente não existam outros meios de investigação menos restritivos dos direitos da pessoa objeto de investigação.

A proporcionalidade em sentido estrito, por sua vez, expressa a valoração das consequências do ato em relação à estigmatização jurídica e social que sofrerá o inculpado.[360]

Nos casos previstos para a interceptação das comunicações em canal fechado, impende avaliar se a medida aplicada no curso da persecução penal não se mostra desproporcional em comparação à pena cominada ao suposto delito. Proibir a violação dos direitos ao sigilo das comunicações e à proteção de dados na investigação de crimes não apenados com reclusão é consideração afinada com os ditames da razoabilidade.

Se no caso concreto inexiste gravidade no crime investigado, não haverá recorrer a este expediente. Outrossim, necessária a presença de fundadas razões que comprovem a insuficiência de outros instrumentos para a elucidação dos fatos (lei nº 9.296/96, art. 2°, parágrafo único).

O princípio da proporcionalidade está intimamente relacionado à dinâmica processual penal que presume a inocência do inculpado. Os processados devem ser tratados como inocentes e nunca equiparados aos definitivamente sentenciados. Assim, a ingerência será constitucionalmente admissível apenas quando no caso concreto os

[360] S. T. BARROS, *O Princípio da Proporcionalidade e o Controle de Constitucionalidade das Leis Restritivas de Direitos Individuais*, Brasília, Brasília Jurídica, 1996, pp. 72-84.

interesses individuais não forem superiores ao interesse estatal do *jus persequendi*, conforme o subprincípio da proporcionalidade em sentido estrito.[361]

A interceptação das comunicações será inadequada quando a intervenção nos dados de tráfego, em razão da menor intensidade da ingerência nos direitos fundamentais do investigado, já se mostre suficiente para lograr êxito. Hipóteses em que a informação buscada é aquela referente ao momento, duração e tamanho (origem e destino da comunicação). É, portanto, medida lógica que se faça todo o possível para evitar a interceptação quando providência menos gravosa possa alcançar os mesmos resultados.

O legislador ordinário furtou-se à responsabilidade de estabelecer um rol indicativo dos crimes passíveis de intervenção nas comunicações, recorrendo a uma genérica previsão de crimes apenados com reclusão. Importante a revisão deste critério e da duração da medida, que não deve ultrapassar o tempo estritamente necessário à realização das operações técnicas pertinentes.

A finalidade das exigências decorrentes do princípio da proporcionalidade é evitar que um meio de obtenção de prova seja utilizado como instrumento processual em permanente desfavor do *status* de inocência do inculpado.

4.7. Controle

Em primeiro lugar, é certo que deve haver uma atuação harmônica de todos os órgãos estatais para a consecução da investigação criminal. Nesse sentido, os instrumentos de caráter infralegal que favoreçam a coordenação entre a Polícia, o Ministério Público e os Tribunais, além das operadoras de telecomunicações e administradores de sistemas.

[361] N. GONZÁLEZ-CUÉLLAR SERRANO, *Garantías constitucionales de la persecución penal en el entorno digital*, in J. L. Gómez Colomer (coord.), *Prueba y Proceso Penal*, Valencia, Tirant lo Blanch, 2008, pp. 161-162.

Incumbe ao Poder Judiciário a apreciação das prorrogações das medidas de intervenção, em caráter de reapreciação da respectiva legalidade. O controle pressupõe a observação do cumprimento material da providência e de sua compatibilidade com os respectivos termos do mandado judicial.[362]

A alta complexidade das formas de comunicação hodiernas faz com que as intervenções sejam praticadas amiúde através dos próprios serviços de comunicação eletrônica. Inevitável, portanto, que a própria resolução judicial imponha condições mínimas à intervenção, tais como, a minuciosa descrição da realização da medida (*v.g.,* dia, hora e duração) e do meio técnico empregado.

Pertinente, ademais, tanto as intervenções praticadas pelos órgãos policiais, como pelos prestadores de serviço, indiquem as pessoas responsáveis pela realização da medida, o procedimento técnico adequado e as providências para a preservação dos dados digitais (*v.* cap. sexto).[363]

O controle judicial possibilita ao magistrado acompanhar os resultados obtidos na investigação, decretar a cessação das medidas restritivas de direitos e alterar os respectivos prazos de duração dos procedimentos técnicos. Apropriada, ainda, a previsão do regime de custódia dos suportes físicos onde armazenados os dados digitais.

Ademais, de rigor as intervenções policiais nas comunicações em canal fechado sejam realizadas por equipe de profissionais distintos daqueles que encabeçam as investigações; rigorosamente apartados os arquivos e as informações submetidas a sigilo[364] daquelas passíveis de revelação.

A lei nº 9.296/96 não abordou aspectos imprescindíveis à salvaguarda do material objeto da intervenção, que se encontre sob a responsabilidade da autoridade policial. Medidas como as garantias de inalterabilidade, autenticidade e integridade dos

[362] Sem perder de vista que o Anteprojeto do Código de Processo Penal (Projeto de lei do Senado nº 156, de 2009), em tramitação na Câmara dos Deputados (PL 8045/2010), para privilegiar a garantia da imparcialidade do julgamento institui a figura do juiz de garantias, responsável pela realização das medidas pré-processuais cabíveis.
[363] J. J. GONZÁLEZ LÓPEZ, *Los Datos de Tráfico*..., *op. cit*., p. 290.
[364] Considere-se, por exemplo, as comunicações entre o investigado e seu advogado, sujeitas ao mais completo sigilo.

dados armazenados em suportes automatizados (para efeito de encaminhamento à autoridade solicitante), foram olvidadas pelo legislador.

Os encarregados de realizar as intervenções responsabilizam-se por fornecer periódica, pontual e frequente atualização das informações coligidas, sempre que instados a tanto. Igualmente relevante a demonstração do emprego de meios e procedimentos que garantam a autenticidade e integridade da informação obtida, assim como o cumprimento das diretrizes de conservação.

O controle das intervenções realizadas pela polícia permite afirmar com maior segurança a autenticidade das gravações. Evita-se assim que as informações coletadas sejam indevidamente manipuladas pelos responsáveis técnicos, assegurando-se a idoneidade das provas e procedimentos.

A participação do Ministério Público no exercício do controle da legalidade da medida é imperativo constitucional. Por força da Constituição de 1988, a instituição desempenha dúplice papel, como *órgão acusador* e *fiscalizador dos Poderes Públicos na aplicação da Lei* (CF, art. 128, I e II). Assim, ao membro do *parquet* impõe não apenas requisitar a intervenção, mas diuturnamente avaliar a presença dos pressupostos, requisitos e limites (objetivo e temporal) da medida.

A decretação de sigilo na obtenção da prova visa impedir que o investigado tenha conhecimento da intervenção e acabe por frustrá-la. Nessas condições, o Ministério Público atuará como órgão institucional encarregado do controle da legalidade da medida. Nos arts. 127, *caput*, e 129, incisos II e VII, da Carta de Direitos, estão presentes os fundamentos do controle e vigilância no curso do processo.

Por fim, lembre-se que o Projeto de lei nº 3.272/2008 propõe, para fins estatísticos, um controle centralizado do número de interceptações autorizadas. O Conselho Nacional de Justiça (CNJ), por meio da Resolução nº 59/2008, determinou o aperfeiçoamento e uniformização do sistema de medidas cautelares referentes às interceptações telefônicas, de informática e telemática. Com vistas à padronização dos procedimentos, obrigatório que os juízos criminais informem às corregedorias dos respectivos tribunais, a quantidade de interceptações em andamento e de ofícios expedidos

às operadoras de telefonia. Enviados ao CNJ, para providências de aperfeiçoamento, os dados coligidos pelas corregedorias.

4.8. Intervenção nas comunicações em canal aberto

A captação de informações no entorno digital pode ocorrer tanto em função da investigação penal, a partir de uma *noticia criminis,* como também, sob a perspectiva de buscas digitais preventivas. O mesmo controle ou vigilância exercido pela polícia nas ruas pode ser realizado na *internet* com o fito de prevenir futuros delitos.

O principal aspecto da intervenção nas comunicações em canal aberto concerne à desnecessidade de resolução judicial que habilite o conhecimento e a apreensão de dados para fins de investigação. O caráter público da informação funda-se no consentimento do seu titular como elemento incidente a elidir a aplicação do segredo da comunicação.[365]

As fontes de prova nas comunicações em canal aberto são plenamente acessíveis ao público. A previsão normativa desta modalidade de buscas digitais se faz necessária em virtude de suas particularidades, principalmente, porque o direito à proteção de dados do investigado resta mitigado no curso das investigações.[366]

O caráter público dos dados pressupõe um consentimento tácito por parte de seu titular. Não deixa de incidir, contudo, a proteção específica relativa à autodeterminação informativa. Não pode haver tratamento inconsentido de dados, de sorte que o titular há de ser informado; vinculado o consentimento a uma finalidade específica e determinada.

[365] O que não autoriza, contudo, o armazenamento de dados sensíveis e a criação de bancos de dados policiais sem previsão legal.
[366] Esta atuação de fiscalização das "cyber polícias" no entorno digital permite que a partir do rastro deixado pelo internauta seja possível identificar o criminoso, por meio de uma lógica de inversão: parte-se do computador da vítima para fazer o caminho inverso ao computador do agressor (B. S. RODRIGUES, *A monitorização dos fluxos ...*, *op. cit.,* p. 91).

Os *blogs* ou foros digitais, espécie de página virtual muito utilizada hodiernamente, caracterizam-se pela gestão do conteúdo, sob a responsabilidade de um ou alguns internautas. Nos *blogs* são introduzidos conteúdos de diversas modalidades, como textos, mensagens, etc., sendo possível aos visitantes responder tópicos e acrescentar observações.

Os dados de localização viabilizados na *internet*, especialmente aqueles disponibilizados em redes sociais, também são alvo de atenção. Por se tratar de dado pessoal disponível a grupos de pessoas, ou até mesmo publicamente, são acentuados os riscos de que estejam sujeitos a tratamento não consentido.

Em todas essas situações, o consentimento é um dado relevante, uma vez que a *internet* é campo propício às infiltrações policiais.[367] O caráter interativo da *internet* facilita a participação em *chats* abertos ao público[368], e a partir da confiança adquirida pelos interlocutores se faz possível o intercâmbio bidirecional de informação. No entanto, é preciso prudência, porque esta prática pode redundar em ilicitude probatória, como em casos de fontes de provas obtidas mediante ameaça ou coação.

O agente infiltrado é meio de busca de prova nominado (lei nº 10.217/01, art. 2º, inciso V), mas que, por carecer de regramento jurídico, constitui meio

[367] A respeito das infiltrações policiais, propício discorrer brevemente sobre precedente do Tribunal de Estrasburgo (caso *Lüdi vs.* Suiça, j. 15 jun.1992). Na ocasião, alegou o requerente, as fontes de prova que fundamentaram a sua condenação se valeram de contatos entre ele e o policial; informações que teriam sido obtidas de maneira fraudulenta, à míngua de consentimento. A Corte entendeu que as atividades do agente encoberto não estavam em desacordo com a tutela da vida privada – o requerente ao vender estupefacientes deveria ter consciência da ilicitude da conduta e do risco que corria de oferecer a substância a um agente infiltrado. No entanto, o argumento da Corte pode ser confrontado com a seguinte pergunta: por que a justificativa se aplica ao agente encoberto e não às interceptações telefônicas? Afinal, não parece razoável afirmar que os criminosos em geral estejam dispostos a correr o risco de ter seus telefones grampeados e de vir submetidos a todos os tipos de captação de comunicações. Para uma abordagem percuciente das infiltrações policiais na *internet, v. Infiltración policial,* J. J. GONZÁLEZ LÓPEZ*…, op. cit.*

[368] Sobre a intervenção em comunicação aberta, no julgamento do Recurso de *Habeas Corpus* 18.116-SP, assim concluiu o Superior Tribunal de Justiça: "*A conversa realizada em 'sala de bate papo' da internet, não está amparada pelo sigilo das comunicações, pois o ambiente virtual é de acesso irrestrito e destinado a conversas informais"*. Consta do voto proferido pelo relator Ministro Hélio Quaglia Barbosa: "*(...) Dos documentos acostados é verificado que a INTERPOL interceptou conversa do acusado em 'sala de bate-papo' na Internet, momento em que foi noticiado a transmissão de imagens pornográficas envolvendo crianças e adolescentes. Esta conduta funcionou como elemento condutor da instauração do referido inquérito policial. (...) Acertada a decisão do e. Tribunal Regional Federal da 3ª Região que sobre o tema entendeu não haver o sigilo das comunicações, uma vez que a conversa fora realizada em 'sala de bate papo' da internet, em que se caracteriza, em 'ambiente virtual de acesso irrestrito e destinado a conversas informais"* (RHC 18.116-SP, rel. Ministro Hélio Quaglia Barbosa, sexta turma, j. 16.02.06).

atípico. Inadmissível, então, o emprego rotineiro desta técnica de investigação pelos órgãos policiais.

A frequência com que empregada a tecnologia para o cometimento de crimes faz refletir sobre a pertinência de uma lei que venha disciplinar o agente encoberto. A autorização legal depende, no entanto, de uma larga discussão acerca do caráter insidioso deste método investigativo. Lembre-se que a interação entre policial e investigado ocorre sem que aquele revele sua verdadeira identidade.

Para os autores que entendem legítimo o uso de agente encoberto no entorno digital, as condições mínimas para seu emprego são a suficiente previsão legal e o controle jurisdicional da medida[369]. A autorização da providência depende dos indícios de materialidade e autoria, da motivação, do juízo de proporcionalidade e da individuação do sujeito passivo. Intoleráveis as buscas indeterminadas, chamadas *fishing expeditions*, com caráter prévio, que vasculham indiscriminadamente as atividades do internauta.[370]

[369] A delimitação do alcance da medida mostra-se pertinente para a determinação dos *sites* sujeitos ao controle, gestão de áreas da comunicação, intercâmbio e participação em redes ou sistemas informáticos (J. J. GONZÁLEZ LÓPEZ, *Infiltración policial* ..., *op. cit*., p. 117).

[370] J. J. GONZÁLEZ LÓPEZ esclarece que a infiltração policial depende de uma série de medidas previamente adotadas pela polícia. Além da autorização judicial é necessária adoção de medidas para que os operadores e servidores de *internet* preservem as fontes de prova obtidas (Idem, pp. 111-115).

CAPÍTULO V – ACESSO AOS DADOS DIGITAIS ARMAZENADOS EM SUPORTE ELETRÔNICO

5.1. Generalidades

Os direitos e garantias individuais previstos na Constituição Federal limitam as hipóteses de busca e apreensão a situações excepcionais. A consagração dos direitos à inviolabilidade do domicílio, intimidade e vida privada (art. 5°, incisos XI e X, respectivamente), bem como do devido processo legal e da proibição de provas ilícitas (art. 5°, incisos LIV e LVI), obriga o Poder Público a exercer o *jus persequendi* apenas nos estritos limites autorizados pelo constituinte.

Para resguardar o domicílio de intromissões ilegítimas, a possibilidade de ingresso sem autorização judicial permanece restrita a situações extraordinárias: mediante o consentimento do morador, em caso de flagrante delito, de desastre ou para prestar socorro. À sua vez, a entrada da polícia judiciária munida de mandado judicial só será possível durante o dia.[371]

As principais diferenças entre as medidas de acesso aos dados armazenados em suporte eletrônico e as intervenções nas comunicações eletrônicas concernem ao momento e ao *modus operandi* com que se obtém a fonte de prova. A opção por abordar em capítulo específico cada uma das medidas, justifica-se pela diversidade de operações técnicas e pelo caráter específico da ingerência nas porções mais íntimas da personalidade. Os critérios norteadores deste exame guardam estreita semelhança com noções já abordadas anteriormente, referentes ao *conceito*, *regulação*, *natureza jurídica*, *condicionantes legais*, *direito de defesa*, *proporcionalidade* e *controle judicial*.

[371] A inviolabilidade do domicílio consta amplamente assegurada também nos documentos internacionais dos quais o Brasil é signatário: art. 11, n. 2, do Pacto de São José da Costa Rica; art. 12, da Declaração Universal dos Direitos Humanos, de 10 de dezembro de 1948, e arts. 22, 27 e 30, da Convenção de Viena, de 18 de abril de 1961.

O conhecimento dos dados digitais armazenados é possível mediante colaboração (do servidor ou de particular) ou por intermédio da busca e apreensão. Nos itens seguintes, particular atenção merece este meio de obtenção de prova, apto a franquear o acesso a diversas modalidades de dados pessoais, muitas vezes, até mesmo pertencentes a mais de um titular.

5.1.1. Conceito

Há um legítimo e inegável interesse de trazer à persecução penal, pessoas, semoventes ou coisas que apresentem relevância para o processo. Para tanto, o Poder Público exerce o *jus persequendi in judicio* na procura ou pesquisa de elementos essenciais para a relação processual.

Como normalmente se procede à apreensão do objeto encontrado[372], esta relação entre meio e fim inspirou o legislador processual penal a tratar conjuntamente dois atos que são independentes. A diversidade dos conceitos pode ser exemplificada no fato da busca impor restrição às garantias de liberdade individual (inviolabilidade de domicílio e da pessoa física), enquanto as apreensões *"emergem como limitações ao poder individual de deter as coisas e de reter as pessoas"*.[373]

A diligência de busca consiste na atividade de esquadrinhar e revistar lugar certo, previamente designado em mandado judicial, de forma clara e completa.[374] Segundo a lição de CLEUNICE BASTOS PITOMBO, o conceito de busca pode ser sintetizado como:

---

[372] O ato de apreensão ocorre em função ou da ilicitude do objeto ou de sua inegável importância para o processo. É possível que a apreensão ocorra em território sujeito a jurisdição alheia, autorizada no seguimento de pessoa ou coisa (CPP, art. 250). Como cautela, exige-se apresentação à autoridade local, antes ou depois, dando ciência dos fatos ocorridos. Diante de situação urgente, o ato de apresentação pode ser realizado posteriormente.

[373] S. PITOMBO, *Do sequestro no processo penal brasileiro*, São Paulo, Bushatsky, 1973, p. 73.

[374] Nesse sentido era a lição de J. M. DE ALMEIDA JUNIOR, que há um século atrás já propugnava a ilegalidade das buscas gerais, *v. O Processo Criminal Brazileiro*, v. II, 2ª ed., Rio de Janeiro, Francisco Alves e Cia, 1911, p. 48.

> "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 a hipótese: de pessoa (vítima de crime, suspeito, indiciado, acusado, condenado, testemunha e perito), semoventes (veículo), coisas (objetos, papéis e documentos), bem como de vestígios (rastros, sinais e pistas) da infração."[375]

Sob outra perspectiva, a apreensão consiste na medida assecuratória que toma algo de alguém ou de algum lugar com a finalidade de produzir prova. Trata-se de ato processual penal de apossamento, remoção e guarda de coisas, semoventes ou pessoas, em cumprimento de ordem ou decisão judicial. O objeto da medida permanece sob custódia enquanto perdurar o interesse processual de resguardá-la.

5.2. Regulação

A evolução doutrinária e jurisprudencial dos meios de busca de prova desdobra-se em algumas etapas. Como exemplo, pense-se no aperfeiçoamento da disciplina da interceptação telefônica. No regime anterior à Constituição de 1988, entendia-se possível realizá-la mesmo à míngua de regulamentação infraconstitucional específica. À época, com fundamento na autorização genérica do art. 57, do Código Brasileiro de Telecomunicações, as interceptações eram prática diuturna.[376]

Com o advento da Carta Cidadã de 1988, discutiu-se a recepção do art. 57, do CBT, em face da disposição contida na parte final do art. 5°, inciso XII, do texto constitucional. A Excelsa Corte, em corajoso entendimento, sustentou a ilegalidade da quebra do sigilo telefônico, com fulcro na ausência de lei específica que regulamentasse o

[375] C. B. PITOMBO, *Da busca e apreensão ...*, *op. cit*., p. 109.
[376] *"Art. 57. Não constitui violação de telecomunicação (...) II – o conhecimento dado (...) e) ao juiz competente, mediante requisição ou intimação deste".*

preceito.[377] Assim, apenas com a entrada em vigor da lei nº 9.296/96, o Poder Legislativo supriu o atraso na regulação da matéria.

No estágio atual, tanto a interceptação telefônica, como a busca e apreensão, possuem disciplina própria; no entanto, as bases concretas estabelecidas pela lei remanescem insuficientes.[378]

A elaboração de um regime jurídico para a busca e apreensão de aparatos eletrônicos pressupõe, pois, o enfrentamento de hipóteses ainda pouco debatidas na doutrina e jurisprudência. Há que refletir sobre o modo de realização e o fundamento legal para as buscas e apreensões de dados, sejam estes conservados pelos provedores de serviços de comunicação ou por quaisquer outros entes privados.

5.2.1. Ordenamento pátrio

O regime jurídico das buscas e apreensões consta do Livro I ("Do processo em geral"), Título VII ("Da prova"), Capítulo XI, do Código de processo penal. O tratamento unitário[379] da busca e apreensão é característico da tradição legislativa e doutrinária pátria:

> "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

[377] HC 69912 RS, rel. Ministro Sepúlveda Pertence, pleno, j. 16.12.1993.
[378] M. M. DE MORALES ROMERO constata estas fases também no Direito espanhol. Até 1988 eram praticadas escutas telefônicas desacompanhadas de base legal, situação modificada em razão da condenação da Espanha no Tribunal Europeu de Direitos Humanos (TEDH). Atualmente as intervenções são praticadas com fundamento normativo, no entanto, a disciplina é claramente insuficiente. A autora procura enfrentar a difícil indagação: pode o Judiciário completar as lacunas e deficiências da lei? (*La intervención judicial ...*, *op. cit*., pp. 156-157).
[379] CLEUNICE BASTOS PITOMBO aduz que regulação em separado de ambos os atos ocorreu apenas *"no Código de Processo Penal Militar (Seção II, arts. 185 a 189), nos Anteprojetos de reforma do atual Código de Processo Penal, elaborados por Hélio Tornaghi (Seção II, arts. 401 a 405) e José Frederico Marques (Seção II, arts, 216 a 220) e, também, no Projeto de 1983 (Seção II, arts. 188 a 192) que a disciplinavam em Seção autônoma"* (*Da busca e apreensão ..., op. cit.*, pp. 102-103).

> distinguem da apreensão, como os meios diferem dos fins".[380]

Em razão de normalmente se proceder à apreensão do que se encontrou, optou o legislador por disciplinar conjuntamente esta relação entre meio e fim no CPP. Contudo, a busca pode (i) não resultar em apreensão; (ii) ser concluída com uma prisão; (iii) ter como objetivo encontrar uma pessoa (*v. g.,* vítima de um crime que se encontra em cativeiro). Também é possível que haja apenas apreensão, na hipótese de ser a coisa entregue espontaneamente à autoridade.

A busca autorizada judicialmente realiza-se pelos investigadores da polícia judiciária ou por oficiais de justiça. O ingresso no domicílio ocorre durante o dia, precedido da apresentação e leitura do mandado ao morador ou a quem o represente. O executor notifica o ingresso, e em caso de negativa do morador, a porta poderá ser arrombada e forçada a entrada, procedendo-se à busca e apreensão. Se a pessoa ou coisa procurada for determinada, o morador será notificado a mostrá-la. Exibindo-a, será apreendida e posta sob custódia da autoridade ou de seus agentes.[381]

No interior da residência, admite-se o emprego da força contra coisas, para descobrir o que se procura, se houver resistência do morador (CPP, art. 245, §§ 3º e 4º).

Encontrado o objeto da busca, proceder-se-á à apreensão, colocando-o sob custódia da autoridade ou de seus agentes. Concluída a diligência, deverá ser lavrado auto circunstanciado, assinado pelos executores do mandado e por duas testemunhas presenciais (CPP, art. 245, § 7º).

Havendo excesso, os autores responderão pelo abuso – sempre que presente violência desnecessária, danos maiores que os indispensáveis ou arbitrariedade e exibicionismo (lei nº 4.898/65, art. 3º, letra *b*). Incorrer em excesso durante a diligência

[380] S. PITOMBO, *Do sequestro no processo penal brasileiro*, São Paulo, Bushatsky, 1973, p. 60.
[381] A procura em lugar público de uso comum do povo (ruas, praças, estradas) dispensa autorização judicial. Por outro lado, a busca em repartição pública pressupõe que o executor da medida esteja munido de mandado judicial.

caracteriza lesão a direito líquido e certo do investigado e autoriza a impetração de mandado de segurança.[382]

Se realizada pessoalmente pela autoridade judicial não há necessidade de mandado. O juiz revela sua identidade ao morador e esclarece o objeto da diligência (CPP, art. 245, § 1º). Em caso de resistência do sujeito passivo ou de terceiro que esteja auxiliando, será possível a prisão em flagrante por crime de resistência (CP, art. 329) ou desobediência (CP, art. 330).

A busca não é possível à noite, porém, iniciada durante o dia, poderá persistir até o período noturno. Para esclarecer o período que se entende por noturno, aplica-se analogicamente o art. 172, do Código de Processo Civil, que dispõe sobre a realização dos atos processuais entre seis e vinte horas. Finda a busca, logo em seguida será lavrado auto circunstanciado em que se consignará tudo quanto ocorrido durante a diligência (CPP, art. 245, § 7º).[383]

A apreensão de dados digitais armazenados em suporte eletrônico, que se encontrem em bases particulares, tem fulcro nas fundadas razões da descoberta *"de objetos necessários à prova de infração ou à defesa do réu"* (CPP, art. 240, § 1º, alínea *e*). Em síntese, informações fidedignas, indícios razoáveis de que o objeto da medida se encontra no local devassado.

No caso de informações em poder dos provedores ou dos serviços de *internet*, a cessão de dados impõe a revelação de conteúdo submetido a tratamento. Embora inexistente disciplina legal, sempre que efetuada qualquer operação técnica de caráter automatizado, a configurar tratamento (*v.* item 6.1), resultará necessário solicitar ao responsável do banco as informações referentes à gestão dos dados digitais.

[382] O *writ* constitucional será também a providência pertinente para a restituição de coisa indevidamente apreendida, quando demonstrado que os objetos não se relacionam com o fato investigado (CPP, art. 6º, inciso II; art. 11; e arts. 240 a 250).
[383] F. DA C. TOURINHO FILHO, *Manual de Processo ..., op. cit.*, p. 584.

5.2.2. Convenção de Budapeste

O art. 8º, da Convenção Europeia de Direitos Humanos, tutela a vida privada e familiar. O Tribunal de Estrasburgo (TEDH), ao interpretar o preceito reconheceu que o âmbito de proteção da inviolabilidade do domicílio incorpora o local de atividades profissionais[384] e a extensão de seus efeitos em favor de pessoas jurídicas.[385]

Caso dados digitais úteis à apuração de um delito não sejam entregues voluntariamente, será possível a realização da busca e apreensão *(search and seizure)* nos termos do Título IV, da Convenção sobre *cyber* criminalidade.

O art. 18, consigna a chamada "ordem de apresentação", com o objetivo de facultar às autoridades competentes o acesso aos dados necessários para identificar certo indivíduo. O dispositivo disciplina a busca de dados em poder de um provedor ou de qualquer outra pessoa física ou jurídica. Há, contudo, alguma indeterminação no preceito, à medida que apenas genericamente se faz menção às garantias fundamentais dos artigos 14 e 15 como critérios a serem observados.

De acordo com a Convenção, os Estados partes devem adotar medidas legislativas ou de outra natureza que possibilitem às autoridades competentes acessar um sistema informático e os dados nele armazenados (art. 19.1). Prevista, caso não sejam entregues voluntariamente, a obrigação dos Estados de autorizar o confisco por suas autoridades.

A apreensão consiste no poder de sequestrar ou assegurar de outro modo o sistema informático, parte dele, ou o meio de armazenamento, realizar cópias dos dados e manter a integridade das informações relevantes armazenadas. As duas funções da

[384] De acordo com a Corte, a proteção à vida associa-se ao direito de estabelecer e desenvolver relações com outras pessoas. Não há razões para excluir as atividades profissionais do conceito de 'vida privada', até mesmo porque o objeto central de proteção do art. 8º, é proteger a pessoa contra arbitrárias interferências das autoridades públicas (*v.* Caso *Niemietz vs.* Alemanha, j. 16 dez. de 1992, parágrafo 29).

[385] A proteção do local de exercício das atividades da pessoa jurídica, ainda que não tenha a mesma intensidade do direito individual de inviolabilidade do domicílio, exige para o ingresso expressa autorização judicial (*v. Caso Stés Colas Est vs.* França, j. 16 abr. de 2002, parágrafo 49).

apreensão consistem na recolha de prova (cópia dos dados) ou no confisco de dados (cópia e posterior medida que torne inacessíveis as informações).

O artigo 19, n. 3, da Convenção, enumera várias medidas tendentes a preservar a integridade e a originalidade da fonte de prova digital: (i) apreender ou obter de modo similar um sistema informático ou uma parte deste, ou um suporte de armazenamento informático; (ii) efetuar e conservar uma cópia desses dados informáticos; (iii) preservar a integridade dos dados informáticos relevantes armazenados; (iv) tornar inacessíveis ou eliminar esses dados informáticos do sistema acessado.

Com clareza, constata-se que a ideia norteadora destas disposições rege-se segundo a concretização da cooperação e assistência mútua entre os Estados.[386] As investidas contra a criminalidade virtual não podem mais permanecer restritas às fronteiras territoriais. O uso dos tradicionais mecanismos internacionais de cooperação policial e judicial deve ser implementado com a maior amplitude possível.[387]

5.3. Natureza Jurídica

As diligências investigativas voltadas a acessar dados digitais armazenados em suportes eletrônicos caracterizam-se como providências de natureza jurídica dúplice: acautelatória e probatória.

[386] Em 26 de julho de 1995, foi assinada a Convenção que instituiu a Europol – órgão supraestatal de combate à criminalidade – em vigor desde 1º de outubro de 1998. Seu objetivo principal é construir um banco de dados para o intercâmbio de informações entre os Estados-parte e combater crimes como o tráfico ilegal de material nuclear e radioativo; as organizações clandestinas de imigração; o tráfico de seres humanos; o tráfico de drogas; o comércio de veículos roubados; o terrorismo; a criminalidade que faz uso dos recursos tecnológicos; a lavagem de dinheiro e a falsificação de moeda. O Serviço Europeu de Polícia baseia-se principalmente em duas estruturas complementares: (i) unidades nacionais, responsáveis pela coleta e entrega de informações úteis para a investigação; (ii) uma estrutura central, sediada em Haia, composta por representantes da polícia dos Estados-membros, que organiza os respectivos dados e encaminha às unidades descentralizadas, a seu pedido (O. DE FROUVILLE, *La preuve pénale: internationalisation et nouvelles technologies,* Paris, La documentation Française*,* 2007, pp. 20-21).

[387] Inclusive mediante acordos bilaterais ou multilaterais entre os Estados relativos ao combate da criminalidade internacional (Convenção de Budapeste, art. 23). J. PÉREZ GIL adverte também para a vocação da Convenção como norma supletiva em matéria de extradição, sempre que ausente Tratado a este respeito e sempre que se tratar de uma das condutas delitivas contempladas entre os artigos 2º a 11 (art. 23.3) (*Medidas de investigación y de aseguramiento de la prueba en el Convenio sobre el Cibercrimen*, in Actualidad penal: Revista semanal técnico-jurídica de derecho penal, n. 36, Madrid, La Ley, 2003, pp. 904-905).

A exemplo da intervenção nas comunicações eletrônicas, a medida de busca e apreensão – providência recorrente para o acesso de informações – tem, sobretudo, natureza de meio de busca de prova. Nos seguintes itens discorre-se sobre o caráter ambivalente da medida, como meio instrumental de investigação e iniciativa processual voltada a assegurar possíveis fontes de provas.[388]

5.3.1. Medida de investigação

O acesso aos dados será permitido pela iniciativa de cessão destas informações ou em razão da realização da diligência de busca e apreensão. A natureza investigativa enquadra-se em uma das seguintes situações:

(i) Na maioria das vezes, a cessão realizar-se-á mediante requisição judicial dirigida ao provedor de *internet* para que forneça dados. O armazenamento destas informações pode decorrer da própria atividade de prestação do serviço, como também pode estar em conformidade com imperativo legal. Em ambos os casos, de rigor a devida colaboração com a Justiça por parte do prestador de serviços.[389]

Por meio das informações cedidas pelos provedores de acesso à *internet* obtém-se: *logs* de acesso[390]; o tempo de conexão; data e hora de início e término da conexão; o IP, instrumento útil à identificação da máquina utilizada.[391]

---

[388] C. B. PITOMBO adverte que o Código de Processo Penal insere a busca e apreensão como *"expediente de consecução de prova, conforme se lê na Exposição de motivos, item VII, ao fim"* (*Da busca e apreensão ..., op. cit*., p. 110).

[389] H. R. L. DA COSTA e M. LEONARDI advertem que as espécies de servidor aos quais solicitar as informações são numerosas: servidor de arquivos, servidor *web*, servidor de *e-mail*, servidor de impressão, servidor de banco de dados, servidor de fax, servidor DNS, servidor *proxy*, servidor de imagens, servidor FTP, servidor *webmail*, servidor de virtualização, entre outros (*Busca e apreensão e acesso remoto a dados em servidores*, Revista Brasileira de Ciências Criminais, n. 88, v. 19, 2011, p. 212). Impõe que a determinação judicial seja direcionada ao respectivo servidor, com a devida identificação da natureza e das características das informações buscadas, mas não parece razoável exigir que a medida judicial tecnicamente diferencie as modalidades de servidores.

[390] As informações constantes nos *logs* de acesso são: *"Login, data de início da conexão, hora de início da conexão, data de término da conexão, hora de término da conexão, tempo que ficou conectado, quantidade de bytes enviados, quantidade de bytes recebidos, telefone que originou a conexão, IP que recebeu na conexão"* (Manual de interceptação telemática do Ministério Público de Santa Catarina, disponível em

(ii) O próprio titular dos dados, figurando como investigado ou réu, poderá franquear o acesso de seu conteúdo. O consentimento livre, inequívoco, específico e prévio se faz imprescindível.

(iii) A cessão pode também decorrer da iniciativa de um dos interlocutores da comunicação. Neste caso, inexiste violação do direito ao sigilo das comunicações, desde que presente justa causa para a iniciativa. Os tribunais vêm entendendo que a justa causa nessas hipóteses se subsume à reação moderada do interlocutor em face de injusta agressão.[392]

(iv) Ainda se tratará de cessão sempre que terceiro proceda à entrega de dados que se encontrem em seu poder. Aqui, os dados estão em poder do proprietário do aparelho eletrônico, que foi utilizado pelo investigado para perpetrar o ilícito (familiares, amigos ou computador do ambiente de trabalho).

Entretanto, o consentimento para o oferecimento dos dados às autoridades competentes não pode ser prestado por terceiro. Nem mesmo o uso inadequado dos meios de comunicação – *v. g.,* em violação dos horários de funcionamento de uma empresa ou sem a permissão do proprietário do computador ou aparato tecnológico – excepciona o necessário consentimento.

Cabe atentar à excepcionalidade da cessão realizada pelo próprio réu ou por um dos interlocutores da comunicação (II e III); nas demais hipóteses é necessária autorização judicial para a coleta dos dados. E sempre o juízo de proporcionalidade guiará a excepcionalidade na determinação destas ingerências.

(v) A busca e apreensão determinada judicialmente convalida-se principalmente para a retenção de dados em poder de particulares. É inexigível que o inculpado colabore com as investigações, em deferência ao direito de não se incriminar (*nemo tenetur se detegere*); ainda com maior razão, tratando-se de colaboração ativa.

---

www.pgj.pb.gov.br/site/.../manual_interceptacao_telematica.doc*,* acesso em 15/10/11, h. 10:20*)*. Advirta-se que o advento da banda larga modificou por completo o acesso à *internet*, se outrora prevalecia o acesso discado, evidenciam-se agora inúmeros outros meios mais modernos e eficientes de acesso à rede.

[391] Podem constar no banco de dados dos provedores, informações cadastrais do usuário, como o nome do cliente, RG, CPF, endereço, telefones para contato e *e-mail*.

[392] O direito fundamental à inviolabilidade das comunicações não se sobrepõe a injusta agressão de terceiro, *v.* item 4.1.1.

(vi) Também será possível a busca e apreensão de dados em poder dos provedores de serviços, em duas hipóteses. Em primeiro lugar, a negativa da entrega de informações judicialmente solicitadas pode caracterizar desobediência a ordem legal de funcionário público (CP, art. 330). Além disso, se presentes indícios de que o requerimento ao provedor, desacompanhado de medidas de resguardo da prova, possa resultar no desaparecimento de dados relevantes para o processo, será oportuna a adoção da providência.

5.3.2. Preservação das fontes de prova

O aspecto acautelatório da apreensão está expresso em sua inegável urgência (*periculum in mora*), que evidencia a perspectiva instrumental e provisória da medida. A noção de *periculum in mora* pode ser sintetizada como uma situação em que há séria possibilidade de dano (perigo de insatisfação ou risco de satisfação tardia). A medida instrumental atende o imperativo de segurança, diretamente associado à presteza e celeridade da providência.[393]

Impera na hipótese, a reserva de jurisdição, cabendo ao Poder Judiciário autorizar o cumprimento da medida. Intenta-se conservar as fontes de provas relevantes para a instrução do processo. Contudo, a consecução desta função preventiva, tipicamente cautelar, pressupõe a restrição de direitos fundamentais.

A obtenção dos dados digitais por meio da cessão ou da apreensão do suporte técnico em que constem armazenados (*CD-Rom*, *pen drive*, disquete, etc.) tem como escopo uma tutela processual de urgência. O juízo provisório que determina a medida guia-se por um crivo de verossimilhança; a acentuada probabilidade de que as informações possam favorecer o esclarecimento da autoria delitiva justifica a tutela temporária.

[393] H. TORNAGHI, *Instituições de Processo Penal*, v. 3, 2ª ed., São Paulo, Saraiva, 1978, pp. 5-7.

Mas não se ignore a opção do legislador de incluir a medida no Título VII, do Código, referente às provas no processo. Atento a esta constatação, GUSTAVO HENRIQUE BADARÓ esclarece que a busca e apreensão não constitui *fonte de prova* ou *meio de prova*[394], uma vez que a busca e a eventual apreensão da coisa, em si, nada provam. Na verdade, por meio dela conservam-se os elementos de prova apreendidos. Em seguida, uma vez obtida a fonte de prova será produzido o meio de prova correspondente. Portanto, afigura-se mais criterioso classificá-la como *meio de busca ou de obtenção de prova.*[395]

Como é sabido, o acesso aos dados informáticos de comunicações concluídas ou de dados armazenados em suporte digital pode realizar-se mediante a busca e apreensão de aparelho eletrônico. A medida constitui diligência investigativa de procura e asseguração de fontes de prova, limitativa de direito individual, destinada a apreender elementos de convicção necessários à prova de infração ou à defesa do réu, decretada sempre mediante autorização judicial.

A fonte da prova digital é o respectivo instrumento tecnológico (*v.g.*, computadores, *laptops*, aparelhos celulares, *smartphones*). A partir deste aparato será produzido, em contraditório, a prova correspondente, resguardada a possibilidade de realização de perícia.[396]

Ainda que o procedimento técnico a ser empreendido pelo perito não tenha previsão legal, a perícia constitui meio de prova regulamentado. Não cabe sustentar a atipicidade nesse caso, pois *"a forma como se dá o trabalho científico não é, via de regra, integrante da tipicidade processual. (...) apenas de maneira excepcional são introduzidos elementos normativos na realização da perícia pelo legislador, e isso se dá por situações*

---

[394] *V.* nota 63.

[395] G. H. BADARÓ, *Direito Processual ...*, *op. cit*., pp. 270-271. M. A. COELHO ZILLI adota a terminologia *meio de busca de prova* para enquadrar a busca e apreensão, interceptação telefônica, quebra de sigilo bancário e fiscal, inspeção judicial e os meios de busca de prova instituídos para o combate das ações praticadas por organizações criminosas: "*Cuidam-se (...) de medidas, por intermédio das quais, busca-se a obtenção de certas provas que, se encontradas, serão transportadas até o processo"* (*A iniciativa instrutória ...*, *op. cit*., p. 199).

[396] O meio de prova pericial encontra-se disciplinado nos arts. 158 a 184, do Código de Processo Penal. O procedimento de perícia em aparelho eletrônico não dispõe de regime jurídico próprio, até mesmo em razão da dificuldade de acompanhar o desenvolvimento científico. Ainda que não se tenha por objetivo apontar todas as etapas para a formalização deste procedimento, algumas diretrizes constam no item 3.4.

normalmente ligadas à tipicidade do delito ou, ainda, como critério uniformizador do trabalho do perito por parte do legislador."[397]

5.3.3. Limitação de direitos fundamentais

Constam no art. 240, do Código de Processo Penal, as modalidades de busca pessoal[398] e domiciliar. A apreensão de suportes eletrônicos para os fins de investigação e instrução penal é possível nestas duas hipóteses, representativas de intromissão estatal no livre exercício de direitos fundamentais (CF, art. 5°, incs. III, X e XI). Ademais, cabe reconhecer a específica e autônoma limitação do direito à proteção de dados.

A consagração da autodeterminação informativa amplia o fundamento jurídico da reação às violações de direitos resultantes do tratamento e controle dos dados. Preserva-se a faculdade de todo cidadão acessar informação publicamente disponível e livremente comunicar-se. A ingerência de terceiro apenas será legítima nos casos apreciados no capítulo anterior, sempre para efeitos de investigação criminal.

Em comparação à enunciação genérica de um direito à intimidade, a tutela específica da proteção de dados mostra-se mais condizente com a defesa efetiva da autodeterminação informativa. Nesse caso, não se trata de excluir do conhecimento de terceiros fatos relativos à esfera pessoal, mas sim, de assegurar o poder de controle ou de decisão sobre os dados pessoais. Assim, o titular tem a faculdade de exigir a retificação de informações a seu respeito, sempre observado o indispensável consentimento para o registro e a cessão.

---

[397] G. M. DEZEM, *Da prova penal: tipo processual, provas típicas e atípicas*, Campinas, Millennium, 2008, p. 194.

[398] Se o sujeito passivo da busca for mulher, consigna o art. 249, do estatuto processual, a revista será feita por outra mulher, se não importar retardamento ou prejuízo da diligência. Contudo, a tutela constitucional da intimidade, inscrita no inc. X, do art. 5º, da Carta Federal, impõe que a norma do art. 249 seja interpretada com maior restrição: a busca em mulher somente poderá ser feita por outra mulher ou, se for o caso, por um médico.

Imprescindível, portanto, que a lei estabeleça os princípios, direitos e deveres que envolvem o tratamento de dados. A previsão de obrigações legais determina uma postura positiva de gestão e desvelo por parte dos responsáveis. Apenas a observância dos deveres de cuidado – consentimento do titular, finalidade, justificação social e veracidade dos dados – convalida a adequada preservação destas informações.

Quando os suportes de informação eletrônica encontrarem-se no domicílio do sujeito passivo ou na respectiva sede social, a realização da providência redundará em mitigação dos direitos à inviolabilidade do domicílio (CF, art. 5°, XI) e da liberdade de associação (CF, art. 5°, XVII), respectivamente.[399]

A busca domiciliar está condicionada a determinação judicial baseada em fundadas razões para procurar o objeto relacionado aos fatos investigados. Cabe mencionar que a casa, aqui, não tem o sentido mais estrito de domicílio, concernente a residência com ânimo definitivo de permanência (Código Civil, art. 70). Trata-se da casa em acepção mais dilatada, propugnada pelo legislador constitucional e penal, que inclui as hipóteses do art. 150, § 4º, do Código Penal.

A procura de coisa ou pessoa realizada em domicílio alheio é designada busca domiciliar. Conforme o art. 5º, inciso XI, da Carta Federal, pode ser realizada mediante autorização judicial. Excepcionalmente, não se exige o mandado em razão do livre e expresso consentimento do morador, ou de flagrante delito, ou quando realizada a diligência pela própria autoridade judiciária. Outras hipóteses de ingresso enquadram-se no crime de violação de domicílio (CP, art. 150).

Consolidada na doutrina e jurisprudência, a abrangência do local de exercício da atividade profissional no conceito de domicílio.[400]

---

[399] Os grupos sociais de que o indivíduo participa possuem o legítimo interesse de atuar para assegurar o exercício de direitos subjetivos: *" (...) o direito reconhece igualmente personalidade a entes morais, sejam os que se constituem de agrupamento de indivíduos que se associam para a realização de uma finalidade econômica ou social (sociedades e associações), sejam os que se formam mediante a destinação de um patrimônio para um fim determinado (fundações), aos quais é atribuída com autonomia e independência relativamente às pessoas físicas de seus componentes e dirigentes"* (C. M. DA SILVA PEREIRA, *Instituições de Direito Civil*, v. I, 21ª ed., Rio de Janeiro, Forense, 2005, pp. 213-214). O direito protegido no estabelecimento comercial diz respeito ao segredo das atividades e negócios da pessoa jurídica.

[400] A interpretação constitucional da casa como asilo inviolável do indivíduo engloba o espaço de *"moradia e residência (apartamento, palácio, palacete, cabana, choça, choupana, barraco, o quarto de hotel ou de*

O advogado é protegido pela inviolabilidade das comunicações com seu cliente, desde que as informações sejam relativas ao exercício da advocacia. A busca e apreensão no local de trabalho do causídico restringe-se às hipóteses em que seja partícipe ou coautor da infração, ou para apreensão de documentos e objetos que constituam elementos do corpo de delito (CPP, art. 243, § 2º).

É de se ponderar que o defensor do acusado poderá figurar como sujeito ativo dos crimes previstos nos arts. 180 e 349, do Código Penal (receptação e favorecimento real). Para a realização da diligência, o Estatuto da Advocacia (lei nº 8.906/94) impõe mandado judicial e que o executor da busca se faça acompanhar de um representante da OAB (art. 7º, § 6º).

A lei nº 11.767, de 7 de agosto de 2008, modificou o inciso II, do art. 7º, do Estatuto, para prever expressamente no âmbito das comunicações eletrônicas: *"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"*.[401]

Por sua vez, na busca pessoal incide a garantia *nemo tenetur se detegere*, fundamento constitucional para o acusado não ser obrigado a contribuir para a iniciativa instrutória dos órgãos de investigação. Para a medida, imprescindível conciliar as seguintes regras: *"(1) poder-dever estatal de perquirir sobre fatos ilícitos; (2) respeito à integridade física e moral do indivíduo; (3) indispensabilidade da intervenção; (4) proporcionalidade entre o fato ilícito e a interferência no corpo humano; (5) utilização de meios apropriados e realizada por profissionais habilitados; (6) norma legal autorizadora"*.[402]

Com fulcro no artigo 244, do Código de Processo Penal, a busca poderá ser realizada sem mandado judicial, *"quando houver fundada suspeita de que a pessoa esteja na posse de arma proibida ou de objetos ou papéis que constituam corpo de delito"*.

---

pensão) ou em que alguém tem sua instalação particular (escritório, oficina)" (J. A. DA SILVA, *Comentário contextual ...*, *op. cit*., p. 103).

[401] Para a busca em outros locais protegidos pelo sigilo profissional (como estabelecimentos bancários, comerciais, industriais e consultórios médicos) também se faz necessária a autorização judicial.

[402] C. PITOMBO, *Da busca e da apreensão ...*, *op. cit*., p. 149.

Entretanto, tal situação não autoriza que a busca se torne uma inspeção também sobre os aparelhos eletrônicos que a pessoa tenha em seu poder.[403]

5.3.4. Finalidade e objeto

Como objetivo, pretende-se encontrar coisas (CPP, art. 240, alíneas *b, c, d, e, f, h*), ou pessoas (CPP, alíneas *a, g* – delitos de sequestro, redução à condição análoga à de escravo, rapto, extorsão mediante sequestro, subtração de incapazes). Em ambos os casos o ente perquirido, certo e determinado, deve individualizar-se no corpo do mandado para que sejam fielmente cumpridos os desígnios da requisição (CPP, art. 240, § 1º).

A apreensão tem por escopo a tomada e a conservação de coisas ou a retenção de pessoas, para assegurar a consecução dos fins processuais.[404] HÉLIO TORNAGHI diferencia os objetivos da apreensão, segundo o intento de tornar efetiva a lei penal (art. 240, § 1º, b, c e d), sobretudo, para o recolhimento de coisas destinadas a práticas criminosas, e para realizar fins processuais (art. 240, § 1º, e, f, e h), em razão de objetos necessários à prova da infração ou à defesa do réu ou qualquer outro elemento de convicção.[405]

A finalidade da busca será a apreensão do aparelho eletrônico quando se pretenda acessar dados em suporte automatizado. Não se perca de vista que poucas medidas afiguram-se tão gravosas quanto a apreensão de dados, cujos reflexos podem ser amplamente sentidos em diferentes aspectos da vida pessoal. Mais que simples restrição temporária à propriedade, a medida impõe drásticos limites ao acesso à informação e, por via reflexa, pode comprometer processos comunicativos; relações sociais; obstaculizar parcial ou completamente o exercício de atividades econômicas.

---

[403] Na busca em veículo usado como meio de transporte valem as mesmas regras das buscas pessoais. Excepcionalmente, no caso de veículo que sirva como moradia (*trailer*, barco), aplica-se o regime das buscas domiciliares.

[404] Como ensina ADA PELLEGRINI GRINOVER, as buscas constituem os meios e as apreensões os respectivos fins (*Liberdades Públicas ...*, *op. cit*., p. 202).

[405] *Instituições de Processo ..., op. cit*., pp. 66-67.

Em síntese, enquanto a interceptação exige documentação mediante gravação, com o objetivo de permitir futura reprodução sonora da comunicação, a apreensão é o ato processual de apossamento em sentido material.

Por ser o meio bastante usual de armazenamento de dados, o disco rígido representa fonte de prova relevante para a investigação e aparece frequentemente identificado como objeto da apreensão. Primeiramente, necessário advertir que a conservação de dados desenvolveu-se consideravelmente nos últimos anos, com o aperfeiçoamento dos dispositivos de armazenamento não voláteis. Portanto, a busca nem sempre terá lugar em discos rígidos tradicionais, mas também em suportes como discos magnéticos, discos óticos e unidades de estado sólido (SSD).

Outra advertência que se faz necessária diz respeito ao objeto da medida de apreensão, que não se confunde com o suporte de armazenamento dos dados. Ao decretar a apreensão das informações em si consideradas, deve-se prestigiar técnicas como a cópia-clone (*legal imaging* ou *bit stream image*), que permitem restituir sem demora os aparelhos circunstancialmente recolhidos. Inclusive, em casos de pouca complexidade, que envolvem a apreensão de poucos dispositivos de armazenamento, todos de pequena capacidade, recomendável adotar procedimentos técnicos que permitam copiá-los de imediato, sem demora.[406] Conclui-se, portanto, que a apreensão de dados deve pautar-se pela eficiência, de forma que o confisco temporário de equipamentos tenha lugar somente nas situações em que a complexidade assim o exija.

Duas considerações se fazem aqui necessárias. Sobre a complexidade dos equipamentos e a quantidade de dados armazenados, forçoso reconhecer que ao tratar deste temário juristas e legisladores geralmente tomam por baliza o armazenamento automatizado em pequena escala, restrito a um número bastante reduzido de dispositivos, que podem ser transladados sem dificuldade aos laboratórios de criminalística. Todavia, é preciso que as medidas de busca e apreensão sejam compatíveis com o porte dos dispositivos que se pretende vasculhar, pois há servidores imensos que jamais poderiam ser transportados e exigiriam acurado exame *in locus*.

[406] Imagine-se quanto transtorno pode ser gerado pela apreensão de um simples *smartphone,* onde se armazenam contatos, fotos, compromissos e uma infinidade de informações pessoais e profissionais que podem ser rapidamente copiadas através de programas especializados sem que se faça necessário mantê-lo por dias em um laboratório especializado.

Por fim, necessário ponderar que a ausência de pessoal técnico não pode legitimar o confisco desnecessário de aparelhos eletrônicos que poderiam ser copiados imediatamente e sem demora, por um perito capacitado munido de um computador portátil e de programas adequados. Tão absurdo quanto transladar um imenso servidor ao laboratório de criminalística, seria subtrair à posse do investigado por longos períodos de tempo um dispositivo rudimentar – como um *cd-rom* ou *pendrive*, ausentes particularidades técnicas que demandem complexa análise, como a criptografia – que poderia ser imediatamente acessados.[407]

5.4. Pressupostos, requisitos e limites legais

As buscas e apreensões de aparelhos eletrônicos limitam-se aos casos especialmente graves ou com elevado risco de reiteração, sempre realizadas com objeto especificamente determinado, local identificado e pelo menor tempo possível. Comparada à intervenção nas comunicações eletrônicas, o caráter invasivo da medida significará, na maior parte das vezes, o franqueamento de informações ainda mais íntimas do investigado.[408]

[407] No caso do computador permanecer em funcionamento e à disposição de seu usuário, evidente o modo menos invasivo de realização da diligência investigativa (G. ZICCARDI, *L'ingresso dela computer ...*, *op. cit*., p. 175). Para que assim seja cumprida, necessário averiguar se (i) a polícia técnica está aparelhada para a apreensão dos dados digitais no próprio local; e se (ii) em razão da complexidade da operação é melhor que seja cumprida com mais vagar. Por outro lado, pode se mostrar inviável a apreensão de muitos computadores (como seria o caso de uma grande empresa), hipótese em que mais apropriada a cópia do *hard disk*, sem proceder à apreensão (a análise dos dados será efetuada sobre a cópia).

[408] Sobre a indeterminação dos locais de execução e da finalidade da busca e apreensão, manifestou-se o Supremo Tribunal Federal: *"Sem definir-se a competência, em face da dispersão de votos quanto aos fundamentos da concessão da segurança, os limites objetivos e subjetivos da busca e apreensão hão de estar no ato que a determine, discrepando, a mais não poder, da ordem judicial em vigor delegar a extensão à autoridade policial"* (MS 23.454/DF, rel. Min. Marco Aurélio).

5.4.1. Pressupostos: legalidade e justificação teleológica

O caráter da busca e apreensão como medida restritiva da intimidade e vida privada exige que todo o seu procedimento seja fundado em lei clara e detalhada, sujeita a constante aperfeiçoamento e complementação. As circunstâncias de fato e de direito que autorizem o uso desta medida insidiosa pelo Poder Público deverão estar suficientemente claros e à disposição de todos os indivíduos.

Em face do caráter genérico das disposições do Código de Processo Penal, e da ausência de disposição em lei especial, não se pode sustentar presente base legal concreta que discipline a busca e apreensão dos equipamentos que armazenam dados digitais, bem como das requisições aos provedores de acesso ao conteúdo.

Por se tratar de medida de exceção, a lei deveria ser taxativa ao disciplinar o rol de crimes sujeitos a busca e apreensão, vedada a aplicação de analogia. Entretanto, o emprego da expressão "qualquer elemento de convicção" autoriza o cumprimento da medida em relação a todo objeto que possa influir na medida.[409]

De rigor que a busca e apreensão não se afaste de fim específico e constitucionalmente legítimo. O juízo de ponderação opera-se entre o sacrifício imposto aos direitos fundamentais do investigado e o fato típico objeto de apuração. A indeterminação da medida (autorização em branco) e a mera referência a finalidades genéricas (segurança nacional, segurança pública, bem estar econômico, defesa da ordem e prevenção de infrações) não são suficientes para fundamentar a providência acautelatória.[410]

[409] J. F. MIRABETE, *Processo Penal …*, *op. cit*., p. 347.
[410] B. S. RODRIGUES, *A monitorização dos fluxos …*, *op. cit*., p. 203.

5.4.2. Requisitos: reserva jurisdicional e motivação

A proteção dos dados pessoais depende da plena observância do princípio da reserva de jurisdição, pois a ampliação da legitimidade para a decretação da medida pode legitimar situações excepcionais. A inspeção ou recolha deve ser autorizada expressamente em decisão que descreva a prática do registro dos dados técnicos e cadastrais, bem como de conteúdo. A medida discorre sobre os aparelhos onde possam constar as informações, os métodos de busca ou análise mais apropriados e o tempo necessário para averiguação dos suportes informáticos.[411]

Há casos, contudo, em que o prognóstico das técnicas e métodos específicos não poderá ser pormenorizado, sob pena de se comprometer a própria diligência. Nessas circunstâncias, justifica-se certa margem de discricionariedade na inspeção e coleta dos dados.[412]

No caso de compartilhamento de um mesmo aparelho por mais de um usuário, apenas o consentimento de todos descaracteriza a necessidade de mandado judicial. À polícia judiciária impõe prudência, certificando-se que um aparelho entregue pelo proprietário não seja utilizado, também, por outras pessoas, de modo a evitar a ilicitude da prova.

A reserva jurisdicional estende-se às hipóteses de obtenção de dados de tráfego. Uma das circunstâncias mais habituais diz respeito ao requerimento de listas de chamadas para companhias telefônicas. O regime jurídico a que se sujeitam os dados de tráfego não difere substancialmente dos dados de conteúdo. Impróprio sustentar que, em

[411] N. GONZÁLEZ-CUÉLLAR SERRANO, *Garantías constitucionales …*, *op. cit*., p. 155.
[412] Ata do grupo de trabalho do Ministério Público Federal, direcionado aos crimes informáticos, alertou para a dificuldade no cumprimento de mandados de busca e apreensão e realização de outras diligências pelas delegacias dos diversos Estados federados, em razão do desconhecimento das particularidades da investigação. Na ocasião, sugeriu-se a implementação em todos estes Estados, de delegacias especializadas em crimes cibernéticos (ccr.pgr.mpf.gov.br/.../ata_grupo_sobre_crimes_ciberneticos.pdf, acesso em 13/10/2011, h. 21:30). Algumas medidas prioritárias para a apuração dos delitos são: a formação de profissionais especializados que atuem na persecução dos crimes e elaboração de políticas de segurança; o treinamento e reciclagem profissional; o domínio das operações técnicas de recuperação, análise e interpretação de dados.

razão da natureza menos invasiva da ingerência nos dados de tráfego, poder-se-ia prescindir da observância dos pressupostos, requisitos e limites legais.

É certo que as informações de conteúdo, em geral, revelam dados mais concretos sobre a personalidade de um indivíduo. Contudo, não se ignore que a associação de diversos dados externos das comunicações de um titular podem desvelar sensíveis aspectos de sua personalidade.

O conhecimento dos dados de tráfego de um investigado pode ser adequado e suficiente ao descobrimento dos fatos investigados, mas se o julgador optar por requisitar apenas informações externas à comunicação, não poderá se fundar em um padrão menos exigente de motivação.

A obtenção destes dados, com frequência depende da colaboração do dos provedores que franqueiam conteúdos armazenados em seus servidores ou ainda dos provedores de acesso à *internet*. Os provedores de serviços podem conservar os dados com a finalidade de faturação, para responder reclamações dos usuários, ou ainda, em razão de imposição da lei ou de autoridade jurisdicional. O número considerável de intermediários privados envolvidos na operação de rastro pode demandar mais de uma resolução judicial para o acesso da informação buscada.[413]

A busca e apreensão deve ser fundamentada, a exemplo de eventuais decisões que determinem a continuidade ou modificação do exercício de um direito. O conhecimento dos fundamentos legais assegura a publicidade dos critérios utilizados pelo julgador.

Imprescindível motivação que verse sobre a materialidade e autoria delitiva; identifique a natureza do crime (se apenado com reclusão); delimite o sujeito passivo e discorra detalhadamente sobre o modo de execução da medida. Demonstrar a materialidade equivale a afirmar o crime *in concreto*; não há que se falar em tipicidade e

[413] O servidor de comunicações eletrônicas que se negar a fornecer a informação solicitada judicialmente, incorre na violação do dever de colaboração com a justiça, sujeito à pena prevista para o crime de desobediência (CP, art. 330), sem prejuízo de sanções administrativas. No caso da suspeita de que o requerimento ao provedor permita o desaparecimento de dados de interesse para a causa, possível autorização judicial para a apreensão dos dados em poder do servidor. Esta última hipótese configura medida excepcionalíssima.

antijuridicidade de uma conduta cuja existência é incerta, fundada em meras alusões ou suspeitas. Testificada a conduta, cobra sentido buscar indícios de autoria a partir de elementos informativos da investigação e determinar o estreito liame entre os atos e sujeitos.

Constará no mandado judicial a natureza pormenorizada dos dados requeridos, devidamente especificado o sujeito passivo da medida. A requisição de informações aos provedores de *internet* referentes a grupos indeterminados de pessoas é incompatível com a natureza da medida.

Quando impossível a identificação nominal, será necessária a indicação de aspectos que permitam individualizar a quem se dirige a medida, pois antes de cogitar restrição ao direito à proteção de dados, imprescindível afirmar o liame entre a prática delitiva e o sujeito passivo. Uma requisição dos dados cadastrados no servidor, *v.g.*, em desfavor do criador de uma página *web* com conteúdo ilícito, tem como objetivo a identificação de um sujeito indeterminado, mas determinável. Afinal, a exigência da precisa determinação poderia inviabilizar a consecução da medida.

Superadas estas questões, realiza-se o juízo de proporcionalidade – necessidade, adequação e proporcionalidade em sentido estrito – esclarecidas as razões pelas quais o direito à segurança (CF, art. 5°) ou à incolumidade pública (CF, art. 144) prevalece sobre o direito à inviolabilidade das comunicações.

5.4.3. Limites objetivos, subjetivos e temporais

O art. 243, do Código de Processo Penal, expõe os cuidados necessários para a autorização da busca e apreensão: *"O mandado de busca deverá*: *I - indicar, o mais precisamente possível, a casa em que será realizada a diligência e o nome do respectivo proprietário ou morador; ou, no caso de busca pessoal, o nome da pessoa que terá de sofrê-la ou os sinais que a identifiquem; II - mencionar o motivo e os fins da diligência; III - ser subscrito pelo escrivão e assinado pela autoridade que o fizer expedir"*.

O estrito cumprimento do mandado é garantia para quem o executa. Afinal, a observância da determinação comprova que o executor agiu segundo a ordem da autoridade. À medida que a ordem limita os poderes de busca e varejamento, o sujeito passivo também encontra no mandado uma garantia, facultando-lhe a possibilidade de apresentar a pessoa ou coisa procurada.[414]

Desse modo, se a descrição do mandado judicial indicar com precisão os dados digitais ou dispositivos eletrônicos que serão apreendidos (pastas de arquivos armazenados em servidores, *e-mails*, computadores portáteis, discos rígidos, etc.), as buscas que excederem a autorização serão medidas ilegais.

A busca pode ser cumprida antes da instauração do inquérito, durante sua elaboração, no curso da instrução criminal ou na fase de execução. Ocorre com mais frequência durante o inquérito, porque a polícia dispõe de meios mais rápidos e eficazes para assegurar seu êxito.

A determinação da diligência incumbe à autoridade judicial (CF, art. 5°, inciso XI; CPP, art. 241), afinal, a restrição de direito fundamental depende de expressa manifestação do Poder Judiciário. Não cabe às Comissões Parlamentares de Inquérito (CPI's) tal decisão, pois o princípio da reserva de jurisdição impede o exercício concorrente deste direito com qualquer outro órgão.

A autoridade judicial não está adstrita à provocação das partes, é lícito que o juiz atue de ofício para prender criminoso, apreender produto de crime ou do corpo de delito. Sem embargo, podem requerer a medida, a autoridade policial; o Ministério Público; a Comissão Parlamentar de Inquérito (CPI); o particular ofendido; o suspeito, o indiciado ou acusado, e o condenado.[415]

Enquanto no polo ativo figura a própria autoridade (judiciária ou policial), no polo passivo situa-se o titular da esfera de posse, em que se suspeita encontrar a pessoa ou coisa buscada.

---

[414] H. TORNAGHI, *Instituições de Processo ..., op. cit*., p. 62.

[415] C. B. PITOMBO, *Da busca e da apreensão ..., op. cit*., p. 187. Lembre-se que o art. 14, do Código de Processo Penal, assegura ao indiciado o requerimento de qualquer diligência, que será realizada ou não, a juízo da autoridade, valoradas a oportunidade e relevância da medida.

No aspecto temporal, a intervenção está atrelada à urgência na coleta da fonte de prova, em face do risco de perda destes elementos. Poderá ser concretizada durante a investigação criminal ou instrução processual, não sendo imprescindível a existência de inquérito ou ação penal em curso. A continuidade da medida justifica-se enquanto realizados os procedimentos indispensáveis à identificação e registro das informações procuradas.

5.5. Direito de defesa

Ao longo do processo são assegurados às partes direitos iguais de alegar e provar os fatos sustentados, bem como, de demonstrar a inocência ou a diminuição da culpabilidade, e de influenciar o convencimento judicial. O princípio da ampla defesa comporta uma série de faculdades ao inculpado, tais como, o direito de dispor de tempo para a defesa, da assistência de advogado e da possibilidade de contrapor-se às acusações.

O direito de defesa deve ser exercido desde o momento do indiciamento até a conclusão do inquérito ou do processo. A autodefesa e a defesa técnica asseguram o equilíbrio entre as partes processuais e impedem a perpetuação de excessos e arbítrios. Aliás, o direito à assistência técnica restará observado apenas quando a atuação do advogado for efetiva, fundada na contraditoriedade indispositiva.

Ainda que o exercício pleno do contraditório permaneça restrito à fase processual, há de ser assegurada iniciativa de reação do investigado para uma série de situações (relaxamento da prisão legal, juntada de documentos relevantes, localização de testemunhas, formulação de quesitos da prova pericial, impugnação da autenticidade de documentos exibidos, dentre outros).

O conhecimento da medida acautelatória de busca e apreensão por parte do investigado será postergado e sujeitar-se-á ao controle diferido, para não impedir a realização de atos impostergáveis. No rol de direitos que informam a garantia da ampla

defesa encontra-se a faculdade do inculpado de intervir durante a investigação e a instrução para apresentar argumentos pertinentes.[416]

É assegurada a reação aos mandados de busca indeterminados e sem a devida fundamentação, da mesma maneira que preservada a possibilidade de requerimentos, contestações, impugnações e complementação durante o processo judicial.[417]

O exercício do direito de defesa pressupõe o conhecimento dos procedimentos de conservação dos dados e a possibilidade de confrontá-los com os originais. A não alteração dos dados é um aspecto importante, a exigir que toda operação sobre os dados seja realizada nas respectivas cópias. Por certo, o processo de cópia (*legal-imaging*, *v.* item 3.4) deve ser efetuado de forma a não alterar a integridade dos dados originais.

A aquisição da fonte de prova digital também é procedimento delicado, deve tecnicamente assegurar que os dados obtidos permaneçam idênticos aos originais. Como primeiro passo do processo de conservação exige-se cautela na apreensão do aparelho eletrônico para que a cópia a ser extraída guarde conformidade com o original.[418]

---

[416] Para A. SCARANCE FERNANDES, um dos novos perfis da reação defensiva à imputação consiste na sua extensão à fase de investigação *"como exigência da visão garantista do direito processual moderno. Esse traço fica bem manifesto na análise do direito comparado: deixam de ser secretas as investigações presididas por juízes ou pelo Ministério Público, aceitando-se, apenas, período curto em que a autoridade policial incumbida de investigar pode manter em segredo as primeiras diligências tendentes a esclarecer o crime e desvendar a autoria, tanto assim que, se houver um provável autor, deve tomar ciência da imputação e ser ouvido, facultada a presença do advogado em seu interrogatório. A partir desse momento, define-se a situação jurídica da pessoa investigada, que passa a ser imputada e a ter direitos, como o direito de estar assistida por defensor, o direito de ter ciência dos atos a serem realizados, exceto quando urgentes ou exigirem a surpresa, e, eventualmente de acompanhar a realização de tais atos, o direito de propor ou requerer diligências"* (*Reação defensiva à imputação*, São Paulo, Saraiva, RT, 2002, pp. 303-304).

[417] M. SAAD, *O direito de defesa no inquérito policial*, São Paulo, RT, 2004, p. 329.

[418] Para GIOVANNI ZICARDI, os quatro princípios norteadores deste processo são: correta modalidade de conservação; realização da cópia-clone; garantia de não alteração, e apreensão como medida de última *ratio* (*L'ingresso della computer forensics nel sistema processuale italiano: alcune considerazioni informatico-giuridiche*, in Luca Lupária (org.), *Sistema penale e criminalità informatica*, Milano, Giuffrè, 2008, p. 170).

5.6. Princípio da proporcionalidade

Para que a imposição de uma medida restritiva de direitos seja constitucional, inafastável venha aplicada à luz do princípio da proporcionalidade. A intromissão no direito fundamental será ilegítima se não cumprir este requisito. O princípio da proporcionalidade pressupõe a observância da legalidade, justificação teleológica, jurisdicionalidade e motivação, assim como da idoneidade, necessidade e proporcionalidade em sentido estrito.

No processo penal, o emprego de dados digitais de comunicações concluídas obedece à variação do grau de resguardo a que estejam sujeitos. Há uma considerável gradação no caráter invasivo da medida, em razão de se tratar de dados sensíveis, dados pessoais em sentido estrito e dados públicos.

A gravidade do crime deve ser apreciada para aferir a idoneidade da busca e apreensão. No entanto, alusões genéricas ao desvalor da conduta não se compatibilizam com o juízo de razoabilidade. A lei deve indicar o rol de crimes em que se admite a apreensão, pois permitir que todos os crimes apenados com reclusão autorizem o uso deste meio de obtenção de prova atenta contra a idoneidade e proporcionalidade em sentido estrito.

O modo de realização da diligência, circunstanciadamente descrito, será aquele que incorrer nas menores restrições possíveis dos direitos do sujeito passivo. É imprescindível a identificação da pessoa imputada, do terminal empregado para a realização da comunicação eletrônica, dos fatos e fundamentos autorizadores da medida e da respectiva qualificação jurídica.

Conforme exposto anteriormente (*v.* item 4.6), deve ser evitado o sacrifício de direitos fundamentais, optando-se sempre pela medida menos gravosa à pessoa. Igualmente, a restrição deve partir do sério prognóstico de obter-se, por tal meio de

investigação, resultado útil e relevante para o processo, baseado no descobrimento ou na comprovação de algum fato importante para a causa.[419]

A obtenção dos dados, obedecido o critério procedimental aludido (*v.* item 3.4), pressupõe a exclusão daqueles confidenciais (*v.g.,* referentes às comunicações entre advogado e cliente) e o trabalho integrado de equipes profissionais que excluam informações protegidas pelo sigilo.

A medida pode se revelar desnecessária nas situações em que a técnica de espelhamento seja suficiente. Trata-se do procedimento de cópia dos dados a partir da elaboração de algoritmos que criam um número de identificação específico para identificar o fiel retrato das informações constantes em servidores de arquivo, servidores de *e-mail* ou em certo *hard disk*.

Conforme referido no capítulo 2, o regime jurídico de tutela da correspondência é igualmente aplicável ao *e-mail*. Em ambos os casos não se admite interceptação, todavia, possível apreender estes conteúdos, quando concluído o processo comunicativo. A ordem judicial que autoriza a obtenção da correspondência virtual deve balizar-se, além dos critérios referidos neste capítulo, também na impossibilidade de por outro meio serem alcançadas as informações buscadas.

5.7. Controle

A obtenção da fonte de prova no aparelho digital deve seguir um rigoroso procedimento técnico. É pertinente a identificação nominal dos responsáveis técnicos por esta operação, com o respectivo detalhamento dos procedimentos empregados.[420]

[419] Têm precedência lógica as medidas que envolvam a colaboração do investigado sobre as buscas domiciliares, assim como a utilização da técnica de cópia-clone, em comparação com a apreensão do aparelho eletrônico.

[420] Procedimento denominado na doutrina alienígena, tecnicamente, de *chain custody* – requisito técnico para atestar a integridade e autenticidade do documento eletrônico. A participação de todo operador técnico que

O responsável técnico deve realizar seguidas operações: individualizar os dados contidos no aparelho eletrônico que serão objeto de análise; recuperar arquivos deletados; encontrar documentos relevantes escondidos; determinar cronologicamente os arquivos; buscar o histórico de navegação do usuário; identificar os *softwares* e aplicativos usados; encontrar indícios de modificações não autorizadas no aparelho (*v.g. trojan applications*); envidar esforços para facilitar acesso a conteúdos criptografados, dentre outros procedimentos.

A obtenção de dados em suporte eletrônico encontra fundamento parcial no Código de Processo Penal e nas leis especiais. A disciplina, contudo, sobre não satisfazer a exigência de estabelecer concretos limites objetivos, subjetivos e temporais para a medida, também não fixa garantias específicas para a execução da diligência.

O juiz, portanto, atuará como garantidor do equilíbrio no trato dos interesses em conflito, assegurando que a atividade de busca de fontes de provas limite-se ao estritamente necessário para alcançar seu fim. A posição de equidistância do julgador capacita-o como garantidor das bases que fundamentam a investigação ou instrução criminal e da preservação da liberdade individual.[421]

O juízo de proporcionalidade aplica-se aos atos decisórios do julgador, mas não pode ser empregado com o objetivo de suprir a ausência de previsão legal. Ou seja, o princípio da proporcionalidade não pode ser utilizado como critério universal para sanar as omissões do legislador.

É certo que tanto a intervenção nas comunicações eletrônicas, como a busca e apreensão de aparelhos digitais, são providências de recolha de um número acentuado de informações pessoais. Nesses casos, a exclusão de fontes de prova ilícitas é responsabilidade do julgador. Uma solução interessante para que os elementos de

---

tratar as fontes de prova presentes na investigação criminal deve estar documentada. Quanto mais sólido e detalhado o procedimento, menores as possibilidades de sustentar-se a ilegalidade das fontes de prova. O juiz, ao determinar a quebra do sigilo das comunicações telemáticas, pode prever que a prestadora de serviços nomine as pessoas que tiveram conhecimento da medida e incumbiram-se de sua operacionalização, com vistas à individualização de eventual responsabilidade (arts. 8º e 10º, da lei nº 9.296, e da Resolução 59/08, do Conselho Nacional de Justiça).

[421] Os peritos e outros entes auxiliares da Justiça atuam segundo o controle do juiz de instrução para a execução de todas as medidas úteis ao processo. O perito prestará os resultados obtidos e as informações pertinentes.

convicção excluídos não influam na convicção do magistrado é a instituição do chamado juiz de garantias, responsável por dirigir a etapa pré-processual da persecução.

CAPÍTULO VI – DADOS DIGITAIS COMO FONTE DE PROVA: NOÇÕES DE CONSERVAÇÃO, EFICÁCIA E ILICITUDE

6.1. Conservação dos dados digitais e o direito à proteção de dados pessoais

As noções de tratamento e conservação de dados devem ser examinadas para esclarecer o destino dos dados coletados a partir dos meios de obtenção de prova examinados nos capítulos antecedentes. Impõe, especialmente, alertar para a correta gestão dos dados coligidos pelos órgão de investigação e pelos prestadores de serviço na *internet*.

O emprego de modernas tecnologias informativas na administração da Justiça bem demonstra a necessidade de criar um sistema jurídico capaz de disciplinar o tratamento de dados pessoais. Assegurar o respeito à autodeterminação informativa significa condicionar ao consentimento a coleta e o uso dos dados pessoais; assegurar os direitos de acesso, retificação, oposição e cancelamento de informações, prerrogativas inerentes ao titular que não podem mais permanecer a margem de disciplina específica.

O conceito de tratamento traduz-se na realização de operações técnicas, de caráter automatizado ou não, como armazenamento, consulta, utilização, gravação, conservação, modificação, bloqueio, cancelamento ou cessão de dados.

Tais operações destinam-se sempre à consecução de uma finalidade que, uma vez lograda, determina a imediata extinção do tratamento de dados. Os dados digitais oriundos das modalidades de intervenção estudadas nos capítulos anteriores têm caráter pessoal e são suscetíveis de tratamento, mas em razão de estrito vínculo, permanecem inteiramente associados a uma investigação criminal. Em síntese, o tratamento não se considera uma sucessão indefinida de processos, mas um meio voltado a um fim específico; em matéria processual penal presta-se exclusivamente a propiciar

elementos que permitam dilucidar o delito e não se deve protrair além do estritamente necessário.

A obtenção dos dados é medida voltada à apuração de delitos e, de modo geral, à prevenção de perigo grave e real para a segurança pública. A vinculação do tratamento de dados à prevenção ou à investigação criminal busca impedir que a limitação dos direitos fundamentais seja injustificada. Após o decurso do tempo, tornadas desnecessárias, serão canceladas as informações.

Deve prevalecer a noção de que os dados só podem ser armazenados para fins determinados, relacionados sempre à prevenção, investigação, detenção ou execução de sanções penais. O tratamento apenas excepcionalmente será destinado a outro fim, hipótese que deve estar autorizada por lei.[422]

Os dados obtidos no curso da investigação servem para esta persecução penal, desautorizado o acúmulo das informações oriundas de intervenções em comunicações eletrônicas. Os dados obtidos a partir da quebra do sigilo das comunicações não se destinam a alimentar as bases de dados policiais existentes e, muito menos, a serem compartilhados com a Administração pública para servir a propósitos diferentes daqueles que motivaram a coleta.[423]

O tratamento em discordância com a expressa vontade dos legítimos titulares dos dados constitui preocupante afronta ao direito à autodeterminação informativa, pois o consentimento representa a viga mestra de um sistema de proteção dos dados pessoais. Toda iniciativa que se considere um tratamento de dados encontra limites no consentimento, requisito imprescindível à salvaguarda da informação e à manutenção da integridade e confidencialidade das comunicações.

---

[422] As hipóteses excepcionais sujeitam-se ao controle judicial, em razão da modalidade do serviço prestado. O comércio eletrônico exemplifica a necessidade de captação, conservação e tratamento de dados como modo de facilitar a documentação e o cumprimento de obrigações contraídas.

[423] As bases de dados pessoais gerenciadas pela polícia não podem acumular informações obtidas em intervenções nas comunicações eletrônicas. Não há justificação teleológica para uma permanente relativização do direito ao sigilo das comunicações. A respeito das demais bases de dados policiais, o critério essencial para a legitimidade do armazenamento de dados refere-se à finalidade. Os bancos de dados não podem ter caráter universalizador (armazenamento de todas as informações de uma pessoa), uma vez que o princípio da finalidade é critério específico que impossibilita a formação de perfis pessoais (F. J. ÁLVAREZ GARCÍA, *El acceso por parte de las fuerzas y cuerpos de seguridad del estado a ficheros de datos personales*, in E. Pedraz Penalva [coord.], *Protección de datos y proceso penal*, Madrid, La ley, 2010).

O armazenamento e a conservação são atividades que caracterizam tratamento de dados. Se o armazenamento diz respeito à guarda dos dados em suporte adequado, a conservação refere-se às atividades necessárias à manutenção da segurança e da integridade das informações custodiadas. Fundamentais para a preservação dos dados digitais, as medidas de segurança têm caráter técnico, baseiam-se na adoção de mecanismos ou dispositivos voltados a evitar alterações, perdas, ou acessos não autorizados.

A conservação de dados tratados em decorrência de processos telemáticos pressupõe o estabelecimento de critérios para que as operadoras de telecomunicações retenham temporariamente determinados dados tratados, com o intuito de disponibilizá-los, se necessário, aos órgãos policiais ou judiciais. Há que esclarecer o período de armazenamento e também estabelecer se a obrigação se estende a todos os dados relativos às comunicações eletrônicas que não se considerem de conteúdo (dados de tráfego, de localização, etc.) ou limita-se apenas a determinadas categorias.

Em todos os casos, aquele que conserva os dados, quando necessário, deve facilitar aos titulares o acesso, retificação, supressão e bloqueio; ademais obriga-se a garantir a segurança das informações. Porém, a extensão do dever de conservar dados refere-se apenas àqueles indispensáveis para identificar o usuário conectado (*v.g,* data, hora e duração da comunicação).[424]

[424] A disciplina dos chamados arquivos de *log* representa tema importante atualmente em voga no projeto de lei que pretende estatuir princípios, garantias, direitos e deveres para o uso da *internet* no Brasil (PL 2126/2011). Tais arquivos têm natureza de metadados sobre o funcionamento do sistema computacional e atendem a exigências estatísticas, técnicas e de segurança. No rastreamento das operações realizadas pelo usuário é possível identificar os atos preparatórios do cometimento de um crime. A atenção deve estar voltada ao prazo, segundo o qual, os gestores de dados deverão responsabilizar-se pelo armazenamento daqueles relativos ao tráfego telemático. A Diretiva 2006/24/CE, do Parlamento Europeu e do Conselho, de 15 de Março de 2006, relativa à conservação de dados gerados ou tratados no contexto da oferta de serviços de comunicações eletrônicas publicamente disponíveis ou de redes públicas de comunicações, dispõe sobre as categorias de dados a conservar: "*1. Os Estados-Membros devem assegurar a conservação das categorias de dados seguintes em aplicação da presente diretiva: a) Dados necessários para encontrar e identificar a fonte de uma comunicação: 1) no que diz respeito às comunicações telefônicas nas redes fixa e móvel: i) o número de telefone de origem, ii) o nome e endereço do assinante ou do utilizador registrado; 2) no que diz respeito ao acesso à internet, ao correio electrónico através da internet e às comunicações telefônicas através da internet: i) o(s) código(s) de identificação atribuído(s) ao utilizador, ii) o código de identificação do utilizador e o número de telefone atribuídos a qualquer comunicação que entre na rede telefônica pública, iii) o nome e o endereço do assinante ou do utilizador registrado, a quem o endereço do protocolo IP, o código de identificação de utilizador, ou o número de telefone que estavam atribuídos no momento da comunicação*; *b) Dados necessários para encontrar e identificar o destino de uma comunicação: 1) no que diz respeito às comunicações telefônicas nas redes fixa e móvel: i) o(s) número(s) marcados (o número ou*

Advirta-se que soluções tendentes ao armazenamento generalizado de dados, por tempo ilimitado, são incompatíveis com o convívio em uma sociedade democrática. Estas medidas consistem na manutenção sistemática de dados, sem individualizar os sujeitos ou comunicações concretas que devem ser afetados, e sem observar uma finalidade.

Prever situações de risco genérico, dá ensejo a atuações que carecem de legitimidade, convertendo todos em suspeitos, indistintamente. Submeter a generalidade dos cidadãos a medidas de vigilância, pressupõe restringir direitos fundamentais sem que haja qualquer justificação teleológica para tanto.

É conveniente a intervenção do Ministério Público sempre que haja perigo de alteração ou modificação dos elementos probatórios obtidos. O órgão policial

---

*números de telefone de destino) e, em casos que envolvam serviços suplementares, como o reencaminhamento ou a transferência de chamadas, o número ou números para onde a chamada foi reencaminhada, ii) o nome e o endereço do assinante, ou do utilizador registrado; 2) no que diz respeito ao correio eletrônico através da internet e às comunicações telefónicas através da internet: i) o código de identificação de utilizador ou o número de telefone do destinatário pretendido, ou de uma comunicação telefônica através da internet, ii) o(s) nome(s) e o(s) endereço(s) do(s) subscritor(es), ou do(s) utilizador(es) registrado(s), e o código de identificação de utilizador do destinatário pretendido da comunicação; c) Dados necessários para identificar a data, a hora e a duração de uma comunicação: 1) no que diz respeito às comunicações telefônicas nas redes fixa e móvel, a data e a hora do início e do fim da comunicação; 2) no que diz respeito ao acesso à internet, ao correio eletrônico através da internet e às comunicações telefônicas através da internet: i) a data e a hora do início (log-in) e do fim (log-off) da ligação ao serviço de acesso à internet com base em determinado fuso horário, juntamente com o endereço do protocolo IP, dinâmico ou estático, atribuído pelo fornecedor do serviço de acesso à internet a uma comunicação, bem como o código de identificação de utilizador do subscritor ou do utilizador registrado, ii) a data e a hora do início e do fim da ligação ao serviço de correio eletrônico através da internet ou de comunicações telefônicas através da internet, com base em determinado fuso horário; d) Dados necessários para identificar o tipo de comunicação: 1) no que diz respeito às comunicações telefônicas nas redes fixa e móvel: o serviço telefônico utilizado; 2) no que diz respeito ao correio eletrônico através da internet e às comunicações telefônicas através da internet: o serviço internet utilizado**;** e) Dados necessários para identificar o equipamento de telecomunicações dos utilizadores, ou o que se considera ser o seu equipamento: 1) no que diz respeito às comunicações telefônicas na rede fixa os números de telefone de origem e de destino; 2) no que diz respeito às comunicações telefônicas na rede móvel: i) os números de telefone de origem e de destino, ii) a Identidade Internacional de Assinante Móvel ("International Mobile Subscriber Identity", ou IMSI) de quem telefona, iii) a Identidade Internacional do Equipamento Móvel ("International Mobile Equipment Identity", ou IMEI) de quem telefona, iv) a IMSI do destinatário do telefonema, v) a IMEI do destinatário do telefonema, vi) no caso dos serviços pré-pagos de caráter anônimo, a data e a hora da ativação inicial do serviço e o identificador da célula a partir da qual o serviço foi ativado; 3) No que diz respeito ao acesso à internet, ao correio eletrônico através da internet e às comunicações telefônicas através da internet: i) o número de telefone que solicita o acesso por linha telefônica, ii) a linha de assinante digital ("digital subscriber line", ou DSL), ou qualquer outro identificador terminal do autor da comunicação; f) Dados necessários para identificar a localização do equipamento de comunicação móvel: 1) o identificador da célula no início da comunicação; 2) os dados que identifiquem a situação geográfica das células, tomando como referência os respectivos identificadores de célula durante o período em que se procede à conservação de dados. 2. Nos termos da presente diretiva, não podem ser conservados quaisquer dados que revelem o conteúdo das comunicações".*

especializado fornecerá informações relativas aos dados digitais conservados, programas informáticos ou sistemas empregados, demonstrando o uso de medidas técnicas impeditivas da alteração e do acesso de terceiros não autorizados.

O marco legislativo a disciplinar o armazenamento de dados deverá manifestar-se sobre diversas questões, dentre as quais: (a) as categorias de dados conservados; (b) a obrigação dos provedores de serviços de comprovar a identidade dos usuários para conhecer a procedência da comunicação; (c) a duração do armazenamento[425]; (d) as situações em que vedado o armazenamento; (e) possíveis sanções para as atuações prejudiciais de armazenamento; (f) princípios e garantias jurídicos voltados à tutela de direitos fundamentais.

6.2. Eficácia probatória dos dados digitais

Para a utilização da fonte de prova digital, suporte no qual foi gravada a informação que será introduzida no processo (*v.g.,* disco ótico ou magnético, memória *flash*, dentre outros), imprescindível a demonstração da autenticidade, integridade e credibilidade do documento.

Assegurar autenticidade no ambiente digital significa estabelecer vínculos adequados entre os dados obtidos e o respectivo usuário. A comprovação da identidade do responsável deve considerar que os aparelhos eletrônicos têm inúmeros usuários. Demonstra-se a integridade do material com base na precisão e completude dos dados digitais, de forma que se tenha elementos suficientes para refutar qualquer questionamento sobre a originalidade das informações. A respeito da credibilidade, examinadas as circunstâncias, segundo as quais, a fonte de prova foi obtida e tratada.

[425] A indeterminação do prazo gera não apenas insegurança, suscita diversas questões de ordem técnica e econômica. A opção por um prazo dilargado repercute na quantidade dos dados a serem armazenados, o que pode comprometer a qualidade e elevar os respectivos custos do serviço. Impõe compatibilizar as acentuadas despesas dos provedores de serviços de comunicações (situação que pode afetar os preços dirigidos aos clientes e a possibilidade do ingresso de empresas emergentes no mercado) com a necessária eficácia das investigações policiais e a segurança no entorno digital.

A fonte de prova da intervenção nas comunicações eletrônicas será o registro realizado pela polícia ou fornecido pelo intermediário técnico. Neste caso, muitas vezes será necessário trazer aos autos os suportes originais em que constem tais dados (*v.* item 5.3.4), pois de outra maneira não se lograria acessar o conteúdo armazenado.

Obtida a prova a partir da apreensão de dados armazenados em suporte eletrônico, a respectiva fonte será incluída no processo por meio de cópia clone. No caso dos dados de tráfego, serão aportados aos autos a partir de papéis e outros escritos, com base nas informações cedidas pelas operadoras de serviços de telefonia ou *internet*.

Medidas necessárias à preservação da integridade dos dados digitais devem ser adotadas para garantir às partes a possibilidade do exercício do contraditório. Cumpre assegurar a idoneidade dos dados desde a coleta e o armazenamento da informação pela autoridade policial, inclusive o período que permanecer sob custódia do órgão judicial. Às partes processuais será possível, pois, questionar não apenas a finalidade da obtenção destes dados, mas também os procedimentos empregados na conservação.

O sigilo das diligências voltadas à obtenção dos dados digitais deve permanecer enquanto imprescindível para a coleta das informações. Ausentes os motivos que justificaram a ingerência, ao investigado é dado ter conhecimento da realização da medida.

Para assegurar a possibilidade de contraditório, inafastável as partes tenham conhecimento prévio dos dados obtidos, a fim de que formulem as objeções havidas oportunas. Neste momento, os titulares dos dados poderão requerer ao órgão judicial a exclusão de elementos probatórios que careçam de relevância processual.[426]

[426] Interessante a reflexão sobre a possibilidade do fornecimento de cópias dos registros dos dados digitais. Afinal, para tornar substancial o contraditório, de grande valia a consulta das informações na preparação das alegações. Por outro lado, há o inconveniente de que informações disponibilizadas às partes sejam empregadas para devassar a vida privada. A solução usualmente apontada pela doutrina consiste em fornecer as cópias, mas advertir os destinatários que eventuais reproduções ou a revelação das informações referentes à instrução, ensejam responsabilidade (J. J. GONZÁLEZ LÓPEZ, *Los Datos de Tráfico*..., p. 497). O Código de Processo Penal italiano, no art. 268 (6 e 7), buscou minorar a restrição do direito à intimidade. Destarte, as partes podem obter cópia após a individualização dos registros, que devem ser transcritos, e da respectiva conclusão das transcrições; resguardado o direito prévio de examinar, escutar e realizar perícias, mas sem conseguir cópias (*art. 268. 6. "Ai difensori delle parti è immediatamente dato avviso che, entro il termine fissato a norma dei commi 4 e 5, hanno facoltà di esaminare gli atti e ascoltare le registrazioni ovvero di prendere cognizione dei flussi di comunicazioni informatiche o telematiche. Scaduto il termine, il giudice dispone l'acquisizione delle*

A perícia é o instrumento auxiliar para atestar a exatidão das informações. O meio de prova adequado para a incorporação dos dados digitais ao processo é o documento. Aliás, de acordo com o art. 232, do Código de Processo Penal, vigora o conceito amplo de documento.

6.3. Valoração da prova digital

É possível indicar três momentos logicamente distintos e sucessivos da atividade probatória no Direito: (i) a conformação do conjunto de elementos de juízo sobre os quais se adotará a decisão; (ii) a valoração desses elementos; (iii) a adoção da decisão.[427] Sobre estas etapas se faz necessário discorrer brevemente, para em seguida, apresentar as questões mais relevantes relacionadas à prova digital.

O primeiro aspecto evidencia que a decisão judicial apenas poderá estar fundamentada nas provas admitidas no processo. Tanto informações privadas que possam existir sobre o objeto de decisão, como ainda, elementos que tenham sido excluídos do processo em razão da ilicitude, não poderão fundamentar o decreto do magistrado.

O corolário do *livre convencimento* do juiz não autoriza liberdade ilimitada na escolha dos meios probatórios; imprescindível, isto sim, que o julgador esteja atento aos vínculos existentes na atividade de admissão da prova – autêntica seleção que obedece a critérios jurídicos (*admissibilidade*) e lógicos (*pertinência* e *relevância*).[428]

A *admissibilidade* está adstrita à verificação das exigências do legislador para o ingresso da prova; em especial, importa atentar à inexistência de proibições legais. O

---

conversazioni o dei flussi di comunicazioni informatiche o telematiche indicati dalle parti, che non appaiano manifestamente irrilevanti, procedendo anche di ufficio allo stralcio delle registrazioni e dei verbali di cui è vietata l'utilizzazione. Il pubblico ministero e i difensori hanno diritto di partecipare allo stralcio e sono avvisati almeno ventiquattro ore prima. 7. Il giudice dispone la trascrizione integrale delle registrazioni ovvero la stampa in forma intellegibile delle informazioni contenute nei flussi di comunicazioni informatiche o telematiche da acquisire, osservando le forme, i modi e le garanzie previsti per l'espletamento delle perizie. Le trascrizioni o le stampe sono inserite nel fascicolo per il dibattimento").

[427] J. F. BELTRÁN, *La Valoración Racional de la Prueba*, Madrid-Barcelona-Buenos Aires, Marcial Pons, 2007, p. 41.

[428] A. M. GOMES FILHO, *A motivação das decisões penais*, São Paulo, RT, 2001, pp. 150-151.

legislador, ao formular impedimentos, exclui os meios inidôneos para a reconstrução de certos atos; juízo que pode se pautar em aspectos relacionados aos fatos (ilicitude, violação de direito material que permeou a obtenção da prova) ou questões jurídicas ligadas à determinação da regra violada (prova incluída em afronta ao direito processual).

Na conformação do conjunto de elementos de juízo sobre os quais se adotará a decisão, outros dois aspectos devem ser observados: a *pertinência* e a *relevância*. Como esclarece ANTONIO MAGALHÃES GOMES FILHO, ambos estão correlacionados à regra tradicional *frusta probatum non relevant*, porém não se confundem. A *pertinência* expressa uma relação direta entre o fato sobre o qual versa o meio ou fonte de prova e o fato objeto do processo, enquanto a noção de relevância se aplica à chamada prova indireta, demonstrando a aptidão do meio ou fonte de prova para atestar um fato secundário, do qual possa ser inferido o fato principal.[429]

Na etapa seguinte (ii) é de ser valorado o apoio de cada elemento trazido a juízo, na convalidação das hipóteses em conflito, para assim conhecer-lhes o grau de confirmação. Nesse momento a aferição da prova é livre, ou seja, incabível aventar a aplicação de normas de predeterminação do resultado da avaliação.

A racionalidade deve preponderar, as especificidades jurídicas não se manifestam de forma taxativa como na etapa anterior, tem-se aqui a valoração do apoio empírico de um conjunto de elementos para corroborar determinada hipótese. O postulado do livre convencimento, formado após o exame de todo o conjunto probatório, convalida a noção de que o julgador se encontra desvinculado de qualquer critério *a priori* estabelecido. Incumbe ao magistrado motivar a decisão e apontar os elementos que influíram sobre sua convicção.

Apreciado os conjunto de provas carreado aos autos, o valor de cada elemento probatório não é considerado isoladamente, mas em estrita observância ao elo que possa existir entre a informação disponível no processo e a hipótese a ser confirmada. É de se acrescentar, assim, que a valoração consolida as bases para o último momento da atividade probante no processo.

---

[429] Idem, p. 151.

O terceiro momento no contexto da atividade probatória diz respeito à decisão sobre os fatos provados. Conquanto o grau de confirmação nunca possa alcançar níveis de certeza plena, a valoração da prova permitirá a prevalência de uma das hipóteses em conflito, cabendo ao juiz aferir se realmente corroborada por um alto grau de certeza. A motivação expõe as razões da decisão e possibilita o exercício de controle através dos recursos processuais.

Aplicadas tais diretrizes ao tema da prova digital, os dados eletrônicos coletados constituem fonte de prova trazida aos autos de forma impressa ou em suporte digital, consistente na reprodução de arquivos de som e imagem, bem como de palavras, dados, cifras e operações matemáticas. Por se tratar de prova técnica dotada de complexidade, pode ser necessária a perícia informática. O escopo da medida é assegurar a credibilidade da fonte de prova e impedir que a tecnologia seja inadvertidamente aplicada para falsear a realidade.

Em respeito aos direitos e garantias fundamentais, a admissão da "prova eletrônica" não pode prescindir de acurada apreciação quanto à integridade do suporte em que se encontra, autenticidade do conteúdo que apresenta e licitude de sua obtenção.[430]

Nesta modalidade de prova sempre é importante apreciar com cautela o suporte técnico utilizado, pois tanto a estrutura física (*hardware*) quanto o elemento lógico (*software*) podem interferir na prova. O controle do *hardware* pressupõe o exame das etapas de elaboração do documento (variações de temperatura, anomalias da rede elétrica, correntes eletrostáticas, umidade e gestão da informação). Quanto ao *software,* avalia-se a confecção do documento, restrita a pessoas autorizadas pelo sistema.[431]

Como qualquer elemento probatório os dados digitais devem ser valorados a partir do acervo de prova.

Os dados de conteúdo das comunicações eletrônicas têm caráter de prova direta; ou seja, dotados de acentuada possibilidade de demonstrar a ocorrência de

[430] O procedimento e firma ou assinatura digital é meio técnico capaz de creditar confiabilidade aos documentos digitais.
[431] E. DE URBANO CASTRILLO, *La valoración de la prueba electrónica*, Valencia: Tirant lo blanch, 2009, p. 59.

certos fatos. Por outro lado, a obtenção de dados identificadores do local, da duração e destino das comunicações (de tráfego) representa coleta de indícios.

Sobre a prova indireta, sublinhe-se que há um significativo interesse no uso dos dados de tráfego como técnica heurística nas investigações. Os dados externos permitem a identificação da pessoa que realiza uma comunicação por meio de um específico terminal. Mais do que elementos de convicção aptos a indicar uma linha de investigação, estes dados serão úteis para corroborar a tese acusatória ou defensiva.

Infrações penais objeto de apuração por meio do uso de dados de tráfego correspondem, na maior parte das vezes, a investigações criminais iniciadas. Nesses casos, já existe uma denúncia formal e objetiva-se averiguar a identidade do suposto autor e obter indícios que permitam orientar a investigação em determinado sentido.[432]

Quanto à valoração da prova por indícios, não significa que o juiz possa acreditar plenamente em um fato apenas provável, uma vez que a certeza é imprescindível para a comprovação da autoria. Não atingida a convicção *"beyond any reasonable doubt"*, o julgador aplicará a regra de juízo *in dubio pro reo*.

Os mesmos ideais informadores da exigência de que todo o conteúdo das comunicações seja trazido aos autos aplica-se aos dados externos das comunicações. As garantias da autenticidade e integridade referem-se a todas as informações sobre a identidade do emissor, do receptor ou dos interlocutores e quanto sua à localização espaço-temporal.

[432] Controversa a questão da utilização exclusiva dos dados de tráfego para comprovar a culpabilidade do acusado. Aqui, a necessidade de que outros meios de provas auxiliares informem a convicção do julgador representa saída condizente com o seu livre convencimento motivado.

6.4. Prova científica e dados digitais

A criteriosa valoração da prova não compactua com a recepção acrítica de elementos de convicção. As demonstrações científicas são dotadas de grande valor para o processo, mas é necessário que estejam associadas a outras provas. O julgador não está inapelavelmente vinculado às probabilidades técnicas acentuadas destes elementos probatórios – prevalece, em verdade, o livre convencimento motivado do magistrado.

As fontes de provas coletadas no ambiente digital contêm informações cuja autenticidade e integridade devem ser comprovadas. Os sucessivos avanços tecnológicos exigem que os sistemas computacionais sejam diuturnamente testados. A documentação de todas as etapas do tratamento da prova é indispensável para atestar a veracidade dos argumentos e corroborar argumentos.

Para reduzir o risco de equívocos, a credibilidade das ferramentas e técnicas virtuais deve ser testada. No Reino Unido, em 2009, implementada pela UK *Law Comission*, reforma destinada a aperfeiçoar as normas processuais e dispor precisamente sobre a admissibilidade das provas científicas em geral. A respeito das provas digitais discutiu-se a permissão de acesso dos usuários aos códigos fontes referentes aos componentes de um *software*. É certo que esta posição contraria interesses dos produtores de *softwares,* à medida que o sigilo assegura vantagem competitiva; entretanto, não se pode negar em dadas circunstâncias o conhecimento dos códigos permitiria aos programadores de computador identificar possíveis falhas ou estimar a possibilidade de falhas em um *software*.[433] Este caso demonstra perfeitamente como certas opções técnicas converteram-se nos últimos anos em instigantes problemas jurídicos.

Ao jurista não é dado imiscuir-se desnecessariamente em pormenores alheios à sistemática científica quando a solução de boa parte destas controvérsias reside especificamente em sopesar os percalços experimentados durante a produção de provas e

[433] Quando o código fonte não está disponível, a forma de avaliar a credibilidade da fonte de prova é verificar os resultados obtidos utilizando outra ferramenta técnica que assegure os mesmos resultados. No entanto, considerando a velocidade com que a tecnologia computacional modifica-se, é difícil para os especialistas testar todas as inúmeras ferramentas e instrumentos disponíveis (E. CASEY, *Digital evidence ...*, *op. cit.*, p. 74).

os resultados obtidos. Em outras palavras, para validar noveis fontes de provas é necessário, sobretudo, ponderar a confiabilidade dos elementos probatórios a partir de resultados empíricos.

Reconhecer pontos de contato entre o Direito e outras searas do conhecimento expõe a dificuldade de encontrar o equilíbrio entre princípios e metodologias diversas. O papel da ciência como instrumento de confirmação das hipóteses apresentadas pelas partes afigura-se mais acertado que o paradigma da ciência como meio para o alcance de certezas absolutas.

Incluída nos autos, a prova científica deve ser examinada em contraditório. Em nome desta garantia processual franqueia-se a possibilidade de nomear peritos, questionar métodos empregados e resultados alcançados. Oferecer os meios para a contestação da credibilidade das provas proporciona melhores condições para a cognição, ao mesmo tempo que reduz as possibilidades de erro judicial.[434]

6.5. Efeitos da ilicitude probatória em relação aos dados digitais

A Constituição de 1988, no artigo 5º, inciso LVI, prescreveu inadmissíveis no processo as provas obtidas por meios ilícitos. A partir da vedação constitucional, há que se diferenciar duas situações: provas propriamente ilícitas e provas ilegítimas (provas vedadas em sentido absoluto e provas vedadas em sentido relativo).

Considera-se ilegítima a prova produzida ao arrepio da norma, cujo emprego dá ensejo a nulidade ou a outra sanção prevista na própria lei processual. A prova ilícita, por sua vez, é coligida sem respeitar normas ou princípios de direito material, ou seja, a transgressão de um direito marca o momento de sua obtenção.

[434] Para o adequado exercício do contraditório pelas partes *"o perito, notadamente quando utiliza método novo, sobretudo quando ainda não conhecido dos atores processuais, deve utilizar linguagem acessível a todos, de forma a documentar o resultado da perícia da maneira mais clara possível, até mesmo para que possa haver impugnação quanto ao método empregado"* (G. M. DEZEM, *Da prova penal ...*, *op. cit*., p. 196).

O Código de Processo Penal também vedou a utilização de elementos probatórios obtidos a partir de provas consideradas ilícitas, conforme previsto no art. 157, § 1º. Trata-se de imposição lógica, segundo a qual, uma prova é obtida de maneira lícita, mas baseada em uma informação extraída de outra prova alcançada por meio ilícito. Consagrada na matéria, a doutrina dos frutos da árvore envenenada (*fruits of the poisonous tree*); a exemplo da ideia do vício de uma planta que se transmite a todos os seus frutos, consideram-se também ilícitas as provas colidas de uma fonte contrária ao Direito.[435]

O ato de intervenção no sigilo de dados de um investigado pode padecer de três modalidades de ilegalidade: da própria decisão judicial, de sua execução pelos órgãos policiais e do controle judicial da execução da medida.[436]

É possível ainda, que a decisão judicial careça de motivação sobre os pressupostos, requisitos e limites, nos termos abordados nos capítulos anteriores. Em breve apanhado, os vícios podem relacionar-se a ausência de motivação sobre a legalidade, justificação teleológica, competência, limites objetivos, subjetivos e temporais, direito de defesa e juízo de proporcionalidade.

A ilegalidade pode decorrer também da atuação de órgãos policiais que, sem autorização judicial, ampliem o prazo de uma medida, investiguem pessoas diversas do sujeito passivo apontado, ou atuem em desconformidade com o sigilo das informações obtidas.

Por sua vez, a inobservância do adequado controle judicial viola o princípio da paridade de armas, que tem como fundamento o tratamento igualitário e a busca de isonomia entre os sujeitos processuais. O magistrado é responsável pelo conhecimento de todo o desenvolvimento da medida de obtenção da prova e de seus resultados.[437]

---

[435] L. F. TORQUATO AVOLIO, *Provas ilícitas ...*, *op. cit.,* p. 68.
[436] A classificação é adotada por J. L RODRÍGUEZ LAINZ, *Intervención judicial ...*, *op. cit*., p. 412.
[437] A não instauração prévia de inquérito policial não torna ilícita a prova obtida, como já entendeu o Superior Tribunal de Justiça, *v.* HC 85968/SP, rel. Ministro Napoleão Nunes Maia Filho, quinta turma, j. 19.06.2008. No entanto, denúncia anônima, por si só, não autoriza a interceptação telefônica, *v.* HC 64096/PR, rel. Ministro Arnaldo Esteves, quinta turma, j. 27.05.2008.

Também consideram-se ilícitas as fontes de provas coletadas sem observar o dever de sigilo profissional. Preservar informações oriundas do exercício da atividade profissional representa interesse de toda a sociedade, que deve pugnar constantemente pelo respeito aos valores éticos na prestação de determinados serviços. A relevância social das atividades desenvolvidas em certas funções justifica proibir a revelação de informações colidas no exercício do ofício. Se assim não fosse, médicos advogados e religiosos, por exemplo, sujeitar-se-iam a limitações profissionais.

A inviolabilidade das comunicações entre clientes e advogados, constitucionalmente garantida, impõe evidentes limites à arrecadação de dados eletrônicos, confiados pelo investigado a seu patrono. Tais registros não podem ser apreendidos, pois o sigilo profissional alcança também as comunicações viabilizadas no entorno digital e a garantia da ampla defesa impede a retenção de aparatos eletrônicos onde se encontrem armazenadas as informações.[438]

Não apenas as provas coletadas em escritório de advocacia que diretamente afrontem direito material, mas também, todos os dados eventualmente obtidos como resultado de uma violação ao sigilo profissional do advogado deverão ser imediatamente inutilizados.[439]

A declaração da ilicitude de dados de tráfego que tenham servido à identificação de aparelhos eletrônicos apreendidos, ou à interceptação da comunicação, redundará na ilegalidade da prova derivada. Na hipótese em que o conhecimento dos terminais por onde os sujeitos mantinham a comunicação tiver sido viabilizado mediante violação de direito material, como regra geral, a nulidade da prova será absoluta.[440]

---

[438] Quando investigado o próprio advogado sobre autoria ou participação delitiva não se lhe aplica a garantia do sigilo profissional, e excepcionalmente admite-se a realização de buscas ou interceptações em seu escritório (*v.* item 5.3.3).

[439] No julgamento do HC 59967/SP, rel. Ministro Nilson Naves, sexta turma, j. 29.06.2006, prevaleceu no Superior Tribunal de Justiça, por maioria, a ilicitude de fita que continha, em uma parte, entrevista concedida pela ré, e na outra, conversa captada clandestinamente entre ela e seu advogado, exibidas em cadeia de televisão nacional. Segundo o relator, a parte ilícita contaminava a parte lícita, pois ambas formavam um conjunto artístico jornalístico indissociável.

[440] Exceção ocorre nos casos em que a descoberta, a partir de outras linhas de investigação, é inevitável (*inevitable discovery*), e na hipótese do emprego de fonte independente de investigação, sem que haja nexo causal entre a prova originária e as obtidas a partir dela (*independent source*).

As fontes de provas obtidas por meio de interceptação das comunicações eletrônicas, e fundadas na apreensão de suportes automatizados serão ilícitas quando da coleta resulte violação do direito material. Estas provas são particularmente delicadas, pois modificam-se facilmente quando submetidas a tratamento. A contaminação das provas pode ser resultado do modo como utilizados os instrumentos automatizados, ou ainda do escasso conhecimento sobre procedimentos de gestão dos dados. A alteração pode ser resultado do modo como utilizados os instrumentos informáticos, ou em razão do escasso conhecimento do processo de gestão da prova.

O corpo técnico responsável deve resguardar a prova desde o momento da apreensão dos dados até o posterior exame, quando equipamentos específicos permitirão ao especialista analisar e reconstruir os fatos. Não atendidas tais prescrições, como resultado da contaminação, todas as provas decorrentes de um mesmo procedimento ("*step by step*") estarão eivadas de ilicitude.[441]

A gestão da fonte de prova digital será fidedigna, desde que verificada a regularidade de todas as etapas: (i) aquisição; (ii) cadeia de custódia; (iii) autenticação; (iv) recuperação de dados temporários; (v) verificação da autenticidade e confiabilidade da prova.[442]

6.6. Prova digital e sistemas da *Civil Law* e *Common Law*

O emprego dos meios de busca de prova digital na persecução penal varia conforme os critérios que inspiram e fundamentam o ordenamento jurídico. Já não há que se falar em completa dissenção entre os sistemas fundados no Direito romano-germânico ou na *Case Law*. Em verdade, cada sistema encerra características próprias, mas a crescente edição de atos normativos na *Common Law* e reconhecimento de precedentes

[441] Os *softwares* mais recentes permitem verificar hipóteses com o objetivo de gerir, do ponto de vista documental e organizativo, o inteiro processo investigativo. Assim, possível uma clara e completa reconstrução dos fatos, capaz de demonstrar não apenas que o dado originário é autêntico, mas também, que todo o procedimento de análise foi realizado corretamente (G. ZICCARDI, *L'ingresso della computer ..., op. cit.,* p. 174*)*.
[442] Idem, p. 175.

nos ordenamentos de origem romano-germânica, denotam a aproximação recíproca entre estes movimentos.[443]

MICHELLE TARUFFO concebe dois sistemas distintos de provas, relacionados, respectivamente, a cada família jurídica. O autor indica as características do sistema fechado (*Civil Law*): a) todo o fenômeno das provas está compreendido nas normas que delas se ocupam, de modo que apenas interessa aquilo que está positivado; b) provas atípicas estão excluídas; c) a regulação jurídica da prova e o processo constituem um contexto autossuficiente e autônomo em relação a qualquer outro da experiência.[444]

Por outra vereda, conforme a concepção aberta (*Common Law*): a) a prova é, sobretudo, um fenômeno que pertence à lógica e à racionalidade, de forma que alguns aspectos desse fenômeno estão previstos e regulados por normas; b) recepcionam-se provas atípicas; c) as normas em matéria de provas não servem para definir e limitar o conceito jurídico de prova, uma vez que qualquer evento serve para estabelecer um fato, a utilidade maior das normas consiste em excluir a admissão de alguns meios de provas quando presente razão para tanto; d) é possível o emprego de noções, conceitos e modelos de análise provenientes de outros setores da experiência, sejam de caráter científico ou extraídos do sentido comum ou da racionalidade geral.[445]

Desse modo, o contexto da tomada de decisões sobre a prova é distinto em países cujo ordenamento inspira-se na *Civil Law* ou na *Common Law*. Para o Direito continental, a prova não pode ser estudada segundo uma noção demasiado ampla, própria, por exemplo, de uma epistemologia geral (como ocorre nas ciências naturais). A prova admitida pelo Direito, traduz-se em noção especificamente jurídica.[446]

De maneira geral, para a *Common Law* não há vedações prévias ao uso dos meios probatórios. Este critério inclusive incrementa as possibilidades de que a demonstração de um fato corresponda à verdade. No Direito inglês, a admissão de uma

[443] ENNIO AMODIO detalha a aproximação, *v. Libero convincimento e tassatività dei mezzi di prova: un approccio comparativo*, in Rivista italiana di Diritto e Procedura Penale, XLII, n. 1, Milano, 1999, p. 8.
[444] M. TARUFFO, *La prueba ...*, *op. cit*., p. 345.
[445] O autor aponta duas vertentes antagônicas de valoração da prova, compara em sentido amplo a *Civil Law* e a *Common Law*, com o intuito de diferenciar padrões rígidos ou flexíveis de taxatividade sobre os meios de prova. Ou seja, a *Common Law* não espelha exatamente o protótipo de um sistema aberto (à medida que também possui atos normativos em matéria probatória) e a *Civil Law* não representa perfeitamente um sistema fechado (visto que há receptividade para meios atípicos de prova).
[446] J. F BELTRÁN, *La Valoración Racional ..., op. cit.*, pp. 24-25.

evidence[447] em juízo não está condicionada à existência de uma norma permissiva, mas sobretudo, à sua relevância na dialética do contraditório.

A *evidence* possui atributo que, para TARUFFO, evoca a próprio definição de prova: tudo aquilo que serve logicamente para provar um fato. A regra dos ordenamentos da *Common Law,* segundo a qual, todo elemento de prova relevante deve ser admitido, desde que não haja norma ou motivo específico para excluí-lo, deve ser compreendida não apenas como um preceito jurídico mas, principalmente, como princípio geral da razão. A única limitação ao uso dos meios de provas relevantes consiste nas chamadas *exclusionary rules*.[448]

É certo que o sistema da *Common Law* não se pauta, tradicionalmente, por um discurso de busca da verdade no processo.[449] No entanto, na linha dos ensinamentos de TARUFFO e BELTRÁN, a *Common Law*, ao proporcionar amplo recurso às metodologias e análises da epistemologia geral para a valoração da prova, contribui significativamente para que a decisão adotada sobre os fatos corresponda à verdade.[450]

O surgimento de novos meios de obtenção de provas no entorno digital opera-se diferentemente no Direito continental e no Direito anglo-saxão. Uma análise comparativa das soluções dispensadas aos problemas suscitados pelo desenvolvimento tecnológico demonstra que a *Common Law*, ao menos no campo teórico, mostra-se menos refratária a contínuos avanços e aos novos meios probatórios.

---

[447] Denomina-se *evidence* toda a informação capaz de demonstrar um fato e *Law of evidence,* o conjunto das leis (*Acts*) e critérios reguladores dos meios através dos quais os fatos podem ser provados.

[448] A previsão de um conjunto especial de regras de exclusão encontra justificativa no receio de que uma irrestrita apreciação do plexo probatório pelo júri afaste a decisão do inarredável ideal de justiça. Desse modo, tanto para evitar vereditos irracionais, como para preservar os direitos do acusado, gradativamente os precedentes dos Tribunais consolidaram a disciplina das chamadas *exclusionary rules*. O amplo rol de exclusão do moderno *Law of evidence* é reflexo da história da *Common Law*. Muitas destas normas são oriundas de períodos em que os juízes adotaram postura paternalista em relação aos jurados – era comum que a *evidence* relevante fosse excluída (*v.g.*, *hearsey evidence, evidence of character, opinion evidence of non-experts*), pensando que os leigos poderiam superestimar seu valor e importância, ou até mesmo tratá-las como conclusivas (ADRIAN KEANE, *The modern law of evidence*, Oxford, University Press, 2008, pp. 44-47).

[449] A problemática com que nos deparamos não é se o processo deve ou não buscar a verdade dos fatos, ou se a verdade pode ou não ser alcançada em abstrato, mas sim, a compreensão de que a verdade dos fatos, estabelecida pelo julgador para constituir o fundamento da decisão, em nada é absoluta. Por isso, fala-se em verdade contextual e relativa: aquela que signifique a melhor aproximação possível atingida por meio de provas e com base nos fatos relevantes para a decisão (M. TARUFFO, *La prueba ...*, *op. cit*., pp. 522-525).

[450] O contraditório e a imparcialidade são autênticas garantias de verdade do processo (N. GUZMÁN, *La verdad ...*, *op. cit*., p. 137). Ambas as garantias encontram consistente respaldo no sistema adversarial.

Como se afirmou, para a *Common Law* a prova é, sobretudo, um fenômeno que pertence à lógica e à racionalidade, que prescinde de regulação normativa. Nos sistemas de *Civil Law,* todo o fenômeno das provas está compreendido no Direito positivado; desse modo, a proliferação de novos meios probatórios não previstos em lei confronta-se com alguns obstáculos.

A maior flexibilidade da *Common Law* ao uso de meios de busca de prova tecnológicos tem se relevado útil à elucidação de delitos. Por outro lado, o reconhecimento irrefletido dos noveis meios de obtenção de provas, aliado a ausência de disciplina detalhada, pode colocar em risco a tutela dos direitos individuais. As constantes condenações do Reino Unido na Corte Europeia de Direitos Humanos sinalizam que o regime jurídico dos meios de obtenção de prova resulta não raro em violação de direitos.[451]

No sistema processual penal pátrio os meios de prova e os meios de obtenção da prova, como regra, possuem previsão específica; vigora pois o regime de taxatividade.[452] Porém, no artigo 155, parágrafo único do Código, o legislador assegurou também a liberdade probatória: *"Somente quanto ao estado das pessoas serão observadas as restrições estabelecidas na lei civil".*[453]

Assim, (i) se não houver outro meio legal que possa alcançar a mesma finalidade probatória; (ii) se os meios empregados forem idôneos à produção de um resultado útil ao processo; (iii) se não resultar lesão à liberdade moral da pessoa, ao juiz

[451] O caso *Khan vs.* Reino Unido, ganhou notoriedade pelos excessos policiais retratados e trouxe à baila uma habitual invasão de domicílios pela polícia inglesa, para instalar aparelhagens de escuta ambiental fundada em meras em circulares do Ministério do Interior. Constatou-se que mesmo após a entrada em vigor do *Police and Criminal Evidence Act de 1984,* era prática rotineira a expedição de diretivas do Ministério do Interior à polícia para a obtenção de *evidences* de caráter altamente invasivo. À luz da disciplina do *Human Rights Act* de 1998 – documento voltado a efetivar as disposições da Convenção Europeia de Direitos do Homem – o novo Ato de Poderes Investigatórios de 2000 foi alvo de recentes críticas, de juristas e estudiosos da *Common Law* e do direito continental. Sob o pretexto de combater o terrorismo, o *Act* de 2000 diretamente afronta o entendimento da CEDH, por vezes ignorando que a vigilância deve ser proporcional àquilo que se busca encontrar. O ato de Regulação dos Poderes Investigativos (2000) autoriza a chamada vigilância invasiva, que pode ser realizada em qualquer dependência residencial ou veículo privado, na presença da pessoa, até mesmo por meio da instalação de instrumentos de vigilância ocultos.

[452] A taxatividade não vale para as fontes de prova. Todo suporte fisicamente hábil (papel, madeira, fita magnética, mídia digital, disco rígido de computador) para registrar dados juridicamente relevantes, tanto por modo escrito, como através de outros meios (fotográfico, cinematográfico, sonoro, informático...), constitui possível fonte de prova.

[453] Por analogia aplica-se também o art. 332, do Código de Processo Civil: *"todos os meios legais, bem como os moralmente legítimos, ainda que não especificados neste Código, são hábeis para provar a verdade dos fatos em que se funda a ação ou a defesa".*

será dado admitir a prova atípica.[454] Por este viés, concretiza-se o sistema probatório denominado por ENNIO AMODIO como de *estrutura flexível*, capaz de admitir inclusive o ingresso de instrumentos de conhecimento característicos da evolução tecnológica.[455]

Em relação aos meios de obtenção de prova, contudo, a liberdade de adaptação do procedimento probatório é restrita. Como se viu, os meios de busca de prova estudados (capítulos 4 e 5) instrumentalizam a restrição de direitos fundamentais; por esta razão, forçosa a presença dos pressupostos, requisitos e limites para a adoção da medida (legalidade processual penal):

> "O preceito do devido processo legal (art. 5º, inciso XXXIX, CR), em sua feição material *("substantive processo of law"*), associado às regras da legalidade geral (art. 5º, inciso II, CR) e penal material (art. 5º, inciso XXXIX, CR) formam a base jusfundamental que determina a imprescindibilidade de que toda medida estatal processual penal restritiva de direito fundamental seja prévia, escrita e se dirija a um fim constitucionalmente legítimo. Esse é o ponto de união entre os dois pressupostos tratados neste item: é imprescindível uma lei formalmente correta e com um fim constitucionalmente justificável".[456]

Para a intervenção nas comunicações eletrônicas, autorizada no art. 5º, inciso XII, da Carta Federal, o legislador apenas fez remissão ao regime jurídico das comunicações telefônicas (lei 9.296/96, art. 1º, parágrafo único). Embora a lei não explicite, sucintamente, pressupostos, requisitos e limites da medida, é chegada a hora de um novo marco normativo que atente às situações ainda à margem de previsão.

A respeito dos outros meios de pesquisa da prova que não possuem regime jurídico próprio (*v.g.,* as intervenções nas comunicações em canal aberto e a interceptação da comunicação entre presentes), igualmente necessária a intensificação dos

---

[454] Conforme a teoria ampliativa, os meios típicos (de prova ou de investigação) são aqueles que têm previsão legal quanto à sua denominação (nominados) e quanto ao respectivo procedimento. Atípicos são os meios de prova ou de obtenção da prova que não têm previsão normativa sobre o procedimento, bem como aqueles que sequer são nominados pela lei (G. M. DEZEM, *Da prova penal ..., op. cit*., p. 147).

[455] *Libero convincimento ..., op. cit*., pp. 6-7. ANTONIO LARONGA sublinha que a natureza desta escolha é uma opção intermediária entre taxatividade e liberdade dos meios de prova: *"da un lato, ha riconosciuto la possibilità di introdurre nel processo prove non disciplinate dalla legge – per non chiudere la porta di fronte ai continui ritrovati tecnologici che aprono sempre nuove prospettive alle investigative (...) – dall'altro, ha fissato per legge le condizioni cui è subordinata la loro ammissibilità nel processo"* (*Le prove atipiche nel Processo Penale,* Milano, CEDAM, 2002, p. 5).

[456] M. Z. DE MORAES, *Presunção de inocência ...*, *op. cit*., p. 349.

esforços para a regulação da matéria. Ainda que se possa aventar uma aplicação analógica do modelo de outro meio de pesquisa[457], a solução mais condizente é aquela ressaltada por MAURICIO ZANOIDE DE MORAES, *"de que toda medida estatal processual penal restritiva de direito fundamental seja prévia, estrita e se dirija a um fim constitucionalmente legítimo"*.

Por sua vez, a apreensão de dados armazenados em suportes eletrônicos ou físicos que os contenham constitui prova penal atípica, pois carece de disposição que especifique o procedimento de recolha da informação digital. Há necessidade de demonstrar que outros meios de obtenção de prova são inadequados para atingir os mesmos resultados e que a limitação do direito fundamental se faz em consonância com o princípio da proporcionalidade. Neste âmbito, a motivação judicial: (i) versará sobre os aspectos legais indispensáveis à diligência de busca e apreensão (*v.* capítulo 5); (ii) disporá acerca da impossibilidade de produzir a prova por outro meio; (iii) sempre que possível, identificará o modo menos invasivo de execução da diligência.[458]

Ao dirigir o foco de observação para os Estados de tradição romano-germânica em geral, constata-se que a admissão dos meios de prova atípicos nestes ordenamentos tem por finalidade não vedar peremptoriamente o emprego de novas medidas para o conhecimento dos fatos. Com efeito, o influxo das modernas tecnologias no tema das provas processuais penais desvela um constante embate entre a busca da verdade e o risco de que tais instrumentos ocasionem graves lesões aos direitos individuais.

O esforço de tipificação das provas penais assegura previsibilidade e segurança ao método probatório – contínua tentativa de adequação do Direito à realidade.

---

[457] Sobre a aplicação analógica e os meios de busca de prova, *v.* F. R. BECHARA, G. M. DEZEM, *Captação ambiental de imagens: usos e limites*, in A. Scarance Fernandes (org.), *Estudos de Processo Penal*, São Paulo, Scortecci, 2011, pp. 116-140. Para um regime jurídico da interceptação da comunicação entre presentes, *v.* a percuciente análise de M. G. B. ARANTES FILHO, *A interceptação de comunicação ...*, *op. cit*.

[458] Muitas vezes a apreensão do suporte eletrônico não assegura o acesso aos dados relativos à prática criminosa. Tal fato ocorre principalmente nos casos de armazenamento de informações em servidores localizados em outras cidades ou outros países. A participação do Estado brasileiro nesta empreitada efetiva-se pelo aprofundamento das iniciativas de cooperação internacional e a homogeneização das normas internacionais: "*Ed invero, se il diritto penale tradizionale resta essenzialmente legato al territorio ed adatto a sanzionare a condotte poste in essere da individui isolati, l'esistenza di un crimine globale, organizzato in una rete che attraversa le frontiere dei singoli Stati, richiede un'estensione internazionale stricto sensu intesa e l'adozione di norme comune che, se non addirittura unificate, siano almeno omogenee"* (M. DELMAS-MARTY, *Il diritto penale come etica della mondializzazione*, Rivista italiana di Diritto e Procedura Penale, XLIX, n. 1, Milano, Giuffrè, 2006, p. 6.

A exemplo do que afirmou HEGEL sobre o papel da Filosofia, o Direito toma conhecimento dos fatos e passa a regulá-los apenas quando se apresentam à coletividade. Impossível antecipar os rumos da vida social. Assim, o ato normativo chega em atraso para constatar e compreender a realidade: o Direito, como a coruja de Minerva, inicia o seu voo ao entardecer.[459]

Juristas e legisladores parecem sempre um passo atrás das descobertas científicas, como se o progresso tecnológico pudesse continuamente surpreendê-los. O cientista do Direito não pode permanecer inerte, alheio à passagem do tempo, deve manter-se atento ao advento de novos meios de prova e prontamente rechaçá-los ou incorporá-los ao ordenamento. Contudo, o contínuo aperfeiçoamento dos métodos probatórios recomenda prudência: que não sejam atabalhoadamente trazidos ao processo novos meios de prova sem que se possa efetivamente analisar-lhes a constitucionalidade e eficácia.

[459] Nas palavras do filósofo: *"Quando la filosofia dipinge a chiaroscuro, esso non si lascia ringiovanire, ma soltanto riconoscere: la nottola di Minerva inizia il suo volo sul far del crepuscolo"* (G. W. F. HEGEL, *Lineamenti di filosofia del diritto*, trad. Francesco Messineo, Roma, Laterza, 1979, p. 20).

Conclusões

1. Os inegáveis progressos da Cibernética na reprodução mecânica da fisiologia animal, dos eventos naturais e das ações humanas, constituem precedentes para o atual estágio da sociedade tecnológica, na qual os novos inventos desempenham atividades essenciais. Sob a perspectiva comparativa entre máquinas e homens, o computador imita as funções neurofisiológicas humanas e a interconexão destes aparelhos eletrônicos em rede possibilita a conformação de territórios fisicamente inexistentes.

2. O entorno digital designa o conjunto de redes onde se encontra todo tipo de informação. As interações neste espaço imaterial subvertem as noções tradicionais de *território, tempo* e *estrutura*, tornando necessárias novas ponderações para assegurar a compreensão espacial, cronológica e natural da fluidez e multidimensionalidade das relações jurídicas.

3. A apreensão de conceitos relacionados ao entorno digital tornou-se imprescindível à ciência jurídica contemporânea. O franco desenvolvimento das tecnologias informativas, operado nas últimas décadas, representa não apenas um fenômeno que reclama imediata resposta legislativa, mas um processo complexo, cujos efeitos alcançam a própria atividade jurisdicional. A plena interação entre informática e telecomunicações modificou por completo o armazenamento de informações; o acesso a pareceres, decisões, normas, e às fontes do Direito em geral, tornou-se imediato. Sem ignorar os benefícios desta transformação, inadmissível sejam abandonadas as técnicas e premissas hermenêuticas em favor da repetição: é preciso velar para que a interpretação jurídica não se converta em mera reprodução mecânica e irrefletida de conteúdos.

4. No entorno virtual os processos comunicativos aperfeiçoam-se de maneira livre e abrangem um amplo contingente de pessoas. O fluxo incessante de dados é capaz de atenuar a própria noção de autonomia e afirmar a liberdade como reciprocidade – cada indivíduo pode simultaneamente colher e veicular as informações.

5. Por redes de comunicação eletrônica designam-se a *infraestrutura da comunicação*; os *serviços de comunicação eletrônicas*, destinados à transmissão da informação por meio das

infraestruturas de comunicação; e os *recursos associados,* noveis ferramentas interligadas ao fenômeno telecomunicativo.

6. As redes de comunicação permitem obter, processar e veicular conteúdos em tempo real. Esta evolução afeta diretamente as relações interpessoais e dá ensejo a um novo ciclo cultural, marcado pela estreita afinidade entre o tratamento e a transmissão da informação.

7. A tradição constitucionalista pátria consagra a inviolabilidade de domicílio como liberdade da pessoa, isoladamente considerada, que lhe permite resguardar uma projeção espacial íntima. De outra feita, a liberdade de comunicação refere-se ao exercício das faculdades do próprio espírito, à autonomia e independência do pensamento perante terceiros.

8. Considerada um direito de conteúdo eminentemente negativo, a *privacy* não figura apenas como faceta do *direito de estar só*, assume também um viés positivo, enquanto controle direto de informações e da capacidade de comunicá-las e mantê-las para si mesmo.

9. A base axiológica do direito à proteção de dados, reconhecida nas faculdades do titular de dados informáticos – relacionadas ao consentimento, controle, retificação e destruição dos dados –, evidencia o *conteúdo* da autodeterminação informativa como direito humano vocacionado à autonomia.

10. O emprego de técnicas hermenêuticas (interpretação gramatical, histórico-evolutiva e teleológica) e a busca da convergência entre os sentidos, permitem concluir que a expressão *"no último caso"* (CF, art. 5º, inciso XII) refere-se às comunicações telefônicas e de dados.

11. Embora distintos o suporte empregado e o canal de circulação da comunicação, tanto a carta como o correio eletrônico são meios de difusão de ideias e pensamentos que utilizam principalmente caracteres escritos. O caráter íntimo da comunicação, destinada a um receptor determinado, exige total reserva do conhecimento de terceiros. Por esta razão, o regime da inviolabilidade das comunicações postais igualmente se aplica às interceptações ou acessos a mensagens de correio eletrônico.

12. Concluída a comunicação, não cessa a necessidade de tutela jurisdicional para o conhecimento de seu conteúdo, portanto, não há que diferenciar a proteção das comunicações e a proteção dos dados em si mesmos. A mesma liberdade pessoal que permite manter o pensamento sob recato, impede que o Poder Público legitime a obtenção de informações pessoais sem observar a reserva de jurisdição. Se assim não fosse, restariam comprometidas a harmonia e o equilíbrio entre os Poderes, princípio fundamental da República.

13. Sobre a reserva dos dados de tráfego das comunicações telefônicas em curso e dos dados de comunicações concluídas, incide preponderantemente o art. 5°, XII, da Constituição Federal, que permite derrogar o sigilo apenas mediante autorização judicial. Ou seja, a obtenção dos registros telefônicos e dos dados externos empregados em outras modalidades de comunicação depende de ordem judicial motivada.

14. O dado digital constitui a informação de estrutura numérica e imaterial, processada por sistemas computacionais, destinada a desempenhar uma função e representada em diversos formatos informativos (textos, imagens, áudio e vídeo).

15. Os dados de tráfego das comunicações eletrônicas são informações de estrutura digital, geradas ou tratadas no curso do processo comunicativo, e que diferem do conteúdo material. Como utilizados para o fluxo da informação nas redes, estes dados externos permanecem temporariamente armazenados pelas operadoras de serviço.

16. Os aparelhos eletrônicos e o entorno digital aportam inúmeras informações pessoais sobre os investigados, vítimas ou testemunhas de atos criminosos. Os dados digitais amiúde revelam indícios de autoria e materialidade, informações úteis ao processo e indispensáveis à compreensão dos fatos.

17. As investigações policiais prospectivas justificam-se apenas quando realizadas em espaços públicos do entorno digital. O emprego de meios de vigilância pessoal afronta direitos fundamentais e não se compatibiliza com o regime constitucional democrático.

18. O acesso aos dados de tráfego afigura-se decisivo na investigação de determinados delitos. O estudo conjugado dos dados externos à comunicação permite investigar a prática

de crimes, especialmente quando perpetrados nas redes de computadores, pois a partir deles segue-se o rastro de uma comunicação. Ainda que a obtenção de dados de tráfego possa ter intensidade lesiva menor, a autorização judicial é imprescindível em ambos os casos, assim como a precisa individualização dos aspectos subjetivo e objetivo da medida.

19. A tutela constitucional da inviolabilidade das comunicações aplica-se igualmente aos dados de conteúdo e dados de tráfego. A proteção não se modifica em razão da modalidade de dado pessoal ou do tipo de informação aportada, mas sim, em função da inviolabilidade do meio segundo o qual é transportada.

20. O processo comunicativo no entorno digital ocorre em canal aberto ou fechado. No primeiro caso, disponibiliza-se a informação a qualquer pessoa, independentemente de autorização judicial; no segundo, não há consentimento do usuário para que terceiros tenham acesso ao conteúdo da comunicação.

21. A intervenção refere-se a toda ingerência em processo comunicativo que tenha suporte informático, realizada em canal aberto ou fechado. Por outro giro, a interceptação das comunicações eletrônicas designa a interferência executada por terceiros nos processos comunicativos em canal fechado.

22. As intervenções eletrônicas constituem operações técnicas voltadas a captar o conteúdo comunicativo presente em textos, imagens, sons, ou outro conteúdo digital. A intervenção no fluxo de dados (de conteúdo ou de tráfego), meio de obtenção de prova que tem como característica a restrição de direitos fundamentais, pode ocorrer em canal aberto ou fechado. Neste caso, trata-se de medida excepcionalíssima, pois limita o exercício do direito ao segredo das comunicações, da proteção de dados pessoais e da liberdade de pensamento e expressão. Esta medida tem por finalidade viabilizar a investigação dos ilícitos e preservar possíveis fontes de provas.

23. Grande parte dos crimes virtuais transcende os limites espaciais tradicionalmente impostos à atividade delitiva e projetam-se de imediato em diferentes Estados. Uma mesma conduta pode realizar-se simultaneamente em diferentes países, servir-se de meios disponibilizados em lugares completamente distintos e produzir efeitos nas mais variadas partes do globo. A regulação da *cyber* criminalidade deve pautar-se pela cooperação

internacional: ao legislador pátrio não cabe apenas postular a inclusão do Brasil neste cenário, faz-se imprescindível conjugar esforços concretos, que permitam consolidar um sistema transnacional sólido, eficiente e participativo.

24. As intervenções nos processos comunicativos realizados em canal aberto caracterizam-se, principalmente, pela inexigibilidade de resolução judicial que habilite o conhecimento e a apreensão de dados para fins de investigação. A publicidade da informação estriba-se no consentimento do titular, elemento capaz de elidir a aplicação do segredo da comunicação. Incide, no entanto, a proteção específica relativa à autodeterminação informativa.

25. Para que a intervenção nas comunicações eletrônicas e o acesso a dados armazenados em suporte eletrônico conforme-se ao regramento constitucional, a autorização judicial deve estar devidamente fundamentada e atender a finalidade específica, prevista em lei. A licitude destes meios de busca de prova depende da observância dos limites objetivos, subjetivos e temporais, da preservação do exercício do direito de defesa do investigado e do controle judicial da execução da diligência.

26. A intervenção nas comunicações eletrônicas e a busca e apreensão de aparelho digital exigem juízo de proporcionalidade: averiguada a inexistência de outros meios menos lesivos aos direitos do investigado (necessidade); avaliada a eficácia da medida para atender o escopo de apuração dos fatos (idoneidade); valoradas as consequências do ato, em relação à estigmatização jurídica e social que sofrerá o inculpado (proporcionalidade em sentido estrito).

27. O acesso aos dados informáticos de comunicações concluídas ou de dados armazenados em suporte digital concretiza-se mediante cessão ou busca e apreensão das informações. A cessão opera-se por meio de requisição judicial dirigida aos provedores de *internet*, ou fundada no consentimento do próprio titular dos dados ou de um dos interlocutores da comunicação.

28. A busca e apreensão de aparelho eletrônico constitui diligência investigativa de procura e asseguração de fontes de prova, limitativa de direito individual, destinada a apreender elementos de convicção necessários à prova de infração ou à defesa do réu, decretada sempre mediante autorização judicial.

29. Uma vez retido o equipamento, o sujeito passivo da apreensão sofrerá limitação nas comunicações cotidianas e também em sua atividade laboral. Avalia-se a situação concreta para diferenciar casos em que deve haver a retenção e o transporte do aparelho até a sede do centro operacional da polícia especializada (sobretudo, quando exigido tempo para operações técnicas), ou quando a cópia integral dos dados relevantes para a análise do disco rígido ou dispositivo de memória representa medida suficiente.

30. O exercício do direito de defesa pressupõe o conhecimento dos procedimentos de conservação dos dados e a possibilidade de confrontá-los com os originais. A não alteração dos dados é imprescindível, a exigir que todo procedimento técnico seja realizado nas respectivas cópias.

31. O tratamento consiste na realização, ao menos, de uma das seguintes operações técnicas de caráter automatizado ou não: armazenamento, consulta, utilização, gravação, conservação, elaboração, modificação, bloqueio, cancelamento ou cessão de dados.

32. Para que a conservação de dados digitais não viole o direito à proteção dos dados, se faz necessário definir claramente a *finalidade* do tratamento; a *segurança* deve nortear as cautelas de preservação das informações; a medida há que se restringir ao interregno temporal estritamente necessário à consecução dos objetivos que a justificam.

33. Assegurar autenticidade no ambiente digital significa estabelecer vínculos adequados entre dados e sujeitos. A comprovação da identidade do usuário deve fundar-se em procedimentos acurados, que permitam relacionar indivíduos e conteúdos, até mesmo nos casos em que o mesmo aparelho eletrônico seja compartilhado por diversas pessoas. A credibilidade dos dados depende, sobremaneira, das circunstâncias em que foram obtidos e tratados; por conseguinte, a informação deve submeter-se às verificações inerentes ao contraditório.

34. A inclusão de provas científicas no processo criminal não deve comprometer o livre convencimento judicial ou frustrar o contraditório. Quando admitidos, os elementos probatórios constituídos unilateralmente sujeitam-se ao confronto argumentativo conduzido pelos peritos, ainda que seja diferido. A existência de meios que permitam

verificar a credibilidade das provas facilita a cognição e, ao mesmo tempo, reduz as possibilidades de erro judicial.

35. A licitude da fonte de prova digital demanda escorreita gestão dos conteúdos em sua (i) aquisição; (ii) cadeia de custódia; (iii) autenticação; (iv) recuperação de dados temporários; (v) verificação da autenticidade e confiabilidade da prova – enfim, em qualquer etapa do tratamento de dados.

BIBLIOGRAFIA

ABOSO, Gustavo Eduardo, ZAPATA, María Florencia, *Cibercriminalidad y Derecho Penal*, Montevideo-Buenos Aires, Julio César Faira, 2006.

ALEXY, Robert, *Teoría de los Derechos Fundamentales*, 2ª ed., trad. Carlos Bernal Pulido, Madrid, Centro de Estudios Políticos y Constitucionales, 2008.

ALMEIDA JUNIOR, João Mendes, *O Processo Criminal Brazileiro*, v. II, 2ª ed., Rio de Janeiro, Francisco Aves e Cia, 1911.

ALMEIDA, José Raul Gavião de, *Anotações acerca do direito à privacidade*, in J. Miranda, Marco Antonio Marques da Silva (orgs.), *Visão Luso-Brasileira da Dignidade Humana*, 2ª ed., São Paulo, Quartier Latin, 2009.

_____, *O interrogatório à distância*, São Paulo, Tese de Doutorado, 2000.

ÁLVAREZ GARCIA, Francisco Javier, *El acceso por parte de las fuerzas y cuerpos de seguridad del estado a ficheros de datos personales*, in Ernesto Pedraz Penalva (coord.), *Protección de datos y proceso penal*, Madrid, La ley, 2010.

AMODIO, Ennio*, Libero convincimento e tassatività dei mezzi di prova: un approccio comparativo*, in Rivista italiana di Diritto e Procedura Penale, XLII, n. 1, Milano, 1999.

ARANTES FILHO, Marcio Geraldo Britto, *A interceptação de comunicação entre pessoas presentes como meio de investigação de prova no Direito Processual Penal brasileiro*, São Paulo, Dissertação de Mestrado, 2011.

ARAUJO, Jose Laercio, *Intimidade, Vida Privada e Direito Penal*, São Paulo, Habeas, s/d.

ARENAS RAMIRO, Mónica, *El derecho fundamental a la protección de datos personales en Europa*, Valencia, Tirant lo Blanch, 2006.

ARENDT, Hannah, *Entre o passado e o futuro*, trad. Mauro W. Barbosa de Almeida, São Paulo, Perspectiva, 1979.

AVOLIO, Luiz Francisco Torquato, *Provas ilícitas: interceptações telefônicas, ambientais e gravações clandestinas*, 4ª ed., São Paulo, RT, 2010.

BACHELET, Olivier, *La hiérarque des preuves*, in Geneviève Giudicelli-Delage (org.), *Les Transformations de L'administration de la preuve pénale*, Paris, Société de Législation Comparée, 2006.

BADARÓ, Gustavo Henrique Righi Ivahy, *Direito Processual Penal*, tomo I, São Paulo, Elsevier, 2008.

_____, *Interceptação de comunicações telefônicas e telemáticas: limites ante o avanço da tecnologia*, in J. Corrêa de Lima e Rubens R. R. Casara (coords.), *Temas para uma Perspectiva Crítica do Direito*, Rio de Janeiro, Lumen Juris, 2010.

BALLESTEROS MOFFA, Luis Ángel*, La Privacidad Electrónica: internet en el centro de protección*, Valencia, Tirant lo blanch, 2005.

BANDEIRA, Gustavo, *A interceptação do fluxo de comunicações por sistemas de informática e sua constitucionalidade*, in Revista de Direito do TJ/RJ, n. 55, 2003.

BARBALHO, João, *Constituição Federal Brasileira: Commentarios*, Rio de Janeiro, F. Briguet e cia. Editores, 1924.

BARRAGÁN, Julia, *Informática y Decisión Jurídica*, México, Fontamara, 2000.

BARROS, Marco Antonio de, *A Busca da Verdade no Processo Penal*, São Paulo, RT, 2002.

_____*, Processo Penal Impulsionado pela Tecnologia: A Investigação Criminal Realizada com Novos Meios Tecnológicos e a Iminente Semi-Informatização do Procedimento Penal Anunciada pela Lei 11.419/2006*, São Paulo, Tese, 2008.

BARROS, Suzana de Toledo, *O Princípio da Proporcionalidade e o Controle de Constitucionalidade das Leis Restritivas de Direitos Individuais*, Brasília, Brasília Jurídica, 1996.

BASTOS, Celso Ribeiro, MARTINS, Ives Gandra, *Comentários à Constituição do Brasil*, v. 2, São Paulo, Saraiva, 1989.

BASTOS, Celso Ribeiro, MEYER-PFLUG, Samantha, *A interpretação como fator de desenvolvimento e atualização das normas constitucionais*, in V. Afonso da Silva (org.), *Interpretação constitucional*, São Paulo, Malheiros, 2007.

BECHARA, Fábio Ramazzini, MANZANO, Luís Fernando de Moraes, *Crime Organizado e Terrorismo nos Estados Unidos da América,* in J. R. Gavião de Almeida, A. Scarance Fernandes, M. Zanoide de Moraes (orgs.), *Crime organizado: aspectos processuais*, São Paulo, RT, 2009.

BELTRÁN, Jordi Ferrer, *La Valoración Racional de la Prueba*, Madrid-Barcelona-Buenos Aires, Marcial Pons, 2007.

BRANDEIS, Louis, WARREN, Samuel D, *The right to privacy*, *Harvard Law Review*, v. IV, n. 5, dec. 1890.

BRENNER, Susan W., *Cybercrime Metrics: Old wine, new bottles?*, Virginia Journal of Law & Technology Association, v. 9, n. 13, University of Virginia, 2004.

BULOS, Uadi Lammêgo, *Constituição Federal anotada*, 7ª ed., São Paulo, RT, 2007.

CARIDI, Gianfranco, *Metodologia e Tecniche Dell'Informatica Giuridica*, Milano, Giuffrè, 1989.

CASEY, Eoghan, *Digital evidence and computer crime: forensic science, computers and the internet*, New York, Elsevier, 2011.

CASTANHO DE CARVALHO, Luis Gustavo Grandinetti, *Processo Penal e Constituição: Princípios Constitucionais do Processo Penal*, 4ª ed., Rio de Janeiro, *Lumen Juris*, 2006.

CASTRO, Ernesto M. de Melo, *Algorritmos*, São Paulo, Musa, 1998.

CERVINI, Raul, GOMES, Luiz Flávio, *Interceptação telefônica: Lei 9.296, de 24.07.96*, São Paulo, RT, 1997.

CHIAVARIO, Mario, *Diritto Processuale Penale*, 5ª ed., Milano, UTET, 2012.

COSTA, Helena Regina Lobo, LEONARDI, Marcel, *Busca e apreensão e acesso remoto a dados em servidores*, Revista Brasileira de Ciências Criminais, n. 88, v. 19, 2011.

COSTA, Sara, *A Proteção de Dados Pessoais na Internet*, in Revista Jurídica, v. VI, Universidade Eduardo Mondlane, set., 2004.

COSTA JÚNIOR, Paulo José, *O direito de estar só: a tutela penal do direito à intimidade*, 3ª ed., São Paulo, Siciliano, 2004.

CRETELLA JÚNIOR, José, *Comentários à Constituição de 1988*, v. I, Rio de Janeiro, Forense, 1997.

DAVARA RODRIGUEZ, Miguel Ángel, *Manual de Derecho Informático*, Navarra, Thomson Aranzadi, 2008.

DELMAS-MARTY, Mireille, *Il diritto penale come etica della mondializzazione*, Rivista italiana di Diritto e Procedura Penale, XLIX, n. 1, Milano, Giuffrè, 2006.

DELPIAZZO, Carlos E., VIEGA, María José, *Lecciones de derecho Telemático*, Montevideo, Fundación de Cultura Universitaria, 2004.

DEZEM, Guilherme Madeira, *Da prova penal: tipo processual, provas típicas e atípicas*, Campinas, Millennium, 2008.

_____, BECHARA, Fabio Ramazzini, *Captação ambiental de imagens: usos e limites*, in A. Scarance Fernandes (org.), *Estudos de Processo Penal*, São Paulo, Scortecci, 2011.

DIMOULIS, Dimitri, MARTINS, Leonardo, *Teoria Geral dos Direitos Fundamentais*, São Paulo, RT, 2006.

ESPÍNOLA, Eduardo, *Constituição dos Estados Unidos do Brasil*, v. II, Rio de Janeiro, Freitas Bastos, 1952.

FANUELE, Chiara, *Dati genetici e procedimento penale*, Milano, Cedam, 2009.

FEDELI, Ricardo Daniel, POLLONI, Enrico Giulio Franco, PERES, Fernando Eduardo, *Introdução à ciência da computação*, São Paulo, Thomson, 2003.

FERNANDES, Antonio Scarance, *Funções e limites da prisão processual*, *Revista Brasileira de Ciências Criminais*, n. 64, São Paulo, Revista dos Tribunais, 2007.

_____, *O polêmico inciso XII do artigo 5º da Constituição Federal*, Justitia, 64 (197), jul./dez., 2007.

_____*, Processo Penal Constitucional*, 6ª ed., São Paulo, RT, 2010.

_____, *Reação defensiva à imputação*, São Paulo, Saraiva, RT, 2002.

_____, *Reflexões sobre as noções de eficiência e de garantismo no processo penal*, in, Antonio Scarance Fernandes, José Raul Gavião de Almeida, Maurício Zanoide de Moraes (coords.), *Sigilo no Processo Penal*, São Paulo, RT, 2008.

_____, *O sigilo financeiro e a prova criminal,* in Joel de Faria Costa, Marco Antonio Marques da Silva (coords.), *Direito penal especial, processo penal e direitos fundamentais*, São Paulo, Quartier Latin, 2006.

FERRAJOLI, Luigi, *Direito e Razão: Teoria do Garantismo Penal*, trad. Ana Paula Zomer Sica (et alii), 2ª ed., São Paulo, RT, 2006.

FERRAZ JUNIOR, Tércio Sampaio, *A ciência do direito*, São Paulo, Atlas, 2006.

_____, *Introdução ao Estudo do Direito*, 4ª ed*., São Paulo, Atlas, 2003.*

_____, *A invenção do futuro: um debate sobre a pós-modernidade e a hipermodernidade,* in Tércio Sampaio Ferraz Junior (org.), *A invenção do futuro*, São Paulo, Manole, 2005.

_____, *A Liberdade como autonomia recíproca de acesso à informação*, in Marco Aurelio Greco, Ives Gandra da Silva Martins (coords.), *Direito e internet: relações jurídicas na sociedade informatizada*, São Paulo, RT, 2001.

_____, *Liberdade de Informação e Privacidade ou o Paradoxo da Liberdade*, in A. de Almeida Filho (org.), *Estado de Direito e Direitos Fundamentais*, Rio de Janeiro, Forense, 2005.

_____, *Sigilo fiscal e bancário*, in Reinaldo Pizolio, Jayr Viégas Gavalcão Jr. (coords.), *Sigilo fiscal e bancário*, São Paulo, Quartier Latin, 2005.

FERREIRA, Pinto, *Comentários à Constituição brasileira*, v. I, São Paulo, Saraiva, 1989.

FLUSSER, Vilém, *O mundo codificado: por uma filosofia do design e da comunicação*, trad. Raquel Abi-Sâmara, São Paulo, Cosacnaify, 2007.

FROSINI, Vittorio*, Il Diritto nella Società Tecnologica*, Milano, Giuffrè, 1981.

FROUVILLE, Oliver de, *La preuve pénale: internationalisation et nouvelles technologies,* Paris, La documentation Française*,* 2007.

GARCIA MARQUES, LOURENÇO MARTINS, *Direito da informática*, Lisboa, Almedina, 2000.

GARRIGA DOMÍNGUEZ, Ana, *Tratamiento de datos personales y derechos fundamentales*, Madrid, Dykinson, 2004.

GOMES FILHO, Antonio Magalhães, *A motivação das decisões penais*, São Paulo, RT, 2001.

_____, *O "Modelo Garantista" de Luigi Ferrajoli*, Boletim do Instituto Brasileiro de Ciências Criminais, n. 58, 1997.

_____, *Notas sobre a terminologia da prova: reflexos no processo penal brasileiro*, in Flávio Luiz Yarshell, Maurício Zanoide de Moraes (orgs.), *Estudos em homenagem à Professora Ada Pellegrini Grinover*, São Paulo, DPJ, 2005.

GONZÁLEZ-CUÉLLAR SERRANO, Nicolás, *Garantías constitucionales de la persecución penal en el entorno digital*, in J. L. Gómez Colomer (coord.), *Prueba y Proceso Penal*, Valencia, Tirant lo Blanch, 2008.

GONZÁLEZ LÓPEZ, Juan José, *Los Datos de Tráfico de las Comunicaciones Electrónicas en el Proceso Penal*, Madrid, La ley, 2007.

_____, *Infiltración policial en Internet: Algunas consideraciones*, in Revista del Poder Judicial, n. 85, Consejo General del Poder Judicial, 2007.

_____, *Utilización en el proceso penal de datos vinculados a las comunicaciones electrónicas recopilados sin indicios de comisión delictiva,* in Ernesto Pedraz Penalva (coord.), *Protección de datos y proceso penal*, Madrid, La ley, 2010.

GUERRA FILHO, Willis Santiago, *Princípio da proporcionalidade e devido processo legal*, in V. Afonso da Silva (org.), *Interpretação constitucional*, São Paulo, Malheiros, 2007.

_____, *Ensaios de Teoria Constitucional*, Fortaleza-Ceará, Imprensa Universitária da Universidade Federal do Ceará, 1989.

GRINOVER, Ada Pellegrini, FERNANDES, Antonio Scarance, GOMES FILHO, Antonio Magalhães, *As Nulidades no Processo Penal*, 10ª ed., São Paulo, RT, 2007.

GRINOVER, Ada Pellegrini, *Liberdades Públicas e Processo Penal: as interceptações telefônicas*, 2ª ed., São Paulo, RT, 1982.

_____, *Novas Tendências do direito processual*, Rio de Janeiro, Forense Universitária, 1990.

GUZMÁN, Nicolás, *La Verdad en el Proceso Penal*, Buenos Aires, Editores del Puerto, 2006.

HASSEMER, Winfried, *Oportunidades para la privacidad frente a las nuevas necesidades de control y las tecnologías de la información*, trad. Alfredo Chirino Sánchez, in Nueva Doctrina Penal, Buenos Aires, Editores del Puerto, 1999.

HEGEL, Georg Wilhelm Friedrich, *Lineamenti di filosofia del diritto*, trad. Francesco Messineo, Roma, Laterza, 1979.

HERNÁN ORTIZ, Ana Isabel, *La violación de la intimidad en la protección de datos personales*, Madrid, Dykinson, 1998.

HERRERA BRAVO, Rodolfo, NUÑEZ ROMERO, Alejandra, *Derecho Informático*, San Martín, La Ley, 1999.

KELSEN, Hans, *Teoria pura do direito*, trad. João Baptista Machado, São Paulo, Martins Fontes, 2000.

KIM, Joon Ho, *Cibernética, ciborgues e ciberespaço: notas sobre as origens da cibernética e sua reinvenção cultural*, in Horizontes Antropológicos, v. 10, n. 21, Porto Alegre, jan./jun., 2004.

KORSHUNOV, Yu, M., *Fundamentos Matemáticos de la Cibernética*, trad. Roberto Lanier Alvarez, Moscú, Editorial Moscú, s/d.

LAFER, Celso, *Brasil: dilemas e desafios na política externa*, São Paulo, Estudos Avançados, v. 14, n. 38., jan./abr., 2000.

_____, *A Constituição de 1988 e as Relações Internacionais: reflexões sobre o art. 4º,* in Celso Lafer (org.), *A internacionalização dos direitos humanos: Constituição, racismo e relações internacionais*, Barueri, Manole, 2005.

_____ , *Filosofia do direito e princípios gerais: considerações sobre a pergunta "o que é a filosofia do direito"*, in A. Caffé Alves (et alii), *O que é a Filosofia do Direito?*, Barueri, Manole, 2004.

LANCHARRO, Eduardo Alcalde, LOPEZ, Miguel Garcia, FERNANDEZ, Salvador Peñeuelas, *Informática Básica*, trad. Ségio Molina, São Paulo, McGraw-Hill, 1991.

LARONGA, Antonio, *Le prove atipiche nel Processo Penale*, Milano, CEDAM, 2002.

LOSANO, Mario, *Giuscibernetica: machinne e modelli cibernetici nel diritto*, Torino, Einaudi, 1969.

_____, *Lições de Informática Jurídica*, São Paulo, Resenha Tributária, 1974.

_____, *Modelos teóricos, inclusive na prática: da pirâmide à rede*, in Revista do IASP, ano 8, n. 16, jul./dez., 2005.

LUCCA, Newton de, *Títulos e contratos eletrônicos: o advento da informática e seu impacto no mundo jurídico*, in Newton de Luca, A. Simão Filho (orgs.), *Direito & Internet*: *aspectos jurídicos relevantes*, São Paulo, Quartier Latin, 2005.

LUPÁRIA, Luca, ZICCARDI, Giovanni, *Investigazione Penale e Tenologia Informatica*, Milano, Giuffrè, 2007.

MACHADO, André Augusto Mendes, SOUZA, Diego Farjado Maranha Leão, O *Crime Organizado na Colômbia,* in A. Scarance Fernandes, J. R. Gavião de Almeida, M. Zanoide de Moraes (orgs.), *Crime organizado: aspectos processuais*, São Paulo, RT, 2009.

MACHADO, André Augusto Mendes, KEDHI, Andre Pires de Andrade, *Sigilo das comunicações e de dados*, in Antonio Scarance Fernandes, José Raul Gavião de Almeida,

Maurício Zanoide de Moraes (coords.), *Sigilo no Processo Penal: Eficiência e Garantismo*, São Paulo, RT, 2008.

MADRID CONESA, Fulgencio, *Derecho a la Intimidad, Informática y Estado de Derecho*, Valencia, Soler, 1984.

MARÇULA, Marcelo, BENINI FILHO, Pio Armando, *Informática: Conceitos e aplicações*, 2ª ed., São Paulo, Érica, 2007.

MARTÍNEZ DE PISÓN CAVERO, José, *El derecho a la intimidad en la jurisprudencia constitucional*, Madrid, Civitas, 1992.

MAXIMILIANO, Carlos, *Commentarios: Constituição Brasileira*, Rio de Janeiro, Jacinto Ribeiro dos Santos editor, 1918.

_____, *Comentários à Constituição Brasileira*, v. III, Rio de janeiro, Freitas Bastos, 1948.

MELLO, Celso Antonio Bandeira de, *Curso de Direito Administrativo*, São Paulo Malheiros, 2000.

MENDES, Gilmar Ferreira, COELHO, Inocêncio Mártires, BRANCO, Paulo Gustavo Gonet, *Curso de Direito Constitucional*, 4ª ed., São Paulo, Saraiva, 2009.

MESQUITA, Rodrigo Octávio de Godoy Bueno Caldas, *A proteção da privacidade nas comunicações eletrônicas no Brasil,* São Paulo, Dissertação de Mestrado, 2009.

MILTON, Aristide A., *A Constituição do Brazil: notícia, história e texto comentado*, 2ª ed., Rio de Janeiro, Imprensa Nacional, 1898.

MIRABETE, Julio Fabbrini, *Processo Penal*, 18º ed., São Paulo, Atlas, 2007.

MIRANDA, Francisco Cavalcante Pontes de, *Comentários à Constituição de 1946*, tomo IV, Rio de Janeiro, Borsoi, 1960.

_____, *Comentários à Constituição de 1967*, tomo V, São Paulo, RT, 1968.

MOLES PLAZA, Ramón J*, Derecho y control in Internet*, Barcelona, Ariel, 2004.

MORAES, Alexandre, *Constituição do Brasil interpretada*, 6ª ed., São Paulo, Atlas, 2006.

MORAES, Maurício Zanoide de, *Presunção de inocência no processo penal brasileiro: análise de sua estrutura normativa para a elaboração legislativa e para a decisão judicial*, São Paulo, Tese de Livre Docência, 2008.

MORALES PRATS, Fermín, *La tutela penal de la intimidad: privacy e informática*, Barcelona, Ediciones Destino, 1984.

MORALES ROMERO, Marta Muñoz de, *La intervención judicial de las comunicaciones telefónicas y electrónicas*, in A. S. Hermida (org.), *Investigación y prueba en el proceso penal*, Madrid, Colex, 2006.

MORÓN LERMA, Esther, *Internet y Derecho Penal: Hacking y otras Conductas Ilícitas en la Red*, Navarra, Arazandi, 2002.

MOURA, Maria Thereza Rocha de Assis, *A prova por indícios no processo penal*, São Paulo, *Lumen Juris*, 2009.

NERY JUNIOR, Nelson, NERY, Rosa Maria de Andrade, *Constituição Federal comentada*, 2ª ed., São Paulo, RT, 2009.

NUCCI, Guilherme de Souza, *Código de Processo Penal comentado*, 9ª ed., São Paulo, RT, 2009.

OLINET, Maud, MARTIN-CHENUT, Kathia, *La preuve Cybernétique*, Paris, Société de Législation Comparé, 2006.

ORWELL, George, *1984*, trad. Alexandre Hubner, Heloisa Jahn, São Paulo, Companhia das Letras, 2009.

OST, François, KERCHOVE, Michel Van de, *Interprétation*, in Archives de Philosofie du Droit, tomo 35, 1990.

PALAZZI, Pablo Andrés, *Delitos Informáticos*, Buenos Aires, Adhoc, 2000.

PEDRAZ PENALVA, Ernesto, *La utilización en el proceso penal de datos personales recopilados sin indicios de comisión delictiva*, in E. Pedraz Penalva (org.), *Protección de datos y proceso penal*, Madrid, La ley, 2010.

PEREIRA, Caio Mário da Silva, *Instituições de Direito Civil*, v. I, 21ª ed., Rio de Janeiro, Forense, 2005.

PÉREZ GIL, Julio, *Los datos sobre localización geográfica en la investigación penal*, in Ernesto Pedraz Penalva (coord.), *Protección de datos y proceso penal*, Madrid, La ley, 2010.

_____, *Investigación Penal y Nuevas Tecnologías: Algunos de los Retos Pendientes*, in Revista Jurídica de Castilla y León, n. 7, out. 2005.

_____, *Medidas de investigación y de aseguramiento de la prueba en el Convenio sobre el Cibercrimen*, in Actualidad penal: Revista semanal técnico-jurídica de derecho penal, n. 36, Madrid, La ley, 2003.

PÉREZ-LUÑO, Antonio-Enrique, *La tercera generación de derechos humanos*, Navarra, Thomson, 2006.

PITOMBO, Cleunice Bastos, *Da busca e da apreensão no Processo Penal*, 2ª ed., São Paulo, RT, 2005.

PITOMBO, Sérgio, *Do sequestro no processo penal brasileiro*, São Paulo, Bushatsky, 1973.

QUÉMÉNER, Myriam, CHARPENEL, Yves, *Cybercriminalité: Droit pénal appliqué*, Paris, Economica, 2010.

REALE, Miguel, *Filosofia do Direito*, 6ª ed., v.1, São Paulo, Saraiva, 1972.

_____. *Invariantes axiológicos*, in Estudos avançados, v. 15, n. 13, São Paulo, USP, 1991.

REBOLLO DELGADO, Lucrecio, *Derechos Fundamentales y Protección de Datos*, Madrid, Dykinson, 2004.

RODRIGUES, Benjamim Silva, *A monitorização dos fluxos informacionais e comunicacionais*, v. II, Coimbra, Dissertação de Mestrado, 2009.

RODRÍGUEZ LAINZ, José Luis, *Intervención judicial en los datos de tráfico de las comunicaciones*, Barcelona, Bosch, 2003.

ROMEO CASABONA, Carlos M, *La intimidad y los datos de carácter personal como derechos fundamentales y como bienes jurídicos penalmente protegidos*, in Revista de direito da Universidade Estácio de Sá, n. 6, v. 7, Rio de Janeiro, Universidade Estácio de Sá, 2004.

_____, *Tendencias actuales sobre las formas de protección jurídica ante las nuevas tecnologías*, in Revista del Poder Judicial, n. 31, set-1993.

SAAD, Marta, *O direito de defesa no inquérito policial*, São Paulo, RT, 2004.

SARMENTO E CASTRO, Catarina, *Privacidade e proteção de dados em rede*, Lisboa, Associação Portuguesa de Direito Intelectual, 2006.

SCALISI, Antonio, *Il diritto alla riservatezza*, Milano, Giuffrè, 2002.

SCARPELLI, Uberto, *Ética jurídica sin verdad*, Ciudad de México, Fontamara, 2007.

SILVA, José Afonso da, *Comentário contextual à Constituição*, 4ª ed., São Paulo, Malheiros, 2007.

_____. *Curso de Direito Constitucional Positivo*, 25ª ed., São Paulo, Malheiros, 2005.

SILVA, Virgílio Afonso da, *Direitos Fundamentais*, 2ª ed., São Paulo, Malheiros, 2010.

_____. *Interpretação constitucional e sincretismo metodológico*, in V. Afonso da Silva (org.), *Interpretação constitucional*, 1ª ed., São Paulo, Malheiros, 2007.

STAINES, Sarah, *Data Protection Act Guidelines – a Practical Summary*, in United Kingdom Law Articles in English, Pictons Solicitors LLP, May 2004, *http://vlex.com/vid/29346721* (acesso em 30 set. 2010, h. 18:20).

STERN, Enrique, *El sentido de la privacidad, la intimidad y la seguridad en el mundo digital: ámbitos y limites*, in Cuaderno del Instituto vasco de criminología, n. 21, San Sebastián, 2007.

STRECK, Lênio Luiz, *As interceptações telefônicas e os direitos fundamentais*, 2ª ed., Porto Alegre, Livraria dos Advogados, 2001.

TARANTINO, Antonio, *Elementi di Informatica Giuridica*, Milano, Giuffrè, 1998.

TARUFFO, Michele, *La prueba de los hechos*, trad. Jordi Ferrer Beltrán, Madrid, Trotta 2002.

TÉLLEZ AGUILERA, Abel, *Nuevas Tecnologías – Intimidad y Protección de Datos,* Madrid, Edisofer, 2001.

TORNAGHI, Hélio, *Instituições de Processo Penal*, v. 3, 2ª ed., São Paulo, Saraiva, 1978.

TOURINHO FILHO, Fernando da Costa, *Manual de Processo Penal*, 9ª ed., São Paulo, Saraiva, 2007.

TUCCI, Rogério Lauria, *Direitos e Garantias Individuais no Processo Penal Brasileiro*, 3ª ed., São Paulo, RT, 2009.

UBERTIS, Giulio, *Argomenti di Procedura Penale*, Milano, Giuffrè, 2002.

_____, *Argomenti di Procedura Penale*, v. III, Milano, Giuffrè, 2011.

UICICH, RODOLFO D, *El derecho a la intimidad en internet y en las comunicaciones electrónicas*, Buenos Aires, Adhoc, 2009.

URBANO DE CASTRILHO, Eduardo de, *La valoración de la prueba electrónica*, Valencia, Tirant lo blanch, 2009.

ZICCARDI, Giovanni, *L'ingresso della computer forensics nel sistema processuale italiano: alcune considerazioni informatico-giuridiche*, in Luca Lupária (org.), *Sistema penale e criminalità informatica*, Milano, Giuffrè, 2008.

ZILLI, Marcos Alexandre Coelho, *A Iniciativa Instrutória do Juiz no Processo Penal*, São Paulo, RT, 2003.

WALDEN, Ian, *Computer crimes and digital investigation*, New York, Oxford University Press, 2007.

ABREVIATURAS

ANATEL – Agência Nacional de Telecomunicações

AOL IM – *America On Line Instant Messenger*

ARPANET – *Advanced Research Projects Agency*

BGH – *Bundesgerichtshof*

CBT – Código Brasileiro de Telecomunicações

CDR – *Call Data Record*

CE – Conselho da Europa

CEDH – Corte Europeia de Direitos Humanos

CF – Constituição Federal

CGI.br – Comitê Gestor da *Internet* do Brasil

CNJ – Conselho Nacional de Justiça

CP – Código Penal

CPC – Código de Processo Civil

CPI – Comissão Parlamentar de Inquérito

CPP – Código de Processo Penal

DPN – Domínio de Primeiro Nível

ECA – Estatuto da Criança de do Adolescente

FTP – *File Transfer Protocol*

GPS - *Global Positioning System*

GSM – *Global System for Mobile Communications*

HD – *Hard disk*

HTTP – *HyperText Transfer*

ICQ – *I seek you*

INTERPOL – *International Criminal Police Organization*

IRC – *Internet Relay Chat*

LAN – *Local Area Network*

LBS – *Location based services*

MAN – *Metropolitan Area Network*

MSN – *Messenger*

NIC. Br – Núcleo de Informação e Coordenação do Ponto BR

OAB – Ordem dos Advogados do Brasil

OEA – Organização dos Estados Americanos

ONU – Organização das Nações Unidas

SMS – *Short Message Service*

TCP/IP – *Transmission Control Protocol* / *Internet Protocol*

UIT – União Internacional de Telecomunicações

VLR – *Visitor Location Register*

VoIP – Voice over IP

Yahoo IM – *Yahoo Messenger*

WWW – *World Wide Web*

Resumo

Em tempos correntes, importantes processos de comunicação (escrita ou verbal) e armazenamento de informações aperfeiçoam-se por intermédio dos meios eletrônicos. À medida que o acesso à rede mundial de computadores (*internet*) se intensifica em progressões geométricas, multiplicam-se também os dados intercambiados por internautas e emergem técnicas cada vez mais avançadas de coleta e processamento de informações. Atividades rotineiras como a navegação e o envio de mensagens eletrônicas realizam-se apenas à custa de imenso trânsito de informações; como pegadas deixadas pelo caminho, os dados comutados nestas atuações permitem reconstituir os caminhos e atividades empreendidos na rede. A salvaguarda destas informações afigura-se imprescindível à vida privada e demanda rígida disciplina normativa. Não se trata apenas de impedir que dados de tráfego ou de conteúdo sejam empregados contrariamente ao Direito, mas de assegurar também que, em situações excepcionais descritas pelo legislador, sirvam para corroborar investigações criminais.

Pretende-se neste trabalho um exame sistemático dos principais meios de busca da prova digital, com o escopo de delimitar o regime jurídico das intervenções nas comunicações eletrônicas e das medidas de apreensão de dados automatizados. Neste mister, inafastável analisar a disciplina constitucional do sigilo da comunicação de dados (CF, art. 5º, inciso XII) e investigar o fundamento legal das autorizações judiciais para a obtenção de informações eletrônicas.

Sob perspectiva eminentemente interdisciplinar, cumpre discorrer sobre noções de *Cibernética*, *telecomunicações*, *Informática*, *liberdade como autonomia recíproca de acesso à informação* e *comunicações eletrônicas*, imprescindíveis à compreensão deste novo espaço do agir humano: o entorno digital. No campo da hermenêutica constitucional, necessário perquirir relevantes aspectos da vida privada e da proteção da intimidade – antecedentes históricos, direito à *privacy*, hodierna projeção como autodeterminação informativa, teoria das três esferas e inviolabilidade das comunicações – que permitirão opinar sobre a constitucionalidade das interceptações de dados em processos informacionais. Em sequência, devem ser conceituados os *dados digitais* e suas respectivas categorias, as técnicas de investigação penal e o resguardo de fontes de provas digitais. Sem deixar de contribuir para o aperfeiçoamento da normativa legal vigente, de rigor o exame de duas ordens distintas de incorporação dos dados ao processo: a intervenção no fluxo comunicativo destinada a captar dados e a apreensão física do dispositivo informático que alberga as informações. Como meios de busca de prova, esses procedimentos devem ser estudados de maneira individualizada, a partir de aspectos como *conceito*, *regulação*, *natureza jurídica*, *finalidade*, *condicionantes legais* (*pressupostos, requisitos* e *limites*), *direito de defesa*, *juízo de proporcionalidade* e *controle*. Por fim, tecidas as necessárias considerações sobre a conservação, eficácia probatória e valoração dos conteúdos automatizados, impõe-se indagar acerca dos efeitos decorrentes de operações ilícitas perpetradas sobre dados digitais.

Resume

In these days, important communication process (written or verbal) and information storage improve through electronic means. While the access to the computer worldwide web (internet) grows in geometrical progression, it also increases the number of webusers data and more and more advanced technics of gathering and processing information emerge. Routine activities such as sailing or sending electronic messages only happen due to the vast transit of information; like footprints left on the way, the data commutated in these actions allow to re-establish the ways and activities undertaken in the web. The security of these information figures indispensable to private life and demands a severe normative discipline. It is not only a matter of preventing that traffic or contents data may be used against the law. But also to assure that, in exceptional situation described by the legislator, it can be useful to confirm criminal investigation.

This work intends a systematic examination of the main ways of searching digital evidence, with the purpose of delimitate the judiciary system of the intervention in electronic and apprehension extent of automation data. So, it must be analysed the constitutional discipline of communication data secrecy (CF, art. 5º, inciso XII) and even to investigate the legal foundation of judicial authorization to obtain electronic information.

Under a strictly multidiscipline perspective, one must consider some notions of Cybernetics, telecommunication, Informatics, freedom as reciprocal autonomy access to electronic information and communication, which are essential to understand this new area of human act; the digital place. In the field of constitutional interpretation of law, it is necessary to scrutinize considerable aspects of private life and intimacy protection – historical antecedents, privacy right, actual projection such as informative self-determination, three sphere theory and inviolability of communication – so that they will permit to express an opinion about the constitutionality of interception data in informative proceedings. Sequentially, conceptualize the digital data and their respective categories, penal investigation technics and the protection of digital evidence sources. There may be a cooperation to a better improvement of the effective legal normative, an accurate examination of two different disposition of data incorporation to the process, the intervention in the communicative flow just to receive data and physical apprehension of the informatic device which contains information. As a quest in resources of proof, these proceedings must be examined in a individual way, starting with the aspects such as concept, regulation, juridical nature, finality, legal conditioning (presupposed, requisite and limits), right of defence, judgement of proportionality and control. At last, taken into everything about the conservation, evidential efficiency and the value of automatize contents still we have to enquire about the results of illicit operations perpetrated on digital data.

Resumen

En tiempos corrientes, importantes procesos de comunicación (escrita o verbal) y de almacenamiento de informaciones se perfeccionan por intermedio de los medios de comunicación. A medida que el acceso a la red mundial de computadores (*internet*) se intensifica en progresiones geométricas, se multiplican también los datos intercambiados por internautas y emergen técnicas cada vez más avanzadas de colecta y procesamiento de informaciones. Actividades rutineras como la navegación y el envío de mensajes electrónicos se realizan apenas a costa del inmenso tránsito de informaciones; como huellas dejadas por el camino, los datos conmutados en estas actuaciones permiten reconstituir los caminos y actividades emprendidos en la red. La salvaguarda de estas informaciones se hace imprescindible a la vida privada y demanda una rígida disciplina normativa. No se trata apenas de impedir que datos de tráfico o de contenido sean empleados contrariamente al Derecho, sino de asegurar también que, en situaciones excepcionales descritas por el legislador, sirvan para corroborar las investigaciones criminales.

Se pretende en este trabajo un examen sistemático de los principales medios de búsqueda de la prueba digital, con el objetivo de delimitar el régimen jurídico de las intervenciones en las comunicaciones electrónicas y de las medidas de aprehensión de datos automatizados. En este menester, inseparable analizar la disciplina constitucional del sigilo de la comunicación de datos (CF, art. 5º, inciso XII) e investigar el fundamento legal de las autoridades judiciales para la obtención de informaciones electrónicas.

Bajo la perspectiva eminentemente interdisciplinar, cumple discurrir sobre nociones de *Cibernética, telecomunicaciones, Informática, libertad como autonomía recíproca de acceso a la información* y *comunicaciones electrónicas*, imprescindibles a la comprensión de este nuevo espacio del actuar humano: el entorno digital. En el campo de la hermenéutica constitucional, es necesario perquirir relevantes aspectos de la vida privada y de protección de la intimidad – antecedentes históricos, derecho a la *privacy*, hodierna proyección como autodeterminación informativa, la teoría de las tres esferas e inviolabilidad de las comunicaciones – que permitirán opinar sobre la constitucionalidad de las interceptaciones de datos en procesos informacionales. En secuencia, se deben conceptuar los *datos digitales* y sus respectivas categorías, las técnicas de investigación penal y el resguardo de fuentes de pruebas digitales. Sin dejar de contribuir para el perfeccionamiento de la normativa legal vigente, de rigor el examen de dos órdenes distintas de incorporación de los datos al proceso: la intervención en el flujo comunicativo destinada a captar datos y la aprehensión física del dispositivo informático que alberga las informaciones. Como medios de búsqueda de prueba, esos procedimientos deber ser estudiados de manera individualizada, a partir de aspectos como *concepto, regulación, naturaleza jurídica, finalidad, condicionantes legales (presupuestos, requisitos* y *límites), derecho de defensa, juicio de proporcionalidad* y *control.* Por fin, tejidas las necesarias consideraciones sobre la conservación, eficacia probatoria y valoración de los contenidos automatizados, se impone indagar acerca de los efectos decurrentes de operaciones ilícitas perpetradas sobre datos digitales.

Riassunto

Nei nostri tempi, processi importanti di comunicazione (scritta o verbale) e conservazione di informazioni si perfezionano attraverso mezzi elettronici. Siccome l'accesso alla rete mondiale di computer (*internet*) si intensifica in progressione geometrica, si moltiplicano anche i dati che vengono scambiati via *internet* ed emergono tecniche sempre più avanzate di raccolta e trattamento delle informazioni. Attività di routine come la navigazione e l'invio di messaggi elettronici si tengono solo a scapito di immenso traffico di informazioni; come impronte lasciate alle spalle, i dati commutati in queste azioni permettono di riscostruire i percorsi e le attività svolte in rete. Salvaguardare queste informazioni è essenziale per la privacy e richiede rigorosa disciplina normativa. Non si tratta soltanto di impedire che dati di traffico o di contenuto siano impiegati in modo contrario al Diritto, ma anche di garantire che, in situazioni eccezionali descritte dal legislatore, servano a corroborare delle indagini penali.

Questo lavoro ha come obiettivo realizzare un esame sistematico dei principali mezzi di ricerca di prova digitale, allo scopo di definire il quadro giuridico degli interventi nelle comunicazioni elettroniche e delle misure di sequestro di dati automatizzati. In questo proposito, occorre analizzare la disciplina costituzionale del sigillo della comunicazione di dati (CF, art. 5, comma XII) e indagare la base giuridica delle autorizzazioni giudiziarie per ottenere informazioni elettroniche.

Sotto prospettiva eminentemente interdisciplinare, occorre discutere le nozioni di *Cibernetica, telecomunicazioni, Informatica, libertà come autonomia reciproca di accesso alla informazione* e *alle comunicazioni elettroniche*, essenziale per comprendere questa nuova area dell'attività umana: l'ambiente digitale. Nel campo dell'ermeneutica costituzionale, occorre investigare rilevanti aspetti della vita privata e la tutela dell'intimità – fondi storici, diritto alla *privacy*, odierna proiezione come autodeterminazione informativa, teoria delle tre sfere e l'inviolabilità delle comunicazioni – che permetteranno di opinare sulla costituzionalità delle intercettazioni di dati in processi di informazione. In sequenza, vanno concettualizzati i *dati digitali* e le loro rispettive categorie, le tecniche di indagine penale e la salvaguardia delle fonti di prova digitale. Contribuendo anche al perfezionamento della normativa legale in vigore, è di rigore l'esame di due ordini distinti di incorporazione di dati al processo: l'intervento sul flusso comunicativo per la raccolta di dati ed il sequestro fisico del dispositivo informatico che ospita le informazioni. Come mezzi di ricerca di prova, queste procedure vanno studiate in modo individualizzato, a partire di aspetti come *concetto, regolamento, natura giuridica, finalità, vincoli giuridici (presupposti, requisiti* e *limiti), diritto di difesa, giudizio di proporzionalità* e *controllo*. Infine, fatte le necessarie considerazioni sulla conservazione, l'efficacia probatoria e valutazione dei contenuti automatizzati, richiede soltanto domandarsi sugli effetti derivanti da operazioni illecite perpetrate sui dati digitali.