UNIVERSIDADE DE BRASÍLIA
FACULDADE DE DIREITO
MESTRADO EM DIREITO, ESTADO E SOCIEDADE

TATIANA MALTA VIEIRA

O DIREITO À PRIVACIDADE NA SOCIEDADE DA INFORMAÇÃO:
efetividade desse direito fundamental diante dos avanços da tecnologia da informação

BRASÍLIA
2007

TATIANA MALTA VIEIRA

O DIREITO À PRIVACIDADE NA SOCIEDADE DA INFORMAÇÃO:
efetividade desse direito fundamental diante dos avanços da tecnologia da informação

Dissertação apresentada como requisito parcial à obtenção do grau de **mestre** no curso de pós-graduação *stricto sensu* em Direito, Estado e Sociedade: Políticas Públicas e Democracia.

Orientador: Prof. Dr. Gilmar Ferreira Mendes

BRASÍLIA
2007

TATIANA MALTA VIEIRA

O DIREITO À PRIVACIDADE NA SOCIEDADE DA INFORMAÇÃO:
efetividade desse direito fundamental diante dos avanços da tecnologia da informação

Dissertação apresentada como requisito parcial à obtenção do grau de **mestre** no curso de pós-graduação *stricto sensu* em Direito, Estado e Sociedade: Políticas Públicas e Democracia.

Aprovada pelos membros da banca examinadora em 14/03/07, em Brasília-DF,

com recomendação para publicação.

Banca Examinadora:

_____
Prof. Dr. Gilmar Ferreira Mendes – UnB

_____
Prof. Dr. Paulo Luiz Netto Lobo – UnB

_____
Prof. Dr. José Aires Rover – UFSC

Dedico este estudo a Osiris Vargas Pellanda,
meu marido, namorado, companheiro e amigo,
cuja compreensão e apoio durante o processo criador
se fizeram fundamentais para a concretização deste trabalho.
A você, que, tantas vezes, quando tomada
pelo desgaste mental, físico e emocional,
diante da necessidade de conciliar
as atividades profissionais, acadêmicas e familiares
soube cultivar paciência e amor em minha vida,
acolhendo-me em sua intimidade.

AGRADECIMENTOS

Foram muitos os que me ajudaram a concluir este trabalho.

Meus sinceros agradecimentos...

...a Deus, pela dádiva da vida;

...aos meus pais, Geraldo Ribeiro Vieira e Vera de Figueiredo Malta,
pelos valores transmitidos e pelas oportunidades proporcionadas;

...ao Prof. Dr. Gilmar Ferreira Mendes,
por aceitar a orientação deste estudo e conduzir seu desenvolvimento com dedicação;

...à Izabel Mituco Akiyoshi Loureiro,
pelas preciosas sugestões de revisão deste trabalho;

...aos colegas do Gabinete de Segurança Institucional da Presidência da República,
pela compreensão e pela flexibilidade;

...à Beatriz Kicis De Sordi, pelos ensinamentos de paz e de tranqüilidade;

...aos amigos mais íntimos, pelo carinho e pelo constante estímulo.

"*Cada indivíduo é visto, mas não vê;*
objeto de uma informação, nunca sujeito de uma comunicação.
(...) O panoptismo faz funcionar ao arrepio do direito,
uma tecnologia que vai além dos limites traçados."
(Michel Foucault)

RESUMO

Esta pesquisa apresenta uma análise do direito à privacidade na sociedade da informação, segundo perspectiva do direito constitucional e do direito da informática. Objetiva-se (i) mostrar como o ordenamento jurídico nacional, estrangeiro e internacional tratam o direito à privacidade; (ii) analisar as múltiplas dimensões desse direito fundamental, enfatizando o seu aspecto positivo, como forma de contribuir para maior efetividade dessa garantia; e (iii) alertar para os riscos da tecnologia à privacidade no cenário da sociedade da informação. O direito à privacidade protege a intimidade, a vida privada, o domicílio, a correspondência, as comunicações e os dados pessoais de uma pessoa e possui caráter eminentemente elástico e variável, conforme o tempo, o espaço e o titular da garantia. A privacidade de políticos, artistas e atletas sujeita-se a parâmetros de aferição menos rígidos do que a privacidade de pessoas anônimas. Em sua dimensão negativa, o direito à privacidade protege a intimidade e a vida privada do indivíduo contra intromissões do poder público e dos demais concidadãos, ao passo que, em sua dimensão positiva, impõe ao Estado o dever de implementar as medidas administrativas e legislativas necessárias para garantir a privacidade dos cidadãos, protegendo-os das intromissões provenientes de particulares ou de outros Estados. O direito à privacidade tem caráter relativo, sujeitando-se a restrições expressas, nas modalidades direta e indiretamente constitucionais, e a restrições implícitas, quando colide com outros valores constitucionais. No cenário da sociedade da informação, intensifica-se o interesse tanto dos governos quanto da iniciativa privada em imiscuir-se na privacidade alheia. A vigilância sobre os indivíduos sofre devastador avanço com o advento da tecnologia da informação, consumando-se mediante dispositivos que permitem o permanente monitoramento e controle do comportamento das pessoas. Destacam-se os riscos da internet à privacidade, especialmente no que concerne ao tratamento automatizado de dados pessoais, enfatizando-se a necessidade de regulamentação do direito à autodeterminação informativa no que concerne (i) aos princípios aplicáveis ao tratamento de tais dados, (ii) aos direitos garantidos aos titulares das informações, (iii) aos deveres dos responsáveis pelo tratamento, (iv) às sanções aplicáveis pelo descumprimento destes preceitos, dentre outros procedimentos necessários à proteção da intimidade e da vida privada das pessoas diante dos novos recursos tecnológicos.

Palavras-chaves: direitos fundamentais, privacidade, tecnologia da informação.

ABSTRACT

This research presents an analisys on the right to privacy in information society, from a juridical approach towards the constitutional law and cyberlaw. It aims (i) to demonstrate how the national, foreign and international legal systems deal with the right to privacy; (ii) to analyze the multiple dimensions of this fundamental right by emphasizing its positive aspect, in order to contribute for its effectiveness; and (iii) to warn about the risks to privacy brought about by technology in information society scenario. The right to privacy comprises intimacy, private life, dwelling, mail, communications and one's personal data within its protection range, mostly exhibiting an elastic and variable character according to time, place and the right holder. The privacy of politicians, artists and athletes is bond to weaker standards in comparison to anonymous people. In its negative aspect, the right to privacy protects the individual's intimacy and private life against public authorities and other citizens' trespasses, whereas in its positive aspect it imposes the state the duty to carry out administrative and legislative measures needed to ensure citizen's privacy, sheltering them from other people's or other states' trespasses. The right to privacy has a relative figure, conforming to explicit constitutional constraints, either directly or indirectly, as well as implicit constraints, when it collides with other constitutional values. In the background of information society, both governments and the private sector's interest in meddling someone else's privacy increases. Surveillance over individuals experience a stunning improvement as a result of information technology, consisting of devices which allow monitoring and controlling people's behavior. The risks of internet to privacy shall be highlighted, especially when it comes to the automated processing of personal data, in order to emphasize the necessity of regulation of the right to informational self-determination, regarding (i) the principles enforceable to these data processing, (ii) the rights ensured to the information holders, (iii) the duties of the ones who are accountable for the data disclosure, (iv) the sanctions due to the violation of these precepts, among other procedures necessary for protecting people's intimacy and private life opposite the ultimate technological resources.

Keywords: fundamental rights, privacy, information technology.

SUMÁRIO

PARTE II

LISTA DE ABREVIATURAS, SIGLAS E SÍMBOLOS

ABREVIATURAS

ampl. – ampliada
apud – citado por
art. – artigo
atual. – atualizada
ed. – edição ou editora
loc. cit. – *loco citato*
nº – número
op. cit. – *opus citatum* ou *opere citato*
p. – página
pp. – páginas
rev. – revista ou revisada
v. – *versus*
vol. – volume

SIGLAS

ADIN – Ação Direta de Inconstitucionalidade

AIDS – *acquired immune eficiency syndrome* (síndrome de imunodeficiência adquirida)

ARPA – *Advanced Research Projects Agency* (Agência de Projetos de Pesquisa Avançada Americana)

BC – Banco Central do Brasil

CBF – Confederação Brasileira de Futebol

CC – Código Civil

CCJ – Comissão de Constituição e Justiça

CCT – Convenção Coletiva de Trabalho

CCTV – *closed-circuit television* (circuito fechado de televisão)

CDC – Código de Proteção e Defesa do Consumidor

CF – Constituição Federal

CGIbr – Comitê Gestor da Internet no Brasil

CJF – Conselho da Justiça Federal

CLT – Consolidação das Leis do Trabalho

CNIL – *Commission Nationale de l'Informatique et des Libertés* (Comissão Nacional de Proteção de Dados Francesa)

CNPD – Comissão Nacional de Protecção de Dados (Comissão Nacional de Proteção de Dados de Portugal)

CP – Código Penal

CPI – Comissão Parlamentar de Inquérito

CPP – Código de Processo Penal

CTN – Código Tributário Nacional

DARPA – *Defense Advanced Research Projects Agency* (Agência de Projetos de Pesquisa Avançada para a Defesa Americana)

DNA – *deoxyribonucleic acid* (ácido desoxirribonucléico)

DPF – Departamento de Polícia Federal

EC – Emenda Constitucional

ECA – Estatuto da Criança e do Adolescente

EFF – *Electronic Frontier Foundation* (Fundação Fronteira Eletrônica)

ENIAC – *Electronic Numerical Integrator and Computer* (Computador e Integrador Numérico Eletrônico)

EPIC – *Electronic Privacy Information Center* (Instituto de Informações Pessoais Eletrônicas)

EUA – Estados Unidos da América

FAQ – *frequently asked questions* (perguntas freqüentes)

FBI – *Federal Bureau of Investigation* (Agência Federal de Investigação Americana)

FD – Faculdade de Direito

GCHQ – *Government Communications Headquarters* (Agência de Inteligência Britânica)

GPS – *global positioning system* (sistema de posicionamento global)

HC – *Habeas Corpus*

HD – *Habeas Data*

ICANN – *Internet Corporation for Assigned Names and Numbers* (Instituto de Nomes e Números de Domínio da Internet Americano)

IP – *internet protocol* (protocolo de internet)

IRC – *internet relay chat* (protocolo de comunicação da internet)

MP – Ministério Público

NSA – *National Security Agency* (Agência de Segurança Nacional Americana)

NSFNET – *National Science Foundation* (Fundação da Ciência Nacional Americana)

OCDE – Organização para a Cooperação e Desenvolvimento Econômico

OEA – Organização dos Estados Americanos

ONU – Organização das Nações Unidas

RE – Recurso Extraordinário

RESP – Recurso Especial

RFC – *request for comments* (grupo de discussão)

RJ – Rio de Janeiro

RMS – Recurso Ordinário em Mandado de Segurança

SIVAM – Sistema de Vigilância da Amazônia

SP – São Paulo

SPC – Serviço de Proteção ao Crédito

STJ – Superior Tribunal de Justiça

TCP/IP – *transmission control protocol/internet protocol* (protocolo de controle de transmissão/protocolo de internet)

TFR – Tribunal Federal de Recursos

TST – Tribunal Superior do Trabalho

UE – União Européia

UnB – Universidade de Brasília

URSS – União das Repúblicas Socialistas Soviéticas

SÍMBOLOS

§ - parágrafo

§§ - parágrafos

INTRODUÇÃO

Informações sempre moveram a cobiça tanto de governos quanto da iniciativa privada, no afã de aprimorarem conhecimentos e, conseqüentemente, otimizarem resultados que lhes propiciassem dividendos; assim, quanto mais significativo o volume de informações e mais eficiente o gerenciamento de tais dados, maior a probabilidade de se enfrentarem disputas econômicas, sociais e políticas.

Com o desenvolvimento do capitalismo, gradualmente, de *per si,* a informação assume cada vez maior relevância; vislumbra-se, então, uma nova forma de organização social, política e econômica denominada *sociedade da informação*. No cenário que se inaugura, a informação ascende ao posto de principal riqueza, intensificando-se, em todos os setores, o uso da tecnologia da informação para facilitar a coleta, a produção, o processamento, a transmissão e o armazenamento de dados.

O mundo se deslumbra com os novos rumos do conhecimento; a tecnologia da informação ilumina horizontes de todas as esferas: invade o cotidiano, altera a forma de produção das empresas, modifica as atividades do setor público e do setor privado, transforma o padrão cultural das pessoas e as formas de relacionamento, enfim, revoluciona a concepção de vida que até então norteava as ações dos indivíduos, e o homem desperta no universo da tecnologia, deixa-se cativar pela máquina que oferece perspectivas de interação jamais experimentadas, expondo-se, de outro lado, cada vez mais em sua intimidade e vida privada diante dos novos recursos computacionais.

Nesse contexto encontra-se o cidadão comum, cujos dados pessoais caem em domínio público; inerme, o próprio titular já não logra exercer controle sobre informações a seu respeito, sequer sobre as mais íntimas, especialmente após o advento e a massificação da internet. Tradicionalmente, transmitiam-se dados pessoais tão-somente por telefone, rádio ou papel, mas, com a revolução da tecnologia, essas informações passaram a ser veiculadas mediante potentes computadores ligados em rede, que facilitam o acesso, a alteração, a destruição, o armazenamento, a interconexão, e toda espécie de tratamento de dados por terceiros não autorizados.

Em outras situações, a intervenção na privacidade se consuma mediante espionagem em meio eletrônico, promovida por empresas e governos, que interceptam informações pessoais e toda espécie de comunicação ao redor do mundo. Assiste-se, portanto, ao crescimento assustador dos riscos de violação à privacidade, o que merece criterioso estudo não apenas à luz da ciência do direito, mas também da tecnologia.

Este trabalho apresenta-se como dissertação de mestrado à Faculdade de Direito – FD da Universidade de Brasília – UnB, centra seu foco em um estudo a respeito do *direito à privacidade na sociedade da informação* e persegue a meta de contribuir para o debate a respeito das múltiplas dimensões desse direito fundamental nesse novo cenário social, político e econômico, caracterizado pela mitigação da intimidade e da vida privada diante dos avanços da tecnologia da informação.

O direito à privacidade, consagrado desde o século XVI nos ordenamentos jurídicos estrangeiros, traduz-se como uma garantia essencial ao pleno desenvolvimento do indivíduo e ao exercício, com tranqüilidade, da liberdade de consciência, de crença e de expressão. Somente sob esse manto protetor a pessoa se permite despir-se de seu ego, abandonar as máscaras impostas pela sociedade, explorar livremente seu íntimo, exercer, enfim, com consciência, o seu poder de autodeterminação.

Enquanto expressão do princípio da dignidade da pessoa humana, a privacidade impõe-se como um direito tão importante, que sem a proteção dessa garantia todos os outros direitos subjetivos tornar-se-iam irrelevantes para o seu titular. Assim, o direito à privacidade deve ser assegurado como um mínimo invulnerável, merecedor de total atenção pelos mais diversos atores sociais, incluindo-se juristas, sociólogos, filósofos, tecnólogos, burocratas, políticos e todo e qualquer cidadão comum, o que demonstra a relevância do tema exposto.

Na óptica deste trabalho, a privacidade denota um direito fundamental de *dimensão subjetiva* (direito individual oponível ao Estado e aos demais particulares) e também uma garantia de *dimensão objetiva* (valor objetivo que condiciona constitucionalmente toda a atuação dos poderes constituídos, irradiando-se por todos os ramos do direito, vinculando entes públicos e privados). Assim, sob a *dimensão subjetiva*, o direito à privacidade consiste na faculdade que tem cada pessoa de obstar a intromissão de estranhos na sua intimidade e vida privada, de se autodeterminar e de controlar os próprios dados pessoais; e sob a *dimensão objetiva*, configura-se como um dos valores fundantes do ordenamento jurídico, representando a essência do Estado

Democrático de Direito, ao proporcionar o livre exercício da liberdade de consciência, de crença e de expressão.

Observa-se, todavia, que a doutrina, ao mencionar esse direito fundamental, ressalta apenas seu aspecto *negativo*, ou seja, o direito que se concede ao titular de exigir a abstenção, a não intromissão do Estado e de terceiros em sua intimidade e vida privada. Uma análise mais acurada, no entanto, demonstra que esse mesmo direito, para sua plena eficácia, precisa ser interpretado também sob o enfoque *positivo*, isto é, deve amparar a faculdade conferida ao titular de exigir uma atuação do poder público, a fim de criar os pressupostos fáticos que garantam a efetividade de tal garantia, vedando-se a omissão estatal diante das ameaças provenientes de terceiros.

Nesse sentido, busca-se, por meio do presente estudo, uma interpretação mais ampla desse direito fundamental, no intuito de contribuir para um debate que contemple a construção de um paradigma distinto daquele adotado pelo Estado Liberal Burguês, ainda predominante na doutrina pátria no que concerne aos direitos fundamentais de primeira geração.

O trabalho persegue, então, os seguintes objetivos: (i) mostrar como a doutrina, a jurisprudência, enfim, o ordenamento jurídico nacional, estrangeiro e internacional tratam o direito à privacidade; (ii) analisar as múltiplas dimensões desse direito fundamental, enfatizando o seu aspecto positivo, como forma de contribuir para maior efetividade dessa garantia; (iii) alertar para os riscos aos quais a privacidade se vê exposta no cenário da sociedade da informação.

Para alcançar as finalidades propostas, utilizou-se neste trabalho a técnica de pesquisa bibliográfica, fazendo-se uso da doutrina e da jurisprudência nacionais, estrangeiras e internacionais; da técnica de pesquisa documental, valendo-se de materiais que não receberam tratamento analítico, como artigos em meio eletrônico, reportagens de revistas, documentos do Comitê Gestor da Internet no Brasil – CGIbr e participação em congressos; e também da técnica de pesquisa de campo, estudando-se – com base na observação – o comportamento de determinadas comunidades da internet, como o *Orkut* e o *ParPerfeito*, bem como as tendências, os conhecimentos e as opiniões manifestados na rede mundial de computadores, em páginas como a da Comissão Nacional de Protecção de Dados – CNPD, da *Commission Nationale de l'Informatique et des Libertés* – CNIL, da *Electronic Frontier Foundation* – EFF, da *National Science Foundation* – NSFNET, e tantas outras.

A dissertação ordena-se em duas partes: a primeira, dedicada às noções iniciais sobre privacidade e ao estudo desse preceito na teoria geral dos direitos fundamentais; a outra, centrada no exame da privacidade no contexto da sociedade da informação.

A primeira parte se desenvolve nos dois capítulos iniciais. O primeiro capítulo apresenta o assunto, aludindo-se ao conceito e às espécies de privacidade, à distinção entre intimidade e vida privada, ao panorama histórico do direito à privacidade, à relação entre a privacidade e os demais direitos da personalidade, à aplicabilidade do direito à privacidade às pessoas jurídicas de direito público e privado, e à distinção entre privacidade e sigilo.

No segundo capítulo, analisa-se a privacidade sob a luz da teoria geral dos direitos fundamentais, destacando-se a classificação dos direitos fundamentais enquanto regras e princípios; o caráter relativo dos direitos fundamentais; a conformação do direito à privacidade na jurisprudência nacional; as dimensões subjetiva e objetiva dos direitos fundamentais; as múltiplas dimensões do direito à privacidade segundo a classificação pelo critério funcional; a eficácia horizontal dos direitos fundamentais; a aplicabilidade do direito à privacidade nas relações privadas; a possibilidade ou não de renúncia ao direito à privacidade, em especial no que concerne aos chamados *reality shows* e aos contratos de trabalho; analisa-se igualmente o âmbito de proteção do direito à privacidade, considerando-se as restrições expressas e implícitas a essa garantia; as colisões do direito à privacidade com outros direitos fundamentais e com outros valores protegidos pela Constituição.

A segunda parte do trabalho também se desenvolve em dois capítulos. No terceiro capítulo, analisa-se o direito à privacidade no cenário da sociedade da informação, expondo-se os fundamentos sociológicos e filosóficos da restrição à privacidade por meio da tecnologia. Inicialmente, enfoca-se a origem e as principais características da sociedade da informação, ressaltando-se os contornos do direito à privacidade diante do crescente interesse do Estado e da iniciativa privada nas informações pessoais identificáveis. Para melhor compreensão do problema exposto, recorre-se ao estudo do *panoptismo* de Michel Foucault, apresentando-se as origens da disciplina e do controle do comportamento dos indivíduos, enquanto mecanismo de exercício do poder. A seguir, expõe-se a tese central deste trabalho: a conformação do direito à privacidade na sociedade da informação; destacando-se os riscos a que a internet expõe esse direito fundamental, a preservação do anonimato na *web*, e a questão da intervenção estatal na esfera da vida privada por meio da coleta de informações pessoais e pela promoção da espionagem eletrônica.

No quarto e último capítulo, estuda-se a questão da proteção de dados pessoais na sociedade da informação. Traçadas as considerações iniciais sobre proteção de dados pessoais, volta-se mais uma vez ao direito comparado, expondo-se a forma como se aborda a questão no contexto do ordenamento jurídico internacional; a seguir, apresenta-se a conformação da proteção de dados pessoais na legislação nacional; os princípios relacionados com o tratamento de dados pessoais, e a questão da regulamentação do direito à autodeterminação informativa.

Em conclusão, expõem-se as idéias enunciadas ao longo de todo o trabalho.

No primeiro e no segundo capítulos, analisa-se o tema sob a luz da ciência do direito, utilizando-se conceitos operacionais do direito civil e da teoria geral dos direitos fundamentais, tais como: intimidade, vida privada, liberdade, sigilo, direito da personalidade, dignidade da pessoa humana, domicílio, pessoa jurídica, Estado, direito fundamental, normas-regra, normas-princípio, medida do tudo-ou-nada, medida do possível, subsunção, ponderação, âmbito de proteção, núcleo essencial, reserva legal simples e qualificada, restrição expressa e implícita, colisão de direitos fundamentais, direito de defesa, direito a prestação, eficácia horizontal.

No terceiro capítulo, a autora deste trabalho socorre-se da especulação filosófica e da investigação sociológica, e também de expressões do ramo da informática, tais como: *e-mail*, segurança da informação, agente inteligente, criptografia, *site*, *log*, *chat*, vírus, *spyware*, *backdoor*, *internet protocol*, servidor *proxy*, rede *wireless*, e tantas outras explicadas no corpo do texto e nas notas de rodapé. Todavia, este estudo não deve ser entendido como uma pesquisa situada nas áreas da filosofia jurídica ou da sociologia do direito, e nem na área da informática; o que demandaria conhecimentos mais aprofundados acerca de tais ciências.

No quarto capítulo, lança-se mão do recurso do direito comparado, apresentando-se conceitos utilizados em um ramo denominado na União Européia – UE *direito da sociedade da informação*, tais como: dados pessoais, dados sensíveis, tratamento, autodeterminação informativa, direito à informação, direito de oposição, princípio da caducidade, princípio da segurança no tratamento, princípio da exatidão e atualização dos dados, princípio da caducidade, *soft-laws*.

Apesar do emprego de conceitos e de expressões de diversas áreas para melhor compreensão do tema proposto, dedica-se este trabalho especialmente à doutrina constitucional e ao recente ramo do direito da sociedade da informação, conhecido por alguns pesquisadores como direito da tecnologia da informação ou direito da informática.

PARTE I

CAPÍTULO 1 NOÇÕES INICIAIS SOBRE PRIVACIDADE

1.1 Relação entre privacidade e liberdade

Privacidade e liberdade se amalgamam como duas faces de uma mesma moeda, uma vez que tão-somente o manto de proteção da privacidade proporciona a um indivíduo o direito ao exercício da liberdade. Exercer com tranqüilidade a liberdade de consciência, de crença e de expressão supõe o exercício do direito que se concede a qualquer pessoa, de dispor de um espaço reservado em que possa voltar-se para si mesma, sem prender-se ao jugo de qualquer censura, sem sentir-se cativa da observação de outrem. Nesse sentido, a privacidade proporciona ao indivíduo a oportunidade de desvencilhar-se de todas as máscaras que a sociedade lhe impõe, ou seja, confere-lhe um espaço reservado, seguramente inviolável, em que ele pode explorar livremente o seu íntimo, despido do temor de uma reprimenda externa, para exercer, enfim, o seu direito de autodeterminação.

A filosofia de Ortega y Gasset ressalta a necessidade que move o ser humano de voltar-se para si mesmo, de introjetar-se em seu interior, de concentrar-se, seja para relacionar-se melhor com seus semelhantes, seja por qualquer outro motivo. A esse processo chamou de *ensimesmamento*, isto é, a ação de introjetar-se e de ficar concentrado, que se destaca como o diferencial por excelência entre o homem e os outros seres viventes. O homem, ao contrário dos outros animais, detém a prerrogativa de realizar a denominada torção radical, ou seja, abandonar o mundo externo e voltar-se para dentro de si, ocupando-se apenas de si próprio e não do outro. Essa faculdade de ensimesmar-se implica dois poderes: o de desatender ao mundo externo e o de desenvolver com liberdade as próprias idéias[1]. Daí a necessidade de proteção à privacidade, como

[1] ORTEGA Y GASSET, José. Obras completas. Madrid: Alianza Editorial, 1994, Tomo 5, pp. 301-302 apud SANTOS, Antonio Jeová. **Dano moral na internet**. São Paulo: Método, 2001, pp. 167-169.

o único meio de se garantir ao indivíduo a possibilidade de *ensimesmamento* e, desta forma, conferir-lhe um espaço livre de ingerências e de intervenções advindas de censura externa.

Leonardo Roscoe Bessa, citando a obra *Privacy and freedom,* de Alan Westin, aponta que, sob os ditames da privacidade, protegem-se outros interesses, como *personal autonomy, emotional release*, *self-evaluation* e *limited and protected communication*. A privacidade impõe-se como condição essencial para o desenvolvimento do senso da individualidade, pois, destituído de tal prerrogativa, o ser humano não lograria perscrutar-se para sondar o que pensa e sente, não poderia dispor da solitude indispensável para imergir nos próprios pensamentos e emoções. Também é necessária para que a pessoa possa liberar suas emoções sem constrangimentos, na medida em que, destituído de tal condição, o indivíduo não disporia do espaço íntimo, tão-somente seu, para deixar de representar papéis, liberando-se a si mesmo da encenação que exibe no seu cotidiano diante da sociedade. Abandonados os disfarces, o indivíduo pode finalmente exercer a auto-avaliação, refletir sobre o que lhe pertence e sobre a posição que deseja assumir diante do bombardeamento externo de informações. Por fim, a privacidade resguarda as comunicações pessoais que não podem ser compartilhadas com o público em geral[2].

De outro lado, observa-se que a privacidade, na mesma medida em que protege a liberdade, também depende dessa mesma condição para garantir a sua existência. Em regimes de repressão – como em regimes de ditadura, fascismo e nazismo – o Estado cerceia radicalmente o direito à privacidade aos cidadãos. A manutenção do poder, além da utilização de outros mecanismos, requer o controle dos pensamentos, das crenças e da expressão de toda a coletividade, sendo, portanto, medida indispensável a intromissão – velada ou ostensiva – na vida particular dos indivíduos. Não se assegura privacidade sem liberdade, e não se exercita liberdade sem privacidade.

A interdependência entre privacidade e liberdade ocorre ainda no momento em que o indivíduo invoca o seu direito à proteção da intimidade e da vida privada no que concerne ao titular desse direito decidir não apenas o que deseja expor e o que não deseja expor a respeito de si mesmo; mas também, de forma ainda mais grave, igualmente se deseja arrogar a si tal direito perante terceiros. Observa-se, portanto, que o exercício do direito à privacidade nada mais representa que o exercício do direito à liberdade, tanto a liberdade de se expor ou não quanto a de

[2] WESTIN, Alan. Privacy and freedom. New York: Atheneum, 1967, p. 8 apud BESSA, Leonardo Roscoe. **O consumidor e os limites dos bancos de dados de proteção ao crédito**. São Paulo: Revista dos Tribunais, 2003, pp. 86-87.

decidir em que medida pretende o titular revelar sua intimidade e sua vida privada para o mundo exterior.

Conforme expõe Gilberto Haddad Jabur, o direito à privacidade decorre do direito à liberdade, na medida em que o primeiro abriga o direito à quietude, à paz interior, à solidão e ao isolamento contra a curiosidade pública, em relação a tudo o quanto possa interessar à pessoa, impedindo que se desnude sua vida particular; enquanto o segundo resguarda o direito a uma livre escolha daquilo que o indivíduo pretende ou não expor para terceiros, protegendo o seu círculo restrito da forma como lhe aprouver[3].

Constatada a íntima relação entre privacidade e liberdade, alteia-se a importância de proteção desse direito que se impõe como a única forma capaz de resguardar o livre desenvolvimento e a autodeterminação inerentes a cada indivíduo. Passemos, pois, à delimitação do conceito de privacidade.

1.2 Conceito e espécies de privacidade

Primeiramente, há que se distinguir *proteção da honra* de *proteção à privacidade*. No direito brasileiro, essa diferenciação remonta a Paulo José da Costa Júnior, que separa a *esfera individual* da *esfera privada*. A primeira esfera refere-se à proteção do nome e da reputação contra abusos de terceiros e contra ataques difamatórios. Já a esfera privada concerne ao aspecto da individualidade, correspondendo à aspiração do indivíduo de preservar a sua tranqüilidade de espírito, aquela paz interior que uma intromissão alheia viria perturbar. Na esfera individual, o cidadão do mundo acha-se relacionado com seus semelhantes; na esfera privada, ao contrário, o cidadão se situa na intimidade ou no recato, em seu isolamento moral, convivendo com a própria individualidade[4]. Assim, embora o direito à honra e o direito à privacidade sejam amparados pelo mesmo dispositivo constitucional (CF, art. 5º, inciso X), dispõem de âmbitos de proteção

[3] JABUR, Gilberto Haddad. **Liberdade de pensamento e direito à vida privada**: conflito entre direitos da personalidade. São Paulo: RT, 2000, p. 260.
[4] COSTA JÚNIOR, Paulo José da. **O direito de estar só**: tutela penal da intimidade. 3ª ed. São Paulo: Siciliano Jurídico, 2004, p. 28.

diversos, sendo objeto deste estudo apenas o direito à privacidade. Passe-se, portanto, à conceituação de tal direito.

Para Celso Bastos, a privacidade é a "*faculdade que tem cada indivíduo de obstar a intromissão de estranhos em sua vida privada e familiar, assim como de impedir-lhes o acesso a informações sobre a privacidade de cada um, e também impedir que sejam divulgadas informações sobre esta área da manifestação existencial do ser humano [sic]*"[5]. Gilberto Haddad Jabur ressalta, como atributo da privacidade, a faculdade de se excluir do conhecimento de terceiros as informações que o titular quer preservar para si próprio; o direito de viver em isolamento sem ser submetido a uma publicidade que não desejou[6]. Em complemento, Marcelo Pereira, ao analisar o conceito do direito à privacidade, observa que "*o direito à intimidade seria (...) o poder das pessoas de controlar suas informações pessoais, as quais, ainda que não formem parte da vida privada das mesmas, possam revelar aspectos de sua personalidade*"[7].

Buscando um conceito abrangente, o direito à privacidade consistiria em um direito subjetivo de toda pessoa – brasileira ou estrangeira, residente ou transeunte, física ou jurídica – não apenas de constranger os outros a respeitarem sua esfera privada, mas também de controlar suas informações de caráter pessoal – sejam estas sensíveis ou não – resistindo às intromissões indevidas provenientes de terceiros. Nesse sentido, *o direito à privacidade traduz-se na faculdade que tem cada pessoa de obstar a intromissão de estranhos na sua intimidade e vida privada, assim como na prerrogativa de controlar suas informações pessoais, evitando acesso e divulgação não autorizados*. Tutela, portanto, o direito que se confere ao indivíduo de manter um afastamento confortável em relação ao mundo exterior, preservando esse distanciamento necessário ao exercício de sua autodeterminação. Tem, intrinsecamente, natureza negativa ao proteger o titular das intromissões de terceiros; e, de outro lado, natureza positiva ao permitir que o próprio indivíduo controle o que deve ser conhecido e o que não deve ser conhecido pelos demais, expressão da liberdade que lhe é ínsita.

Conforme exposto, a intromissão por terceiros na privacidade de um indivíduo pode consumar-se por meio do *acesso não autorizado* ou da *divulgação indevida*. No primeiro caso, a aquisição das informações pessoais é ilegítima; no segundo, mesmo que legítima essa aquisição

[5] BASTOS, Celso Ribeiro; MARTINS, Ives Gandra. **Comentários à Constituição do Brasil**. São Paulo: Saraiva, 1989, vol. 2, p. 63.
[6] JABUR, Gilberto Haddad. **Liberdade de pensamento e direito à vida privada**. Op. cit., p. 254.
[7] PEREIRA, Marcelo Cardoso. **Direito à intimidade na internet**. 2ª ed. Curitiba: Juruá Editora, 2004, p. 140.

de informações, não é lícita a ulterior revelação. Neste caso, a violação ocorre por meio da difusão não autorizada da intimidade alheia. Paulo José da Costa Júnior cita essas duas formas de violação da privacidade:

> Na expressão "direito à intimidade" são tutelados dois interesses, que se somam: o interesse de que a intimidade não venha a sofrer agressões e o de não venha a ser divulgada. O direito, porém, é o mesmo. O que pode assumir uma gama diversa é o interesse protegido pelo direito. São duas esferas de interesses, abarcadas no mesmo raio de proteção do mesmo direito. No âmbito do direito à intimidade, portanto, podem ser vislumbrados esses dois aspectos: a invasão e a divulgação não autorizada da intimidade legitimamente conquistada. Em termos de conteúdo, todavia, não deve prevalecer a distinção.[8]

Observa-se, ainda, que outra forma de intromissão na privacidade pode ocorrer por meio da identificação do titular de determinadas informações legitimamente acessadas. Neste caso, o acesso às informações é autorizado, sendo ilegítima, entretanto, a identificação de seu titular. Em algumas estatísticas, tais como as de portadores de certas doenças, deve ser preservado o anonimato dos elementos submetidos a tal estudo, o que impede a identificação dos titulares cujos dados constem na pesquisa. Assim, a violação da privacidade pode ocorrer não só em relação a pessoas identificadas, mas também em relação a pessoas identificáveis, conforme será detalhado no capítulo 4.

Aspecto que ainda merece destaque nas considerações preliminares deste estudo é a classificação da privacidade em diferentes categorias, conforme seu âmbito de proteção: física, do domicílio, das comunicações, *decisional* e *informacional*. A *privacidade física* protege o corpo do indivíduo contra procedimentos invasivos não autorizados pelo próprio indivíduo, como a realização forçada de testes de drogas e de exames genéticos. Existindo outros meios para se comprovar a paternidade, deve-se preservar o direito à privacidade, proibindo-se a realização forçada de exame de DNA (*deoxyribonucleic acid* ou ácido desoxirribonucléico), conforme se observa nos seguintes acórdãos do Supremo Tribunal Federal – STF:

> EMENTA. INVESTIGAÇÃO DE PATERNIDADE - EXAME DNA - CONDUÇÃO DO RÉU "DEBAIXO DE VARA".
> Discrepa, a mais não poder, de garantias constitucionais implícitas e explícitas – preservação da dignidade humana, da intimidade, da intangibilidade do corpo humano, do império da lei e da inexecução específica e direta de obrigação de fazer – provimento judicial que, em ação civil de investigação de paternidade, implique determinação no sentido de o réu ser conduzido ao laboratório, "debaixo de vara", para coleta do material indispensável à feitura do exame DNA. A recusa resolve-se no plano jurídico-instrumental, consideradas a

[8] COSTA JÚNIOR, Paulo José da. Op. cit., p. 33.

> dogmática, a doutrina e a jurisprudência, no que voltadas ao deslinde das questões ligadas à prova dos fatos.[9]
>
> EMENTA. DNA: submissão compulsória ao fornecimento de sangue para a pesquisa do DNA: estado da questão no direito comparado: precedente do STF que libera do constrangimento o réu em ação de investigação de paternidade (HC 71.373) e o dissenso dos votos vencidos: deferimento, não obstante, do HC na espécie, em que se cuida de situação atípica na qual se pretende - de resto, apenas para obter prova de reforço - submeter ao exame o pai presumido, em processo que tem por objeto a pretensão de terceiro de ver-se declarado o pai biológico da criança nascida na constância do casamento do paciente: hipótese na qual, à luz do princípio da proporcionalidade ou da razoabilidade, se impõe evitar a afronta à dignidade pessoal que, nas circunstâncias, a sua participação na perícia substantivaria.[10]

O Tribunal Constitucional Federal alemão reconheceu o direito *à privacidade física,* em decisão datada de 10 de junho de 1963 (*BverfGe 16,194 – Liquorentnahme*), em que julgou procedente a reclamação constitucional impetrada por um pequeno empresário, que, em processo criminal por delito para o qual se previa pena pecuniária, foi forçado a se submeter a uma intervenção cirúrgica para retirada de líquido cefalorraquiano a fim de provar sua imputabilidade. Segundo o Tribunal, o interesse público no esclarecimento de crimes não justifica a violação à incolumidade física do reclamante, ainda mais por tratar-se de delito de menor potencial ofensivo[11].

A segunda espécie aponta para o *direito à privacidade do domicílio,* protegida pelo inciso XI do art. 5º da CF, que assim dispõe: "*a casa é asilo inviolável do indivíduo, ninguém nela podendo penetrar sem consentimento do morador, salvo em caso de flagrante delito ou desastre, ou para prestar socorro, ou, durante o dia, por determinação judicial*". Entende-se por domicílio a residência ou qualquer local delimitado ou separado que alguém ocupa com exclusividade como quartos de hotel e escritórios profissionais, desde que haja intenção de estabelecimento. Assim, a violação do domicílio torna-se possível tão-somente em casos de flagrante delito ou de

---

[9] BRASIL. Supremo Tribunal Federal. HC nº 71373-RS. Impetrante: José Antônio Gomes Pinheiro Machado. Relator para o Acordão: Marco Aurélio. Brasília, DF, 10 de novembro de 1994. **Diário da Justiça da República Federativa do Brasil**, Brasília, DF, 22 nov. 1996, p. 45686. Disponível em <http://www.stf.gov.br/jurisprudencia>. Acesso em: 30 jan. 2007. Grifos nossos.

[10] BRASIL. Supremo Tribunal Federal. HC nº 76060-SC. Impetrante: Elisa Pimenta. Paciente: Arante José Monteiro Filho. Relator: Sepúlveda Pertence. Brasília, DF, 31 de março de 1998. **Diário da Justiça da República Federativa do Brasil**, Brasília, DF, 15 maio 1998, p. 00044. Disponível em <http://www.stf.gov.br/jurisprudencia>. Acesso em: 30 jan. 2007. Grifos nossos.

[11] MARTINS, Leonardo (Org.). **Cinqüenta anos de jurisprudência do Tribunal Constitucional Federal Alemão**. Montevidéu: Fundação Konrad Adenauer, 2005, pp. 294-296.

desastre ou para se prestar socorro, não importando a hora do dia ou da noite; ou durante o dia por ordem judicial, resguardando-se nos demais casos a privacidade de seus moradores.

A terceira categoria contempla o *direito à privacidade das comunicações,* prevista no inciso XII do art. 5º da CF, que garante ser "*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*". Protege todas as espécies de comunicação contra interceptação por terceiros e contra o próprio Estado, admitindo-se a intromissão na privacidade apenas quando houver decisão judicial e para salvaguardar outros interesses públicos. Ressalte-se que o dispositivo, além de estabelecer expressamente a inviolabilidade da correspondência e das comunicações em geral, implicitamente proíbe o conhecimento de seu conteúdo por terceiros, garantindo-se o sigilo das informações trafegadas, inclusive por meio eletrônico.

O quarto tipo contempla o *direito à privacidade decisional*, entendida esta como o atributo inato ao indivíduo, ao ser humano, de decidir seu próprio destino, de tomar as próprias decisões, enfim, de buscar a felicidade naquilo que lhe é reservado ao foro íntimo, o que se nomearia também *direito à autodeterminação*. Essa espécie de privacidade foi reconhecida pela jurisprudência americana em casos relacionados com o uso de anticoncepcionais e com o aborto, ao se preservar ao casal o direito de decidir, em foro íntimo, sobre o curso de suas vidas, sem qualquer interferência estatal. A autodeterminação também já foi reconhecida pelo Tribunal Constitucional Federal alemão, no que concerne ao direito de o indivíduo determinar autonomamente o seu destino, como casar-se ou não, ter filhos ou não, definir sua orientação sexual, expor em público sua própria imagem, voz e honra pessoal[12], e demais direitos nessa mesma linha, desde que não afetassem direitos de terceiros, nem a lei moral, nem a ordem constitucional[13].

Em 1965, a Suprema Corte Americana, no caso *Griswold v. Connecticut,* afirmou a inconstitucionalidade de lei estadual, que caracterizava como crime, inclusive entre casais casados, o uso de métodos anticoncepcionais artificiais. Fundamentou-se tal decisão no *right to privacy* que, embora não previsto expressamente no texto constitucional americano, poderia ser inferido mediante interpretação sistemática, protegendo-se decisões individuais a respeito de

[12] A questão da auto-exposição será tratada nos itens 2.6, 2.8 e 3.6.
[13] MARTINS, Leonardo (Org.). Op. cit., p. 189.

questões envolvendo a vida familiar, o uso de anticoncepcionais, a escolha de escola para os filhos, dentre outros temas. No caso *Roe v. Wade*, em 1973, a Corte foi mais além, decidindo que o direito à privacidade se impõe com amplitude suficiente para conferir à mulher a decisão de interromper ou não a gravidez até o terceiro mês. Em 1986, ocorreu um certo retrocesso quando, no caso *Bowers v. Hardwick*, a Suprema Corte rejeitou por 5 (cinco) votos contra 4 (quatro) a tese de que o direito à privacidade compreenderia a faculdade de adultos do mesmo sexo de manterem relações sexuais dentro de um espaço privado, afirmando a constitucionalidade da lei estadual que caracterizava como crime tal conduta[14].

Por fim, a última espécie diz respeito à *privacidade informacional*, que cinge em seu âmbito de proteção, as informações sobre determinada pessoa, abarcando não só aquelas relacionadas a sua esfera mais íntima, mas também dados pessoais[15] que possam conduzir à identificação de tal titular. O referido direito foi reconhecido pela primeira vez na jurisprudência do Tribunal Constitucional Federal alemão, no caso da Lei do Censo (*Volkszählungsgesetz*) de 1983, de 25 de março de 1982, em que se ordenou – para fins estatísticos – o recenseamento geral da população coletando-se dados relacionados à profissão, à moradia, ao domicílio e à renda. A Lei buscava reunir informações tanto sobre o crescimento populacional, distribuição espacial das pessoas, composição segundo características demográficas e sociais, quanto sobre atividades econômicas. O ato normativo previa também a possibilidade de comparação dos dados levantados com registros públicos já existentes e a transmissão das informações colhidas a repartições públicas federais, estaduais e municipais. A Corte, em decisão datada de 15 de dezembro de 1983 (*BverfGe 65,1 – Volkszählungsurteil*), julgou nulos os dispositivos relacionados à comparação e à transmissão dos dados para repartições públicas; reconhecendo o *direito à autodeterminação informativa*, ou seja, o direito que cabe a cada indivíduo de controlar e de proteger os próprios dados pessoais, tendo em vista a moderna tecnologia e processamento de informação[16].

Hoje, o *direito à privacidade informacional* ou *direito à autodeterminação informativa* já foi incorporado nas constituições de diversos países como Portugal, Eslovênia, Rússia e Espanha. Na Constituição brasileira não existe dispositivo que faça referência expressa à privacidade

[14] SARMENTO, Daniel. **Direitos fundamentais e relações privadas**. Rio de Janeiro: Lumen Juris, 2004, pp. 204-206.
[15] Dado pessoal é o dado relacionado a um indivíduo identificado ou identificável, independentemente do suporte em que se encontre registrado (escrita, imagem, som ou vídeo).
[16] MARTINS, Leonardo (Org.). Op. cit., pp. 233-235.

informacional, podendo-se, entretanto, cotejar o já citado inciso XII do art. 5º, quando menciona "dados", com o inciso X do mesmo artigo que protege a intimidade e a vida privada de forma genérica. Este tema será explorado com maior detalhamento nos itens 2.4.2.4.2 e 4.6.

1.3 Distinção entre intimidade e vida privada

Resgatando-se o conceito exposto no item anterior – o direito à privacidade traduz-se na faculdade inerente a cada pessoa de obstar a intromissão de estranhos em sua *intimidade* e *vida privada*, assim como a de controlar as próprias informações, evitando-se acesso e divulgação não autorizados – observa-se que o direito à privacidade evidencia, em seu âmbito de proteção, dois atributos, existindo certa distinção entre ambos.

Intimidade reflete os pensamentos do indivíduo, suas idéias e emoções, relacionando-se a uma zona mais estrita da pessoa, àquilo que deve ser mantido em sigilo por revelar o íntimo do indivíduo; vida privada, de outro lado, é a vida pessoal e familiar do indivíduo, que pode ser de conhecimento daqueles que desfrutam de sua convivência. Percebe-se, pois, que a última tem maior abrangência do que a primeira, conforme noticia Alexandre de Moraes "*os conceitos constitucionais de intimidade e vida privada apresentam grande interligação, podendo, porém, ser diferenciados por meio da menor amplitude do primeiro que encontra-se no âmbito de incidência do segundo [sic]*"[17].

Sidney Guerra também traz alguns esclarecimentos em relação à distinção entre intimidade e vida privada:

> Assim, para melhor esclarecimento, verifica-se que a intimidade é algo a mais do que a vida privada, ou seja, a intimidade caracteriza-se por aquele espaço, considerado pela pessoa como impenetrável, intransponível, indevassável e que, portanto, diz respeito única e exclusivamente a pessoa, como, por exemplo, recordações pessoais, memórias, diários, etc. Este espaço seria de tamanha importância que a pessoa não desejaria compartilhar com ninguém. São os segredos, as particularidades, as expectativas, enfim, seria, o que vamos chamar de o 'canto sagrado' que cada pessoa possui. Já a vida privada consiste naquelas particularidades que dizem respeito, por exemplo, à família, problemas envolvendo parentes próximos, saúde física e mental etc. Seria então aquela esfera íntima de cada um, que vedasse a intromissão alheia. Entretanto, percebe-

[17] MORAIS, Alexandre de. **Direito constitucional**. 12ª ed. São Paulo: Atlas, 2002, p. 80.

> se que neste caso a pessoa poderia partilhá-la com as pessoas que bem lhe conviesse, sendo da família ou apenas um amigo próximo.[18]

Observa-se que a intimidade, por corresponder à esfera mais interior do indivíduo, deve ser sempre mantida em segredo, inacessível e escondida, sendo de conhecimento apenas do próprio titular. Esse espaço interior do indivíduo – onde ele pode livremente construir seu agir e processar a vida interior descobrindo-se a si próprio – é denominado pela cultura ocidental *consciência* e pela cultura oriental *coração*. Assim, pode-se dizer que no âmago, no núcleo central da pessoa, na sua consciência ou no seu coração, conforme a cultura subjacente, radica a intimidade[19]. É o lugar onde se aninham os pensamentos do indivíduo, onde ele pode descobrir-se a si próprio, onde se cultua o seu núcleo sagrado e que deve ser protegido contra qualquer intromissão por terceiros, até mesmo contra aqueles que participam da convivência diária do mesmo indivíduo. Enfim, a intimidade revela aquilo que entretece o recôndito do ser, a esfera mais reservada de uma pessoa; configurando-se como o espaço necessário ao autoconhecimento.

Vida privada abrange confidência, reserva e todo ato humano externo, social, lícito, que a pessoa queira preservar de divulgação ou de conhecimento por terceiros em geral. Situa-se no campo dos atos humanos externos, lembrando que se refere a atos que a pessoa não deseja publicar nem divulgar, quer que o conhecimento de tais atos permaneça limitado a um círculo restrito de pessoas[20]. Assim, da intimidade não participam outras pessoas, apenas o próprio indivíduo em seu isolamento ou *ensimesmamento*; da vida privada participam as pessoas da íntima convivência do indivíduo que têm acesso a informações sobre sua vida pessoal e familiar.

Na Alemanha, a doutrina distingue *intimidade* e *vida privada* por meio da denominada *teoria das esferas* (*Sphärentheorie*) que divide a privacidade em três círculos concêntricos: *Privatsphäre, Intimsphäre* e *Geheimsphäre.* O primeiro círculo, de maior amplitude, representa a esfera privada – *Privatsphäre* ou *sphere of privacy* dos norte-americanos – excluindo-se do conhecimento de terceiros aspectos específicos da vida da pessoa. O segundo – *Intimsphäre* – compreende os valores atinentes ao âmbito da intimidade ou esfera confidencial, cujo acesso é mais restrito, somente permitido àqueles indivíduos com os quais a relação pessoal se desenvolve

[18] GUERRA, Sidney. **O direito à privacidade na internet**: uma discussão da esfera privada no mundo globalizado. Rio de Janeiro: América Jurídica, 2004, p. 55.
[19] ALONSO, Félix Ruiz. Pessoa, intimidade e o direito à privacidade. In: MARTINS, Ives Gandra; PEREIRA JÚNIOR, Antonio Jorge (coordenadores). **Direito à privacidade**. São Paulo: Centro de Extensão Universitária, 2005, pp. 16-20.
[20] ALONSO, Félix Ruiz. Op. cit., pp. 24-25.

de forma mais intensa. O terceiro e mais fechado dos círculos – *Geheimsphäre* – abrange a reserva, o sigilo, o segredo, as mais profundas manifestações espirituais da pessoa, caracterizadoras da vida íntima *stricto sensu*[21].

Paulo José da Costa Júnior, adotando a doutrina alemã, ressalta que no círculo externo (*Privatsphäre*) situam-se todos os fatos e comportamentos que o indivíduo deseja resguardar para que não se tornem de domínio público. No segundo círculo (*Intimsphäre*) concentram-se as informações compartilhadas apenas com as pessoas com as quais o indivíduo estabelece uma relação de confiança, excluindo-se o público em geral e as pessoas de sua convivência em relação às quais não confia. No menor dos círculos concêntricos (*Geheimsphäre*) depositam-se as informações que devem ser mantidas em sigilo ou em segredo, ou seja, aquelas nunca compartilhadas e aquelas reveladas apenas para as pessoas extremamente íntimas[22].

Adotando-se a *teoria das esferas*, pode-se nitidamente concluir pela distinção entre *intimidade* e *vida privad*a e, mais ainda, diferenciá-las do segredo. A proteção da vida privada – esfera de maior amplitude – consiste no direito de subtrair do conhecimento do público em geral fatos da vida particular que não revelam aspectos extremamente reservados da personalidade do indivíduo. Já a intimidade – *Intimsphäre* ou intimidade, em sentido lato na teoria alemã, refere-se à prerrogativa de se excluirem do conhecimento de terceiros as informações mais sensíveis do indivíduo, tais como aspectos atinentes à vida sexual, religiosa e política; compartilhadas apenas com as pessoas mais íntimas e em caráter reservado. Por fim, a esfera do segredo, *Geheimsphäre* ou intimidade em sentido estrito na teoria alemã, compreende as informações relacionadas com os sentimentos, com os sonhos e com as emoções da pessoa; não compartilhadas com ninguém ou compartilhadas apenas com amigos mais íntimos.

Apesar de ter sido largamente questionada pela impossibilidade de se determinarem cientificamente as fronteiras que demarcam os três círculos (*Privatsphäre, Intimsphäre* e *Geheimsphäre*), em face da incontornável relatividade que se estabelece entre eles, a *teoria das esferas* (*Sphärentheorie*) foi adotada pelo Tribunal Constitucional Federal alemão no caso da Lei do Microcenso. Na decisão, datada de 16 de julho 1969 (*BverfGe 27,1 – Mikrozensus*), o Tribunal afirmou que o terceiro e mais fechado dos círculos – *Geheimsphäre* – não pode ser violado pelo Estado nem mesmo por lei, por ser tal âmbito um recinto inatingível da vida privada, que não

[21] JABUR, Gilberto Haddad. **Liberdade de pensamento e direito à vida privada**. Op. cit., p. 257.
[22] COSTA JÚNIOR, Paulo José da. Op. cit., p. 34.

pode ser submetido a qualquer ação do poder público. Assim, certas informações de caráter pessoal não podem ser exigidas dos cidadãos, ainda que sejam mantidas dentro do sigilo de uma pesquisa estatística. Esse "espaço interior", no qual o cidadão "pertence a si mesmo" e ao qual "pode se recolher", deve ser preservado contra qualquer acesso por terceiros. De outro lado, as informações solicitadas pelos órgãos públicos, que exorbitem essa esfera e que não violem a dignidade ou a autodeterminação do indivíduo, devem ser prestadas ao Estado para pesquisas estatísticas, por exemplo. No caso em exame, o Tribunal considerou que a Lei do Microcenso não viola a *Geheimsphäre*, confirmando a constitucionalidade do ato normativo[23].

Fulgêncio Madrid Conessa critica o esforço para formulação e para compreensão da *teoria das esferas*, sugerindo a chamada *teoria do mosaico.* Para ele, o fato de a informação pertencer à esfera da vida privada, da intimidade ou do segredo parece irrelevante, pois o que importa é o uso que dela se fará. Ressalta que existem dados que, a princípio, mostram-se com aparência de inofensivos à violação, até mesmo da esfera da vida privada, que é a menos íntima das três, mas que, uma vez cotejados com outros dados, oferecem grave risco à violação da privacidade de seu titular. Assim, as informações pessoais, segundo Fulgêncio, devem ser protegidas com a mesma intensidade, independentemente da esfera em que se situem (vida privada, intimidade ou segredo). Dados pessoais assemelham-se a pequeninas pedras que formam um mosaico, ou seja, vistas por si sós nada representam, mas, uma vez unidas, formam um conjunto pleno de significado, que, neste caso, compõe a personalidade do indivíduo[24].

A par das críticas que se tecem em relação à *teoria das esferas*, a distinção entre intimidade e vida privada impõe-se como salutar no momento da avaliação dos danos materiais e morais acarretados pelo indevido acesso ou pela divulgação não consentida de informações de caráter pessoal. Quanto mais interior a esfera atingida, ou seja, quanto mais íntima a informação divulgada, mais grave se caracteriza a conduta de quem acessou ou de quem divulgou indevidamente tais dados, devendo-se, neste caso, aplicar-se sanção mais severa, aumentando-se o valor da indenização. Não se pode, todavia, refutar, de plano, a *teoria do mosaico*, que contribui significativamente para a compreensão do problema da coleta e do armazenamento de dados pessoais por entidades públicas e privadas, especialmente no que concerne à interconexão de tais informações por modernos recursos tecnológicos que permitem traçar com velocidade e

[23] MARTINS, Leonardo (Org.). Op. cit., pp. 215-217.
[24] MIGUEL, Carlos Ruiz. Em torno a la protección de los datos personales automatizados. Revista de Estudios Políticos. Madrid, n. 84, pp. 242-243, abr./jun. 1994 apud BESSA, Leonardo Roscoe. Op. cit., p. 91.

com acuidade o perfil dos titulares de tais dados, tema que será apresentado com maior detalhamento no capítulo 4.

Nesse sentido, percebe-se a relevância da distinção entre intimidade e vida privada, não sob o aspecto da proteção dos dados em si, conforme demonstra a *teoria do mosaico*, que ressalta a necessidade de proteção de qualquer informação pessoal por mais irrelevante que ela pareça ser, mas sob o aspecto de delimitação da gravidade dos danos relacionados ao acesso ou à divulgação indevidos de informação pessoal. Quanto mais interior for a esfera atingida, maiores serão os danos à privacidade, exigindo-se, por essa razão, maior rigor por parte do Estado na punição de tal conduta.

1.4 Panorama histórico do direito à privacidade

No século XVI, já se proclamava na Inglaterra o *princípio da inviolabilidade do domicílio*, reverberado no brocardo *man's house in his castle*. Todavia, tal proteção não se estendia a outras espécies de privacidade (física, das comunicações, *decisional* e *informacional*), o que veio a ocorrer somente no século XIX, quando essas formas de privacidade ganharam contornos de um direito autônomo. Em 1846, foi publicado na Alemanha o trabalho de David Augusto Röder, intitulado *Grundzüge des Naturrechts oder der Rechtsphilosophie,* no qual o autor definiu como atos violadores ao direito natural à vida privada, entre outros, incomodar alguém com perguntas indiscretas ou entrar num aposento sem se fazer anunciar. Em 1858, o direito à privacidade foi reconhecido pela primeira vez na França, em sede jurisprudencial, quando o Tribunal de Séné, no conhecido caso *Affaire Rachel*, reconheceu à família de uma famosa atriz o direito de não publicarem sua imagem no leito de morte[25].

O grande marco doutrinário, entretanto, só ocorreu em 1890, nos Estados Unidos da América – EUA, quando Samuel Dennis Warren e Louis Demitz Brandeis publicaram um artigo na *Harvard Law Review* intitulado *Right to privacy*. Analisando-se alguns precedentes judiciais da Suprema Corte dos EUA referentes à propriedade, direitos autorais e difamação, os autores

[25] SAMPAIO, José Adércio. **Direito à intimidade e à vida privada**: uma visão jurídica da sexualidade, da família, da comunicação e informações pessoais, da vida e da morte. Belo Horizonte: Del Rey, 1998, pp. 55-60.

concluíram que se poderia extrair das decisões até então proferidas o estatuto de um *direito geral à privacidade*. Defenderam a necessidade de reconhecimento pelas Cortes do denominado *right to privacy*: o direito de o indivíduo estar só com seus pensamentos, emoções e sentimentos, independentemente da forma de expressão (manifestos em cartas, diálogos, livros, desenhos, pinturas ou composições musicais). De outro lado, prestaram grande contribuição doutrinária, ao diferenciar o *right to privacy* da *proteção da honra,* na medida em que, enquanto esta última protege o indivíduo contra a divulgação de fatos inverídicos e maliciosos, aquele protege seu titular até mesmo contra fatos verdadeiros quando o autor não autoriza a divulgação de tais fatos na esfera do conhecimento geral. No final, os articulistas ainda concluíram que o *direito de estar só* não seria absoluto, podendo ser mitigado caso se enquadrasse em determinadas hipóteses, como nos casos de publicação de matéria de interesse geral do público; autorização legal; e, também, caso o próprio indivíduo permitisse a divulgação, pois seu consentimento faria cessar o *right to privacy*[26].

Após o avanço doutrinário e jurisprudencial, o direito à privacidade ganhou contornos internacionais ao ser reconhecido na Declaração Universal dos Direitos do Homem, aprovada em 10 de dezembro de 1948, conforme dispõe o artigo XII: "*Ninguém será objeto de ingerências arbitrárias em sua vida privada, sua família, seu domicílio ou sua correspondência, nem de ataques a sua honra ou a sua reputação. Toda pessoa tem direito à proteção da lei contra tais ingerências e ataques*"[27].

Em 1950, foi novamente previsto em documento internacional, destacando-se o art. 8º da Convenção para a Proteção dos Direitos do Homem e das Liberdades Fundamentais assinada em Roma:

> Direito ao respeito pela vida privada e familiar
> 1.Qualquer pessoa tem direito ao respeito da sua vida privada e familiar, do seu domicílio e da sua correspondência.
> 2. Não pode haver ingerência de autoridade pública no exercício desse direito senão quando esta ingerência estiver prevista na lei e constituir uma providência que, numa sociedade democrática, seja necessária para a segurança nacional, para a segurança pública, para o bem-estar econômico do país, a defesa da

[26] WARREN, Samuel; BRANDEIS, Louis D. The right to privacy. **Harvard Law Review**. Cambridge: Harvard Law Review Association, n. 193, 1890. Disponível em <http://www.louisville.edu/library/law/brandeis/privacy.html>. Acesso em: 30 jan. 2007.
[27] ONU. Declaração Universal dos Direitos do Homem. **Resolução n. 217A (III) da Assembléia Geral das Nações Unidas**. 10 de dezembro de 1948. Disponível em <http://www.mj.gov.br /sedh/ct/legis_intern/ddh_bib_inter_universal.htm>. Acesso em: 30 jan. 2007.

> ordem e prevenção das infrações penais, a proteção da saúde ou da moral o a proteção dos direitos e liberdades de terceiros.[28]

Em 1966, foi regulado pelo Pacto Internacional de Direitos Civis e Políticos, que trouxe praticamente a mesma redação da Declaração Universal dos Direitos do Homem, conforme dispõe o art. 17: "*§ 1. Ninguém poderá ser objeto de ingerências arbitrárias ou ilegais em sua vida privada, em sua família, em seu domicílio ou em sua correspondência, nem de ofensas ilegais à sua honra e reputação. § 2. Toda pessoa terá direito à proteção da lei contra essas ingerências ou ofensas*"[29].

Em 1967, o tema privacidade foi profundamente discutido por uma comissão internacional de juristas na Conferência Nórdica sobre o Direito à Intimidade, realizada em Estocolmo. A referida comissão concluiu que o direito à intimidade constituía o direito de o homem viver de forma independente a sua vida, com um mínimo de ingerência alheia, destacando-se como principais ofensas a esse direito as seguintes: (a) penetração no retraimento da solidão da pessoa, incluindo-se espreitá-la pelo seguimento, pela espionagem ou pelo chamamento constante ao telefone; (b) gravação de conversas e tomadas de cenas fotográficas e cinematográficas das pessoas em seu círculo privado ou em circunstâncias íntimas ou penosas a sua moral; (c) audição de conversações privadas por interferências mecânicas em telefone e em microfilmes dissimulados deliberadamente; (d) exploração de nome, de identidade ou de semelhanças de uma pessoa sem o seu consentimento; (e) utilização de falsas declarações, revelação de fatos íntimos, e crítica da vida das pessoas[30].

Finalmente, em 1969, o direito à privacidade foi previsto no art. 11 da Convenção Americana sobre Direito Humanos, no Pacto de São José da Costa Rica, que reproduziu novamente a redação da Declaração Universal dos Direitos do Homem[31].

Todavia, a par de todo o avanço da discussão no cenário internacional e aprovação de diversos documentos – Declaração Universal dos Direitos do Homem, Convenção Européia dos Direitos do Homem, Pacto Internacional de Direitos Civis e Políticos e Convenção Americana

---

[28] CONSELHO DA EUROPA. **Convenção para a Proteção dos Direitos do Homem e das Liberdades Fundamentais**. Roma. 4 de novembro de 1950. Disponível em <http://www.hrea.org/erc/Library/hrdocs/coe/echr_pt.pdf>. Acesso em: 30 jan. 2007.

[29] ONU. Pacto Internacional de Direitos Civis e Políticos. **Resolução n. 2200-A (XXI)**. 16 de dezembro de 1966. Disponível em <http://www.cidadevirtual.pt/cpr/asilo2/2pidcp.html> Acesso em: 30 jan. 2007.

[30] GUERRA, Sidney. Op.cit., p. 73.

[31] OEA. Pacto de San Jose da Costa Rica. **Convenção Americana sobre Direito Humanos**. 22 de novembro de 1969. Disponível em <http://www.mj.gov.br/sedh/ct/legis_intern/conv_americana_dir_humanos.htm>. Acesso em: 30 jan. 2007.

sobre Direito Humanos – verificou-se que a efetiva proteção do direito à privacidade só ocorreria mediante conscientização interna – dentro de cada país – da importância desse preceito, recomendando-se a edição de leis de abrangência nacional com aplicabilidade imediata pelo Judiciário. Quanto a este ponto, destaca-se como elucidativa a explicação de David H. Flaherty:

> Historicamente, a privacidade tratava-se de um conceito não previsto em lei, no sentido de que os indivíduos reivindicavam suas privacidades individualmente de forma mais ampla ou mais restrita, defendendo-se livremente quando havia qualquer ameaça. Essa concepção foi drasticamente alterada desde o início da industrialização no século XIX. Apesar dos esforços para manutenção da privacidade, fez-se necessária a instituição de autoridades e, ainda, a edição de leis para preservação deste direito.[32]

Seguindo a referida recomendação internacional, a Alemanha organizou, em 1957, em Düsseldorf, o 42° Congresso Jurídico, para tratar do tema privacidade, quando se elaborou um projeto de lei regulando formas de agressão cometidas na esfera da vida privada. Em 1967, tal direito foi incorporado à legislação penal alemã, que, inclusive, incluiu formas de punição, com pena de prisão de até seis meses ou multa não apenas àquele que, ilicitamente, registrasse, em gravador, quaisquer palavras proferidas por outrem em ambiente reservado, mas também aquele que ouvisse, com aparelho de escuta, quaisquer palavras proferidas por outrem nas mesmas circunstâncias, ou utilizasse ou permitisse a terceiros utilizarem registros obtidos nas referidas condições. O Código Penal alemão atual, com redação de 10 de janeiro de 1987, tipifica o crime de violação da confidencialidade da palavra, de violação de correspondência, de espionagem de dados, de violação de privacidade e de utilização de segredo alheio, sendo a antijuridicidade excluída apenas em casos de salvaguarda de interesses públicos relevantes[33].

Na Itália, o tema privacidade foi abordado em um simpósio internacional realizado em 1962, na cidade de Trento, quando foi reconhecido o direito à intimidade, com algumas limitações. Em 1963, o tema foi novamente discutido nas Jornadas Jurídicas Ítalo-Iugoslavas sobre os Direitos da Personalidade. Em 1974, acresceu-se ao Código Penal italiano, em vigor, o art. 615, destinado à tutela da intimidade, ao vedar a filmagem ou a gravação de imagens atinentes à vida privada. Nos anos seguintes, vários países, como a Áustria, a Dinamarca, a Suíça

---

[32] FLAHERTY, David H. On the utility of constitutional rights to privacy and data protection. **Case Western Reserve Law Review**, vol. 41, 1990-1991, pp. 831-855: *Historically, privacy has been largely a nonlegal concept in the sense that individuals have asserted both broad and narrow claims to individual privacy and could largely defend themselves against any challengers...This has changed dramatically since early phases of industrialization in the nineteenth century. Despite one's best-intentioned efforts to maintain privacy, the operation of external laws and authorities has became essential for its preservation*. Tradução livre.

[33] COSTA JÚNIOR, Paulo José da. Op. cit., pp. 81-82.

e Portugal, introduziram em sua legislação penal, pouco a pouco, normas para proteger a privacidade das pessoas[34].

Finalmente, após todo esse processo de proteção na esfera criminal, o direito à privacidade começou a ser incluído na legislação civil – enquanto direito da personalidade – sendo, ao final, reconhecido como direito fundamental protegido em sede constitucional. Dentre as constituições atuais, observa-se que algumas Cartas prevêem a privacidade apenas de forma genérica; em outras, a privacidade nos meios de comunicação e, por fim, há aquelas que protegem a privacidade sob esses dois aspectos e também a *privacidade informacional*, como as de Portugal, Hungria, Eslovênia e Rússia.

Ainda mais inovadora se apresenta a Constituição espanhola que além de garantir o direito à intimidade e à vida privada, a privacidade do domicílio, a privacidade das comunicações, ainda limita o uso da informática para garantir a intimidade pessoal e familiar, nos seguintes termos:

> Artículo 18.
> 1. Se garantiza el derecho al honor, a la intimidad personal y familiar y a la propia imagen.
> 2. El domicilio es inviolable. Ninguna entrada o registro podrá hacerse en él sin consentimiento del titular o resolución judicial, salvo en caso de flagrante delito.
> 3. Se garantiza el secreto de las comunicaciones y, en especial, de las postales, telegráficas y telefónicas, salvo resolución judicial.
> 4. La ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos.[35]

Diante desse cenário histórico, constata-se a rápida evolução do direito à privacidade. Uma vez reconhecido no plano internacional, aos poucos incorporou-se ao ordenamento jurídico interno de cada país – especialmente nas áreas civil e criminal – o que acarretou grande avanço doutrinário e jurisprudencial. Hoje, a maior parte dos países democráticos tutela a privacidade na própria Constituição, exceto alguns países da raiz do *common law,* como o Reino Unido, que reconhece o direito à privacidade mediante jurisprudência. Entretanto, ainda se observa a necessidade de maior avanço na tutela desse preceito, especialmente no que concerne à proteção dos dados pessoais diante das ameaças que pululam no meio da informática, tema a ser discorrido nos capítulos 3 e 4.

---

[34] COSTA JÚNIOR, Paulo José da. Op. cit., p. 84.

[35] ESPANHA. **Constituição Espanhola de 1978**. Disponível em <http://www.congreso.es/funciones/constitucion/const_espa_texto.pdf>. Acesso em 30 jan. 2007.

1.5 Privacidade e direitos da personalidade

Em conformidade com o exposto no item anterior, após previsão nos tratados internacionais de direitos humanos, lembre-se ainda uma vez, o direito à privacidade gradualmente foi sendo incorporado às legislações criminais e civis de cada país, até ser reconhecido como direito fundamental previsto na maior parte das constituições modernas. Na área civil, protege-se o direito à privacidade incluindo-o na categoria dos *direitos da personalidade* juntamente com a proteção do corpo, da honra, da imagem e do nome.

Carlos Alberto Bittar divide os *direitos da personalidade* em direitos físicos, direitos psíquicos e direitos morais. Entre os *físicos* protege-se o direito à vida, à integridade física, ao corpo e suas partes, à imagem e à voz. Entre os *psíquicos* abriga-se o direito à liberdade de pensamento, de culto, de expressão e de outras manifestações; incluem-se no mesmo nicho o direito à intimidade; o direito à integridade psíquica e o direito ao segredo. No grupo dos direitos *morais* situam-se os direitos à identidade, à honra, à reputação e o direito às criações intelectuais[36].

Independentemente da categoria em que se enquadrem – físicos, psíquicos ou morais – os *direitos da personalidade fazem incidir o foco de proteção no indivíduo em si, conferindo-lhe um direito subjetivo de exigir dos outros o respeito a seu ser, sem o que não poderia livremente desenvolver sua personalidade*. Esclarecedoras são as palavras de Jorge Miranda:

> Os direitos da personalidade são posições jurídicas fundamentais do homem que ele tem pelo simples facto de nascer e viver; são aspectos imediatos da exigência de integração do homem; são condições essenciais ao seu ser e devir; revelam o conteúdo necessário da personalidade; são emanações da personalidade humana; são direitos de exigir de outrem o respeito da própria personalidade; têm por objeto, não algo de exterior ao sujeito, mas modos de ser físicos e morais da pessoa ou bens da personalidade física, moral e jurídica ou manifestações parcelares da personalidade humana.[37]

Alguns autores mencionam que os direitos da personalidade surgiram na Idade Média, quando o homem começou a cultuar a espiritualidade; outros dizem que foi na Antiguidade clássica. Apesar das divergências quanto à origem, há consenso de que foi o cristianismo o

[36] BITTAR, Carlos Alberto. **Os direitos da personalidade**. 5ª ed. Rio de Janeiro: Forense Universitária, 2001, pp. 64-65.
[37] MIRANDA, Jorge. **Manual de direito constitucional**. 2ª ed. Coimbra: Coimbra Editora, 1998, Tomo IV, pp. 58-59.

propulsor do reconhecimento desses direitos pelo Estado, apoiado nos ideais de dignidade e de igualdade dos homens. No século XVII, a Escola do Direito Natural exaltou os direitos da personalidade, considerando-os inerentes à pessoa e preexistentes ao Estado, que deveria simplesmente reconhecê-los e respeitá-los. No século XX, tais direitos foram gradualmente introduzidos nos códigos civis e, depois, nas constituições de cada país[38].

Os direitos da personalidade são tão importantes que, caso deles o homem não pudesse dispor, todos os outros direitos subjetivos seriam irrelevantes para seu titular, o que significa que, sem a conquista dessa prerrogativa, nenhum outro direito existiria como tal. Foram instituídos com a finalidade da proteção direta da pessoa – que é o valor máximo do ordenamento – devendo ser, por esse motivo, tutelados nas diversas situações e integrados por todo o ordenamento[39].

Traçadas essas breves considerações a respeito dos direitos da personalidade, ressaltem-se suas principais características, lembrando-se que tais propriedades se aplicam também ao direito à privacidade; uma de suas espécies: são *personalíssimos* (exaurem-se na própria pessoa, embora os herdeiros em alguns casos sejam legitimados por lei para sua defesa); *gerais* (concedidos a todos); *inatos* ou *originários* (adquiridos automaticamente com o nascimento); *necessários* (indispensáveis ao desenvolvimento da personalidade humana[40]); *vitalícios*, *perenes* ou *perpétuos* (perduram por toda a vida e em alguns casos têm eficácia *post mortem*, como em questões nas quais se empresta defesa aos familiares, cite-se o caso de lesão à honra do morto[41]); *impenhoráveis* (não se admite que a penhora ou qualquer outro ato de alienação incida sobre eles[42]); *absolutos* (oponíveis *erga omnes*); *indisponíveis* (estão fora do comércio); *irreúnciáveis* (não podem ser renunciados); *imprescritíveis* (o transcurso do tempo e o eventual desinteresse do titular em nada afetam a existência e a possibilidade de gozá-los[43]); *inexpropriáveis* (não podem ser destacados da pessoa humana); *extrapatrimoniais* (não são computáveis na aferição da situação econômica de seu titular, apesar de poderem trazer alguma utilidade financeira como, por exemplo, mediante exploração da própria imagem[44]).

---

[38] BESSA, Leonardo Roscoe. Op. cit., pp. 61-64.
[39] DONEDA, Danilo César Maganhoto. Considerações iniciais sobre os bancos de dados informatizados e o direito à privacidade. In: TEPEDINO, Gustavo (Coordenador). **Problemas de direito constitucional**. Rio de Janeiro: Renovar, 2000. Disponível em: <http://www.doneda.net/pdp/docs/Consideracoes.pdf>. Acesso em: 30 jan. 2007.
[40] GOMES, Orlando. **Introdução ao direito civil**. 11ªed. Rio de Janeiro: Forense, 1995, p. 153.
[41] LÔBO, Paulo Luiz Netto. Danos morais e direitos da personalidade. **Revista Trimestral de Direito Civil**. Rio de Janeiro: Ed. Patmas, n. 6, pp. 79-97, abr./jun. 2001, p. 82.
[42] JABUR, Gilberto Haddad. **Liberdade de pensamento e direito à vida privada**. Op. cit., p. 62.
[43] JABUR, Gilberto Haddad. **Liberdade de pensamento e direito à vida privada**. Op. cit., p. 64.
[44] JABUR, Gilberto Haddad. **Liberdade de pensamento e direito à vida privada**. Op. cit., pp. 49-50.

Enquanto proteção direta do indivíduo, os direitos da personalidade decorrem do princípio da *dignidade da pessoa humana* – o princípio dileto do ordenamento jurídico. Atribui-se à *dignidade da pessoa humana* um valor espiritual e moral inerente à pessoa, que se manifesta singularmente na autodeterminação consciente e responsável da própria vida. Imbui-se da pretensão ao respeito à pessoa por parte das demais, sendo considerada um mínimo invulnerável que todo estatuto jurídico deve assegurar, de modo que apenas excepcionalmente possam ser aceitas limitações à vida privada, à intimidade, à honra e à imagem – espécies de direitos da personalidade[45]. A Constituição Federal – CF resguarda a *dignidade da pessoa humana* ao defini-la como um dos fundamentos do Estado Democrático de Direito (art. 1º, inciso III) e da proteção da família (art. 226, no § 7º); e por meio da proteção dos direitos fundamentais, que também são sua expressão. Diz-se, portanto, que o princípio da dignidade da pessoa humana atua como o epicentro axiológico do sistema pátrio, balizando tanto o direito público como o privado.

Não se estabelece divergência doutrinária a respeito do princípio da dignidade da pessoa humana como fundamento dos direitos da personalidade, considerando-se que tais direitos contemplam, como âmbito de proteção, o ser físico, o ser moral e o ser psíquico das pessoas. Todavia, muito se discute sobre o caráter dos direitos da personalidade na sociedade atual: se possuem caráter individualista ou comunitarista.

Aqueles que defendem o caráter individualista dos direitos da personalidade apregoam que o foco da proteção centra-se na pessoa em si mesma, ou seja, em seu patrimônio individual (intimidade, vida privada, honra e imagem). Aqueles que ressaltam o caráter comunitarista enfatizam que os direitos da personalidade devem eleger como foco de proteção não apenas o indivíduo em si, mas toda a coletividade, não se admitindo proteção a interesses egoístas de uma única pessoa em detrimento dos interesses de todo um grupo social.

Com o avanço do terrorismo, a corrente comunitarista conquista cada vez mais adeptos. Analisa-se a proteção da intimidade e da vida privada das pessoas não mais sob o aspecto do interesse individual de invocar-se o direito subjetivo de estar só e não ser importunado por intervenções de terceiros, mas em razão dos interesses de todo um grupo social. Revistas íntimas em aeroportos, câmeras de vigilância instaladas indiscriminadamente, interconexão de informações pessoais armazenadas em diferentes bancos de dados, preenchimento de extensos

[45] MORAIS, Alexandre de. **Direito humanos fundamentais**: teoria geral, comentários aos arts. 1º e 5º da Constituição da República Federativa do Brasil, doutrina e jurisprudência. 6ª ed. São Paulo: Atlas, 2005, p. 48.

formulários, interceptações telefônicas sem individualização dos investigados, monitoramento eletrônico, e tantas outras medidas evidenciam-se como procedimentos a que os governos recorrem para combater as organizações criminosas, cerceando, em conseqüência, a privacidade das pessoas em benefício de toda a coletividade.

Todo cidadão deve estar atento tanto para o novo cenário mundial que se descortina quanto para a necessidade de se combater com veemência a atividade ilícita em referência, que provoca a morte de tantos inocentes; entretanto, há que se ter um mínimo de razoabilidade para não se descambar para extremismos, numa irreversível aniquilação da privacidade. Deve o caráter comunitarista traduzir-se por ações em exata medida que não fulminem a privacidade – preceito tão caro à dignidade da pessoa humana e indispensável à preservação da liberdade de consciência, de crença e de expressão, bem como ao livre desenvolvimento da personalidade. O direito à privacidade e o bem jurídico *segurança pública* devem ser devidamente sopesados mediante aplicação do *princípio da proporcionalidade*, previsto expressa ou implicitamente na Constituição de todos os Estados Democráticos de Direito.

Outra recente discussão doutrinária em torno dos direitos da personalidade relaciona-se à existência ou não de um *direito geral da personalidade*. Há um direito geral da personalidade ou há direitos da personalidade? Os direitos da personalidade são *numerus apertus* ou *numerus clausus*?

Os doutrinadores que defendem a existência de um *direito geral da personalidade* entendem-no *numerus apertus*, isto é, que esse direito exibe natureza jurídica meramente enunciativa, tendo em vista a impossibilidade de previsão na legislação de todas as hipóteses de direitos inatos. Isto permite o reconhecimento de outros direitos da personalidade relacionados com a proteção da dignidade humana não previstos expressamente no ordenamento jurídico[46]. Exemplificando-se: os direitos de família puros – como o direito ao reconhecimento da paternidade e o direito aos alimentos – incluem-se entre os direitos de personalidade por apresentarem as mesmas características dos demais direitos da personalidade, embora não tenham sido previstos na legislação brasileira dentro de tal categoria[47].

De outro lado, existem autores que apregoam que os direitos da personalidade são *numerus clausus*, ou seja, que tais direitos recaem apenas sobre os *bens jurídicos expressamente*

[46] LÔBO, Paulo Luiz Netto. **Danos morais e direitos da personalidade**. Op. cit., pp. 84-85.
[47] VENOSA, Sílvio de Salvo. **Direito civil**: parte geral. 6ª ed. São Paulo: Atlas, 2006, p. 173.

previstos na legislação, não se admitindo uma interpretação elástica, sob pena de causar insegurança jurídica, ainda que o bem jurídico protegido também guarde relação com o princípio da dignidade da pessoa humana.

A primeira corrente – a que apóia a previsão *numerus apertus* – denomina-se *teoria monista* dos direitos da personalidade por defender a existência de um único *direito geral da personalidade*. A segunda – a que apregoa a previsão *numerus clausus* – nomeia-se *teoria pluralista* por defender a existência de *vários direitos da personalidade* interconectados entre si.

A *teoria pluralista* durante muito tempo preponderou por permitir uma tutela mais concreta dos direitos da personalidade ao enunciá-los separadamente. Assim, os códigos civis ao redor do mundo registram referência expressa aos direitos da personalidade, como forma de melhor protegê-los. Hoje, entretanto, discute-se novamente a questão, e a *teoria monista* ressurge em razão da complexidade do mundo moderno e da impossibilidade de previsão expressa de todos os direitos da personalidade.

Diante da controvérsia que se estabelece entre os adeptos das teorias monista e pluralista, sustenta-se a necessidade de regulamentação expressa de alguns direitos da personalidade – como fez o Código Civil – CC brasileiro nos arts. 11 a 21, facilitando a aplicabilidade pelo Judiciário – sem prejuízo de reconhecimento jurisprudencial de outros direitos relacionados com o princípio da dignidade da pessoa humana em suas projeções física, moral e psíquica, ou seja, sob fundamento da existência de um *direito geral da personalidade*.

1.6 Pessoas jurídicas de direito público e privado: privacidade e sigilo

À medida que as pessoas jurídicas se fortalecem no cenário social, alguns direitos fundamentais, antes reservados apenas às pessoas físicas, como o direito de associação, gradualmente são reconhecidos também para essas novas formações sociais. Atualmente já se discute sobre a existência ou não de um direito à privacidade de pessoas jurídicas.

Antes de se enfrentar a questão propriamente dita, ressalte-se apenas que a admissão da existência do direito à privacidade de pessoas jurídicas não deverá implicar prejuízo à liberdade das pessoas físicas que integram a organização. Assim, em nome da privacidade da pessoa

jurídica, não será legítima a aniquilação dos direitos fundamentais de membros e de empregados de uma entidade, como a liberdade de manifestação do pensamento (CF, art. 5º, inciso IV); a liberdade de consciência e de crença (CF, art. 5º, inciso VI); a liberdade de expressão da atividade intelectual, artística, científica e de comunicação (CF, art. 5º, inciso IX); a privacidade das comunicações (CF, art. 5º, inciso XII); a liberdade de exercício de qualquer trabalho, ofício ou profissão (CF, art. 5º, inciso XIII); a liberdade de associação para fins lícitos (CF, art. 5º, inciso XVII); e tantos outros previstos ao longo da Constituição. Em caso de conflito entre o direito à privacidade da pessoa jurídica e o direito à privacidade das pessoas físicas que participam da entidade, aplique-se o princípio da proporcionalidade e seus subprincípios, conforme será exposto no capítulo 2.

Superada essa premissa, parte-se para a análise da existência ou não do direito à privacidade de pessoas jurídicas. Alguns autores, entre os quais Pietro Perlingieri, posicionam-se no sentido de que o segredo, a privacidade e a informação só assumem valor existencial para as pessoas humanas, uma vez que, para pessoas jurídicas, tais atributos revestem-se de valor apenas patrimonial. O valor do sujeito pessoa física sobreexcede o valor da pessoa jurídica; assim, esta última não logra titularidade ao direito da personalidade – emanação da dignidade da pessoa humana por excelência – e, por conseqüência, nenhum amparo encontra a pessoa jurídica em sua aspiração ao direito à privacidade. O sigilo bancário das pessoas jurídicas, segundo o autor, merece ser protegido no ordenamento jurídico, mas não sob o fundamento dos direitos da personalidade[48].

Outra corrente, defendida por De Cupis e por Ariel Dotti, entende que as pessoas jurídicas têm direito à privacidade, apesar de não serem titulares dos direitos da personalidade. Ainda outra linha de entendimento, defendida por Pierre Kayser, vai mais além, ao pregar que pessoas jurídicas também exercem os direitos da personalidade, como o direito ao nome, à honra e também à privacidade[49].

Inclina-se a defesa, neste trabalho, pela corrente doutrinária que reconhece a existência do direito à privacidade de pessoas jurídicas enquanto *direito fundamental*, não se admitindo, entretanto, a classificação desse direito como um *direito da personalidade*. Embora o direito da personalidade sustente-se como um direito fundamental, nem todo direito fundamental se reveste

[48] PERLINGIERI, Pietro. **Perfis do direito civil**: introdução ao direito civil constitucional. Tradução de Maria Cristine de Cicco. Rio de Janeiro: Renovar, 1997, p. 158.
[49] SAMPAIO, José Adércio. Op. cit., pp. 214-218.

das características de direito da personalidade, como o direito que se confere às entidades associativas de representarem seus filiados, tanto judicial quanto extrajudicialmente (CF, art. 5º, inciso XXI); a função social da propriedade (CF, art. 5º, inciso XXIII); o direito à indenização em dinheiro por desapropriação por necessidade ou utilidade pública, ou por interesse social (CF, art. 5º, inciso XXIV); o caráter inafiançável e imprescritível da ação de grupos armados, civis ou militares, contra a ordem constitucional e o Estado Democrático (CF, art. 5º, inciso XLIV); entre outros.

Conforme se expôs no item anterior, os direitos da personalidade expressam o *princípio da dignidade da pessoa humana*, objetivam a proteção direta da pessoa, focalizam o indivíduo em si, enfim, atribuem a seu titular o direito subjetivo de exigir dos outros o respeito ao seu ser, humano, que, destituído de tal condição, não poderia livremente desenvolver a própria personalidade. Assim sendo, não se poderia imaginar – sem se perder a coerência teórica – a existência de um direito de personalidade de pessoa jurídica pelo simples fato de não se identificar a pessoa jurídica como *pessoa humana*. Além disso, os direitos da personalidade destacam-se pelo caráter eminentemente *extrapatrimonial*, que não se compatibiliza com a natureza das pessoas jurídicas, as quais – salvo algumas exceções, como as fundações, buscam apenas o lucro e a maior eficiência.

Tal tese, embora pareça oferecer mais consistência teórica, não foi adotada pelo legislador ordinário que – diante da controvérsia doutrinária – optou no art. 52 do novo CC, instituído pela Lei nº 10.406, de 10 de janeiro de 2002, pela extensão às pessoas jurídicas dos direitos da personalidade, nos seguintes termos: "*aplica-se às pessoas jurídicas, no que couber, a proteção dos direitos da personalidade*"[50].

A respeito dessa temática, esclarecedoras são as palavras de Danilo Doneda:

> A extensão dos direitos da personalidade às pessoas jurídicas é assunto controverso. (...) É certo que a pessoa jurídica, criada pelo homem e dotada de uma personalidade jurídica que com a dele possui semelhança, é merecedora de tutela. (...) Isto ocorre, por exemplo, na proteção do sigilo industrial ou comercial, que pode assemelhar-se, mas não coincide com o direito à privacidade; assim é com o direito ao nome comercial, cuja natureza não coincide com a do direito ao nome. No novo Código Civil, o legislador inclui os direitos da personalidade no Capítulo II do Título I, no âmbito das pessoas naturais. Posteriormente, no artigo 52, concede às pessoas jurídicas, "no que couber", a proteção dos direitos da personalidade. Cabe ao intérprete, portanto, a

[50] BRASIL. **Lei nº 10.406, de 10 de janeiro de 2002**. Disponível em: <http://www.planalto.gov.br/ccivil_03/LEIS/2002/L10406.htm>. Acesso em: 30 jan. 2007.

> delimitação do que "cabe" à pessoa jurídica. (...) Evidente é, antes de tudo, que alguns direitos da personalidade somente cabem às pessoas humanas por motivos naturais – o direito à integridade psicofísica, por exemplo, nunca caberá às pessoas jurídicas; o problema não maior não são estes casos, para cuja solução basta o bom senso [sic]. A questão se coloca com maior dificuldade em relação a interesses da pessoa jurídica que apresentam similitude com aspectos da personalidade humana. (...) A fundamentação constitucional dos direitos da personalidade e a elevação da pessoa humana ao valor máximo do ordenamento não deixam dúvidas sobre a preponderância do interesse que a ela se refere, interesse este presente na pessoa jurídica apenas de forma indireta. Uma extensão apriorística dos direitos da personalidade às pessoas jurídicas, o que infelizmente pode ser o resultado do artigo 52, passaria ao largo de qualquer consideração a este respeito, podendo chegar a comprometer a tábua axiológica constitucional. A proteção dos interesses da pessoa jurídica através de direitos da personalidade, portanto, é algo que não se adapta à trajetória e à função dos direitos da personalidade no ordenamento jurídico, e a tutela dos interesses da pessoa jurídica que apresentem semelhança com os direitos da personalidade deve ser cogitado suplementariamente [sic] e nas ocasiões em que não conflitem com direitos da personalidade, estes exclusivos da pessoa humana.[51]

Embora não se concorde com a extensão dos direitos da personalidade às pessoas jurídicas, o posicionamento em questão não impede o reconhecimento de proteção à honra, reputação, nome, marca, símbolos, propriedade intelectual, segredo, sigilo, privacidade, e assim a todas as garantias que, com o avanço do direito, fizerem-se necessárias ao desenvolvimento dessas entidades, desde que essas mesmas prerrogativas apresentem-se como *direitos fundamentais.*

A jurisprudência brasileira – com a edição da Súmula nº 227, do Superior Tribunal de Justiça - STJ[52] – pacificou o entendimento de que pessoas jurídicas podem, até mesmo, ser afetadas em sua *honra,* por meio da divulgação de informações errôneas sobre a empresa, protesto indevido de título de crédito ou publicação de escrito em jornal, conforme demonstram os acórdãos que seguem:

> EMENTA. RESPONSABILIDADE CIVIL. DANO MORAL**.** PESSOA JURÍDICA**.** POSSIBILIDADE. ENUNCIADO N. 227, SÚMULA/STJ. RECURSO DESACOLHIDO.
> Nos termos do enunciado n. 227 da súmula/STJ, a pessoa jurídica pode sofrer dano moral. Voto. Não se pode negar, a possibilidade de ocorrer ofensa ao nome

[51] DONEDA, Danilo César Maganhoto. Os direitos da personalidade no novo Código Civil. In: TEPEDINO, Gustavo (Org.). **A parte geral do novo Código Civil**: estudos na perspectiva civil-constitucional. Rio de Janeiro: Renovar, 2002. Disponível em: <http://www.buscalegis.ufsc.br/arquivos/130820061.pdf>. Acesso em: 30 jan. 2007. Grifos nossos.

[52] BRASIL. Superior Tribunal de Justiça. **Súmula nº 227**. A pessoa jurídica pode sofrer dano moral. Disponível em <http://www.stj.gov.br/SCON/pesquisar.jsp>. Acesso em: 30 jan. 2007.

> da empresa, à sua reputação, que, nas relações comerciais alcançam acentuadas proporções em razão da influência que o conceito da empresa exerce.[53]
>
> EMENTA. DANO MORAL. PESSOA JURÍDICA. PROVA DO DANO. PROTESTO INDEVIDO DE TÍTULO. SÚMULA N. 227 DA CORTE.
> 1. Está alinhada a jurisprudência da Corte no sentido de que a pessoa jurídica pode sofrer dano moral (Súmula nº 227 da Corte).
> 2. Provado o fato gerador do dano moral, no caso, o indevido protesto, impõe-se deferir a indenização.
> 3. Recurso especial conhecido e provido.[54]
>
> EMENTA. LEI DE IMPRENSA. LEGITIMIDADE ATIVA. PESSOA JURÍDICA. LEGITIMIDADE PASSIVA. EMPRESA E JORNALISTAS. VALOR DA INDENIZAÇÃO.
> 1. A pessoa jurídica pode ser atingida em sua honra objetiva e por isso tem legitimidade para promover ação de indenização por escrito publicado em jornal.
> 2. A responsabilidade pela publicação no jornal é da empresa que o explora e dos jornalistas autores da notícia.[55]
>
> EMENTA. CIVIL. RESPONSABILIDADE CIVIL. DANOS MORAIS. PESSOA JURIDICA. POSSIBILIDADE. HONRA OBJETIVA. DOUTRINA. PRECEDENTES DO TRIBUNAL.
> Recurso provido para afastar a carência da ação por impossibilidade jurídica. A evolução do pensamento jurídico, no qual convergiram jurisprudência e doutrina, veio afirmar, inclusive nesta Corte, onde o entendimento tem sido unânime, que a pessoa jurídica pode ser vítima também de danos morais, considerados esses como violadores de sua honra objetiva.[56]

Assim, admite-se a existência do direito à privacidade de pessoas jurídicas, especialmente diante da necessidade a que essas organizações se obrigam não apenas de manter suas informações estratégicas sob sigilo, mas, também, de resguardar o segredo de suas comunicações com advogados, consultores e demais especialistas que lhes prestam serviços de caráter

---

[53] BRASIL. Superior Tribunal de Justiça. RESP nº 163900/RJ. Recorrente: Pancrom Indústria Gráfica Ltda. Relator: Sálvio de Figueiredo Teixeira. Brasília, DF, 02 de março de 2000. **Diário da Justiça da República Federativa do Brasil**, Brasília, DF, 10 abr. 2000, p. 93. Disponível em <http://www.stj.gov.br/SCON/jurisprudencia>. Acesso em: 30 jan. 2007. Grifos nossos.

[54] BRASIL. Superior Tribunal de Justiça. RESP nº 538687/RS. Recorrente: BQ Administração e Serviços Ltda. Relator: Carlos Alberto Menezes Direito. Brasília, DF, 16 de dezembro de 2003. **Diário da Justiça da República Federativa do Brasil**, Brasília, DF, 29 mar. 2004, p. 237. Disponível em <http://www.stj.gov.br/SCON/jurisprudencia>. Acesso em: 30 jan. 2007. Grifos nossos.

[55] BRASIL. Superior Tribunal de Justiça. RESP nº 164421/RJ. Recorrente: O Globo Empresa Jornalística Ltda. Relator: Ruy Rosado de Aguiar. Brasília, DF, 10 de novembro de 1998. **Diário da Justiça da República Federativa do Brasil**, Brasília, DF, 16 ago. 1998, p. 73. Disponível em <http://www.stj.gov.br/SCON/jurisprudencia>. Acesso em: 30 jan. 2007. Grifos nossos.

[56] BRASIL. Superior Tribunal de Justiça. RESP nº 134993/MA. Recorrente: Indústrias Químicas do Norte S.A. Relator: Sálvio de Figueiredo Teixeira. Brasília, DF, 03 de fevereiro de 1998. **Diário da Justiça da República Federativa do Brasil**, Brasília, DF, 16 mar. 1998, p. 144. Disponível em <http://www.stj.gov.br/SCON/jurisprudencia>. Acesso em: 30 jan. 2007. Grifos nossos.

esporádico ou não. Impõe-se, por esse motivo, uma verificação da legislação vigente relacionada com a proteção da privacidade das pessoas jurídicas.

A alínea "g" do art. 482, da Consolidação das Leis do Trabalho – CLT, aprovada pelo Decreto-lei nº 5.452, de 1º de maio de 1943, dispõe que constitui justa causa para rescisão de um contrato de trabalho pelo empregador a "*violação de segredo da empresa"*, ou seja, protege a privacidade da empresa contra atos de seus próprios empregados para que não sejam reveladas, sem expressa autorização, informações estratégicas da organização.

O Código Penal – CP, aprovado pelo Decreto-lei nº 2.848, de 7 de dezembro de 1940, também protege a privacidade das pessoas jurídicas nos seguintes dispositivos:

> Art. 152 - Abusar da condição de sócio ou empregado de estabelecimento comercial ou industrial para, no todo ou em parte, desviar, sonegar, subtrair ou suprimir correspondência, ou revelar a estranho seu conteúdo:
> Pena - detenção, de três meses a dois anos.
> Parágrafo único - Somente se procede mediante representação.
> [grifos nossos]
>
> Art. 154 - Revelar alguém, sem justa causa, segredo, de que tem ciência em razão de função, ministério, ofício ou profissão, e cuja revelação possa produzir dano a outrem:
> Pena - detenção, de três meses a um ano, ou multa.
> Parágrafo único - Somente se procede mediante representação.
> [grifos nossos]

O art. 152 tutela o sigilo da correspondência comercial, tendo como sujeito ativo os sócios e os empregados do estabelecimento, e como sujeito passivo a empresa remetente ou a empresa destinatária da correspondência. O art. 154 resguarda o sigilo profissional, tendo como sujeito ativo aquele que teve conhecimento de informação secreta em razão de função, ministério, ofício ou profissão – como síndicos, diretores, advogados, engenheiros e especialistas em geral – e como sujeito passivo as pessoas físicas ou jurídicas interessadas na preservação do sigilo da informação.

O inciso XI do art. 195 da Lei nº 9.279, de 14 de maio de 1996, dispõe que pratica concorrência desleal aquele que "*divulga, explora ou utiliza-se, sem autorização, de conhecimentos, informações ou dados confidenciais, utilizáveis na indústria, comércio ou prestação de serviços, excluídos aqueles que sejam de conhecimento público ou que sejam evidentes para um técnico no assunto, a que teve acesso mediante relação contratual ou empregatícia, mesmo após o término do contrato*". O dispositivo protege a privacidade das pessoas jurídicas, no que concerne às informações sigilosas relacionadas às suas invenções,

modelos de utilidade, desenhos industriais e outras formas de propriedade intelectual, para que tais informações não sejam divulgadas por empregados ou especialistas contratados durante e após o término do vínculo trabalhista ou contratual.

De forma ainda mais explícita, o inciso VIII do art. 2º da Lei nº 7.232, de 29 de outubro de 1984, que dispõe sobre a Política Nacional de Informática, protege a privacidade das pessoas jurídicas nos seguintes termos:

> Art. 2º A Política Nacional de Informática tem por objetivo a capacitação nacional nas atividades de informática, em proveito do desenvolvimento social, cultural, político, tecnológico e econômico da sociedade brasileira, atendidos os seguintes princípios:
> .....
> VIII - estabelecimento de mecanismos e instrumentos legais e técnicos para a proteção do sigilo dos dados armazenados, processados e veiculados, do interesse da privacidade e de segurança das pessoas físicas e jurídicas, privadas e públicas;
> [grifos nossos]

Aprofundando-se mais na temática proposta, e aproveitando-se a redação do dispositivo acima quando menciona "*interesse da privacidade e de segurança das pessoas físicas e jurídicas, privadas e públicas*", depara-se com a questão não apenas da aplicabilidade ou não do direito à privacidade às pessoas jurídicas; mas também se órgãos e entidades públicas teriam direito à privacidade ou estariam sujeitos ao princípio da publicidade.

O *princípio da publicidade* consagra o dever dos órgãos públicos de manterem plena transparência de seus atos, não sendo permitido – no Estado Democrático de Direito – sigilo aos administrados a respeito de assuntos de interesse geral. Nas palavras de Hely Lopes Meirelles, em princípio todo ato administrativo deve ser publicado, porque pública é a administração que o realiza, admitindo-se sigilo apenas em casos de segurança nacional, investigações policiais ou de interesse superior da administração, a ser preservado em processo previamente declarado sigiloso nos termos da lei. O princípio da publicidade dos atos e dos contratos administrativos tem por meta propiciar conhecimento e controle de informações pelos interessados diretos e pelo povo em geral, bem como fiscalizar a atuação das condutas internas dos agentes públicos. Pareceres, ofícios, memorandos, despachos intermediários, processos administrativos, atas de reuniões,

comprovantes de despesas, prestações de contas, enfim, tudo isso é considerado *documento público* e por isso pode ser examinado e copiado na repartição por qualquer pessoa[57].

Alexandre Dias Pereira estabelece uma distinção entre *documentos públicos* e *documentos nominativos.* Os primeiros identificam aqueles de interesse da coletividade, em relação aos quais deve ser conferido amplo acesso pelo poder público em observância ao *princípio da publicidade*; os segundos abrangem aqueles que contêm informações pessoais, devendo o seu acesso ser controlado pelo Estado, sob pena de responsabilização pelos danos acarretados por indevida divulgação da informação. Assim, o poder público deve controlar as informações constantes nas bases de dados públicas, ora conferindo amplo e irrestrito acesso, ora restringindo acesso e divulgação por diversas razões, dentre as quais, a segurança nacional (informações classificadas como sigilosas), privacidade de pessoa físicas e jurídicas, preservação de direito autoral, sigilo empresarial, segredo de Justiça. O *princípio da liberdade de acesso*, apesar da larga abrangência, não se configura de forma ilimitada e incondicional, devendo submeter-se a restrições para proteção de outras garantias[58].

Nesse sentido, *todos os atos, contratos e documentos da administração pública direta e indireta, em âmbito federal, estadual, distrital e municipal, são públicos e de livre acesso e cópia por qualquer interessado, ressalvados apenas aqueles cujo acesso ou divulgação são restritos por determinação legal, a exemplo, dos documentos classificados como sigilosos por serem imprescindíveis à segurança da sociedade e do Estado e os relacionados à privacidade das pessoas físicas e jurídicas.*

Esse entendimento foi adotado pelo extinto Tribunal Federal de Recursos – TFR, em decisão que negou o pedido de *Habeas Data* ao impetrante porque a informação requisitada classificava-se como sigilosa. O relator para o acórdão, ministro Milton Pereira, fundamentou sua decisão nos dispositivos constitucionais que permitem a atribuição de sigilo às informações imprescindíveis à segurança da sociedade e do Estado*, verbis*:

> EMENTA. CONSTITUCIONAL – HABEAS DATA – CF ART. 5, LXXII, E XXXIII, ARTS. 102, I, E 105, I.
> 1. *Habeas Data:* segurança jurídica para a observância e garantia de direitos fundamentais, no aspecto da reserva legal da intimidade ou privacidade**.**

[57] MEIRELLES, Hely Lopes. **Direito administrativo brasileiro**. 25ª ed. rev. atual. São Paulo: Malheiros, 2000, pp. 87-89.
[58] PEREIRA, Alexandre Dias. Bases de dados de órgãos públicos. In: ASCENSÃO, José de Oliveira (Org.). **Direito da sociedade da informação**. Coimbra: Coimbra Ed., 2002, pp. 243-295, vol. III, pp. 271-275.

> 2. Ancorado em norma constitucional preceptiva, promana eficácia plena, como remédio assentado no direito público subjetivo, prescindindo de *interpositio legislatoris*.
> 3. Em se tratando de dado pessoal (ou personalíssimo), somente a pessoa em cujo nome constar o registro tem legitimação ativa *ad causam* ou legitimação para agir, exceção feita aos mortos, quando, então, o herdeiro legítimo ou o cônjuge supérstite poderão impetrar o *writ*.
> 4. (...).
> 5. O direito de ação relativamente ao *habeas data* nasce da negativa no fornecimento das informações, sendo indispensável a provocação de um ato gerador de conflito para atrair o provimento judicial.
> 6. Frente à cláusula do sigilo (art. 5, XXXIII, CF), por indeclinável submissão ao interesse público (segurança da sociedade e do Estado), não é absoluto o direito de acesso as informações. Compete ao judiciário examinar a alegação do sigilo, avaliando da sua procedência ou não, compatibilizando a segurança do Estado com o direito a revelação das informações pretendidas.
> 7. (...).
> 8. *Habeas data* não conhecido.[59]

Neste contexto, resgatem-se os dispositivos constitucionais que regulam a questão do sigilo na administração pública:

> Art. 5º Todos são iguais perante a lei, sem distinção de qualquer natureza, garantindo-se aos brasileiros e aos estrangeiros residentes no País a inviolabilidade do direito à vida, à liberdade, à igualdade, à segurança e à propriedade, nos termos seguintes:
> .....
> XXXIII - todos têm direito a receber dos órgãos públicos informações de seu interesse particular, ou de interesse coletivo ou geral, que serão prestadas no prazo da lei, sob pena de responsabilidade, ressalvadas aquelas cujo sigilo seja imprescindível à segurança da sociedade e do Estado;
> XXXIV - são a todos assegurados, independentemente do pagamento de taxas:
> a) o direito de petição aos Poderes Públicos em defesa de direitos ou contra ilegalidade ou abuso de poder;
> b) a obtenção de certidões em repartições públicas, para defesa de direitos e esclarecimento de situações de interesse pessoal;
> [grifos nossos]
>
> Art. 37. A administração pública direta e indireta de qualquer dos Poderes da União, dos Estados, do Distrito Federal e dos Municípios obedecerá aos princípios de legalidade, impessoalidade, moralidade, publicidade e eficiência e, também, ao seguinte:
> .....
> § 3º A lei disciplinará as formas de participação do usuário na administração pública direta e indireta, regulando especialmente:

[59] BRASIL. Tribunal Federal de Recursos. HD nº 0000001/DF. Relator para o Acórdão: Milton Pereira. Brasília, DF, 02 de fevereiro de 1989. **Diário da Justiça da República Federativa do Brasil**, Brasília, DF, 02 maio 1989. Disponível em <http://www.stj.gov.br/SCON/juritfr/doc.jsp?livre=habeas+adj+data+e+sigilo&&b=TFRC&p=true&t=&l=20&i=1> Acesso em: 30 jan. 2007. Grifos nossos.

> I - as reclamações relativas à prestação dos serviços públicos em geral, asseguradas a manutenção de serviços de atendimento ao usuário e a avaliação periódica, externa e interna, da qualidade dos serviços;
> II - o acesso dos usuários a registros administrativos e a informações sobre atos de governo, observado o disposto no art. 5º, X e XXXIII;
> III - a disciplina da representação contra o exercício negligente ou abusivo de cargo, emprego ou função na administração pública.
> [grifos nossos]

Edilsom Farias ressalta que o § 3º do art. 37 da CF foi inserido pela Emenda Constitucional – EC nº 19, de 04 de junho de 1998, com o objetivo de assegurar formas de participação do cidadão na administração pública, prevendo explicitamente o denominado *direito ao arquivo aberto*, conhecido na doutrina e na jurisprudência estrangeiras como direito ao *open file*. Este direito objetiva resguardar o *princípio da administração aberta,* que só pode ser mitigado pelo direito à honra, à intimidade, à vida privada e à imagem das pessoas, bem como pela necessidade de se protegerem matérias relativas à segurança da sociedade e do Estado. A livre informação aos administrados traduz uma mudança da administração liberal para uma nova administração emergente no século XX, calcada na idéia de *democracia participativa*, haja vista ser esta a única forma de se conferir *transparência* e *visibilidade* às atuações estatais e garantir a participação do cidadão na arena pública. A transparência do poder público permite ao cidadão controlar tanto o governo quanto a gestão da coisa pública, o que revela uma evolução mais que desejada das democracias contemporâneas em que a regra é a *publicidade* e não o segredo[60].

Analisando-se a legislação vigente, constata-se que os incisos XXXIII e XXXIV do art. 5º e o § 3º do art. 37 da CF foram regulados pela Lei nº 8.159, de 08 de janeiro de 1991, que dispõe sobre a Política Nacional de Arquivos Públicos e Privados; e pela Lei nº 11.111, de 05 de maio de 2005, que dispõe sobre o acesso aos documentos de interesse particular e aos documentos classificados no mais alto grau de sigilo, dentre outras providências. De salutar importância na normatização do tema é o art. 23 da Lei nº 8.159/91, que expressamente prevê que decreto fixará as categorias de sigilo que deverão ser observadas pelos órgãos públicos.

Onze anos após a edição da referida Lei nº 8.159/91, foi publicado o Decreto nº 4.553, de 27 de dezembro de 2002, que dispõe a respeito da salvaguarda de dados, de informações, de documentos e de materiais sigilosos de interesse da sociedade e do Estado, no âmbito da administração pública federal. Este decreto fixa quatro categorias de sigilo (ultra-secreto, secreto,

[60] FARIAS, Edilsom. **Colisão de direitos**: a honra, a intimidade, a vida privada e a imagem versus a liberdade de expressão e informação. Porto Alegre: Fabris, 1996, pp. 172-175.

confidencial e reservado); regula os procedimentos de classificação, reclassificação e desclassificação de informações sigilosas; dispõe sobre expedição, transporte e guarda dessas informações, dentre outras providências. Foi depois parcialmente modificado pelo Decreto nº 5.301, de 09 de dezembro de 2004, que regulamentou a Medida Provisória nº 228, de 09 de dezembro de 2004, convertida na Lei nº 11.111/05.

Analisando-se minuciosamente toda a legislação em vigor, *constata-se que a classificação de uma informação pública como sigilosa – por mitigar o princípio da publicidade – torna-se possível apenas quando tal ato se impuser como imprescindível à segurança da sociedade e do Estado*. Avalie-se, portanto, o disposto no Decreto nº 4.553/02, no que concerne à classificação das informações como sigilosas:

> Art. 5º Os dados ou informações sigilosos serão classificados em ultra-secretos, secretos, confidenciais e reservados, em razão do seu teor ou dos seus elementos intrínsecos.
>
> § 1º São passíveis de classificação como ultra-secretos, dentre outros, dados ou informações referentes à soberania e à integridade territorial nacionais, a planos e operações militares, às relações internacionais do País, a projetos de pesquisa e desenvolvimento científico e tecnológico de interesse da defesa nacional e a programas econômicos, cujo conhecimento não-autorizado possa acarretar dano excepcionalmente grave à segurança da sociedade e do Estado.
>
> § 2º São passíveis de classificação como secretos, dentre outros, dados ou informações referentes a sistemas, instalações, programas, projetos, planos ou operações de interesse da defesa nacional, a assuntos diplomáticos e de inteligência e a planos ou detalhes, programas ou instalações estratégicos, cujo conhecimento não-autorizado possa acarretar dano grave à segurança da sociedade e do Estado.
>
> § 3º São passíveis de classificação como confidenciais dados ou informações que, no interesse do Poder Executivo e das partes, devam ser de conhecimento restrito e cuja revelação não-autorizada possa frustrar seus objetivos ou acarretar dano à segurança da sociedade e do Estado.
>
> § 4º São passíveis de classificação como reservados dados ou informações cuja revelação não-autorizada possa comprometer planos, operações ou objetivos neles previstos ou referidos.
>
> [grifos nossos]

Observa-se que os §§ 3º e 4º do art. 5º do Decreto nº 4.553/02 violam frontalmente o inciso XXXIII do art. 5º da CF e, por conseqüência, o art. 23 da Lei nº 8.159/91 que regula esse dispositivo constitucional. O § 3º permite a classificação no grau de sigilo *confidencial* de dado ou informação "*que, no interesse do Poder Executivo e das partes, devam ser de conhecimento restrito e cuja revelação não-autorizada possa frustrar seus objetivos ou acarretar dano à*

segurança da sociedade e do Estado". A conjunção correta deveria ser *e* – e não *ou* – em razão de o permissivo constitucional para mitigação do princípio da publicidade apresentar restrita aplicação, ou seja, admite o sigilo apenas fins de segurança da sociedade e do Estado, sendo inconstitucional a parte do dispositivo que autoriza a classificação com base apenas na possibilidade de "*frustrar os objetivos do Poder Executivo e das partes*". O § 4º – de redação ainda mais nebulosa – autoriza a classificação no grau de sigilo *reservado* dos dados e informações "*cuja revelação não-autorizada possa comprometer planos, operações ou objetivos neles previstos ou referidos*", ou seja, mitiga o princípio da publicidade fora das hipóteses previstas na própria Constituição – segurança da sociedade e do Estado – bastando o "*comprometimento de planos, operações ou objetivos neles previstos ou referidos*".

Superada a questão da ilegalidade e da inconstitucionalidade do ato de classificação de uma informação como sigilosa fora dos parâmetros constitucionais, tendo em vista a vinculação do poder público aos princípios da legalidade e da publicidade, retorne-se ao questionamento do *direito à privacidade, para se verificar se tal preceito pode ser estendido aos órgãos e às entidades de caráter público.*

Conforme exposto no item 1.2, o direito à privacidade consiste em uma prerrogativa inerente a toda pessoa de constranger os outros a respeitarem sua esfera privada, bem como de controlar suas informações de caráter pessoal resistindo às intromissões indevidas provenientes de terceiros. Traduz-se, portanto, na faculdade que tem cada pessoa de obstar a intromissão de estranhos na sua intimidade e na sua vida privada, assim como de controlar informações pessoais que não deseja partilhar com outrem, evitando acesso e divulgação não autorizados. Analisando-se este conceito, observa-se que o âmbito de proteção da privacidade abrange o *controle de informações de caráter pessoal, ou seja, o controle de informações – sensíveis ou não – cujo acesso ou divulgação possa comprometer os interesses da pessoa física ou jurídica titular da garantia*.

De outro lado, verifica-se que órgãos e entidades públicos são regidos pelos princípios da legalidade, da impessoalidade, da moralidade, da publicidade, da supremacia do interesse público, da motivação, da transparência, dentre tantos outros que impedem o agente público de negar a qualquer cidadão acesso a informações constantes nos registros públicos baseado em alguma das seguintes motivações: (a) as informações são de caráter pessoal, ou melhor, institucional do órgão ou da entidade e não interessam à coletividade: as informações constantes

nos registros públicos, ressalvadas as classificadas como sigilosas na forma da lei, são consideradas públicas, devendo o acesso a tais informações ser liberado para se efetivar o controle do Estado pelos administrados; (b) o acesso ou a divulgação das informações compromete os interesses do órgão ou da entidade pública: o poder público deve buscar sempre o *interesse público primário*, ou seja, o interesse da coletividade em geral que não se confunde com o *interesse público secundário*, isto é, o interesse das pessoas estatais; (c) o acesso ou a divulgação das informações compromete interesses de agentes públicos: os princípios da moralidade e da impessoalidade impedem uso da máquina estatal para defesa de interesses pessoais dos agentes públicos; (d) as informações são classificadas como sigilosas para preservação de "interesses" do poder público: este tipo de classificação ofende o *princípio da legalidade* que deve nortear sempre o agente público, ou seja, ao contrário dos particulares, esse mesmo agente público poderá agir somente quando existir uma lei que fundamente seu ato e, neste caso, a lei exige como requisito para classificação "*que o sigilo da informação seja imprescindível à segurança da sociedade e do Estado*".

Conforme dispõe expressamente o § 1º do art. 23 da Lei nº 8.159/91 e o art. 2º da Lei nº 11.111/05, só podem ser consideradas sigilosas pelo poder público as informações relacionadas "*ao resguardo da inviolabilidade da intimidade, da vida privada, da honra e da imagem das pessoas*" e as "*imprescindíveis à segurança da sociedade e do Estado*", todas as demais são ostensivas, ou seja, podem e devem ser consultadas pelo público em geral, como um mecanismo de efetivo controle dos atos e dos contratos administrativos, bem como das condutas dos agentes públicos.

Ademais, *os órgãos e as entidades de caráter público* não podem ser titulares de direitos fundamentais, dentre os quais o direito à privacidade. As pessoas jurídicas de direito público, pertencentes da administração direta e indireta são destinatárias das normas de direitos fundamentais, mas nunca titulares. Caso contrário, ter-se-ia uma identidade entre o pólo ativo e o pólo passivo que esvaziaria por completo o sentido de tais normas[61].

Diante do exposto, atente-se para a nítida incompatibilidade entre a proteção da intimidade e da vida privada e os princípios da legalidade e da publicidade que devem nortear sempre os órgãos e entidades públicas, podendo-se concluir que *o direito à privacidade não é aplicável às pessoas jurídicas de direito público, mas tão-somente às pessoas jurídicas de direito*

[61] MARTINS, Leonardo (Org.). Op. cit., p. 169.

privado. Pelos mesmos motivos, considere-se inconstitucional o inciso VIII do art. 2º da Lei nº 7.232/84 no que concerne à proteção da "*privacidade das pessoas jurídicas públicas*". Nos órgãos e entidades públicos, por força do *princípio da transparência*, a regra é arquivos abertos ou *open file*, devendo-se resguardar sigilo apenas em excepcionais hipóteses de proteção da privacidade das pessoas físicas e das pessoas jurídicas de direito privado ou salvaguarda da segurança da sociedade e do Estado, na forma da lei.

CAPÍTULO 2 A PRIVACIDADE NA TEORIA GERAL DOS DIREITOS FUNDAMENTAIS

2.1 Explicação inicial

Traçadas as noções iniciais sobre a privacidade, impõe-se a análise e a interpretação desse direito na *teoria geral dos direitos fundamentais*, com o fito de contribuir para a construção de um novo paradigma que abranja suas múltiplas dimensões. Objetiva-se, a partir da reflexão a respeito da sociedade atual, conferir subsídios doutrinários para maior efetividade desse preceito fundamental.

Diante do extraordinário avanço tecnológico e do exponencial incremento da criminalidade que exige constantes restrições às liberdades públicas pelos governos; observa-se a silenciosa, e, ao mesmo tempo, nefasta mitigação do direito à privacidade. Nesse cenário, alguns questionamentos podem ser levantados a respeito do caráter do direito fundamental à privacidade (caráter negativo e/ou caráter positivo); da aplicabilidade dessa garantia nas relações jurídicas privadas; do papel do Estado na conformação desse preceito; da possibilidade do indivíduo renunciar a esse direito nas relações jurídicas assimétricas; da possibilidade dos empregadores monitorarem as comunicações eletrônicas dos empregados; da amplitude do âmbito de proteção desse direito fundamental; da extensão do sigilo de correspondência às comunicações por *e-mail*; da possibilidade de limitação do sigilo das comunicações e de correspondência dos presos sem autorização judicial; dos parâmetros para resolução dos conflitos entre o direito fundamental à privacidade e o direito à liberdade de expressão e de comunicação; da colisão entre o direito à privacidade e o valor constitucional segurança pública; dentre outros.

Para responder a todas essas questões e a outras que surgirem nos itens subseqüentes, impõe-se a construção de um *pré-conhecimento*[62]*,* ou seja, de uma pré-compreensão desse direito. Para isso, recorre-se à *teoria geral dos direitos fundamentais* – a chave de compreensão de toda a

[62] A hermenêutica contemporânea destaca a importância da pré-compreensão, do pré-conhecimento ou do preconceito para a interpretação de um objeto, ou seja, de um processo cognitivo para compreensão de um tema. COELHO, Inocêncio Mártires. Elementos da teoria da Constituição e de interpretação constitucional. In MENDES, Gilmar Ferreira; COELHO, Inocêncio Mártires; BRANCO, Paulo Gustavo Gonet. **Hermenêutica constitucional e direitos fundamentais**. 1ª ed. Brasília: Brasília Jurídica, 2002, pp. 15-16.

pesquisa. Apresentam-se os conceitos operacionais utilizados pelos operadores técnico-jurídicos adotados no estudo para, em seguida, adentrar-se nos questionamentos levantados diante da problemática da sociedade da informação.

2.2 Direitos fundamentais como regras e princípios

Existem duas construções acerca dos direitos fundamentais: uma estreita e exata no sentido de defender que tais direitos apresentam-se como regras, e outra, ampla e holística, que os entende como princípios[63]. Os sistemas jurídicos que compreendem os direitos fundamentais apenas como *regras* são fechados e vinculados ao *positivismo* ou ao *legalismo*; já os sistemas jurídicos que classificam os direitos fundamentais como *princípios* são abertos e vinculados ao *constitucionalismo*[64]. Diante dessa dualidade, logo no primeiro momento se percebe como a distinção entre regras e princípios é essencial para a interpretação e aplicação dos direitos fundamentais, bem como para a compreensão do sistema jurídico subjacente. Estabelecer a diferença entre regras e princípios se apresenta como o próximo passo deste trabalho.

Tanto as regras como os princípios situam-se entre espécies do gênero normas jurídicas, daí falar-se em *normas-regra* e *normas-princípio*, conforme as peculiaridades do dispositivo. A distinção, no âmbito do superconceito norma, entre regras e princípios é tarefa particularmente complexa, mas de crucial importância no estudo dos direitos fundamentais. Gomes Canotilho sugere a adoção de alguns critérios para efetuar tal distinção:

> a) Grau de abstração: os *princípios* são normas com um grau de abstração relativamente elevado; de modo diverso, as *regras* possuem uma abstração relativamente reduzida.
>
> b) Grau de determinabilidade na aplicação do caso concreto: os *princípios*, por serem vagos e indeterminados, carecem de mediações concretizadoras (do legislador, do juiz), enquanto as *regras* são suscetíveis de aplicação direta.
>
> c) Carácter de fundamentalidade no sistema das fontes de direito: os *princípios* são normas de natureza estruturante ou com um papel fundamental no ordenamento jurídico devido à sua posição hierárquica no sistema das fontes

[63] ALEXY, Robert. Direitos fundamentais, ponderação e racionalidade. Tradução de Luís Afonso Heck. **Revista de Direito Privado**, São Paulo: RT, n. 24, pp. 334-343, out./dez. 2005, pp. 334-337.
[64] QUEIROZ, Cristina M. M. **Direitos fundamentais**: teoria geral. Coimbra: Coimbra Editora, 2002, p. 127.

(ex: princípios constitucionais) ou à sua importância estruturante dentro do sistema jurídico (ex: princípio do Estado de Direito).

d) Proximidade da idéia de direito: princípios são "*standards*" juridicamente vinculantes radicados nas exigências de "justiça" (Dworkin) ou na "idéia de direito" (Larenz); as *regras* podem ser vinculativas com um conteúdo meramente funcional.

e) Natureza normogenética: os *princípios* são fundamento das *regras*, isto é, são normas que estão na base ou constituem a *ratio* de regras jurídicas, desempenhando, por isso, uma função normogenética fundamentante.[65]

Adotando-se tais critérios – apenas em nível exemplificativo – identificam-se na Carta Constitucional brasileira alguns direitos fundamentais que se configuram como *regras* (aplicáveis através do mecanismo de *subsunção*[66]) e outros que se configuram como *princípios* (aplicáveis através do mecanismo de *ponderação*[67]). Diante da alta densidade normativa e da possibilidade de aplicação direta, reconhecem-se como *normas-regra* os seguintes dispositivos do art. 5º: VII[68], XIX[69], XXI[70], XXV[71], XXVI[72], XLII[73], XLIII[74], XLIV[75], LXX[76]. De outro lado, verificado o alto

[65] CANOTILHO, José Joaquim Gomes. **Direito constitucional e teoria da Constituição**. 7ª ed. Coimbra: Almedina, 2003, pp. 1160-1161.

[66] Subsunção é o ato de subordinação do fato à norma pelo juiz no momento da resolução do caso concreto. Trata-se de ato de participação criadora do juiz na interpretação e aplicação da norma jurídica. In REALE, Miguel. **Lições preliminares de direito**. 21ª ed. São Paulo: Saraiva, 1994, p. 298.

[67] Ponderação é o ato de balanceamento de valores e interesses. Ponderar é sopesar, balancear, atribuir peso. In CANOTILHO, José Joaquim Gomes. **Direito constitucional e teoria da Constituição**. Op. cit., p. 1161.

[68] "*Art. 5º VII - é assegurada, nos termos da lei, a prestação de assistência religiosa nas entidades civis e militares de internação coletiva*;" In BRASIL. **Constituição da República Federativa do Brasil de 1988**. São Paulo: Revista dos Tribunais, 2004.

[69] "*Art. 5º XIX - as associações só poderão ser compulsoriamente dissolvidas ou ter suas atividades suspensas por decisão judicial, exigindo-se, no primeiro caso, o trânsito em julgado*;" In BRASIL. **Constituição da República Federativa do Brasil de 1988**. Op. cit.

[70] "*Art. 5º XXI - as entidades associativas, quando expressamente autorizadas, têm legitimidade para representar seus filiados judicial ou extrajudicialmente*;" In BRASIL. **Constituição da República Federativa do Brasil de 1988**. Op. cit.

[71] "*Art. 5º XXV - no caso de iminente perigo público, a autoridade competente poderá usar de propriedade particular, assegurada ao proprietário indenização ulterior, se houver dano*;" In BRASIL. **Constituição da República Federativa do Brasil de 1988**. Op. cit.

[72] "*Art. 5º XXVI - a pequena propriedade rural, assim definida em lei, desde que trabalhada pela família, não será objeto de penhora para pagamento de débitos decorrentes de sua atividade produtiva, dispondo a lei sobre os meios de financiar o seu desenvolvimento*;" In BRASIL**. Constituição da República Federativa do Brasil de 1988**. Op. cit.

[73] "*Art. 5º XLII - a prática do racismo constitui crime inafiançável e imprescritível, sujeito à pena de reclusão, nos termos da lei*;" In BRASIL. **Constituição da República Federativa do Brasil de 1988**. Op. cit.

[74] "*Art. 5º XLIII - a lei considerará crimes inafiançáveis e insuscetíveis de graça ou anistia a prática da tortura, o tráfico ilícito de entorpecentes e drogas afins, o terrorismo e os definidos como crimes hediondos, por eles respondendo os mandantes, os executores e os que, podendo evitá-los, se omitirem*;" In BRASIL. **Constituição da República Federativa do Brasil de 1988**. Op. cit.

grau de generalidade e abstração, a necessidade de mediações concretizadoras (do legislador e/ou do juiz) e a fundamentalidade, identificam-se como *normas-princípio* os seguintes incisos: I (princípio da igualdade entre homens e mulheres)[77]; II e XXXIX (princípio da legalidade)[78]; III (princípio da dignidade da pessoa humana)[79]; IV e IX (princípio da liberdade de expressão e de comunicação)[80]; VI (princípio da liberdade de consciência e crença)[81]; XIII (princípio da liberdade de profissão)[82]; XVII e XX (princípio da liberdade de associação)[83]; XXIII (princípio da função social da propriedade)[84]; XXXII (princípio da defesa do consumidor)[85]; XL (princípio da irretroatividade da lei penal não benéfica)[86]; XLVI (princípio da individualização da pena)[87]; LIV (princípio do devido processo legal)[88]; LV (princípio do contraditório e da ampla defesa)[89]; e

---

[75] "*Art. 5º XLIV - constitui crime inafiançável e imprescritível a ação de grupos armados, civis ou militares, contra a ordem constitucional e o Estado Democrático*;" In BRASIL. **Constituição da República Federativa do Brasil de 1988**. Op. cit.

[76] "*Art. 5º LXX - o mandado de segurança coletivo pode ser impetrado por: a) partido político com representação no Congresso Nacional; b) organização sindical, entidade de classe ou associação legalmente constituída e em funcionamento há pelo menos um ano, em defesa dos interesses de seus membros ou associados*;" In BRASIL. Constituição da República Federativa do Brasil de 1988. Op. cit.

[77] "*Art. 5º I - homens e mulheres são iguais em direitos e obrigações, nos termos desta Constituição*;" In BRASIL. **Constituição da República Federativa do Brasil de 1988**. Op. cit.

[78] "*Art. 5º II - ninguém será obrigado a fazer ou deixar de fazer alguma coisa senão em virtude de lei; XXXIX - não há crime sem lei anterior que o defina, nem pena sem prévia cominação legal*;" In BRASIL. **Constituição da República Federativa do Brasil de 1988**. Op. cit.

[79] "*Art. 5º III - ninguém será submetido a tortura nem a tratamento desumano ou degradante*;" In BRASIL. **Constituição da República Federativa do Brasil de 1988**. Op. cit.

[80] "*Art. 5º IV - é livre a manifestação do pensamento, sendo vedado o anonimato; IX - é livre a expressão da atividade intelectual, artística, científica e de comunicação, independentemente de censura ou licença*;" In BRASIL. **Constituição da República Federativa do Brasil de 1988**. Op. cit.

[81] "*Art. 5º VI - é inviolável a liberdade de consciência e de crença, sendo assegurado o livre exercício dos cultos religiosos e garantida, na forma da lei, a proteção aos locais de culto e a suas liturgias*;" In BRASIL. **Constituição da República Federativa do Brasil de 1988**. Op. cit.

[82] "*Art. 5º XIII - é livre o exercício de qualquer trabalho, ofício ou profissão, atendidas as qualificações profissionais que a lei estabelecer*;" In BRASIL. **Constituição da República Federativa do Brasil de 1988**. Op. cit.

[83] "*Art. 5º XVII - é plena a liberdade de associação para fins lícitos, vedada a de caráter paramilitar; XX - ninguém poderá ser compelido a associar-se ou a permanecer associado*;" In BRASIL. **Constituição da República Federativa do Brasil de 1988**. Op. cit.

[84] "*Art. 5º XXIII - a propriedade atenderá a sua função social*;" In BRASIL. **Constituição da República Federativa do Brasil de 1988**. Op. cit.

[85] "*Art. 5º XXXII - o Estado promoverá, na forma da lei, a defesa do consumidor*;" In BRASIL. **Constituição da República Federativa do Brasil de 1988**. Op. cit.

[86] "*Art. 5º XL - a lei penal não retroagirá, salvo para beneficiar o réu*;" In BRASIL. **Constituição da República Federativa do Brasil de 1988**. Op. cit.

[87] "*Art. 5º XLVI - a lei regulará a individualização da pena e adotará, entre outras, as seguintes: a) privação ou restrição da liberdade; b) perda de bens; c) multa; d) prestação social alternativa; e) suspensão ou interdição de direitos*;" In BRASIL**. Constituição da República Federativa do Brasil de 1988**. Op. cit.

[88] "*Art. 5º LIV - ninguém será privado da liberdade ou de seus bens sem o devido processo legal*;" In BRASIL. **Constituição da República Federativa do Brasil de 1988**. Op. cit.

[89] "*Art. 5º LV - aos litigantes, em processo judicial ou administrativo, e aos acusados em geral são assegurados o contraditório e ampla defesa, com os meios e recursos a ela inerentes*;" In BRASIL. **Constituição da República Federativa do Brasil de 1988**. Op. cit.

LVII (princípio da presunção de inocência)[90]. Entretanto, depara-se com a complexidade da distinção entre *regras* e *princípios* ao se enfrentar uma *zona cinzenta* em que alguns dispositivos do art. 5º ora se parecem com regras, ora se parecem com princípios, a depender da análise do caso concreto em exame.

Robert Alexy e Ronald Dworkin destacam-se como os grandes marcos doutrinários na construção da moderna concepção de um *sistema jurídico aberto e constitucionalista* em oposição a um *sistema jurídico fechado e positivista ou legalista*. O *sistema fechado* apresenta-se exclusivamente formado por *regras* aplicáveis por meio da técnica da *subsunção*, o que exige uma disciplina legislativa ininterrupta e exaustiva, daí falar-se em *legalismo jurídico*. A vantagem deste sistema é que, ao reservar um diminuto espaço para complementação pelos órgãos julgadores, acaba por conferir maior *segurança jurídica*, ou seja, menor divergência entre as decisões judiciais; a desvantagem é que não logra preencher as infinitas lacunas que se abrem, justamente por ser humanamente impossível prever todas situações de litígio que podem surgir.

O *sistema aberto* – como apregoam Alexy e Dworkin – compõe-se tanto de *regras* como de *princípios*. Não se apóia apenas em *regras*, porque, se assim fosse, o sistema apresentaria tantas lacunas que difícil seria imaginá-lo como apto a resolver os problemas concretos; de outro lado, também não é composto somente de *princípios*, uma vez que, desta forma, seria extremamente indeterminado, abalando-se a *segurança jurídica*.

Alexy distingue as regras dos princípios primordialmente pela maior generalidade e abstração destes em comparação àquelas, ou seja, os princípios têm alto grau de generalidade, enquanto as regras têm baixo grau. Além desta diferença de caráter quantitativo, outra distinção mais importante de conotação qualitativa se impõe: os princípios são normas que ordenam que algo seja realizado da melhor forma possível, dentro das possibilidades fáticas e jurídicas existentes, isto é, são *mandados de otimização*; enquanto, as regras só podem ser cumpridas na *medida do tudo-ou-nada*[91].

Nesse sentido, a aplicabilidade dos princípios distingue-se da aplicabilidade das regras: enquanto estas são aplicadas na *medida do tudo-ou-nada*; os princípios são aplicados na *medida do possível*. Na condição de *mandados definitivos*, as regras ou são cumpridas ou não são

---

[90] "*Art. 5º LVII - ninguém será considerado culpado até o trânsito em julgado de sentença penal condenatória*;" In BRASIL. **Constituição da República Federativa do Brasil de 1988**. Op. cit.

[91] ALEXY, Robert. **Teoria de los derechos fundamentales**. Tradução de Ernesto Garzón Valdés. Madrid: Centro de Estúdios Políticos y Constitucionales, 1997, pp. 86-87.

cumpridas, não se submetendo à *ponderação*, mas sim à *subsunção*. Já os princípios submetem-se à técnica da *ponderação*, isto é, decide-se em favor daquele que tem um peso relativamente maior, sem que o princípio descartado seja excluído ou ignorado do ordenamento jurídico, como ocorreria se houvesse um conflito entre regras. Nesse sentido, os princípios – enquanto *mandados de otimização* – são mais ou menos satisfeitos, o que permite seu cumprimento em variados graus. Quanto maior for o grau de cumprimento de um princípio, menor será o grau de cumprimento do princípio oposto[92].

Para Dworkin a diferença entre regras e princípios não é de *natureza quantitativa* e *qualitativa*, mas sim de *natureza lógica*. Regras apresentam em sua estrutura lógica uma hipótese e uma conseqüência determinadas, ou seja, descrevem situações e imputam resultados específicos. Assim, quando duas regras colidem, a solução deve dar-se pelo abandono de uma delas ou o estabelecimento de uma regra de exceção, pois funcionam na base do *tudo-ou-nada*, ou seja, uma delas deve ser considerada inválida e a outra válida. Para tal aferição, o juiz coteja uma regra com outras, em criteriosa seleção, como a que determina a precedência da regra promulgada por autoridade superior, da promulgada mais recentemente ou da mais específica. Já os princípios têm caráter aberto e não pretendem reger situações de aplicação, de modo que, em caso de tensão entre dois princípios, não há perda da validade de um deles, apenas se aplica o princípio mais adequado para regular o caso concreto[93].

Dworkin ressalta, ainda, que os princípios, por se revestirem de alto grau de abstração, dispensam corporificação em dispositivos legais, bastando a apresentação de argumentos em favor dos direitos fundamentais. Quando princípios se entrecruzam, o árbitro deve sopesar a força relativa de cada um deles. Já as regras são sempre corporificadas em dispositivos legais e aplicadas a *maneira do tudo-ou-nada*: dados os fatos, ou a regra é aplicável ou não é aplicável, ou é válida ou não é válida. Embora a teoria se coloque em tais termos, em muitos casos é difícil estabelecer se um dispositivo é uma regra ou é um princípio[94], conforme se demonstrou nos exemplos citados acima.

A teoria de Alexy, apesar de inovadora, foi muito criticada por Klaus Günter e Jürguen Habermas, justamente por considerar os princípios como *mandados de otimização*, ou seja,

---

[92] ALEXY, Robert. Direitos fundamentais no Estado Constitucional Democrático. Tradução de Luís Afonso Heck. **Revista de Direito Administrativo**, Rio de Janeiro: Renovar, n. 217, jul./set. 1999, pp. 64-65.
[93] DWORKIN, Ronald. **Levando os direitos à sério**. Tradução de Nelson Boeira. São Paulo: Martins Fontes, 2002, pp. 41-43.
[94] DWORKIN, Ronald. Op. cit., pp. 35-45.

preceitos que podem ser mais ou menos satisfeitos. Segundo os autores, considerar os princípios como *mandados de otimização* permite que sejam cumpridos em variados graus conforme a vontade do órgão julgador; subordinando a competência do Legislativo, de conformar os direitos fundamentais mediante legislação ordinária, à jurisdição constitucional, ou seja, à interpretação do Judiciário. Alexy rebate a crítica alertando que não ocorrerá preponderância da jurisdição constitucional em relação à atividade do Legislativo porque os direitos fundamentais de feição negativa e com previsão de *restrição expressamente constitucional* (reserva legal simples e reserva legal qualificada)[95] sempre se submeterão à discricionariedade do legislador no momento em que forem regulamentados. Os direitos fundamentais de caráter positivo, de outro lado, deixam ao legislador a tarefa de eleger os meios mais adequados para se chegar ao fim almejado, restando sempre uma margem de decisão ao Legislativo[96].

Superado esse embate teórico-doutrinário, ressalte-se que, apesar do esforço para se estabelecer distinção entre normas-regra e normas-princípio, tal tarefa não se propõe a evidenciar que estas sejam hierarquicamente superiores àquelas. De acordo com o *princípio da unidade da Constituição*, aceito de forma majoritária em diferentes ordenamentos jurídicos, inexiste hierarquia entre normas constitucionais, independentemente de sua espécie[97]. Todas as normas contidas em uma Constituição têm igual dignidade, não se estabelecendo hierarquia de supra-infra-ordenação entre os mesmos dispositivos, sejam eles *regras* ou *princípios*. Apesar de se defender neste trabalho a inexistência de hierarquia entre as diferentes espécies de normas constitucionais em razão da aplicabilidade do *princípio da unidade da Constituição*, não se pode ignorar o esforço de parte da doutrina que adota a denominada *teoria da hierarquização de princípios constitucionais*.

O Tribunal Constitucional Federal alemão criou uma escala de valores entre os direitos fundamentais como forma de facilitar a resolução dos eventuais conflitos entre esses preceitos: 1) a dignidade da pessoa humana é considerada um valor superlativo e por isso não pode ser contrapesada em face de outros valores ou bens constitucionalmente protegidos; 2) os direitos

[95] Direitos fundamentais sujeitos a restrições expressamente constitucionais são aqueles subordinados a limitações previstas pela própria Constituição. Este tema será abordado detalhadamente nos itens 2.9 e 2.10.
[96] ALEXY, Robert. **Epílogo a la teoria de los derechos fundamentales**. Tradução de Carlos Bernal Pulido. Madrid: J. San José, 2004, pp. 33-35.
[97] BARROSO, Luís Roberto. **Interpretação e aplicação da Constituição**: fundamentos de uma dogmática constitucional transformadora. 5ª ed. rev. atual. ampl. São Paulo: Saraiva, 2003, p. 203.

fundamentais subtraídos ao poder de revisão por cláusula pétrea preponderam em relação aos outros valores ou bens constitucionalmente protegidos[98].

Na Constituição brasileira, caso se adotasse tal teoria, seria possível ventilar a preponderância em abstrato de dois princípios: *dignidade da pessoa humana* e *justiça social.* A respeito da prevalência do princípio da dignidade humana no ordenamento jurídico pátrio, observa o ministro Gilmar Ferreira Mendes:

> Embora o texto constitucional brasileiro não tenha privilegiado especificamente determinado direito, na fixação de cláusulas pétreas (CF, art. 60, IV), não há dúvida de que, também entre nós, os valores vinculados ao princípio da dignidade humana assumem peculiar relevo (CF, art. 1º, III). Assim, devem ser levados em conta, em eventual juízo de ponderação os valores que constituem inequívoca expressão desse princípio (inviolabilidade de pessoa humana, respeito à integridade física e moral, inviolabilidade do direito de imagem e da intimidade).[99]

Outro postulado que poderia ser ventilado caso se defendesse a *teoria da hierarquização de princípios constitucionais* seria o da preponderância dos *direitos fundamentais relativos às pessoas* em face dos relativos a *valores de índole material*. Entretanto não se recomenda a hierarquização dos princípios constitucionais pela melhor doutrina; primeiro, porque não existe princípio absoluto – conforme será exposto no próximo item –, segundo, porque a adoção de tal concepção levaria à afronta o *princípio da unidade da Constituição*.

Com base no que foi até agora exposto, ressalta-se a relevância da distinção entre regras e princípios como forma de facilitar a interpretação dos dispositivos constitucionais, em especial dos direitos fundamentais. As *regras* se impõem como mandados definitivos e, nesse sentido, possuem as seguintes características: alta densidade normativa; baixo grau de abstração e generalidade; sujeitas à aplicação direta; natureza exclusivamente funcional; aplicáveis por subsunção; cumpridas na medida do tudo-ou-nada (ou são cumpridas ou não são cumpridas); e subordinadas à verificação de validade pelo órgão julgador. Os *princípios*, de outro lado, são mandados de otimização, possuindo os seguintes atributos: baixa densidade normativa; alto grau de abstração e generalidade; sujeitos à aplicação indireta por carecerem de mediações concretizadoras do legislador e/ou do juiz; natureza estruturante dentro do sistema jurídico (constituem a *ratio* das regras jurídicas); aplicáveis por ponderação; cumpridos dentro das

[98] QUEIROZ, Cristina M. M. Op. cit., p. 206.
[99] MENDES, Gilmar Ferreira. **Direitos fundamentais e controle de constitucionalidade**: estudos de direito constitucional. 3ª ed. rev. e ampl. São Paulo: Saraiva, 2004, p. 95. Grifos nossos.

possibilidades fáticas e jurídicas existentes, e não sujeitos à verificação de validade pelo órgão julgador.

Para efeito deste estudo, e recorrendo-se às premissas teóricas apresentadas, o sistema jurídico brasileiro apresenta-se como um *sistema aberto e constitucionalista*, comportando tanto *normas-regra* como *normas-princípio*, conforme bem demonstrado por meio da análise do art. 5º da CF. Assim, enquanto as normas-regras implementam a segurança jurídica do ordenamento jurídico, as normas-princípio abrem espaço para a livre complementação e desenvolvimento do sistema por meio da jurisdição constitucional.

Nesse contexto, protege-se o *direito à privacidade que se configura ora como norma-regra, ora como norma-princípio – a depender do caso concreto em exame*. A privacidade do domicílio e a privacidade das comunicações – previstas nos incisos XI e XII do art. 5º da CF[100] – mais se parecem com regras diante da alta densidade normativa, do baixo grau de abstração e da possibilidade de aplicação imediata. De outro lado, também se configuram como princípios ao se contatar que as garantias se estendem para além das hipóteses expressamente previstas nos dispositivos constitucionais como a inviolabilidade da "casa" e do sigilo de correspondência e das comunicações telegráficas e telefônicas, abrangendo outras espécies de domicílio e de comunicações, conforme será analisado no item 2.8.

O inciso X do art. 5º da CF[101], de outro lado, mais se parece com uma norma-princípio, diante do elevado grau de abstração e generalidade, embora seja passível de aplicação direta quanto à sua parte final que prevê a possibilidade de "indenização por dano material ou moral decorrente de sua violação". Enfim, a análise dependerá de cada caso concreto, apresentando-se o direito à privacidade tanto como norma-regra como uma norma-princípio. Essa perspectiva é de particular importância no desenvolvimento da temática apresentada, devendo nortear os operadores técnico-jurídicos na interpretação e aplicação desse direito fundamental, em especial na resolução dos conflitos com outros preceitos constitucionais.

---

[100] "*Art. 5º XI - a casa é asilo inviolável do indivíduo, ninguém nela podendo penetrar sem consentimento do morador, salvo em caso de flagrante delito ou desastre, ou para prestar socorro, ou, durante o dia, por determinação judicial; XII - 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*;". In BRASIL. **Constituição da República Federativa do Brasil de 1988**. Op. cit.

[101] "*Art. 5º X - são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação*;" In BRASIL. **Constituição da República Federativa do Brasil de 1988**. Op. cit.

2.3 Caráter relativo dos direitos fundamentais

Consoante o exposto no item anterior, os direitos fundamentais podem ser classificados ora como regras, ora como princípios. Entretanto, independentemente da forma como se apresentam, esses preceitos não são absolutos, possuem *caráter relativo*, ou seja, sujeitam-se às restrições impostas pelo próprio legislador – no momento de sua conformação normativa – ou pelo juiz, ao serem invocados em ação judicial, conforme será detalhado no item 2.9 deste capítulo.

Norberto Bobbio observa que, entre os direitos fundamentais, bem raros são aqueles que não entram em *concorrência com outros direitos fundamentais*, que não são *suspensos em determinadas circunstâncias* ou que não são *negados a determinadas categorias de pessoas*, por isso diz-se que não possuem *caráter absoluto*[102].

Analisando a Constituição brasileira, identificam-se – mesmo em abstrato – possíveis colisões entre direitos fundamentais, o que demonstra a necessidade de se admitir seu caráter relativo como a única forma de resolução dos conflitos nos casos concretos. A concorrência pode incidir entre direitos fundamentais: (a) *de igual conteúdo, mas de diferentes titulares*: a exemplo da vida do feto *versus* vida da mãe, no caso de solicitação de autorização para realização de aborto, quando a gravidez é de risco para a gestante; (b) *de conteúdo diverso de diferentes titulares*: exemplificando-se pela liberdade de comunicação *versus* direito à privacidade, quando há solicitação ao Judiciário da ordem de proibição de vinculação de determinada notícia que revele assuntos relacionados à intimidade ou à vida privada de alguém, ou pela liberdade de expressão *versus* direito à honra e à imagem; (c) *de igual ou diferente conteúdo de sujeitos individuais e coletivos*: a exemplo do livre acesso aos registros públicos *versus* segurança da sociedade e do Estado, quando há classificação de informações como sigilosas sob fundamento de garantia da segurança nacional, ou privacidade *versus* saúde pública na obrigatoriedade de vacinação em áreas endêmicas.

Em conformidade com o que leciona Norberto Bobbio, o caráter relativo dos direitos fundamentais torna-se evidente também quando se verifica a possibilidade de suspensão de tais

[102] BOBBIO, Norberto. **A era dos direitos**. 19ª Reimpressão. Tradução de Carlos Nelson Coutinho. Rio de Janeiro: Elsevier, 1992. p. 40.

direitos em determinadas circunstâncias. No ordenamento jurídico nacional, como se pode constatar, prevê-se suspensão do direito de reunião e do direito à privacidade em estado de defesa, conforme disposto no § 1º do art. 136: "*§ 1º - O decreto que instituir o estado de defesa determinará o tempo de sua duração, especificará as áreas a serem abrangidas e indicará, nos termos e limites da lei, as medidas coercitivas a vigorarem, dentre as seguintes: I - restrições aos direitos de: a) reunião, ainda que exercida no seio das associações; b) sigilo de correspondência; c) sigilo de comunicação telegráfica e telefônica; II - ocupação e uso temporário de bens e serviços públicos, na hipótese de calamidade pública, respondendo a União pelos danos e custos decorrentes*".

Por fim, ainda seguindo o raciocínio do autor, verifica-se que alguns direitos fundamentais são considerados relativos por contemplarem apenas determinadas categorias de pessoas, excluindo-se os demais indivíduos; o que se pode demonstrar pelos seguintes dispositivos da Constituição brasileira: direitos dos trabalhadores urbanos e rurais que não são aplicáveis aos desempregados e àqueles que vivem na economia informal (arts. 7º a 11); direitos políticos por serem aplicáveis apenas aos alistáveis e elegíveis (art. 14); direito de amparo às crianças e aos adolescentes carentes que não são aplicáveis aos adultos e aos afortunados (art. 203, inciso II); direito ao benefício social mensal aos deficientes e idosos carentes por serem aplicáveis apenas a essas minorias (art. 203, inciso V); dentre outros.

Norberto Bobbio complementa sua idéia de *ilusionismo do caráter absoluto dos direitos fundamentais* com o seguinte argumento: a história demonstra que os direitos fundamentais formam uma classe variável no tempo e no espaço. Direitos que foram declarados absolutos e invioláveis no final do século XVIII, como a *propriedade*, foram submetidos a radicais limitações nas declarações contemporâneas; direitos que as declarações do século XVIII nem sequer mencionavam, como os *direitos sociais*, são agora proclamados com grande ostentação nas recentes declarações. No futuro poderão emergir novas pretensões, inimagináveis no momento, como o direito de respeitar a vida dos animais. Assim, não existem direitos fundamentais "por natureza"; o que parece "fundamental" em uma época histórica e em uma determinada civilização não se afigura "fundamental" em outras épocas e em outras culturas[103].

Cristina Queiroz ressalta que os direitos fundamentais se relacionam com a noção de "perigo", sendo variáveis ao longo do tempo e do espaço, à medida que surgem novas ameaças

[103] BOBBIO, Norberto. Op. cit., p. 38.

ao homem e ao cidadão. Os direitos fundamentais variam no espaço, isto é, segundo o "Estado Constitucional"; e no tempo, ou seja, de acordo com o período histórico no que concerne à distribuição de papéis do Estado no desenvolvimento jurídico. Não existe *numerus clausus* de direitos fundamentais, assim como não existe *numerus clausus* dos perigos, daí a origem da expressão "proteção dinâmica dos direitos fundamentais", utilizada pelo Tribunal Constitucional Federal alemão, o que corresponde a uma tutela flexível, móvel e aberta e que tais garantias abarcam[104]. Assim, o caráter relativo dos direitos fundamentais desponta como uma medida necessária à "realização cooperativa" desses preceitos, isto é, necessária à conformação desses mesmos preceitos, segundo as exigências da sociedade e em observância às novas ameaças que surgirem.

Apesar da essencialidade e da fundamentalidade nos ordenamentos jurídicos, conclui-se que os *direitos fundamentais têm, intrinsecamente, caráter relativo*; submetendo-se às restrições impostas pelo Legislativo – no momento da conformação legislativa – e pelo Judiciário – no momento da resolução dos casos concretos. Essas restrições ocorrem especialmente em caso de colisão com outros direitos fundamentais – de igual conteúdo de diferentes titulares ou de conteúdo diverso de diferentes titulares – ou com outros valores constitucionais. São também considerados relativos por excluírem determinadas categorias de pessoas em alguns casos especiais e por serem variáveis no tempo e no espaço.

2.3.1 Caráter relativo do direito à privacidade na jurisprudência nacional

Embora o texto constitucional brasileiro resguarde o direito à privacidade, observa-se na jurisprudência a freqüente mitigação desse preceito fundamental diante da necessidade de preservação de outros interesses que logram preponderar, o que demonstra o caráter relativo do direito à privacidade.

Um dos interessantes casos relaciona-se com a *privacidade física*, isto é, com o direito de o indivíduo ter seu corpo protegido contra procedimentos invasivos não autorizados. Reclamação, em tais termos, foi ajuizada no STF pela extraditanda *Glória de Los Ángeles Treviño Ruiz,* ao

[104] QUEIROZ, Cristina M. M. Op. cit., pp. 48-50.

tomar conhecimento – alguns dias antes do parto de seu filho – da ordem judicial para realização, à sua revelia, da coleta de material da placenta, com o propósito de se averiguar a paternidade do nascituro. Invocou violação ao direito à intimidade e à vida privada de sua própria pessoa e de seu filho, sustentando que a medida só poderia ser adotada após sua prévia autorização. Nos autos constou informação de que a ordem judicial para a realização de tal exame destinava-se à comprovação da inocência de servidores do Departamento de Polícia Federal – DPF, acusados de estupro pela extraditanda, ocorrência consumada durante o período em que a reclamante se encontrava em cárcere sob custódia daquele órgão. No mérito, o Tribunal manteve a decisão judicial de primeira instância para realização do exame, sob o fundamento de que o direito à privacidade não se impõe como um direito absoluto, devendo ceder quando em colisão com a necessidade de se salvaguardar a moralidade administrativa e a segurança pública, bem como a imagem de policiais federais acusados pela reclamante de estupro, *verbis*:

> EMENTA. RECLAMAÇÃO. RECLAMANTE SUBMETIDA AO PROCESSO DE EXTRADIÇÃO Nº 783, À DISPOSIÇÃO DO STF.
> 2. Coleta de material biológico da placenta, com propósito de se fazer exame de DNA, para averiguação de paternidade do nascituro, embora a oposição da extraditanda.
> 3. Invocação dos incisos X e XLIX do art. 5º, da CF/88.
> 4. Ofício do Secretário de Saúde do DF sobre comunicação do Juiz Federal da 10ª Vara da Seção Judiciária do DF ao Diretor do Hospital Regional da Asa Norte - HRAN, autorizando a coleta e entrega de placenta para fins de exame de DNA e fornecimento de cópia do prontuário médico da parturiente.
> 5. Extraditanda à disposição desta Corte, nos termos da Lei nº 6.815/80. Competência do STF, para processar e julgar eventual pedido de autorização de coleta e exame de material genético, para os fins pretendidos pela Polícia Federal.
> 6. Decisão do Juiz Federal da 10ª Vara do Distrito Federal, no ponto em que autoriza a entrega da placenta, para fins de realização de exame de DNA, suspensa, em parte, na liminar concedida na Reclamação. Mantida a determinação ao Diretor do Hospital Regional da Asa Norte, quanto à realização da coleta da placenta do filho da extraditanda. Suspenso também o despacho do Juiz Federal da 10ª Vara, na parte relativa ao fornecimento de cópia integral do prontuário médico da parturiente.
> 7. Bens jurídicos constitucionais como "moralidade administrativa", "persecução penal pública" e "segurança pública" que se acrescem – como bens da comunidade, na expressão de Canotilho – ao direito fundamental à honra (CF, art. 5°, X), bem assim direito à honra e à imagem de policiais federais acusados de estupro da extraditanda, nas dependências da Polícia Federal, e direito à imagem da própria instituição, em confronto com o alegado direito da reclamante à intimidade e a preservar a identidade do pai de seu filho.
> 8. Pedido conhecido como reclamação e julgado procedente para avocar o julgamento do pleito do Ministério Público Federal, feito perante o Juízo Federal da 10ª Vara do Distrito Federal.

> 9. Mérito do pedido do Ministério Público Federal julgado, desde logo, e deferido, em parte, para autorizar a realização do exame de DNA do filho da reclamante, com a utilização da placenta recolhida, sendo, entretanto, indeferida a súplica de entrega à Polícia Federal do "prontuário médico" da reclamante.[105]

Outro caso de relevo na jurisprudência do STF – também relacionado à *privacidade física* – refere-se à submissão do réu em ação de investigação de paternidade ao exame de DNA contra sua vontade. O relator para o acórdão, ministro Maurício Côrrea, entendeu inexistir, na espécie, violação ao direito à privacidade que deveria ceder diante do interesse do menor e do Estado de verem reconhecida a paternidade, decorrência lógica do direito à dignidade da pessoa humana, à filiação, ao respeito e à convivência familiar. É o que se lê na seguinte passagem de seu voto:

> Por outro lado, tenho como de exagerado rigor e flagrante improcedência o argumento do recorrido de que a norma ordinária fere o princípio constitucional assegurado no inciso X do art. 5º relativamente à intimidade, à vida privada, à imagem e à honra das pessoas. Tal preceito, como se sabe, deve ser entendido com temperamento, sobretudo quando se põe em jogo a vida do menor que merece da ação estatal o amparo indispensável. (...) O direito à intimidade não pode consagrar a irresponsabilidade paterna, de forma a inviabilizar a imposição ao pai biológico dos deveres resultantes de uma conduta volitiva e passível de gerar vínculos familiares. De qualquer sorte, essa garantia encontra limites no direito da criança e do Estado em ver reconhecida, se for o caso, a paternidade.[106]

Mais um julgado curioso relaciona-se com a questão da *privacidade informacional,* que tem em seu âmbito de proteção as informações atinentes a determinada pessoa e o controle das mesmas informações pelo próprio titular. Trata-se da decisão prolatada pelo STJ, em sede do Recurso Ordinário em Mandado de Segurança – RMS, interposto por *Waldemiro Hauck* para contestar acórdão que denegou a ordem impetrada contra decisão do juízo federal, o qual autorizou a quebra de sigilo bancário requerida pelo Ministério Público – MP. O relator para o acórdão, ministro Luiz Fux, entendeu que a quebra para fins de investigação de suspeita de crime financeiro não viola a privacidade do impetrante, porque o sigilo bancário não é um direito absoluto, literalmente:

---

[105] BRASIL. Supremo Tribunal Federal. Reclamação nº 2040/DF. Recorrente: Glória de Los Ángeles Treviño Ruiz. Relator: Néri da Silveira. Brasília, DF, 21 de fevereiro de 2002. **Diário da Justiça da República Federativa do Brasil**, Brasília, DF, 27 jun. 2003, p. 00031. Disponível em <http://www.stf.gov.br/jurisprudencia/nova/pesquisa.asp>. Acesso em: 30 jan. 2007. Grifos nossos.

[106] BRASIL. Supremo Tribunal Federal. RE nº 248869/SP. Recorrente: Ministério Público Estadual. Relator: Maurício Côrrea. Brasília, DF, 07 de agosto de 2003. **Diário da Justiça da República Federativa do Brasil**, Brasília, DF, 12 mar. 2004, p. 00038. Disponível em <http://www.stf.gov.br/jurisprudencia/nova/pesquisa.asp>. Acesso em: 30 jan. 2007. Grifos nossos.

> EMENTA. RECURSO ORDINÁRIO. MINISTÉRIO PÚBLICO. SIGILO BANCÁRIO. DIREITO RELATIVO. SUSPEITA DE CRIME FINANCEIRO.
> 1. A suspeita de crime financeiro, calcado em prova de lesividade manifesta, autoriza a obtenção de informações preliminares acerca de movimentação bancária de pessoa física ou jurídica determinada por autoridade judicial com o escopo de instruir inquérito instaurado por órgão competente.
> 2. A quebra do sigilo bancário encerra um procedimento administrativo investigatório de natureza inquisitiva, diverso da natureza do processo, o que afasta a alegação de violação dos Princípios do Devido Processo Legal, do Contraditório e da Ampla Defesa.
> 3. O sigilo bancário não é um direito absoluto, deparando-se ele com uma série de exceções previstas em lei ou impostas pela necessidade de defesa ou salvaguarda de interesses sociais mais relevantes. (Vide §§ 3º e 4º do art. 1º e art. 7º da Lei Complementar 105/2001)
> 4. Recurso ordinário improvido.[107]

Tendo relacionado todos esses julgados, torna-se possível verificar algumas hipóteses em que se restringe o direito à privacidade diante do conflito com outros direitos fundamentais ou com outros valores constitucionalmente protegidos; ressaltando-se apenas que esta avaliação pode ser realizada tão-somente pelo Judiciário na resolução de casos concretos, ou pelo Legislativo no momento da conformação do direito fundamental mediante lei ordinária.

2.4 Dimensões subjetiva e objetiva dos direitos fundamentais

2.4.1 Noção inicial

Os direitos fundamentais possuem duas dimensões: uma subjetiva que será explorada nos próximos itens; e uma objetiva que será delineada no item 2.4.3.

A *dimensão subjetiva* dos direitos fundamentais corresponde à característica desses direitos de conferir ao seu titular a pretensão de exigir de alguém – do Estado e dos demais particulares – um determinado comportamento em seu favor. Nas palavras de Paulo Gonet Branco: "*Nessa perspectiva, os direitos fundamentais correspondem à exigência de uma ação*

[107] BRASIL. Superior Tribunal de Justiça. RMS nº 15146/SC. Recorrente: Waldemiro Hauck. Relator: Luiz Fux. Brasília, DF, 18 de março de 2003. **Diário da Justiça da República Federativa do Brasil**, Brasília, DF, 07 abr. 2003, p. 223. Disponível em <http://www.stj.gov.br/SCON/jurisprudencia>. Acesso em: 30 jan. 2007. Grifos nossos.

negativa (em especial, de respeito ao espaço de liberdade do indivíduo) ou positiva de outrem, e, ainda, correspondem a competências – em que não se cogita de exigir comportamento ativo ou omissivo de outrem, mas do poder de modificar-lhe as posições jurídicas"[108].

A *dimensão objetiva* dos direitos fundamentais, de outro lado, significa que tais direitos representam a essência do Estado Democrático de Direito, operando tanto como limite quanto como diretriz para a atuação do poder público. Os direitos fundamentais, em sua dimensão objetiva, representam os valores a serem perseguidos pelo Estado, porque representam a base de todo o ordenamento jurídico[109].

Em breves linhas: os direitos fundamentais, em sua *dimensão subjetiva*, produzem efeitos sobre as relações jurídicas das pessoas físicas e jurídicas com o Estado e com os demais particulares; em sua *dimensão objetiva*, produzem efeitos sobre toda a ordem jurídica, dirigindo e vinculando o Executivo, o Legislativo e o Judiciário por meio dos valores que protegem.

2.4.2 Dimensão subjetiva

2.4.2.1 Caráter negativo e caráter positivo dos direitos fundamentais

Em sua *dimensão subjetiva,* o mesmo direito fundamental pode assumir tanto um caráter negativo como positivo. Focando-se o *caráter negativo*, o direito fundamental atribui ao seu titular o direito de exigir do Estado uma abstenção de intervenção na sua esfera jurídica, ou seja, impõe ao poder público o dever de não agredir a esfera jurídica do cidadão[110]. Pelo *caráter positivo*, o Estado deve criar condições fáticas e jurídicas para o exercício do direito fundamental, bem como proteger seu titular de agressões provenientes de terceiros.

---

[108] BRANCO, Paulo Gustavo Gonet. Aspectos da teoria geral dos direitos fundamentais. In MENDES, Gilmar Ferreira; COELHO, Inocêncio Mártires; BRANCO, Paulo Gustavo Gonet. **Hermenêutica constitucional e direitos fundamentais**. Brasília: Brasília Jurídica, 2002, p. 152.
[109] BRANCO, Paulo Gustavo Gonet. Op. cit., p. 153.
[110] CANOTILHO, José Joaquim Gomes. **Estudos sobre direito fundamentais**. Coimbra: Coimbra Editora, 2004, p. 76.

O *caráter negativo* dos direitos fundamentais relaciona-se com a *teoria liberal do estado de direito burguês*, defendida por Carl Schmitt, na qual o Estado deve respeitar a esfera jurídica do cidadão, não assumindo, entretanto, nenhum dever para a realização das liberdades públicas. Essa teoria foi superada pela *teoria do estado social,* que enfatiza o *caráter positivo* dos direitos fundamentais, ao demonstrar que, para se atingir a liberdade real, em contraposição à liberdade meramente jurídica, impõe-se uma série de prestações estatais. A liberdade de imprensa, entendida conforme a *teoria do estado social*, fundamenta a obrigação estatal de propiciar condições econômicas que incentivem a pluralidade de empresas do setor de comunicação; a liberdade de culto exige do Estado a criação das bases econômicas para a existência das comunidades religiosas[111].

A respeito do aspecto positivo dos direitos fundamentais, leciona Ernst-Wolfgang Böckenförde:

> Si los derechos fundamentales de libertad co-garantizan los pressupuestos sociales de su posibilidad de ser realizados como pretensión inmediata de derecho fundamental, la libertad religiosa significa al mismo tiempo la responsabilización del Estado por la base económica existencial da las comunidades religiosas; la libertad de prensa, la obligación estatal de mantener los pressupuestos económicos de la pluralidad de la prensa (mediante protección de la competencia, subvenciones, entre otras cosas); la libertad de sindicación, la finaciación estatal de los sindicatos; la libre elección de los centros de enseñanza, la obligacion estatal de proveer suficientes titulaciones educativas para los deseos profesionales individuales, sean o no necessarias.[112]

A *teoria do estado social* muda a concepção de que os direitos fundamentais são direitos de caráter negativo voltados exclusivamente às agressões do Estado, ou seja, supera a visão restritiva dos direitos fundamentais. O paradigma do *Welfare State*, destaca uma nova teoria dos direitos fundamentais, a denominada *teoria institucional dos direitos fundamentais*, segundo a qual os direitos fundamentais, para serem efetivos, precisam ser protegidos institucionalmente e enriquecidos por atos normativos que lhes ofereçam direção, segurança, conteúdo e função. As leis, contrariando a concepção da *teoria liberal do estado de direito burguês*, ao invés de limitarem os direitos fundamentais, servem para concretizá-los. Ressalte-se que a *teoria institucional dos direitos fundamentais* se aplica tanto em relação aos direitos fundamentais de

[111] BÖCKENFÖRDE, Ernst-Wolfgang. **Escritos sobre derechos fundamentales**. Tradução de Juan Luis Requejo Pagés e Ignacio Villaverde Menéndez. Baden-Baden: Nomos, 1993, pp. 63-64. Grifos nossos.
[112] BÖCKENFÖRDE, Ernst-Wolfgang. Op. cit., pp. 78-79. Grifos nossos.

caráter expressamente institucional, como em relação aos direitos fundamentais em geral, especialmente aqueles relacionados com a liberdade[113].

Segundo o paradigma do *Welfare State*, o legislador deixa de ser um inimigo dos direitos fundamentais e passa a ser diretamente responsável por sua efetividade na sociedade civil. O Estado, na condição de principal protetor dos direitos fundamentais, obriga-se a criar instituições e remodelar as já existentes, pois mesmo os direitos individuais de matriz liberal exigem a atuação estatal. Por fim, o poder público tem o dever de assegurar proteção em face de ameaças a direitos fundamentais provenientes de outros particulares ou de Estados estrangeiros[114].

Konrad Hesse ressalta o importante papel do legislador no processo de concretização dos direitos fundamentais:

> Para poder tornar-se eficazes, a maioria dos direitos fundamentais carece da organização jurídica das condições de vida e âmbitos de vida que eles devem garantir. Essa organização é, em primeiro lugar, tarefa da legislação. Ela pode assentar-se em um encargo constitucional expresso, que obriga o legislador a regular os "pormenores". (...) Ela torna clara, em medida especial, que o legislador, a quem essa organização incumbe preferência, não só pode ser considerado como inimigo dos direitos fundamentais, mas que no âmbito dos direitos fundamentais, cabe a ele uma tarefa positiva.[115]

A partir do paradigma do duplo caráter dos direitos fundamentais, surge a seguinte classificação: direitos fundamentais como *direitos de defesa*, *direitos a prestação* e *direitos de proteção*. A função de *direitos de defesa* é cumprida sob dupla perspectiva: constituem normas de competência negativa para os poderes públicos, proibindo a ingerência de tais poderes na esfera individual e, de outro lado, implicam o poder de exigir omissões do Estado. Cumpre-se a função de *direitos a prestação* ao se conferir ao particular o direito de obter algo por meio do poder público. Por fim, a função de *direitos de proteção* é exercida quando seus titulares exigem do Estado uma proteção perante terceiros, exemplificando-se pelo direito à inviolabilidade de domicílio, direito de proteção de dados informáticos, direito de associação, dentre outros[116].

---

[113] BÖCKENFÖRDE, Ernst-Wolfgang. Op. cit., pp. 53-54.
[114] SARMENTO, Daniel. Op. cit., pp. 161-162.
[115] HESSE, Konrad. **Elementos de direito constitucional da República Federal da Alemanha**. Tradução de Luís Afonso Heck. Porto Alegre: Sergio Antonio Fabris, 1998, pp. 247-248. Grifos nossos.
[116] CANOTILHO, José Joaquim Gomes. **Direito constitucional e teoria da Constituição**. Op. cit., pp. 408-409.

2.4.2.2 A teoria dos quatro status de Jellinek

A classificação dos direitos fundamentais como direitos de defesa, direitos a prestação ou direitos de proteção, ressaltando-se no primeiro caso seu caráter negativo e nos demais seu caráter positivo, decorre da chamada *dimensão subjetiva* dos direitos fundamentais. Conforme exposto no item 2.4.1, por *dimensão subjetiva* entende-se a característica dos direitos fundamentais de ensejarem uma pretensão jurídica perante o Estado e os demais particulares, ou seja, o direito que cabe ao titular de exigir uma ação negativa ou positiva de alguém.

Coube ao alemão Georg Jellinek sistematizar na doutrina a dimensão subjetiva dos direitos fundamentais, em obra intitulada *Sistema dos direitos públicos subjetivos* (*System der subjecktiv öffentlichen Rechte*), na qual desenvolveu a conhecida *teoria dos quatro status.* Segundo essa teoria, os direitos fundamentais asseguram aos indivíduos quatro espécies de estados jurídicos em relação ao Estado: passivo, negativo, positivo e ativo.

Jellinek descreve *status* como um elemento que caracteriza a relação jurídica entre o indivíduo e o Estado, conferindo ao primeiro uma posição de sujeito de deveres ou titular de direitos diante do poder público. Ao ser reconhecido como membro de uma comunidade, o indivíduo adquire uma personalidade que, teoricamente, apresenta-se como uma relação que o qualifica dentro do Estado. Essa personalidade evidencia uma situação jurídica, um status, a que se pode vincular um dever ou um direito[117].

O *status passivo* ou *status subjetionis* recebe de Jellinek um tratamento com relativa brevidade. Impõe ao indivíduo uma subordinação aos poderes estatais, posicionando-o como mero detentor de deveres e não de direitos perante o Estado. A relação jurídica é de sujeição aos mandamentos e às proibições do Estado, caracterizando-se pela ausência de liberdade individual. Esse status cessa apenas caso o Estado perca a competência de impor deveres aos indivíduos. Ocorrendo qualquer mudança do Estado; afeta-se o status, mas este continua existindo. Assim, diz-se que as obrigações impostas podem variar conforme ocorram mudanças no Estado; entretanto, o status passivo continua perene, apesar de sofrer algumas alterações[118].

---

[117] JELLINEK, Georg. System der Subjektiven Öffentlichen Rechte, 1919, pp. 83-84 apud GAVARA DE CARA, Juan Carlos. **Derechos fundamentales y desarollo legislativo**: la garantia del contenido esencial de los derechos fundamentales em la Ley Fundamental de Bonn. Madrid: Centro de Estudios Constitucionales, 1994, p. 233.
[118] ALEXY, Robert. **Teoria de los derechos fundamentales**. Op. cit., pp. 248-250.

Gavara de Cara ressalta que o *status passivo*, ao impor ao indivíduo uma submissão ao Estado, sinaliza o abandono da concepção jusnaturalista da liberdade pré-estatal. A soberania do Estado aniquila a liberdade e a autodeterminação do indivíduo, que se subordina aos mandamentos do poder público. Essa soberania, entretanto, revela-se limitada, pois só pode ser exercida para atender aos interesses da coletividade, devendo-se respeitar a esfera do indivíduo na qual ele é senhor absoluto, uma esfera em que o Estado não pode intervir, pois não haveria interesse jurídico para a coletividade. A essa esfera de liberdade, ambiente em que não pode haver intervenção estatal, Jellinek denomina *status negativo*[119].

O *status negativo* corresponde à esfera em que o indivíduo circula livre diante do Estado, ao qual não se submete. O poder estatal juridicamente se limita, devendo respeitar a liberdade do indivíduo cuja conduta não afete a coletividade. Os fins estritamente pessoais encontram a correspondente satisfação no exercício da liberdade individual que precisa ser resguardada. Assim, o status negativo abrange atos dos cidadãos que não afetem o Estado, ou seja, os atos que não provocam efeitos juridicamente relevantes. Jellinek classifica como juridicamente irrelevantes os atos que não são nem ordenados nem proibidos, quando se permite tanto sua omissão quanto sua comissão. Assim, diz-se que o status negativo vincula as autoridades que não podem proibir nem impor conduta aos súditos sem fundamento legal[120].

O *status negativo,* ao corresponder à esfera de liberdade do indivíduo em face do Estado, encontra-se em situação de contradição com o *status passivo* que, ao vincular o indivíduo a determinadas prestações estatais, coloca-o em posição de sujeição ou de subordinação em relação ao poder público. Nesse sentido, o status negativo resguarda a liberdade do indivíduo perante o Estado, por ser sua ação juridicamente irrelevante para a comunidade, relacionando-se diretamente à liberdade em sentido kantiano. Para Kant a diferença entre *direito* e *moral* é que o primeiro regula as condutas externas, enquanto a segunda, as condutas internas. O status negativo de Jellinek resguarda as ações que são irrelevantes para o direito, protegendo a liberdade do indivíduo e devolvendo-lhe a opção pela moral de Kant[121].

Sob uma perspectiva mais moderna – distante do paradigma de atos irrelevantes para a comunidade – como ressaltou Jellinek, verifica-se que o *status negativo* confere uma garantia ao indivíduo em face do legislador ordinário, visto que este só pode restringir a liberdade do cidadão

[119] GAVARA DE CARA, Juan Carlos. Op. cit., pp. 233-234.
[120] ALEXY, Robert. **Teoria de los derechos fundamentales**. Op. cit., pp. 251-253.
[121] GAVARA DE CARA, Juan Carlos. Op. cit., pp. 235-236.

nos estritos limites da Constituição. Esta idéia se relaciona com o estudo das restrições aos direitos fundamentais, que só podem ser limitados pela própria Constituição (restrição expressa diretamente constitucional), por lei ordinária, quando houver autorização constitucional (restrição expressa indiretamente constitucional) ou quando houver autorização implícita à restrição pela identificação dos denominados limites imanentes (restrições implícitas)[122].

Assim, diz-se que a limitação ao direito fundamental pode ser feita pela própria Constituição ou pelo legislador ordinário ou pelo órgão julgador diante das autorizações constitucionais. A autorização constitucional pode ser expressa, prevendo-se explicitamente a edição de lei para a conformação do direito fundamental (restrição indiretamente constitucional com reserva legal simples ou qualificada); ou implícita, quando se edita uma lei para sanar eventual conflito entre o direito individual e outro direito fundamental ou outro bem constitucionalmente protegido (restrição implícita ou tácita). Este tema será aprofundado nos itens 2.9 e 2.10.

Prosseguindo na teoria dos quatro status, Jellinek se refere ao terceiro status como *status positivus* – também denominado *status civitatis*. Este status assegura ao indivíduo a possibilidade não apenas de utilizar-se das instituições estatais, mas também de exigir que o Estado adote determinadas ações positivas. Significa que o indivíduo pode exigir prestações positivas do Estado, impondo ações estatais para resguardo de seus interesses individuais. Apresenta-se como um reflexo do *status negativo* ao outorgar ao indivíduo a pretensão de exigir uma ação estatal, enquanto este outorga a pretensão de uma omissão estatal. De outro lado, forma uma relação de mão dupla com o *status passivo*: pelo status positivo, o Estado deve prestações ao cidadão; pelo status passivo, o indivíduo deve obrigações ao Estado[123].

Por fim, o quarto status, denominado *status activus*, garante ao indivíduo o direito de participar ativamente da formação da vontade do Estado. Corresponde à cidadania ativa do indivíduo, exemplificando-se pelo direito de votar e de participar como membro da organização estatal. Também está relacionado com os demais status, pois a participação do indivíduo no Estado pode decorrer tanto de uma obrigação (*status passivo*), a exemplo do serviço militar obrigatório, como de um direito (*status positivo*), a exemplo do sufrágio[124].

---

[122] Este tema será abordado com profundidade no item 2.9.
[123] ALEXY, Robert. **Teoria de los derechos fundamentales**. Op. cit., pp. 256-257.
[124] ALEXY, Robert. **Teoria de los derechos fundamentales**. Op. cit., p. 260.

Analisando a teoria dos quatro status de Jellinek, Peter Häberle destaca, dentro do status ativo, o denominado *status ativo processual,* segundo o qual o Estado tem que gerar mecanismos procedimentais para exercício dos direitos fundamentais. O *direito de acesso à informação* evidencia esse status ao requerer tanto a regulamentação de procedimentos para seu exercício em órgãos públicos como também a disponibilização das informações nos meios de comunicação de massa com rádio e televisão. Objetiva-se, pelo reconhecimento do *status ativo processual*, fomentar a criação de uma sociedade aberta de intérpretes da Constituição em que se garanta o pluralismo mediante participação de todos, resguardada pela regulamentação dos procedimentos[125].

O *status ativo processual* – enquanto espécie do gênero status ativo – relaciona-se diretamente com o status positivo, na medida em que confere ao indivíduo o direito de exigir prestações do Estado, embora se tinja de uma conotação política mais forte, quando ressalta a necessidade de o poder público implementar procedimentos que fomentem, no seio da comunidade, a necessidade da participação popular na interpretação das normas constitucionais.

2.4.2.3 A classificação pelo critério funcional

Com base na *teoria dos quatro status* de Jellinek, a doutrina moderna classifica os direitos fundamentais pelo *critério funcional*, ou seja, *identifica as funções que os direitos fundamentais assumem diante do poder do Estado,* dividindo-os em dois grandes grupos: direitos fundamentais como *direitos de defesa* e direitos fundamentais como *direitos a prestação*. Alguns doutrinadores ainda mencionam outra subclassificação: *direitos de participação*. Os *direitos de defesa* correspondem ao *status negativo*; os *direitos a prestação* relacionam-se com o *status positivo*; por fim, os *direitos de participação* refletem o *status ativo*. Os direitos de defesa se relacionam com o status negativo porque colocam o indivíduo em posição de defesa contra as intromissões estatais na sua esfera de liberdade. Os direitos a prestação vinculam-se ao status positivo por conferirem ao indivíduo situação jurídica de sujeito de direitos perante o Estado que lhes deve uma atuação

[125] HÄBERLE, Peter. **Pluralismo y Constitución**: estudios de teoría constitucional de la sociedad abierta. Tradução de Emilio Mikunda. Madrid: Tecnos, 2002, p. 194.

positiva. Por fim, os direitos de participação refletem o status ativo por garantirem a participação do cidadão na organização do Estado.

A classificação pelo critério funcional, largamente adotada pelos constitucionalistas, foi concebida sob diferentes modelos. *Alexy divide os direitos fundamentais em dois grandes grupos: direitos de defesa e direitos a prestação.* Os direitos a prestação abrangem os *direitos prestacionais em sentido amplo* (direitos de proteção e direitos à organização e ao procedimento) e os *direitos prestacionais em sentido estrito,* que correspondem aos direitos sociais. Pereira Farias, de forma diversa, divide os direitos fundamentais em três grupos: *direitos de defesa, direitos a prestação* e *direitos de participação*. Para este autor, os direitos a prestação encontram-se subdivididos em prestações jurídicas e prestações materiais, enquanto os direitos de participação correspondem aos direitos políticos[126].

A classificação em três categorias, adotada por Pereira Farias e concebida pelo próprio Georg Jellinek, foi rechaçada por alguns doutrinadores, os quais constataram que a subclassificação dos direitos de participação, correspondente aos direitos políticos, na verdade cuida de categoria mista, agregando elementos dos direitos de defesa e elementos dos direitos a prestação. Assim, tal duplicidade de funções não justifica o enquadramento dos direitos políticos em grupo distinto, podendo ser ora classificados como direitos de defesa ora como direitos a prestação dependendo de sua conformação[127]. Constatadas as divergências entre os dois modelos, adota-se no presente trabalho a classificação binária de Alexy a qual se analisa a seguir.

Os *direitos de defesa* caracterizam-se por impor ao Estado um dever de abstenção, um dever de não interferência e de não intromissão. Correspondem aos direitos fundamentais de *primeira geração,* que surgiram no cenário histórico do Estado Liberal Burguês como uma forma de limite aos poderes do soberano. Estão relacionados principalmente com a proteção da vida e da propriedade e com as liberdades individuais, tais como, liberdade pessoal de pensamento, de religião e de profissão, mostrando uma vertente da doutrina do direito natural. Têm por titular o indivíduo e são oponíveis ao Estado, traduzindo-se como faculdades ou como atributos da pessoa de se opor ou de resistir ao poder estatal, ostentando elevado grau de subjetividade. Valorizam primeiro o homem-singular, o homem das liberdades abstratas, o homem da sociedade mecanicista que compõe a chamada sociedade civil. Além de entrarem na categoria do *status negativo* de

[126] SARLET, Ingo Wolfgang. **A eficácia dos direitos fundamentais**. 4ª ed. rev. atual. ampl. Porto Alegre: Livraria do Advogado Editora, 2004, p. 174.
[127] SARLET, Ingo Wolfgang. Op. cit., p. 174.

Jellinek, ressaltam a nítida separação entre a sociedade e o Estado, aquilatando o caráter antiestatal das liberdades públicas[128].

Portanto, pode-se dizer que os *direitos de defesa objetivam a limitação do Estado*, evitando os abusos cometidos pelos poderes públicos e assegurando ao indivíduo uma esfera de liberdade. Outorgam um direito subjetivo que permite ao seu titular objetar interferências indevidas no âmbito de proteção do seu direito fundamental, ou, mesmo, eliminar manifestações que agridam a esfera de sua autonomia pessoal. Assim, os direitos de defesa estão voltados contra os atos dos poderes públicos que têm obrigação de abstenção e dever de respeito aos interesses individuais; exigindo-se a omissão de ingerências e a intervenção na esfera de liberdade pessoal apenas em determinadas hipóteses e sob certas condições. Entretanto, essa função defensiva dos direitos fundamentais não implica a exclusão total do Estado, mas apenas a formalização e a limitação dessa intervenção, no sentido da vinculação da ingerência por parte dos poderes públicos a determinadas condições e pressupostos de natureza material e procedimental, de forma que a intervenção atenda a limitações ditadas pela própria Constituição[129].

Enquanto pretensões negativas, os direitos de defesa possuem quatro atributos, traduzidos como: (a) *não impedimento da prática de determinado ato*, vedam interferências estatais no âmbito de liberdade dos indivíduos e, sob esse aspecto, constituem normas de competência negativa para os poderes públicos ao proibirem que o Estado impeça a ação do indivíduo, exemplificando-se pela liberdade de manifestação da fé, pela livre expressão da opinião e pela liberdade de profissão; (b) *não-intervenção em relação a posições subjetivas*, protegem os indivíduos contra ações do próprio Estado e também dos particulares que interferirem em suas posições subjetivas, exemplificando-se pela proteção da vida, pela proibição de violação de domicílio e pela inviolabilidade da intimidade e da vida privada; (c) *não-eliminação de posições jurídicas*, traduzem a obrigação do Estado de não derrogar regulamentações jurídicas necessárias à proteção de algum direito fundamental, exemplificando-se pela proibição do Estado de extinguir a regulamentação sobre a propriedade e a herança; (d) *faculdade de não fruir posições previstas na norma*, garantem ao titular de um direito fundamental a faculdade de não exercer determinado poder; exemplificando-se pelo direito de não se reunir, embora detentor do direito de se reunir, e de não se associar, embora detentor do direito de livre associação[130].

---

[128] BONAVIDES, Paulo. **Curso de direito constitucional**. 13ª ed. São Paulo: Malheiros, 2003, p. 563.
[129] SARLET, Ingo Wolfgang. Op. cit., pp. 180 e s.
[130] BRANCO, Paulo Gustavo Gonet. Op. cit., pp. 141-142.

Os *direitos a prestações, de outro lado, exigem uma ação positiva por parte do Estado* a fim de criar os pressupostos fáticos necessários ao exercício efetivo dos direitos fundamentais. Na relação jurídica, correspondem a uma obrigação de fazer ou de dar. Assim, o titular do direito fundamental dispõe de pretensão a prestações por parte do Estado, sejam estas de caráter legislativo, sejam de caráter administrativo, vedando-se a omissão estatal. Correspondem aos direitos fundamentais de *segunda geração*, referindo-se principalmente aos direitos sociais previstos nos arts. 6º a 11 da CF. Os direitos fundamentais de *segunda geração* nasceram no século XX, em esfera filosófica e política de cunho ideológico fundada no princípio da igualdade. São os direitos sociais, culturais e econômicos, bem como os direitos coletivos ou de coletividades, proclamados nas declarações solenes das constituições marxistas e também, de maneira clássica, no constitucionalismo da social-democracia do segundo pós-guerra. Apresentam-se como direitos que exigem do Estado prestações materiais, nem sempre resgatáveis por falta de recursos financeiros[131].

Nesse sentido, diz-se que os direitos a prestações vinculam-se à concepção de que ao Estado incumbe não apenas a não-intervenção na esfera da liberdade pessoal dos indivíduos, mas também a tarefa de colocar à disposição dos cidadãos os meios necessários ao exercício dessas liberdades. Garante-se, desta forma, não só a liberdade-autonomia, mas também a liberdade por intermédio do Estado, partindo-se da premissa de que o exercício dos direitos fundamentais depende de uma postura ativa dos poderes públicos, que corresponde ao *status positivo* de Jellinek[132].

Ainda seguindo a classificação de Alexy, ressalta-se a importância dos denominados *direitos de proteção*, subclassificação dos *direitos a prestações em sentido amplo*. Estes outorgam ao indivíduo o direito de exigir do Estado a necessária proteção contra ingerências propiciadas por terceiros. Ao Estado, em decorrência do dever geral de efetivação dos direitos fundamentais, incumbe zelar pela proteção dos direitos fundamentais dos indivíduos, não só contra ingerências indevidas por parte dos poderes públicos, mas também contra agressões provindas de particulares e até mesmo de outros Estados. Reconhece-se dever de proteção tanto em *caráter repressivo*, quanto *preventivo,* por meio da adoção de medidas positivas para garantir e para proteger de forma efetiva a fruição dos direitos fundamentais. Assim, são múltiplos os modos de realização dessa proteção,

[131] BONAVIDES, Paulo. Op. cit., pp. 564-565.
[132] SARLET, Ingo Wolfgang. Op. cit., p. 200.

podendo ocorrer pela edição de normas penais, de normas procedimentais, de atos administrativos e até mesmo por uma atuação concreta dos poderes públicos[133].

Por esse motivo, os direitos de proteção, na qualidade de direitos a prestação em sentido amplo, impõem ao Estado não apenas o dever de abster-se de lesar os bens jurídicos fundamentais, mas também o dever de atuar positivamente promovendo e protegendo tais bens de quaisquer ameaças, inclusive as que provenham de outros indivíduos ou de outros Estados. Gilmar Ferreira Mendes divide-os em três categorias: (a) dever de proibição (*Verbotspflicht*), consistente no dever de proibir determinadas condutas lesivas aos direitos fundamentais; (b) dever de segurança (*Sicherheitspflicht*), que impõe ao Estado o dever de proteger o indivíduo contra ataques de terceiros mediante adoção de medidas diversas; (c) dever de evitar riscos (*Risikopflicht*), que imputa ao Estado o dever de atuar com o objetivo de evitar riscos para o cidadão, especialmente em relação ao desenvolvimento técnico e tecnológico[134].

Um dos problemas relacionados com os direitos de proteção consiste na identificação das medidas necessárias à promoção da segurança dos direitos fundamentais perante terceiros. Segundo Peter Häberle, os direitos prestacionais são sempre abertos, sendo, portanto, "*menos normativos y sobre todo menos densos que el ius cogens, debido em parte a su proprio y siempre necessario margem de elasticidade, margem como es sabido, requerido para su gestión por la Administración*"[135]. Assim, ainda que os particulares identifiquem que em determinada situação faz-se necessária uma atuação do poder público diante dos demais concidadãos ou Estados estrangeiros, ao final, ficam à mercê do administrador público que tem ampla liberdade de conformação na satisfação do direito a ser protegido. Podem ser adotadas medidas efetivas na promoção da segurança e na diminuição dos riscos de violação dos direitos fundamentais, mas também podem ser eleitas medidas ineficazes, sob alegação de exercício de poder discricionário. À baixa densidade normativa dos direitos de proteção, soma-se ainda a questão de que tal efetivação deve submeter-s à *reserva do financeiramente possível*, tema largamente estudado, especialmente quanto à efetividade dos direitos sociais.

Os *direitos a prestações em sentido amplo*, sob a concepção de *direitos à organização e ao procedimento*, vinculam-se a idéia de que certos direitos fundamentais dependem, para sua realização, de providências estatais com o objetivo de criar e de conformar órgãos, setores ou

[133] ALEXY, Robert. **Teoria de los derechos fundamentales**. Op. cit., pp. 435 e ss.
[134] MENDES, Gilmar Ferreira. **Direitos fundamentais e controle de constitucionalidade**. Op. cit., p. 12.
[135] HÄBERLE, Peter. **Pluralismo y Constitución**. Op. cit., p. 165.

repartições destinados a ordenar a fruição das referidas garantias, configurando-se como verdadeiras garantias institucionais. Em alguns casos, a organização e o procedimento representam, inclusive, o único meio para se atingir a eficácia do direito fundamental; o que conduz ao argumento de que alguns direitos fundamentais conferem autênticos direitos subjetivos de proteção por meio da organização e do procedimento[136].

Desta forma, os direitos à organização e ao procedimento exigem igualmente uma prestação normativa a fim de se criarem as estruturas organizacionais necessárias e estabelecerem-se os procedimentos reclamados de forma direta ou indireta pelo direito fundamental. Após a criação do órgão e a organização dos procedimentos, estará garantida a eficácia do direito fundamental[137]. Entretanto, em interpretação mais ampla daquilo que seja direito à organização e ao procedimento, pode-se supor que basta o reconhecimento de normas e/ou princípios necessários à preservação do direito fundamental, sendo desnecessária a criação de um órgão específico responsável pelo zelo do direito fundamental ventilado[138].

Exemplos dos direitos à organização e ao procedimento são a liberdade de associação (CF, art. 5º, inciso XVII), as garantias processuais de defesa e de contraditório (CF, art. 5º, inciso LV), o direito ao juiz natural (CF, art. 5º, inciso XXXVII), o direito dos partidos políticos aos recursos partidários e à propaganda política gratuita nos meios de comunicação[139].

Por fim, há os *direitos a prestações em sentido estrito,* que correspondem aos *direitos sociais*, vinculados à concepção do *Welfare State*. Foram concebidos para atenuar as desigualdades de fato da sociedade e para ensejar a libertação das necessidades de maior número de indivíduos. Na Constituição brasileira encontram-se enumerados com destaque no art. 6º sendo relacionados à educação, à saúde, ao trabalho, ao lazer, à segurança, à previdência social, à proteção da maternidade, à assistência aos desamparados. Da mesma forma que os direitos de proteção, os direitos a prestações em sentido estrito, em geral, revestem-se de baixa densidade normativa, o que dificulta sua aplicabilidade pelo Judiciário, além de se submeterem *à reserva do financeiramente possíve*l, ou seja, são direitos dependentes da existência de recursos financeiros para sua

[136] HESSE, Konrad. Bestand und Bedeutung der Grundrechte in der Bundesrepublik Deutschland, 1978, p. 82 apud SARLET, Ingo Wolfgang. Op. cit., p. 210.
[137] CANOTILHO, José Joaquim Gomes. **Direito constitucional e teoria da Constituição.** Op. cit., p. 651.
[138] ALEXY, Robert. **Teoria de los derechos fundamentales**. Op. cit., pp. 456-457.
[139] MENDES, Gilmar Ferreira. Os direitos individuais e suas limitações: breves reflexões. In MENDES, Gilmar Ferreira; COELHO, Inocêncio Mártires; BRANCO, Paulo Gustavo Gonet. **Hermenêutica constitucional e direitos fundamentais**. 1ª ed. Brasília: Brasília Jurídica, 2002, p. 206.

efetivação. Destaca-se, portanto, a dimensão econômica dos direitos sociais que devem submeter-se à dependência da efetivação de políticas públicas para que sua implementação se materialize.

Apresentada a *classificação dos direitos fundamentais pelo critério funcional*, ressalte-se que a *divisão entre direitos de defesa e direitos a prestação não é fixa*, pois o mesmo direito fundamental, ora pode apresentar-se como um direito de defesa, ora como um direito a prestação, dependendo da posição que seu titular assumir diante do Estado. Portanto, a inclusão de um direito fundamental em um ou em outro grupo se baseia na predominância do caráter defensivo ou prestacional observado no caso concreto, o que não anula sua outra dimensão.

Importante destacar, ainda, a íntima relação que se estabelece – mesmo no plano doutrinário – entre os direitos de defesa e os direitos a prestação. Reconhecer direitos de defesa significa impor direito à existência de tribunais, direito à jurisdição, direito à decisão judicial, direito à execução de sentenças judiciais, pois tais direitos são realizados eficazmente tão-somente se o Estado criar tribunais, estabelecer processos e procedimentos, organizar a magistratura e impuser o cumprimento das decisões judiciais. Sob tal perspectiva, os direitos de defesa, na prática, não se diferenciam muito dos modernos direitos a prestação, como o direito à saúde, direito à escola, direito à habitação, já que também exigem a mesma estrutura básica de prestações fáticas do Estado[140].

Nesse sentido, conclui-se que quaisquer direitos materiais – incluídos os direitos de defesa – postulam uma dimensão procedimental, e, por isso, reconhecê-los implica necessariamente reconhecer direitos subjetivos à prestação para a garantia desses mesmos direitos. Resumindo-se, os *cidadãos têm a faculdade de exigir do Estado os procedimentos adequados que garantam seus direitos perante o poder público e os concidadãos*[141]. Seguindo a doutrina de Alexy – divisão dos direitos fundamentais em direitos de defesa e direitos a prestação, e destes em direito a prestação em sentido amplo (direitos de proteção e direitos à organização e ao procedimento) e direitos a prestação em sentido estrito (direitos sociais) – entende-se por *faculdade de exigir do Estado os procedimentos adequados*, o exercício de um direito prestacional à organização e ao procedimento; por *direitos perante o poder público*, o exercício dos direitos de defesa; e por *direitos perante os concidadãos*, a manifestação dos direitos de proteção.

[140] CANOTILHO, José Joaquim Gomes. **Estudos sobre direito fundamentais**. Op. cit., p. 77.
[141] CANOTILHO, José Joaquim Gomes. **Estudos sobre direito fundamentais**. Op. cit., p. 78.

2.4.2.4 O direito à privacidade na classificação pelo critério funcional

2.4.2.4.1 Privacidade como direito de defesa

Delineadas as premissas teóricas, passa-se à análise do direito à privacidade, ressaltando-se as múltiplas dimensões de tal direito. Logo no primeiro momento, desponta o *caráter negativo*, ou seja, o direito que se outorga ao titular de exigir do Estado e dos demais particulares uma abstenção de intervenção na sua esfera jurídica, ou seja, a prerrogativa de impor a terceiros o respeito à sua intimidade e à sua vida privada. Ao proteger a esfera individual do titular contra intromissões do poder público e dos demais concidadãos, o direito à privacidade caracteriza-se como típico *direito de defesa*.

Assim, o disposto nos incisos X e XII do art. 5º da CF[142], em sua dimensão negativa, resguarda o titular de intromissões de terceiros em sua esfera de intimidade e vida privada, conferindo-lhe um distanciamento confortável do mundo exterior. Observa-se igualmente uma feição negativa do direito à privacidade nos arts. 15 e 17 do Estatuto da Criança e do Adolescente – ECA, que resguardam, como direito fundamental, a inviolabilidade física, psíquica e moral da criança e do adolescente, bem como a preservação da sua autonomia, dos seus espaços e objetos pessoais:

> Art. 15. A criança e o adolescente têm direito à liberdade, ao respeito e à dignidade como pessoas humanas em processo de desenvolvimento e como sujeitos de direitos civis, humanos e sociais garantidos na Constituição e nas leis.
> (...)
> Art. 17. O direito ao respeito consiste na inviolabilidade da integridade física, psíquica e moral da criança e do adolescente, abrangendo a preservação da imagem, da identidade, da autonomia, dos valores, idéias e crenças, dos espaços e objetos pessoais.[143]

Enquanto pretensão negativa perante o Estado e demais indivíduos, o direito à privacidade assegura ao titular a fruição de três dentre os quatro atributos dos direitos de defesa, expostos no item anterior: (a) *como não-intervenção em relação a posições subjetivas*: proteção dos indivíduos contra ações do próprio Estado e também dos particulares que interfiram em sua intimidade e vida

---

[142] "*Art. 5º X - são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação*;" In BRASIL. **Constituição da República Federativa do Brasil de 1988**. Op. cit.

[143] BRASIL. Estatuto da Criança e do Adolescente. **Lei nº 8.069, de 13 de julho de 1990**. Disponível em: <http://www.planalto.gov.br/ccivil/LEIS/L8069.htm>. Acesso em: 30 jan. 2007.

privada; (b) *como não-eliminação de posições jurídicas*: proibição de o Estado extinguir o direito fundamental à privacidade ou limitá-lo de tal forma que reste afetado seu núcleo essencial; (c) *como faculdade de não fruir posições previstas na norma*: discussão em torno da possibilidade de renúncia e não exercício do direito à privacidade.

A *não-intervenção em relação a posições subjetivas impõe-se* como atributo de singular importância, ao se considerar que a proteção do direito à privacidade faz-se necessária à garantia de outros direitos fundamentais, tais como a liberdade de pensamento (CF, art. 5º, inciso IV); a liberdade de consciência e de crença (CF, art. 5º, inciso VI); a liberdade de expressão (CF, art. 5º, inciso IX). No caso da criança e do adolescente, a liberdade de opinião e de expressão (ECA, art. 16, inciso II); a liberdade de crença e culto religioso (ECA, art. 16, inciso III); a liberdade de buscar refúgio, auxílio e orientação (ECA, art. 16, inciso VII). O exercício dos referidos preceitos requer que o indivíduo disponha de uma esfera inviolável – intocável pelo Estado e pelos demais particulares – onde possa se desprender de seu ego, tocar sua consciência, libertando-se das amarras impostas pela sociedade. Apenas quando sente resguardada a sua privacidade, o indivíduo adquire autonomia para pensar, sentir e se expressar sem constrangimentos externos; buscando dentro de si o refúgio contra as agressões provenientes de terceiros.

O aspecto da *não-eliminação de posições jurídicas* tem relação com a investigação a que se procede a respeito do *âmbito de proteção* do direito à privacidade e da delimitação de seu *núcleo essencial*. Não há controvérsias doutrinárias a respeito da impossibilidade de extinção deste direito fundamental, mesmo porque está protegido por cláusula pétrea (CF, art. 60, § 4º, inciso IV)[144], mas observa-se a carência de um estudo mais aprofundado sobre as possíveis restrições à fruição deste direito fundamental, especialmente no que se refere às restrições implícitas, tema a ser abordado no item 2.10.

Quanto à *faculdade de não fruir posições previstas na norma*, tal problema gira em torno da possibilidade de *renúncia* a um direito fundamental. Conforme leciona Jorge Miranda, em princípio os direitos fundamentais são *irrenunciáveis* por estarem assentes no princípio basilar da dignidade da pessoa humana. Isto, entretanto, não impede que se estabeleça uma *limitação temporária do seu exercício* ou uma *auto-restrição*, sem afetar o núcleo essencial do direito fundamental. Nesse contexto, o cidadão tem a liberdade de não avocar para si um direito

[144] "*Art. 60. § 4º - Não será objeto de deliberação a proposta de emenda tendente a abolir: I - a forma federativa de Estado; II - o voto direto, secreto, universal e periódico; III - a separação dos Poderes; IV - os direitos e garantias individuais*". In BRASIL. **Constituição da República Federativa do Brasil de 1988**. Op. cit.

fundamental, pois de tal avocação flui sempre uma vertente positiva e uma vertente negativa, o que retira a obrigatoriedade de seu exercício a critério do próprio titular[145]. Este tema será, todavia, exposto com maior detalhamento no item 2.6.

Na condição de *direito de defesa*, o direito à privacidade confere a seu titular os seguintes direitos subjetivos: *pretensão de abstenção* e *pretensão de consideração*. De acordo com o primeiro, requer-se a não intromissão pelo poder público e pelos demais particulares na sua intimidade e vida privada, conforme já exposto; de acordo com o segundo, exige-se do Judiciário e do Legislativo a consideração do direito à privacidade quando este entrar em conflito com outros direitos fundamentais ou outros valores constitucionalmente protegidos.

Discute-se atualmente na doutrina se a *pretensão de abstenção* de intromissões de terceiros nas comunicações dos indivíduos foi mitigada pelo fenômeno da privatização dos serviços públicos de telecomunicações, o que implicaria um enfraquecimento do direito à privacidade enquanto *direito de defesa*. Alguns autores defendem que as privatizações não alteraram a substância dessa garantia, na medida em que o Estado tem tanto o dever de não intromissão, como o dever de resguardar o sigilo das comunicações; podendo-se falar em responsabilidade estatal pelos resultados da privatização, que ocorre por meio da edição de normas adequadas e da fiscalização das empresas telefônicas. Outros autores defendem que, em tal caso, o sigilo das comunicações configura-se como um *direito a prestação* – na modalidade *direito de proteção* – na medida em que exige do Estado a adoção de providências para que terceiros não interceptem as comunicações de forma indevida. Nesse sentido, o poder público deve atuar de forma positiva, não só por meio da normalização e fiscalização das telefônicas, mas especialmente garantindo-se a efetividade dessa proteção nos casos concretos, porque o cidadão-cliente-usuário desses serviços sente-se tão impotente perante a complexidade funcional dessas empresas quanto se sentiria perante a máquina estatal[146].

A *pretensão de consideração* pode ser exemplificada pela jurisprudência do STF que, no HC nº 71373/RS, julgou inconstitucional – por ofensa à dignidade da pessoa humana, à intimidade e à intangibilidade do corpo humano – a condução forçada de réu em ação de investigação de

[145] MIRANDA, Jorge. **Manual de direito constitucional**. Op. cit., pp. 357-358.
[146] CANOTILHO, José Joaquim Gomes. **Estudos sobre direito fundamentais**. Op. cit., pp. 163-167.

paternidade ao laboratório para realização de exame de DNA, quando o juízo poderia valer-se de outras provas distintas do exame para chegar à admissibilidade ficta da paternidade[147].

Por fim, ressalte-se que, apesar de o direito à privacidade proteger o indivíduo contra interferências indevidas na sua esfera pessoal, não logra impedir tal intervenção de forma absoluta, pois, presentes os pressupostos de natureza material e procedimental, estará autorizada a intromissão do Estado e demais particulares. Daí a expressa previsão da possibilidade de violação da privacidade domiciliar e da privacidade das comunicações, desde que atendidos os pressupostos previstos nos incisos XI e XII do art. 5º da CF[148]; tendo sido o último regulamentado pela Lei nº 9.296[149], de 24 de julho de 1996, atualmente em fase de revisão no Ministério da Justiça. No caso da preservação da privacidade das crianças e dos adolescentes, ainda que o ECA não tenha previsto expressamente restrições ao exercício deste direito fundamental, entende-se cabível a intervenção nos casos de regular exercício do pátrio poder.

Em conclusão, o direito à privacidade, enquanto expressão do denominado status negativo de Jellinek e direito de defesa, confere a seu titular uma garantia perante o Estado e demais concidadãos que só podem intervir na privacidade alheias nos estritos limites da Constituição, ou seja, quando houver previsão de restrição expressa ou implícita ao preceito fundamental.

2.4.2.4.2 Privacidade como direito a prestação

Em que pese a predominância da dimensão negativa, verifica-se que a efetividade do direito à privacidade requer não apenas uma abstenção estatal, mas também uma atuação do poder público no sentido de garantir a não intromissão de terceiros na intimidade e na vida

---

[147] BRASIL. Supremo Tribunal Federal. HC nº 71373-RS. Impetrante: José Antônio Gomes Pinheiro Machado. Relator para o Acordão: Marco Aurélio. Brasília, DF, 10 de novembro de 1994. Op. cit.

[148] "*Art. 5º XI - a casa é asilo inviolável do indivíduo, ninguém nela podendo penetrar sem consentimento do morador, salvo em caso de flagrante delito ou desastre, ou para prestar socorro, ou, durante o dia, por determinação judicial; XII - 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*;". In BRASIL. **Constituição da República Federativa do Brasil de 1988**. Op. cit.

[149] Referida lei está sendo objeto de revisão por grupo de trabalho constituído no âmbito do Ministério da Justiça e coordenado pela professora doutora Ada Pellegrini Grinover. O grupo propõe a revogação da lei em vigor e a edição de nova lei prevendo um rol taxativo dos crimes sujeitos à interceptação telefônica; a possibilidade do próprio denunciado pedir a quebra do sigilo como meio de prova de sua inocência; e a regulamentação da escuta ambiental, dentre outras alterações na legislação vigente. In GRINOVER, Ada Pellegrini. Interceptação de Dados Telemáticos. In: **II Congresso Internacional de Direito Eletrônico**: Instituto Brasileiro de Direito Eletrônico – IBDE e Universidade da Amazônia - UNAMA, Belém-PA, 02 a 06 de outubro de 2006.

privada alheias, ou seja, exige-se uma atuação positiva do Estado, expressão do *status positivo* de Jellinek e dos *direitos a prestação*. Assim, a *privacidade informacional* – também chamada *direito à autodeterminação informativa* – além de se configurar como um direito fundamental de feição negativa, também pode ser classificada como um *garantia institucional* (*Einrichtungsgarantien*) com forte dimensão positiva.

Conforme exposto no item 1.2, o referido direito foi reconhecido, pela primeira vez, pela Corte Constitucional Alemã, em decisão datada de 15 de dezembro de 1983, que declarou a inconstitucionalidade parcial da Lei do Censo de 1983 (*Volkszählungsgesetz*), de 25 de março de 1982, no que dizia respeito à obrigatoriedade, por parte dos cidadãos alemães, de responder a um questionário que serviria tanto para fins estatísticos como também para outra finalidades, visto que os dados recolhidos seriam distribuídos para diferentes entidades administrativas. O Tribunal Constitucional Federal alemão, por unanimidade, reconheceu o *Recht auf Informationelle Selbstbestimmung* ou *direito à autodeterminação informativa*, conferindo *status constitucional à proteção de dados pessoais* e garantindo aos cidadãos alemães o direito de negarem informações de caráter pessoal, opondo-se a coleta, armazenamento, difusão ou qualquer outra espécie de tratamento irrestrito e não autorizado pelo próprio titular. A decisão (*BverfGe 65,1 – Volkszählungsurteil*) fundamentou-se nos arts. 1º e 2º da Constituição da República Federal da Alemanha, que protegem a dignidade da pessoa humana e os direitos da personalidade[150]. Incidentalmente, a Corte ainda conferiu status constitucional às *Agências de Proteção de Dados Pessoais, frisando que sua existência era um requisito indispensável à coleta de informações de caráter pessoal e à proteção da privacidade dos cidadãos alemães*[151].

Segundo o Tribunal, o *direito à autodeterminação informativa* pressupõe que, mesmo sob as condições da moderna tecnologia de processamento de informações – que permite a coleta, o

[150] "*Artigo 1[Dignidade da pessoa humana; obrigatoriedade do respeito aos direitos fundamentais pelo Poder Público] 1. A dignidade da pessoa humana é inviolável. Toda autoridade pública terá o dever de respeitá-la e protegê-la. 2. Com isso, o Povo Alemão declara invioláveis e inalienáveis os direitos da pessoa humana, como fundamento de toda comunidade humana, da paz e da justiça no mundo. 3. Os Poderes Legislativo, Executivo e Judiciário estarão obrigados a considerar como diretamente aplicáveis os direitos fundamentais a seguir enunciados. Artigo 2 [Liberdade de ação; liberdade da pessoa; direito à vida] 1. Toda pessoa terá direito ao livre desenvolvimento da sua personalidade, na medida em que não violar os direitos de outrem e não infringir a ordem constitucional ou a lei moral. 2. Toda pessoa terá direito à vida e à integridade física. A liberdade da pessoa será inviolável. Ninguém poderá interferir nesses direitos, senão em virtude de lei*". In ALEMANHA. **Constituição da Alemanha de 1949**. Disponível em <http://www.alemanha.org.br/embaixadabrasilia/spr_2/willkommen/infos/grundgesetz/constituicao.htm>. Acesso em: 30 jan. 2007.

[151] FLAHERTY, David H. Op. cit.: The German Federal Constitutional Court's decision has also effectively given constitutional standing to data protection agencies by insisting that their existence is essencial for data collection to occur (Tradução Livre).

armazenamento e a interconexão de dados a qualquer momento, a qualquer distância, em segundos e de forma ilimitada –, que o indivíduo exerça a sua liberdade de decisão sobre as ações a serem procedidas ou omitidas em relação aos seus dados. O que importa para a decisão sobre a possibilidade de coleta dos dados não são os dados em si, mas o uso que se fará deles. Por isso o indivíduo deve ter conhecimento do contexto da utilização de seus dados, devendo o Estado intervir para que exista uma efetiva prestação de informações pelas entidades responsáveis pela coleta. *Nesse contexto, o direito à autodeterminação informativa exige a regulamentação por parte do Estado a respeito dos limites em relação à coleta e armazenamento de dados pessoais; e também a criação de organismos independentes para fiscalizar essa atividade, considerando a falta de transparência para o cidadão na armazenagem e uso de dados após o advento da tecnologia de processamento eletrônico de informações*[152].

Esta decisão da Corte Constitucional Alemã demonstra a amplitude do *direito à autodeterminação informativa*, diante de sua configuração, tanto como direito de defesa, de sentido negativo, ao conferir ao indivíduo a garantia de negar informações de caráter pessoal[153]; como *direito a prestação*, de *caráter positivo*, ao exigir do Estado a implementação de procedimentos administrativos necessários à efetividade do preceito fundamental. Trata-se de uma típica *garantia institucional*, na medida em que depende da atuação do Estado para sua concretização.

A respeito da dimensão positiva do direito à autodeterminação informativa, leciona Catarina Sarmento Castro:

> Na sua dimensão subjectiva, assume-se como direito que garante ao respectivo titular posições jurídicas perante o Estado para defesa de abusos relativos à utilização da sua informação pessoal, seja pela negativa – enquanto «Abehrrecht», obrigando-o a abster-se de tratar os seus dados –, seja pela positiva – enquanto «Schutzrecht», impondo-lhe a adopção de medidas de protecção. Na sua dimensão objectiva, comunitária, externa ou horizontal, impõe ao Estado a adopção de providências de defesa perante agressões de terceiros. O *Recht auf informationelle Selbsbestimmung* autonomizado pela jurisprudência constitucional alemã, em 1983, refere-se a isto mesmo: ao poder reconhecido ao indivíduo, como resultado da noção de autodeterminação, de decidir, ele mesmo, acerca da utilização que pode ser feita das suas informações pessoais, devendo ser o próprio a determinar quando, e em que medida, as revela.[154]

[152] MARTINS, Leonardo (Org.). Op. cit., pp. 237-240.
[153] Trata-se do exercício do direito de oposição que será detalhado no item 4.5.5.
[154] CASTRO, Catarina Sarmento. **Direito da informática, privacidade e dados pessoais**. Coimbra: Almedina, 2005, p. 28.

Assim, o direito à autodeterminação informativa requer, para sua efetiva concretização, a regulamentação da atividade de coleta e de uso de dados pessoais, definindo tanto limites quanto o dever de informação e esclarecimento ao titular dos dados; e, também, a criação de entidades independentes, responsáveis pela fiscalização e controle dessa atividade, em especial no que concerne ao tratamento de dados por meio de sistemas informatizados. Enfim, devem ser implementadas condições materiais para que os cidadãos não se tornem simples objetos de informação, no contexto do levantamento e da manipulação automatizada de dados após o incremento da tecnologia da informação[155].

Atualmente o direito à autodeterminação informativa já foi incorporado na Constituição de diversos países como Portugal[156], Eslovênia[157], Rússia[158] e Espanha[159], além de ter sido regulamentado por três Directivas do Parlamento Europeu e do Conselho da Europa, vulgarmente

[155] MARTINS, Leonardo (Org.). Op. cit., p. 241.

[156] "Artigo 35º *Utilização da informática. 1. Todos os cidadãos têm o direito de acesso aos dados informatizados que lhes digam respeito, podendo exigir a sua retificação e atualização, 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 proteção, 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 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*." In PORTUGAL. **Constituição Portuguesa de 1976**. Disponível em <http://www.parlamento.pt/const_leg/crp_port/>. Acesso em: 30 jan. 2007.

[157] "Artigo 38 Dados Pessoais. *(1) A proteção dos dados pessoais relacionados a um único cidadão deve ser garantida. Todo e qualquer uso de dados pessoais deverá ser proibido quando conflitar com o propósito inicial pelo qual fora proposto. (2) A coleta, o tratamento,o processamento e a proteção de dados pessoais será regulamentada por lei. (3) Todo cidadão tem direito de acessar seus dados pessoais e recorrer ao Judiciário contra qualquer abuso relacionado aos mesmos (Tradução Livre)*." In ESLOVÊNIA. **Constituição Eslovena de 1991**. Planalto, Brasília, DF. Disponível em <http://www.us-rs.si/en/index.php?sv_path=3583,3519>. Acesso em: 30 jan. 2007.

[158] "Artigo 24 *Proteção dos dados pessoais. 1) É defeso coletar, armazenar e disseminar informações sobre a vida privada de qualquer pessoa sem o seu próprio consentimento. 2) Os órgãos governamentais federais e locais são obrigados a fornecer acesso a documentos e materiais relacionados à própria pessoa e que possam afetar seus direitos e liberdades, exceto se de outro modo for estipulado por lei* (Tradução Livre)." In RÚSSIA. **Constituição Russa de 1993**. Disponível em <http://www.departments.bucknell.edu/russian/const/ch2.html>. Acesso em: 30 jan. 2007.

[159] "Artículo 18. (...) *4. La ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos*". In ESPANHA. **Constituição Espanhola de 1978**. Op. cit.

chamadas *Privacy Directives*. A Directiva 95/46/CE[160], de 24 de outubro de 1995, harmoniza a legislação da Europa que trata da proteção de dados pessoais, tendo em vista a diversidade de regulamentações a respeito dos procedimentos de transmissão e de arquivamento nos diferentes países. A Directiva 97/66/CE[161], de 15 de dezembro de 1997, regula o tratamento de dados pessoais no setor de telecomunicações. Por fim, a Directiva 2002/53/CE[162], de 12 de julho de 2002, dispõe sobre o tratamento de dados pessoais no setor de comunicações eletrônicas.

Observa-se, pois, que a partir do reconhecimento do direito à autodeterminação informativa na Alemanha, a privacidade passou a ser classificada também como um *direito a prestação* na modalidade, *direito à organização e ao procedimento*, na medida em que exige, em nível procedimental, que o Estado institua uma entidade competente (Comissão Nacional de Informática, Provedor de Informática, Autoridade Nacional do *Habeas Data* ou outra denominação qualquer), à qual o cidadão pode dirigir-se para garantir o seu direito de decidir, autônoma e livremente, quanto e dentro de que limites, seus dados pessoais podem ser suscetíveis de informatização e publicidade[163].

Verifica-se, por essa breve análise, que o *direito à privacidade em sua dimensão positiva impõe ao Estado o dever de implementar procedimentos administrativos necessários à salvaguarda das informações pessoais armazenadas tanto pelo setor público como pelo privado*. Tendo em vista a constante evolução das tecnologias utilizadas para coleta, arquivamento, transmissão e interconexão de dados; *também é necessária designação ou criação de um órgão responsável pela permanente revisão e aperfeiçoamento desses procedimentos, sendo esta a melhor forma de se garantir a proteção de dados pessoais dos cidadãos e a conseqüente eficácia do direito à privacidade informacion*al.

Ainda como direito a prestação, o direito à privacidade se configura também como um *direito de proteção*, ou seja, requer a proteção do Estado contra intromissões indevidas de outros

---

[160] UNIÃO EUROPÉIA. Directiva 95/46/CE do Parlamento Europeu e do Conselho da Europa, de 24 de outubro de 1995, relativa à protecção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados. **Jornal Oficial das Comunidades Europeias**. Portugal, 23 nov. 1995. nº L 281, pp. 31-50.
[161] UNIÃO EUROPÉIA. Directiva 97/66/CE do Parlamento Europeu e do Conselho da Europa, de 15 de dezembro de 1997, relativa ao tratamento de dados pessoais e à protecção da privacidade no sector das telecomunicações. **Jornal Oficial das Comunidades Europeias**. Portugal, 30 jan. 1998. nº L 24, pp. 1-8.
[162] UNIÃO EUROPÉIA. Directiva 2002/58/CE do Parlamento Europeu e do Conselho da Europa, de 12 de julho de 2002, relativa ao tratamento de dados pessoais e à protecção da privacidade no sector das comunicações electrónicas (Directiva relativa à privacidade e às comunicações electrónicas). **Jornal Oficial das Comunidades Europeias**. Portugal, 31 jul. 2002. nº L 201, pp. 37-47.
[163] CANOTILHO, José Joaquim Gomes. **Estudos sobre direito fundamentais**. Op. cit., p. 84.

particulares ou de outros Estados. Gomes Canotilho exemplifica uma situação em que este direito fundamental assume tal configuração: "*Um indivíduo, do sexo feminino, candidata-se a um emprego numa empresa privada, tendo ficado selecionado em primeiro lugar depois de testes de qualificação e entrevista. Todavia, antes da realização do contrato, a empresa exigiu-lhe um teste de gravidez, o qual ela recusou por se tratar de um atentado ao direito fundamental da intimidade e da vida privada e familiar (CRP, art. 26.º/1)*"[164]. Neste caso, a agressão é proveniente de outro particular, que se encontra em situação de preponderância ou exercício de poder, devendo o Estado proteger a parte mais débil da relação jurídica, como a única forma de garantir a efetividade do direito fundamental violado. Essa temática será ventilada com maior detalhamento ao se abordar o estudo da eficácia horizontal dos direitos fundamentais (item 2.5).

Na medida em que cabe ao Estado garantir não só a não interferência por parte dos poderes públicos na esfera da intimidade e da vida privada dos cidadãos, como também que os demais particulares não violarão tal preceito fundamental, o direito à privacidade configura-se como *direito de proteção*. Uma vez identificada grave ameaça à privacidade dos cidadãos, seja em decorrência de atos da iniciativa privada, seja de outros Estados, deve haver intervenção estatal. Além das medidas de caráter coercitivo, compete ainda ao Estado atuar de forma preventiva mediante implementação de medidas administrativas que proporcionem o incremento da privacidade dos cidadãos. Neste caso, depois de sopesados os interesses contrapostos e consideradas as limitações financeiras, poderão ser editados atos normativos de natureza penal, civil e administrativa que promovam a proteção da privacidade.

2.4.3 Dimensão objetiva

Conforme exposto no item 2.4.2.2, a *teoria dos quatro status* de Georg Jellinek – descrita na obra intitulada *Sistema dos direitos públicos subjetivos* (*System der subjecktiv öffentlichen Rechte*) – concebia os direitos fundamentais apenas sob sua dimensão subjetiva, seguindo-se o paradigma reinante no século XIX.

[164] CANOTILHO, José Joaquim Gomes. **Estudos sobre direito fundamentais**. Op. cit., p. 70. Grifos nossos.

As primeiras fissuras a minarem as estruturas dessa teoria ocorreram com a *teoria do estado social,* que enfatizou a necessidade de o Estado implementar uma série de prestações estatais para garantir a efetividade dos direitos fundamentais, em especial dos *direitos sociais* classificados como *direitos a prestação em sentido estrito*; e com a *teoria institucional dos direitos fundamentais*, desenvolvida sob égide de Peter Häberle, segundo a qual os direitos fundamentais, para sua satisfação, dependeriam da sua correspondente conformação legislativa para conferir-lhes direção, conteúdo e função, bem como da criação de instituições para lhes oferecer segurança.

Apesar da grande contribuição oferecida por essas teorias*,* os direitos fundamentais até o século XX ainda eram interpretados como *direitos individuais oponíveis ao Estado*, ou seja, como *direitos subjetivos*. Ora focava-se seu *caráter negativo* como *direitos de defesa* sob inspiração da *teoria liberal do estado de direito burguês*; ora seu *caráter positivo* como *direitos a prestação em sentido estrito* sob inspiração da *teoria do estado social*; ora seu *caráter positivo* como *direitos a prestação em sentido lato* sob inspiração da *teoria institucional*.

Nas palavras de Peter Häberle, reconhece-se a semente da *dimensão objetiva* dos direitos fundamentais:

> El concepto de status es, por ello, especialmente adecuado para la descripción de la dimensión como derechos individuales de los derechos fundamentales, porque en él se unen los elementos de lo activo y lo positivo, porque coordina positivamente al individuo com las correspondientes relaciones vitales y lo inserta en el conjunto de la sociedad, y porque permite manifertarse al derecho fundamental, en cuanto derecho individual subjetivo, en sus rasgos objetivos, que están fora del poder de disposición del sujeito. (...) El concepto de status aclara, po ultimo, que el individuo tiene una tarea a realizar en las correspondientes relaciones vitales y que la posición jurídica individual constituye un conjunto objetivo y supraindividual del que brotan los singulares derechos subjetivos y deberes[165].

Apesar da colaboração de Peter Häberle, o *caráter objetivo* dos direitos fundamentais desponta somente com o advento da denominada *teoria dos valores*. Segundo essa teoria, os direitos fundamentais constituem *valores objetivos que formam um sistema unitário de princípios decorrentes da dignidade da pessoa humana*. Assim, para além de sua função de direitos subjetivos, os direitos fundamentais constituem também valores objetivos, bens jurídicos que se impõem à observância de todos por força da própria Constituição. Logo após o fim da Segunda Guerra Mundial, diante da necessidade de maior proteção da dignidade da pessoa humana,

[165] HÄBERLE, Peter. **La garantía del contenido esencial de los derechos fundamentales en la Ley Fundamental de Bonn**: una contribución a la concepción institucional de los derechos fundamentales y a la teoría de la reserva de la ley. Tradução de Joaquín Brage Camazano. Madrid: Dykinson, 2003, pp. 113-114. Grifos nossos.

desconsiderada durante os longos anos de combate, a *dimensão objetiva* dos direitos fundamentais ressaltada pela *teoria dos valores* encontra terreno fértil para vicejar[166].

Desenvolve-se, nos Estados sociais e democráticos do pós-guerra, mesmo que difusamente, a noção de que os direitos fundamentais constituem, no seu conjunto, *uma ordem objetiva de valores que condiciona constitucionalmente toda a atuação dos poderes constituídos, irradiando-se por todos os ramos do ordenamento jurídico*. *Mesmo em relação às normas de direitos fundamentais que prevêem primariamente posições subjetivas, deve-se reconhecer uma dimensão objetiva*. Dessa dimensão se extrai não apenas o dever do Estado de se abster de intervenções na esfera privada, mas também o dever de atuar positivamente no sentido de permitir seu exercício efetivo e estruturar as condições necessárias à efetiva proteção dos direitos fundamentais[167].

Tal concepção da Constituição, como *estatuto axiológico* da sociedade, evidencia-se como produto do constitucionalismo germânico, baseado na idéia de que o arsenal de valores estabelecidos nesse documento deveria orientar e conformar não apenas a ordem jurídica estatal, mas também todos os setores da sociedade. A formulação dessa tese insere-se em um contexto de reaproximação dos postulados jusnaturalistas após a experiência do regime nazista. Os direitos fundamentais, simultaneamente, asseguram posições jurídicas subjetivas aos indivíduos em face do Estado, e veiculam uma ordem de valores objetiva, que há de comandar toda a vida em sociedade[168].

Enfim, *sob a dimensão objetiva, os direitos fundamentais protegem os bens jurídicos mais caros da sociedade, ou seja, aqueles que são expressão do princípio da dignidade da pessoa humana; formam um sistema unitário dos valores a serem perseguidos pelo poder público, vinculando Executivo, Judiciário e Legislativo; e constituem a base do ordenamento jurídico de um Estado Democrático de Direito, estendendo-se a todos os seus ramos*.

Não há como pensar em proteção de direitos fundamentais apartada de um Estado Democrático de Direito, tendo em vista a íntima relação que se estabelece entre esses dois elementos, sendo um deles o pressuposto da existência do outro. Os direitos fundamentais, ao mesmo tempo em que são respeitados tão-somente nos ordenamentos jurídicos que impõem

---

[166] NOVAIS, Jorge Reis. **As restrições aos direitos fundamentais não expressamente autorizadas pela Constituição**. Coimbra: Coimbra Editora, 2003, pp. 63-64.
[167] NOVAIS, Jorge Reis. Op. cit., pp. 57-58.
[168] PEREIRA, Jane Reis Gonçalves. Apontamentos sobre a aplicação das normas de direito fundamental nas relações jurídicas entre particulares. In BARROSO, Luís Roberto. **A nova interpretação constitucional**: ponderação, direitos fundamentais e relações privadas. Rio de Janeiro: Renovar, 2003, pp. 149-150.

limitação dos poderes do Estado, ou seja, nos Estados Democráticos de Direito, formam um sistema de princípios norteadores do poder público, que deve considerá-los no momento da criação, da interpretação e da aplicação das demais normas que integram o ordenamento jurídico. *Observa-se, pois, a íntima relação entre a democracia e a dimensão objetiva dos direitos fundamentais.*

Robert Alexy apresenta três modelos de visão da relação entre os direitos fundamentais e a democracia: um *ingênuo,* um *idealista e* um *realista*. Pela perspectiva *ingênua,* não se percebe contradição entre direitos fundamentais e democracia porque ambos são bons e não existe contradição entre coisas boas que devem ser protegidas simultânea e ilimitadamente. Segundo o autor, essa visão não prospera, pois, diante da finitude e da escassez dos recursos, algumas coisas boas serão sempre sacrificadas. A visão *idealista*, ao modo rousseauniano, vislumbra a perfeita conciliação entre direitos fundamentais e a democracia em uma sociedade politicamente perfeita. Para Alexy, esse é um ideal inalcançável, devendo-se adotar uma visão *realista*, segundo a qual, a relação entre direitos fundamentais e democracia se fundamenta em uma contradição: direitos fundamentais são democráticos e direitos fundamentais são ademocráticos. São democráticos na medida em que, ao garantir a liberdade de opinião, imprensa, reunião e associação, assim como o direito eleitoral e outras liberdades políticas, asseguram as condições funcionais do processo democrático; são ademocráticos porque subtraem da maioria parlamentar legitimada pela última eleição o poder de decisão, vinculando o Legislativo[169].

O posicionamento do jurista é salutar no que concerne às denominadas visões *ingênua* e *idealista*. Seria realmente pueril conceber um modelo de relação entre direitos fundamentais e democracia sob a concepção de uma sociedade política ideal e utópica, em que houvesse plena liberdade e igualdade dos indivíduos e a política fosse fundada apenas no interesse geral e coletivo da maioria, conforme descreve Jean-Jacques Rousseau na obra intitulada *Contrato social*. Todavia, questiona-se a visão *realista* do autor, segundo a qual os direitos fundamentais podem ser considerando tanto *democráticos* como *ademocráticos*. *Entende-se que esses são sempre a favor da democracia*, adotando-se a premissa de que, em tal forma de governo[170], o

[169] ALEXY, Robert. **Direitos fundamentais no Estado Constitucional Democrático**. Op. cit., p. 65.

[170] *Formas de governo* não se confundem com sistemas de governo e com formas de Estado. *Forma de governo* é a forma de uma comunidade política organizar o seu poder ou estabelecer a diferenciação entre governantes e governados, regulando a participação dos cidadãos no poder e a divisão do mesmo. São exemplos de *formas de governo* a monarquia absoluta, o governo representativo liberal, o governo jacobino, o governo cesarista, a monarquia constitucional limitada, a democracia, o governo leninista e o governo fascista. São exemplos *de sistemas*

povo é soberano e seus representantes limitados apenas pelo poder constituinte originário, ou seja, pela própria Constituição que instaurou o ordenamento jurídico vigente. *Os direitos fundamentais constituem a garantia da minoria contra o exercício arbitrário do poder pelos representantes eleitos pela maioria.* Mesmo que a maioria – por meio de seus representantes – aprove leis que afrontem os preceitos fundamentais do Estado Democrático de Direito, ainda restará à minoria a garantia da jurisdição constitucional, isto é, o controle de constitucionalidade dos atos normativos.

Conforme expõe Hans Kelsen, o controle de constitucionalidade dos atos normativos garante a regularidade das funções estatais, protege os indivíduos do órgão Legislativo, representando a principal e mais eficaz garantia da Constituição. O Legislativo é um órgão criador do direito e não um órgão de aplicação do direito vinculado pela Magna Carta, portanto, muitas vezes precisa ser limitado por meio da jurisdição constitucional, que dentre outros mecanismos se vale do controle de constitucionalidade dos atos emanados do Legislativo[171]. Considerando que nesta esfera de poder há preponderância dos representantes da maioria, estando estes livres para criar o direito, deve ser resguardado à minoria o poder de acionar a jurisdição constitucional para controlar os atos normativos emanados do Legislativo. Nesse contexto, destaca-se a relevância dos direitos fundamentais enquanto parâmetros de controle da constitucionalidade das leis e, por conseqüência, do regime democrático.

Além desse aspecto, destaque-se o posicionamento de Peter Häberle ao ressaltar que *se os direitos fundamentais não forem garantidos de forma efetiva, as minorias nunca irão conseguir se converter em maioria e, nesse sentido, esses preceitos são eminentemente democráticos*. A manutenção da democracia requer que os cidadãos sejam minimamente politizados e participem ativamente da vontade estatal, mas essa participação mediante voto popular pressupõe a proteção de direitos fundamentais, tais como a liberdade de consciência, de opinião, de reunião e de associação, o que demonstra a íntima relação dos direitos fundamentais com os regimes democráticos[172].

---

de governo o parlamentarismo, o presidencialismo, o sistema orleanista, o semipresidencialismo, o sistema representativo simples e o sistema convencional. São exemplos de formas de Estado o unitário e o federado. In MIRANDA, Jorge. **Teoria do Estado e da Constituição**. Rio de Janeiro: Forense, 2003, pp. 298-299.

[171] KELSEN, Hans. **Jurisdição constitucional**. Introdução e revisão técnica de Sérgio Sérvulo da Cunha. Tradução do alemão de Alexandre Krug, tradução do italiano de Eduardo Brandão e tradução do francês de Maria Ermantina Galvão. São Paulo: Martins Fontes, 2003, pp. 148-150.

[172] HÄBERLE, Peter. **La garantía del contenido esencial de los derechos fundamentales en la Ley Fundamental de Bonn**. Op. cit., p. 20.

Desse modo, conclui-se que os direitos fundamentais são eminentemente democráticos, ou seja, configuram-se como mecanismos de defesa da democracia. Seu caráter objetivo relaciona-se intimamente ao fortalecimento dessa forma de governo, aferindo-se dessa estreita relação a relevância dessa garantias. Ao integrarem o conteúdo principal das constituições dos Estados Democráticos de Direito, juntamente com as normas que organizam e estruturam o Estado propriamente dito, funcionam como uma garantia a favor das minorias contra as opressões da maioria, especialmente no que concerne às liberdades públicas, tais como a privacidade; a liberdade de manifestação do pensamento; a liberdade de consciência e de crença; a liberdade de expressão e de comunicação; a liberdade de profissão; e a liberdade de associação.

Na condição de valores norteadores do Estado – em sua dimensão objetiva – produzem reflexos em todos os ramos do direito, conforme expõe com clareza Daniel Sarmento, *verbis*:

> Esta significa que os valores que dão lastro aos direitos fundamentais penetram por todos os ramos do ordenamento jurídico, condicionando a interpretação das normas legais e atuando como impulsos e diretrizes para o legislador, a administração e o Judiciário. A eficácia irradiante, nesse sentido, enseja a "humanização" da ordem jurídica, ao exigir que todas as suas normas sejam, no momento da aplicação, reexaminadas pelo operador do direito com novas lentes, que terão as cores da dignidade humana, da igualdade substantiva e da justiça social, impressas no tecido constitucional. A eficácia irradiante tem na interpretação conforme a Constituição um dos seus mais férteis instrumentos. Esta técnica, segundo a doutrina autorizada, desempenha concomitantemente os papéis de princípio hermenêutico e mecanismo de controle de constitucionalidade. (...) Porém a eficácia irradiante não se exaure nessa técnica, pois ela não é mobilizada apenas nos momentos de patologia da ordem jurídica (...). Na verdade, a eficácia irradiante transcende este plano, pois deve ser operacionalizada no dia-a-dia do direito, nas suas aplicações mais banais e corriqueiras, e não apenas nos momentos de crise do ordenamento.[173]

Da *eficácia irradiante* dos direitos fundamentais por todo o ordenamento jurídico – como expressão de sua *dimensão objetiva* – resultam, dentre outras, as seguintes conseqüências: (a) proibição dos atos normativos de qualquer ramo do direito a afrontarem esse sistema de valores, sob pena de serem julgados inconstitucionais; (b) interpretação restritiva das leis que estabelecem restrições aos direitos fundamentais, sob pena de inconstitucionalidade; (c) vinculação do Poder Judiciário aos direitos fundamentais na resolução dos casos concretos quando se constatar lacuna na legislação; (d) eficácia dos direitos fundamentais nas relações privadas; (e) obrigação do Estado de prover as condições objetivas mínimas para um efetivo exercício dos direitos fundamentais mediante normas de organização e procedimento; (f) dever estatal de proteger os

[173] SARMENTO, Daniel. Op. cit., p. 155. Grifos nossos.

particulares contra a violação de seus direitos fundamentais não só perante entes públicos, mas também diante de ameaças provindas de outros particulares[174].

Quanto à inconstitucionalidade das leis que afrontam os direitos fundamentais, conforme já exposto, trata-se de uma garantia da minoria contra o exercício arbitrário do poder exercido pelos representantes da maioria. Daí resulta a necessidade de criação, interpretação e aplicação das normas de todos os ramos do direito em conformidade à Constituição. Quanto à interpretação restritiva das leis que restringem direitos fundamentais, observa-se que estes possuem limites que não podem ser ultrapassados sob pena de sua total descaracterização. Esse mínimo insuscetível de restrição ou redução pelas leis restritivas é denominado *núcleo essencial* do direito fundamental, tema a ser explorado no item 2.7. Por fim, uma observação quanto à eficácia dos direitos fundamentais nas relações privadas, também denominada *eficácia horizontal*; segundo a doutrina mais moderna, os direitos fundamentais vinculam não só o Estado como também os demais particulares, conforme se detalhará no próximo item deste capítulo.

O aspecto objetivo dos direitos fundamentais no ordenamento jurídico nacional pode ser demonstrado na análise do dispositivo constitucional que atribui status de *cláusula pétrea* a esses preceitos (CF, art. 60, § 4º). O constituinte explicitou o especial significado dos direitos fundamentais como elementos que estruturam a ordem jurídica objetiva, conferindo-lhes tanto uma dimensão negativa como uma dimensão positiva. Essa concepção coloca o Estado não só na posição de adversário dos direitos fundamentais, mas especialmente como seu guardião. Assim, ainda que não se reconheça ante o Estado uma pretensão subjetiva (direito de defesa), identifica-se uma pretensão objetiva de se tomarem providências para a concretização do direito fundamental, proibindo-se, no caso, a omissão do poder público[175].

Nesse contexto, registra-se uma passagem bem ilustrativa do voto proferido pelo ministro Marco Aurélio, em sede de HC, expondo o posicionamento STF no que concerne ao aspecto objetivo dos direitos fundamentais. Segundo o ministro, os direitos fundamentais formam um sistema de valores objetivos, verdadeiros princípios estruturantes do ordenamento jurídico, que devem nortear a atuação dos três poderes, *verbis*:

> 6. A Imprescritibilidade e o Sistema dos Direitos Fundamentais
> A Constituição de 1988 representou um divisor de águas entre o antigo regime totalitário e um período de redemocratização do País, marcando, dessa forma, uma época que tem como modelo de atuação do Estado o respeito incondicional

[174] NOVAIS, Jorge Reis. Op. cit., pp. 81-82.
[175] MENDES, Gilmar Ferreira. **Direitos fundamentais e controle de constitucionalidade**. Op. cit., pp. 119-120.

> aos direitos fundamentais. Por isso mesmo, o sistema constitucional dos direitos fundamentais, previsto no artigo 5º da Carta, com os eventuais acréscimos do § 2º, reflete, em rigor e em larga medida, a própria essência da Constituição e a retomada do processo de democratização e da garantia do cidadão contra abusos e arbitrariedades no exercício do Poder Público.
> Os direitos fundamentais são hoje verdadeiros princípios estruturantes da organização e do funcionamento do Estado, valores objetivos que servem como norte da atuação estatal em seus mais diferentes níveis: no Legislativo, formam um catálogo de princípios e garantias que informam e direcionam toda a atividade de criação das normas de nosso ordenamento jurídico e de concretização dos preceitos constitucionais; no Executivo, mostram-se como verdadeiros limites ao exercício do poder administrativo, servindo como trincheiras de proteção da liberdade do cidadão; e, no Judiciário, refletem a base e o fundamento necessário da compreensão e interpretação de nossas normas – efeito interpretativo -, evitando que a atividade jurisdicional se transforme em medidas discricionárias ou providências ilegítimas de opções políticas pautadas em escolhas pessoais dos juízes.
> A conservação de um sistema sólido, moderno e socializante de direitos fundamentais significa, em última instância, a manutenção e o aprimoramento do próprio regime democrático de um Estado constitucional. É dever da sociedade, dos juristas, dos intérpretes, dos juízes e, principalmente, nosso, membros deste Tribunal, guardião oficial e final da Constituição, garantir que esse sistema permaneça com a máxima eficácia possível, reconhecendo-lhe e mesmo concedendo-lhe força normativa por meio de nossas decisões, de maneira a manter tais direitos fundamentais vivos e eficazes perante o Estado e a sociedade civil. Essa é a posição que devemos adotar na análise dos problemas constitucionais que diariamente nos chegam, e é nesse ponto que reside nossa função institucional e, mais do que isso, a própria esperança do cidadão nas instituições brasileiras, especialmente no Supremo Tribunal Federal, a quem incumbe, na República Federativa do Brasil, a última palavra sobre os descompassos havidos.
> Essa postura democraticamente adequada em face da Constituição obriga-nos, por imposição dos princípios constitucionais, a interpretar abrangentemente os direitos fundamentais, de modo a compreender as exceções a esse sistema de maneira rigorosamente estrita. Assim sendo, cabe ao Supremo Tribunal Federal ampliar a proteção dos direitos fundamentais mediante construção constitucional e restringir-se a uma interpretação quase que literal nas hipóteses de limitação a esses direitos, ainda que expressas no corpo da própria Carta Política. Não é permitido a este Tribunal ou a qualquer hermeneuta da Constituição interpretar de forma aberta ou ampliativa preceitos que impliquem a diminuição de eficácia dos direitos fundamentais.[176]

Em reforço ao que foi anteriormente mencionado a respeito da íntima relação entre democracia e direitos fundamentais, destaque-se também outro interessante trecho do voto do ministro Marco Aurélio neste HC. Conforme expõe o ministro, os direitos fundamentais

[176] BRASIL. Supremo Tribunal Federal. HC nº 82424/RS. Impetrante: Werner Cantalício João Berker. Relator para o Acórdão: Maurício Corrêa. Brasília, DF, 17 de setembro de 2003. **Diário da Justiça da República Federativa do Brasil**, Brasília, DF, 19 mar. 2004, p. 00017. Disponível em <http://www.stf.gov.br/jurisprudencia/nova/pesquisa.asp>. Acesso em: 30 jan. 2007. Grifos nossos.

fortalecem o princípio democrático, especialmente mediante a garantia da liberdade de expressão e comunicação:

> Pode-se concluir que os direitos fundamentais localizam-se na estrutura de sustento e de eficácia do princípio democrático. Nesse contexto, o específico direito fundamental da liberdade de expressão exerce um papel de extrema relevância, insuplantável, em suas mais variadas facetas: direito de discurso, direito de opinião, direito de imprensa, direito à informação e a proibição da censura. É por meio desse direito que ocorre a participação democrática, a possibilidade de as mais diferentes e inusitadas opiniões serem externadas de forma aberta, sem o receio de, com isso, contrariar-se a opinião do próprio Estado ou mesmo a opinião majoritária. E é assim que se constrói uma sociedade livre e plural, com diversas correntes de idéias, ideologias, pensamentos e opiniões políticas. Na feliz e apropriada redação utilizada pelo Professor Catedrático de Direito Público e História Constitucional da Universidade de Friburgo, Ernst-Wolfgang Böckenförde, utilizando-se de expressão cunhada pela Corte Constitucional Alemã, os direitos de comunicação, em que se inclui a liberdade de opinião, são "constitutivos do princípio democrático por antonomásia", já que promovem a autonomia individual e formam o ambiente plural de participação democrática. (...) Kelsen, quando afirma que a democracia se constrói sobretudo quando se respeitam os direitos da minoria, mesmo porque esta poderá um dia influenciar a opinião da maioria [sic]. E venho adotando esse princípio diuturnamente, daí a razão pela qual, muitas vezes, deixo de atender ao pensamento da maioria, à inteligência dos colegas, por compreender, mantida a convicção, a importância do voto minoritário.[177]

Diante do exposto, conclui-se que os direitos fundamentais possuem dupla dimensão: uma subjetiva, enquanto garantia individual de exigir do Estado e dos demais particulares determinados comportamentos negativos ou positivos; e uma objetiva, na condição de sistema de valores de um Estado Democrático de Direito, que funciona simultaneamente como diretriz e como limite ao poder público. Estabelece-se íntima relação entre direitos fundamentais e democracia, o que se demonstra pelas seguintes constatações: (a) funcionam como um mecanismo de defesa da minoria contra a maioria, pois garantem ao primeiro grupo o exercício da jurisdição constitucional para ver declarada a inconstitucionalidade de leis votadas pelos representantes do segundo grupo; (b) protegem as liberdades públicas tão caras nos regimes democráticos e inexistentes nos regimes de exceção; (c) garantem o voto universal e secreto.

Resta apenas, para fins de encerramento desse item, ressaltar que a *dimensão objetiva e a dimensão subjetiva dos direitos fundamentais são complementares entre si*. Conforme expõe Peter Häberle, o fortalecimento da dimensão subjetiva dos direitos fundamentais acarreta o fortalecimento da dimensão objetiva e vice-versa. Uma teoria de direitos fundamentais que

[177] Loc. cit. Grifos nossos.

descuida de seu aspecto objetivo acaba, ao final, enfraquecendo seu conteúdo subjetivo[178]; o que não é desejável para uma efetiva proteção desses preceitos fundamentais.

2.5 Eficácia horizontal dos direitos fundamentais

Os direitos fundamentais foram reconhecidos no século XIX como *direitos subjetivos públicos oponíveis em face do Estado*. Na condição de limitações impostas ao poder público, este era o único destinatário de tais preceitos; o que representava um obstáculo à sua aplicação nas relações privadas. No século XX, todavia, a publicação da Declaração Universal dos Direitos do Homem descortinou possibilidades para se invocarem os direitos fundamentais no tratamento das relações entre particulares. Na década de 40, surgiu na jurisprudência americana a denominada *state action*, segundo a qual os direitos fundamentais poderiam ser invocados na órbita privada. Na Alemanha, o tema ganhou evidência na década de 50 sob a expressão *Drittwirkung der Grundrechte,* traduzida como *eficácia dos direitos fundamentais perante terceiros*[179].

A doutrina do *state action* foi adotada pela Suprema Corte americana nos julgamentos em que se invocava a 14ª Emenda do *Bill of Rights* ou, mais concretamente, a cláusula da *equal protection of the laws*[180]. Embora tenha representado grande avanço doutrinário quanto à aplicação dos direitos fundamentais nas relações privadas, essas garantias continuaram a ser interpretadas sob um viés exclusivamente publicístico. *Segundo seus defensores, os direitos fundamentais poderiam ser invocados nas relações privadas na hipótese de existência de alguma ação estatal, ainda que indireta; ou quando o particular se comportasse como se Estado fosse.* Neste último caso, embora se admitisse a ausência de participação direta ou indireta do Estado, os direitos fundamentais seriam aplicáveis diante da constatação da nítida preponderância de uma das partes na relação jurídica, à semelhança da situação que se estabelece em relações de caráter público.

---

[178] HÄBERLE, Peter. **La garantía del contenido esencial de los derechos fundamentales en la Ley Fundamental de Bonn**. Op. cit., p. 74.
[179] PEREIRA, Jane Reis Gonçalves. Op. cit., pp. 132-134.
[180] PEREIRA, Jane Reis Gonçalves. Op. cit., p. 169.

Conforme o exposto no item 2.4.3, essa visão restritiva do *Estado Liberal Burguês* de que os direitos fundamentais configuravam-se apenas como *direitos subjetivos públicos*, gradualmente foi superada pelo paradigma do *Welfare State,* segundo o qual os direitos fundamentais também ostentavam uma *dimensão objetiva.* Esta última concepção, de que os direitos fundamentais representam o *estatuto axiológico da sociedade*, o *sistema unitário de princípios da comunidade*, a *base estruturante de todo o ordenamento jurídico*; teve o mérito de ampliar seu âmbito de aplicação transitando, desta forma, para o âmbito das relações privadas.

Seguindo esse raciocínio, parte da doutrina aponta duas razões para a aplicação dos direitos fundamentais nas relações privadas, denominada *eficácia horizontal dos direitos fundamentais*: a compreensão de que a Constituição, como estatuto axiológico, tem como objetivo ordenar não só as relações com o Estado, mas também com os demais particulares; e a constatação de que o fenômeno do poder não é exclusivo das relações com o Estado, também se manifestando no seio da sociedade civil[181]. O poder não se manifesta como privilégio do Estado apenas, exterioriza-se também nas relações econômicas, empresariais, sindicais, trabalhistas, religiosas e em tantas outras. Assim, os direitos fundamentais devem ser aplicados não só nas relações com o Estado, mas também nas relações entre os particulares, configurando-se como o estatuto de princípios que devem nortear toda a ordem jurídica.

Segundo Jane Pereira, a complexidade da vida contemporânea compreende relações jurídicas entre particulares verticais, desiguais, ou de sujeição, em que se constata a predominância de uma das partes. É possível verificar essa prevalência de poder entre as pessoas em família, em partidos políticos, em associações, em organizações religiosas, em relações empregatícias, e em outras tantas. A aplicação dos direitos fundamentais nessas relações eminentemente desiguais tem por fim proteger a *liberdade* e a *autodeterminação* da parte da mais fraca, o que explica a grande aceitação desta doutrina na área trabalhista[182].

Outra corrente doutrinária aponta algumas razões para a inadmissibilidade de aplicação dos direitos fundamentais nas relações privadas: primeiro, o fato de que a Constituição foi concebida como um documento com o objetivo de organizar e de limitar a atuação dos poderes

[181] PEREIRA, Jane Reis Gonçalves. Op. cit., p. 143.
[182] PEREIRA, Jane Reis Gonçalves. Op. cit., pp. 147-149.

públicos e não para regular a atuação dos particulares; segundo, que a extensão dos direitos fundamentais às relações privadas fulminaria a própria liberdade e autonomia privadas[183].

Esses argumentos, porém, devem ser veementemente contestados. Apesar de os direitos fundamentais, em sua maioria, regularem as relações com o poder público; também se aplicam nas relações entre particulares, como os direitos trabalhistas, o direito à livre associação profissional e sindical, o direito à greve, o direito ao meio ambiente saudável, o direito à proteção do consumidor, o direito à proteção da criança e do adolescente, o direito à proteção do idoso, e tantos outros espalhados pela Constituição. Quanto ao perigo de se fulminarem a liberdade e a autonomia dos particulares, existem relações privadas em que uma das partes não dispõe de autonomia, estando completamente subjugada pela parte mais forte.

Em complemento, Rafael de Asís Roig destaca que certos direitos fundamentais, como o direito à vida, à integridade física, à honra e à intimidade parecem ser passíveis de transgressão não só pelo poder público, mas também por particulares. *Alerta também para o fato de que determinados grupos privados exercem mais poder até em relação ao próprio Estado sendo, portanto, inviável restringir a aplicabilidade dos direitos fundamentais apenas às relações com o poder público*. Assim, quando se defende que os direitos fundamentais limitam o poder, deve-se entender "poder" em acepção ampla, capaz de abranger os diversos poderes econômicos e sociais que exercem uma certa *potestade jurídica* mediante regulamentações de caráter geral[184]. Nas palavras do autor:

> Con todo ello, parece que la fórmula 'derechos fundamentales como límites al poder', descriptiva, relativamente, del primer momento en el que puede hablarse de derechos fundamentales, es incompleta y puede ser fuente de confusiones si no se matiza. Digo que es relativamente descriptiva porque no puede afirmarse que todos los derechos frente al Estado, más bien se trata de pretensiones, exigencias o valores que pueden ser afectados por la actividad no sólo del Estado sino de los restantes individuos. Peró además, esta expressión ex incompleta ya que, aparte de lo anteriormente señalado, ni expressa tampouco incidencia de los grupos 'privados' en lo referente a su desfrute. Por último, la fórmula puede resultar confusa ya que parece situar al poder como único posible transgressor de estos derechos, cuando en múltiples ocasiones es elemento necesario para su realización.[185]

[183] ASÍS ROIG, Rafael de. **Las paradojas de los derechos fundamentales como límites al poder**. Madrid: Editorial Debate, 1992, pp. 106-107.
[184] ASÍS ROIG, Rafael de. Op. cit., pp. 108-113.
[185] ASÍS ROIG, Rafael de. Op. cit., p. 117. Grifos nossos.

Gomes Canotilho oferece uma contribuição para o caso, em que se reconhece a eficácia horizontal do direito fundamental à intimidade, verificada a ausência de autonomia da parte mais fraca e a afronta à sua autodeterminação. Nas palavras do autor:

> Caso 2 – A "terceira mulher", da "mulher diabolizada" e da "mulher exaltada" à "mulher criadora do seu papel". Este caso é hoje sobejamente conhecido com o caso do "diferencialismo das executivas". A história tem mulheres de carne e osso e conta-se também em curtas palavras. Uma multinacional propõe a uma sua executiva de top a colocação imediata num importante posto de chefia com a cláusula de proibição de gravidez ou de "barriga de aluguer" durante 10 anos. A opção para a mulher de 26 é clara: ser mãe ou ser mulher de sucesso. A "proibição de gravidez" é uma cláusula constitucionalmente proibida; mas como proibir, no mundo da autonomia contratual-global, a inserção de uma condição que não é, segundo alguns, que a invenção da "terceira mulher", a "mulher criadora do seu papel"?[186]

Hoje, após tortuosos debates doutrinários, pacificou-se o reconhecimento da eficácia horizontal dos direitos fundamentais, havendo divergência apenas quanto à forma de aplicação dessa garantia, que varia conforme se adote a *teoria da eficácia direta ou imediata* ou a *teoria da eficácia indireta ou mediata.*

A *teoria da eficácia indireta ou mediata* foi desenvolvida na doutrina por Günter Dürig em 1956, na obra intitulada *Grundrechte und Zivilrechtsprechung*, tornando-se a concepção dominante na jurisprudência alemã. Segundo o autor, *para que o direito privado se submeta aos valores constitucionais, é necessária a construção de certas pontes representadas pelas cláusulas gerais e conceitos jurídicos indeterminados acolhidos pelo legislador.* A aplicação direta dos direitos fundamentais não pode ser admitida, pois desfiguraria o direito privado ao convertê-lo em mera concretização do direito constitucional; além de conferir demasiado poder ao Judiciário, sujeitando a aplicação de leis ordinárias ao arbítrio de juízes. Assim, para os adeptos dessa teoria, os direitos fundamentais serão aplicáveis nas relações privadas apenas nas hipóteses em que couber ao Judiciário colmatar as lacunas das *cláusulas gerais* e dos *conceitos jurídicos indeterminados,* deixados pelo legislador; e nos julgamentos de inconstitucionalidade de leis incompatíveis com os direitos fundamentais[187].

---

[186]. CANOTILHO, José Joaquim Gomes. Civilização do direito constitucional ou constitucionalização do direito civil? A eficácia dos direitos fundamentais na ordem jurídico-civil no contexto do direito pós-moderno. In: GRAU, Eros Roberto; GUERRA FILHO, Willis Santiago (Org.). **Direito constitucional**: estudos em homenagem a Paulo Bonavides. São Paulo: Malheiros, 2001, p. 111.

[187] SARMENTO, Daniel. Op. cit., pp. 238-241.

Segundo os defensores da *teoria da eficácia indireta ou mediata,* dentre os quais Dürig, Leiner e Konrad Hesse, a aplicação dos direitos fundamentais às relações privadas deve efetivar-se por meio de "mecanismos típicos" de direito privado, ou seja, devem ser "recepcionados" por este ramo do direito. Justifica-se tal recepção pela necessidade de coordenação dos direitos fundamentais com os direitos subjetivos privados, levando-se em conta a especialidade dessas relações, para que não se sufoque a liberdade contratual[188].

A *teoria da eficácia direta ou imediata* foi defendida inicialmente na Alemanha por Hans Carl Nipperdey, sob o fundamento de que os perigos que espreitam os direitos fundamentais não provêm apenas do Estado, mas também dos poderes sociais em geral e de terceiros. Segundo Nipperdey, *os direitos fundamentais devem ser aplicados nas relações entre particulares, sendo desnecessária qualquer mediação legislativa ou qualquer "artimanha interpretativa" para serem aplicados*. Ao se referir à desnecessidade de "artimanha interpretativa", Nipperdey faz referência às denominadas *cláusulas gerais* e aos *conceitos jurídicos indeterminados* utilizados para infiltração dos direitos fundamentais nas relações privadas. Assim, de acordo com essa teoria, *os direitos fundamentais são aplicáveis diretamente a todas as relações entre particulares, o que significa, em termos concretos, que os indivíduos podem recorrer aos direitos fundamentais para fazê-los valer contra atos de outros indivíduos ou de pessoas jurídicas*[189].

Admitindo-se a *eficácia direta ou imediata* dos direitos fundamentais nas relações privadas, a doutrina chega à conclusão de que, se as entidades privadas desrespeitarem esses preceitos recorrendo a contratos ou a cláusulas contratuais, tais subterfúgios deverão ser considerados nulos. Dependendo do caso concreto, ainda pode ser ventilada uma obrigação de indenização pelos danos acarretados à parte mais fraca da relação jurídica[190].

A Constituição portuguesa expressamente prevê a *eficácia horizontal direta* no art. 18º, nº 1: "*Os preceitos constitucionais respeitantes aos direitos, liberdades e garantias são directamente aplicáveis e vinculam as entidades públicas e privadas*"[191]. Nas palavras de Jorge Miranda, os direitos fundamentais incidem, e podem incidir, tanto nas relações com entidades públicas quanto nas relações com particulares, como se depreende dos seguintes dispositivos:

---

[188] SILVA, Vasco Manuel Pascoal Dias Pereira da. Vinculação das entidades privadas pelos direitos, liberdades e garantias. **Revista de Direito Público**. São Paulo: STJ, n. 82, abr./jun. 1987, p. 45.
[189] NIPPERDEY, Hans C. Boykott und freie MeinungsäuBerung, Deutsches Verwaltungsblatt 73 (1958), p. 447 apud SILVA, Virgílio Afonso da. **A constitucionalização do direito**: os direitos fundamentais nas relações entre particulares. São Paulo: Malheiros, 2005, p. 90.
[190] SILVA, Vasco Manuel Pascoal Dias Pereira da. Op. cit., pp. 50-51.
[191] PORTUGAL. **Constituição Portuguesa de 1976**. Op. cit.

proteção da reserva da intimidade e da vida privada (art. 26º, nº 1 da CRP)[192]; proibição de acesso de terceiros aos arquivos de dados pessoais (art. 35º, nº 2 da CRP)[193]; direito de retificação, resposta e indenização por danos sofridos por meio da imprensa (art. 37º, nº 4 da CRP)[194]; direito dos consumidores à informação, à proteção da saúde e dos seus interesses econômicos e à reparação de danos (art. 60º, nº 1 da CRP)[195]; direitos do autor (art. 42º, nº 2 da CRP)[196]. Esta fórmula foi inspirada na necessidade de se limitar não só o poder político, mas também todas as demais pessoas; considerando-se que o respeito à dignidade da pessoa humana e à autonomia do indivíduo devem ser resguardados não apenas nas relações com o Estado, mas também nas relações que as pessoas estabelecem entre si[197].

A Constituição brasileira não registra preceito semelhante ao art. 18º, nº 1 da Constituição portuguesa, mas a jurisprudência nacional demonstra que em nosso ordenamento jurídico também é admitida a *eficácia horizontal direta ou imediata* dos direitos fundamentais. Um caso interessante que deve ser mencionado relaciona-se com a exclusão de associados de uma cooperativa, sem observância das regras estatutárias e com ofensa ao direito à ampla defesa. Segundo o relator, ministro Marco Aurélio, a garantia da ampla defesa está insculpida em preceito de ordem pública, razão por que não passível de transgressão em nenhum âmbito, inclusive nas relações entre particulares. Destaque-se o seguinte trecho de seu voto:

> Exsurge, na espécie, a alegada contrariedade ao inciso LV do rol das garantias constitucionais. Conforme ressaltado pela Procuradoria-Geral da República, os Recorrentes foram excluídos do quadro de associados da Cooperativa em caráter punitivo, tal como se depreende do acórdão atacada [sic] (folhas 245 a 249). O Colegiado de origem acabou por mitigar a garantia da ampla defesa, levando em conta o desafio lançado pelos Recorrentes no sentido de serem julgados pela Assembléia da Cooperativa. A exaltação de ânimos não é molde a afastar a incidência do preceito constitucional assegurador da plenitude da defesa nos processos em geral. Mais do que nunca, diante do clima reinante, incumbia à

[192] "Art. 26º 1. *A todos são reconhecidos os direitos à identidade pessoal, ao desenvolvimento da personalidade, à capacidade civil, à cidadania, ao bom nome e reputação, à imagem, à palavra, à reserva da intimidade da vida privada e familiar e à protecção legal contra quaisquer formas de discriminação*". Loc. cit.
[193] "*Art. 35º 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*". Loc. cit.
[194] "Art. 37º 4. *A todas as pessoas, singulares ou colectivas, é assegurado, em condições de igualdade e eficácia, o direito de resposta e de rectificação, bem como o direito a indemnização pelos danos sofridos*". Loc. cit.
[195] "Art. 60º 1. *Os consumidores têm direito à qualidade dos bens e serviços consumidos, à formação e à informação, à protecção da saúde, da segurança e dos seus interesses económicos, bem como à reparação de danos*". Loc. cit.
[196] "Art. 42º 2. *Esta liberdade compreende o direito à invenção, produção e divulgação da obra científica, literária ou artística, incluindo a protecção legal dos direitos de autor*". Loc. cit.
[197] MIRANDA, Jorge. **Manual de direito constitucional**. Op. cit., pp. 321-325.

> Cooperativa, uma vez instaurado o processo, dar aos acusados a oportunidade de defenderem-se e não serem excluídos sumariamente do quadro de associados. (...) Fulmino o ato da assembléia da Recorrida que implicou na exclusão dos Recorrentes do respectivo quadro social, reintegrando-os, assim, com os consecutários pertinentes e que estão previstos no Estatuto da Recorrida.[198]

Outro caso curioso relaciona-se com a aplicação desse direito fundamental no que concerne ao direito à igualdade em relações trabalhistas – relações de caráter eminentemente privado. Trata-se da decisão prolatada pelo STF, em sede de Recurso Extraordinário – RE interposto por *Joseph Halfin* contra a companhia aérea *Air France*, sediada no Brasil. A empresa – na condição de empregadora – negou ao recorrente – seu empregado – a concessão de benefícios previstos no Estatuto do Pessoal da Empresa, por ter o mesmo recorrente nacionalidade brasileira e não francesa. O relator para o acórdão, ministro Carlos Veloso, acolhendo parecer da Procuradoria da República, manifestou-se pela proibição de qualquer discriminação entre empregados franceses e brasileiros em empresa sujeita às leis nacionais, por ofensa ao princípio da isonomia consagrado pela Constituição, *verbis*:

> EMENTA. CONSTITUCIONAL. TRABALHO. PRINCÍPIO DA IGUALDADE. TRABALHADOR BRASILEIRO EMPREGADO DE EMPRESA ESTRANGEIRA: ESTATUTOS DO PESSOAL DESTA: APLICABILIDADE AO TRABALHADOR ESTRANGEIRO E AO TRABALHADOR BRASILEIRO. CF, 1967, art. 153, § 1º; CF, 1988, art. 5º, caput.
> I – Ao recorrente, por não ser francês, não obstante trabalhar para a empresa francesa, no Brasil, não foi aplicado o Estatuto do Pessoal da Empresa, que concede vantagens aos empregados, cuja aplicabilidade seria restrita ao empregado de nacionalidade francesa. Ofensa ao princípio da igualdade: CF, 1967, art. 153, § 1º; CF, 1988, art. 5º, caput).
> II. – A discriminação que se baseia em atributo, qualidade, nota intrínseca ou extrínseca do indivíduo, como o sexo, a raça, a nacionalidade, o credo religioso etc., é inconstitucional. Precedente do STF: Ag 110.846(AgRg)-PR, Célio Borja, RTJ 119/465.
> III. – Fatores que autorizariam a desigualização não ocorrentes no caso.
> IV. - R.E. conhecido e provido.[199]

---

[198] BRASIL. Supremo Tribunal Federal. RE nº 158215/RS. Recorrentes: Airton da Silva Capaverde e outros. Relator: Marco Aurélio. Brasília, DF, 30 de abril de 1996. **Diário da Justiça da República Federativa do Brasil**, Brasília, DF, 07 jun. 1996, p. 19830. Disponível em <http://www.stf.gov.br/jurisprudencia/nova/pesquisa.asp>. Acesso em: 30 jan. 2007. Grifos nossos.

[199] BRASIL. Supremo Tribunal Federal. RE nº 161243/DF. Recorrente: Joseph Halfin. Relator: Carlos Veloso. Brasília, DF, 29 de outubro de 1996. **Diário da Justiça da República Federativa do Brasil**, Brasília, DF, 19 dez. 1996, p. 00057. Disponível em <http://www.stf.gov.br/jurisprudencia/nova/pesquisa.asp>. Acesso em: 30 jan. 2007. Grifos nossos.

Pelo exposto, observa-se que atualmente já se consagrou na doutrina a vinculação das entidades privadas aos direitos fundamentais, havendo divergência apenas quanto à forma de aplicação desses preceitos, conforme se adote a *teoria da eficácia direta ou imediata* ou a *teria da eficácia indireta ou mediata*. De acordo com a primeira teoria, os direitos fundamentais aplicam-se obrigatória e diretamente nas relações privadas individuais e coletivas, sendo desnecessária qualquer mediação concretizadora por parte dos poderes públicos. Para a segunda teoria, os direitos fundamentais são aplicáveis unicamente nas relações privadas em que se estabelecem mediações do Legislativo ou do Judiciário. Observe-se, ainda, uma tendência da jurisprudência nacional pela adoção da *teoria da eficácia direta ou imediata.*

2.5.1 A eficácia horizontal do direito à privacidade na jurisprudência do Superior Tribunal de Justiça

A jurisprudência do STJ é farta de casos em que o direito à privacidade é invocado em face não do Estado, mas sim de outros particulares.

Um caso interessante refere-se à violação da *privacidade das comunicações*, sob a relatoria do ministro Adhemar Maciel. Marido traído resolve efetuar interceptação telefônica de conversa entre sua esposa e o amante. A decodificação da conversa telefônica é depois utilizada em processo criminal em que a esposa é acusada de ministrar tóxico às filhas menores. O Tribunal julgou a prova ilícita por violação aos incisos X e XII do art. 5º, determinando seu desentranhamento dos autos:

> EMENTA. CONSTITUCIONAL E PROCESSUAL CIVIL. MANDADO DE SEGURANÇA. ESCUTA TELEFONICA. GRAVAÇÃO FEITA POR MARIDO TRAIDO. DESENTRANHAMENTO DA PROVA REQUERIDO PELA ESPOSA: VIABILIDADE, UMA VEZ QUE SE TRATA DE PROVA ILEGALMENTE OBTIDA, COM VIOLAÇÃO DA INTIMIDADE INDIVIDUAL. RECURSO ORDINÁRIO PROVIDO.
> I – A impetrante/recorrente tinha marido, duas filhas menores e um amante medico. Quando o esposo viajava, para facilitar seu relacionamento espúrio, ela ministrava "lexotan" às meninas. O marido, já suspeitoso, gravou a conversa telefônica entre sua mulher e o amante. A esposa foi penalmente denunciada (tóxico). Ajuizou, então, ação de mandado de segurança, instando o desentranhamento da decodificação da fita magnética.
> II – Embora esta turma já se tenha manifestado pela relatividade do inciso XII (última parte) do art. 5º da CF/1988 (HC 3.982/RJ, rel. Min. Adhemar Maciel,

> DJU de 26/02/1996), no caso concreto o marido não poderia ter gravado a conversa a arrepio de seu cônjuge. Ainda que impulsionado por motivo relevante, acabou por violar a intimidade individual de sua esposa, direito garantido constitucionalmente (art. 5º, X). Ademais, o STF tem considerado ilegal a gravação telefônica, mesmo com autorização judicial (o que não foi o caso), por falta de lei ordinária regulamentadora (RE 85.439/RJ, Min. Xavier de Albuquerque e HC 69.912/RS, Min. Pertence).
> III – Recurso ordinário provido.[200]

Outro caso relevante relaciona-se com a *privacidade informacional*, que detém, em seu âmbito de proteção, informações sobre determinada pessoa e o controle dessas mesmas informações pelo próprio titular. Trata-se de decisão prolatada em Recurso Especial – RESP, interposto por Anália Maria Patti Souza Varella, que pleiteava indenização por danos morais em virtude da indevida veiculação de anúncio, nas páginas amarelas da lista telefônica, com seu nome e telefone em seção sob título "massagens". Mesmo após ter solicitado a retirada de seus dados do anúncio, a mesma vinculação constou na lista telefônica do ano seguinte. O Tribunal julgou procedente a indenização por violação do direito à privacidade da recorrente, destacando-se o seguinte trecho do voto do relator, ministro Fernando Gonçalves:

> A publicação equivocada do anúncio nas "páginas amarelas" da lista telefônica faz retratar o procedimento pouco diligente da recorrida na prestação do serviço de publicidade. Mais que desídia, sua conduta descreve até certo ponto descaso e também negligência, pois mesmo ciente da insatisfação da recorrente (representada pela reclamação perante o Centro de Informação e Orientação ao Consumidor e pelo ajuizamento da presente ação) nada fez para impedir nova publicação de mensagem lesiva já no ano de 2001. O anúncio erroneamente veiculado representa inequívoco dano, diante da violação ao direito à intimidade da recorrente, que teve publicado seu endereço e telefone residenciais de forma indevida e não autorizada. O direito à intimidade é espécie do gênero "direitos da personalidade" sendo compreendidos como *"direitos considerados essenciais à pessoa humana, que a doutrina moderna preconiza e disciplina, a fim de resguardar a sua dignidade"* (GOMES, Orlando. *Introdução ao direito civil.* 18ª ed., Rio de Janeiro: Forense, 2001, p. 141), de cunho extrapatrimonial. Não se dispensa inteligência superior para verificação do constrangimento e incômodo a que a recorrente esteve exposta, com a publicação (sem autorização) de anúncio mal formulado contendo um nome feminino em uma seção de "massagens" de uma lista telefônica. Em se tratando de direito à intimidade, a obrigação da reparação decorre da própria violação do direito personalíssimo, não havendo de cogitar-se da prova da existência do dano.[201]

---

[200] BRASIL. Superior Tribunal de Justiça. RMS nº 5352/GO. Recorrente: Mara Sueli Neves de Oliveira. Relator para o Acórdão: Adhemar Maciel. Brasília, DF, 27 de maio de 1996. **Diário da Justiça da República Federativa do Brasil**, Brasília, DF, 25 nov. 1996, p. 46227. Disponível em <http://www.stj.gov.br/SCON/jurisprudencia>. Acesso em: 30 jan. 2007. Grifos nossos.

[201] BRASIL. Superior Tribunal de Justiça. RESP nº 506437/SP. Recorrente: Anália Maria Patti Souza Varella. Relator: Fernando Gonçalves. Brasília, DF, 16 de setembro de 2003. **Diário da Justiça da República Federativa do**

Outra decisão curiosa foi tomada pelo STJ no que ser refere à preservação do direito à privacidade de jogadores de futebol. A Confederação Brasileira de Futebol – CBF, sob a alegação de exercício do *direito de arena*, forneceu fotos de alguns jogadores para a Editora Abril, que depois publicou, em álbum de figurinhas, a imagem dos esportistas. O direito de arena consiste no direito de os clubes explorarem imagens de partidas desportivas e encontra-se regulamentado pelo art. 42, caput, da Lei nº 9.615, de 24 de março de 1998, que traz a seguinte redação: "*Às entidades de prática desportiva pertence o direito de negociar, autorizar e proibir a fixação, a transmissão ou retransmissão de imagem de espetáculo ou eventos desportivos de que participem*". O referido direito – de titularidade das entidades de prática desportiva – permite que os clubes transmitam imagens de jogo, mas não outorga a esses mesmos clubes o direito de explorarem a imagem dos esportistas após o término da partida, o que exige prévia negociação individualizada. Os atletas lesados ajuizaram ação de reparação de danos em virtude da violação de seu direito à intimidade, vida privada e imagem. Ganharam em primeira e em segunda instâncias, subindo os autos ao STJ por recurso da CBF que foi julgado improcedente, *verbis*:

> EMENTA. DIREITO A IMAGEM. DIREITO DE ARENA. JOGADOR DE FUTEBOL. ALBUM DE FIGURINHAS.
> O direito de arena que a lei atribui às entidades esportivas limita-se a fixação, transmissão e retransmissão do espetáculo desportivo público, mas não compreende o uso da imagem dos jogadores fora da situação específica do espetáculo, como na reprodução de fotografias para compor "álbum de figurinhas". Lei nº 5.989/73, artigo 100; Lei nº 8.672/93.[202]

Mais um caso de relevo relacionado com o direito à *privacidade informacional* e à imagem refere-se à publicação de matéria em revista sem prévia autorização do entrevistado. A jornalista Lílian Wite Fibe forneceu entrevista para a Editora Abril, autorizando a publicação de matéria na Revista Veja. A Editora, sem prévia autorização da entrevistada, publicou, na Revista Caras, matéria com informações pessoais e fotos havidas durante a entrevista, o que levou a jornalista ao ajuizamento de ação por danos morais. O Tribunal, sob a relatoria do ministro Ruy Rosado de Aguiar, entendeu existir, na espécie, violação ao direito à intimidade e vida privada da recorrente:

Brasil, Brasília, DF, 16 out. 2006, p. 280. Disponível em <http://www.stj.gov.br/SCON/jurisprudencia>. Acesso em: 30 jan. 2007. Grifos nossos.

[202] BRASIL. Superior Tribunal de Justiça. RESP nº 46420/SP. Recorrente: Confederação Brasileira de Futebol e Editora Abril S.A. Relator: Ruy Rosado Aguiar. Brasília, DF, 12 de setembro de 1994. **Diário da Justiça da República Federativa do Brasil**, Brasília, DF, 05 dez. 1994, p. 33565. Disponível em <http://www.stj.gov.br/SCON/jurisprudencia>. Acesso em: 30 jan. 2007.

> EMENTA. RESPONSABILIDADE CIVIL. DANO MORAL. FOTOGRAFIAS. REVISTA.
> A cessão de fotografias feitas para um determinado fim, mostrando cenas da intimidade da entrevistada, é fato ilícito que enseja indenização se, da publicação desse material, surgir constrangimento à pessoa, não tendo esta concedido entrevista ao veículo que o divulgou. Recurso conhecido e provido.[203]

Outro acórdão que merece registro refere-se à possibilidade de o Banco Central do Brasil – BC fornecer informações de titulares de contas bancárias para fins de ajuizamento de ação de execução por terceiros. O STJ, em sede de RESP, julgou incabível o fornecimento pelo BC de endereço de titular de conta bancária, sob o fundamento de que a quebra do sigilo bancário viola o direito individual à proteção de dados pessoais:

> EXECUÇÃO - REQUISIÇÃO DE INFORMAÇÃO DE ENDEREÇO DO RÉU AO BANCO CENTRAL - IMPOSSIBILIDADE.
> 1. Embora na hipótese dos autos não se pretenda, através de requisição ao Banco Central, obter informações acerca de bens do devedor passíveis de execução, mas tão-somente o endereço, o raciocínio jurídico a ser adotado é o mesmo.
> 2. O contribuinte ou o titular de conta bancária tem direito à privacidade em relação aos seus dados pessoais, além do que não cabe ao Judiciário substituir a parte autora nas diligências que lhe são cabíveis para demandar em juízo.
> 3. Recurso especial não conhecido.[204]

Diante de todos esses julgados, conclui-se que, no ordenamento jurídico nacional, apesar de inexistir expresso dispositivo constitucional determinando *a aplicação direta ou imediata dos direitos fundamentais nas relações entre particulares*, tal medida configura-se como uma decorrência lógica do caráter objetivo dos direitos fundamentais. *Enquanto garantia integrante do estatuto axiológico do ordenamento jurídico nacional, o direito à privacidade estende-se por todos os ramos do direito, vinculando tanto o poder tanto o poder público como os demais particulares de forma direta ou imediata, conforme a jurisprudência colacionada acima.*

[203] BRASIL. Superior Tribunal de Justiça. RESP nº 221757/SP. Recorrente: Lílian Vite Fibe. Relator: Ruy Rosado de Aguiar. Brasília, DF, 16 de setembro de 1999. **Diário da Justiça da República Federativa do Brasil**, Brasília, DF, 27 mar. 2000, p. 267. Disponível em <http://www.stj.gov.br/SCON/jurisprudencia>. Acesso em: 30 jan. 2007. Grifos nossos.

[204] BRASIL. Superior Tribunal de Justiça. RESP nº 306570/SP. Recorrente: Regina Célia Rebello da Silva Furtado. Relatora: Eliana Calmon. Brasília, DF, 18 de outubro de 2001. **Diário da Justiça da República Federativa do Brasil**, Brasília, DF, 18 fev. 2002, p. 340. Disponível em <http://www.stj.gov.br/SCON/jurisprudencia>. Acesso em: 30 jan. 2007. Grifos nossos.

2.6 Renúncia à privacidade: *reality shows* e contratos de trabalho

Adotando-se a premissa de que o direito à privacidade é um direito da personalidade, conforme descrito no item 1.5, e de que os direitos da personalidade têm como característica a irrenunciabilidade, coloca-se em questão a possibilidade ou não de renúncia ao direito à privacidade.

Silvia Venosa manifesta-se pela impossibilidade de disposição da privacidade, da liberdade, da integridade física e do nome, uma vez que os direitos da personalidade resguardam a dignidade da pessoa humana – o bem jurídico mais importante de todo o ordenamento jurídico. Reconhece, todavia, que na sociedade atual existem situações que tangenciam a proibição de renúncia aos direitos da personalidade, como ocorre em certos programas de televisão, em que participantes se sujeitam a monitoramento e vigilância permanentes, abdicando do seu direito à privacidade – os denominados *reality shows* – e outros mais em que se coloca a integridade física e psicológica em situação-limite de resistência. Em tais casos, indubitavelmente, os envolvidos negociam direitos em tese irrenunciáveis[205].

A maior parte dos civilistas posiciona-se no sentido de que o direito à privacidade é *irrenunciável*, pois, na condição de *direito da personalidade,* reveste-se de características incompatíveis com o exercício da renúncia: é *necessário*, sendo indispensável ao desenvolvimento da personalidade do indivíduo; *indisponível*, não sendo passível de comercialização ou disposição, seja pelo próprio titular ou por terceiro; e *perpétuo*, devendo perdurar durante toda a vida do indivíduo e ainda produzir efeitos após sua morte. Dispõe expressamente o art. 11 do CC: "*Com exceção dos casos previstos em lei, os direitos da personalidade são intransmissíveis e irrenunciáveis, não podendo o seu exercício sofrer limitação voluntária*".

Mário Luiz Delgado, ao analisar o art. 11 do CC, sustenta que esse dispositivo não proíbe a fruição econômica dos direitos da personalidade, sendo permitida a venda da própria imagem até mesmo em situações de pornografia; não se admite, porém, cessão duradoura quanto ao tempo ou indeterminada quanto ao objeto. De acordo com o autor, o tema foi debatido na I Jornada de Direito Civil, promovida pelo Centro de Estudos do Conselho da Justiça Federal –

[205] VENOSA, Sílvio de Salvo. Op. cit., p. 174.

CJF, em setembro de 2002, chegando os congressistas à conclusão, prevista no Enunciado nº 4 do Evento, de que: "*O exercício dos direitos da personalidade pode sofrer limitação voluntária, desde que não seja permanente nem geral*" [206].

Abandonando-se a interpretação literal do art. 11 do CC e considerando-se o Enunciado nº 4 da I Jornada de Direito Civil promovida pelo Centro de Estudos do CJF, conclui-se que os direitos da personalidade – incluindo-se nesse rol o direito à privacidade – são *irrenunciáveis*, permitindo-se, entretanto, nos casos previstos em lei, a *limitação temporária de exercício, distinguindo-se esta da renúncia pelo fato de ser específica quanto ao objeto, transitória quanto ao tempo e revogável a qualquer momento.*

No caso do direito à privacidade, o art. 20 do CC expressamente prevê a possibilidade de *limitação temporária de exercício*, desde que exista prévia autorização do titular ou quando for necessária tal limitação, em atendimento à administração da Justiça ou à ordem pública: "*Salvo se autorizadas, ou se necessárias à administração da Justiça ou à manutenção da ordem pública, a divulgação de escritos, a transmissão da palavra, ou a publicação, a exposição ou a utilização da imagem de uma pessoa poderão ser proibidas, a seu requerimento e sem prejuízo da indenização que couber, se lhe atingirem a honra, a boa fama ou a respeitabilidade, ou se se destinarem a fins comerciais*".

Sob o enfoque desse dispositivo do CC, devem ser analisados os casos em que pessoas comuns ou notórias – valendo-se do *direito à autodeterminação* – propõem-se a expor para o público imagens ou informações pessoais; sejam aspectos de sua vida sexual, religiosa e política, sejam sentimentos em geral. Quanto a essa perspectiva, lembre-se a íntima relação que se estabelece entre privacidade e liberdade: a proteção da intimidade e da vida privada é antes de tudo um pressuposto para o exercício da liberdade de consciência, de crença e de expressão, configurando-se como uma proteção contra "ingerências alheias" que perturbem o livre desenvolvimento da personalidade, o que não veda a auto-exposição a critério do próprio titular. Trata-se de um "direito" da personalidade e não um "dever" da personalidade, sendo seu exercício "pleno" ou "limitado" segundo a íntima convicção do indivíduo.

Para exemplificar tal situação, ventile-se a hipótese de edição de uma lei que proíba a divulgação na internet, pelo próprio titular, de informações de caráter pessoal – filiação

[206] DELGADO, Mário Luiz. Big Brother Brasil: *reality shows* e os direitos da personalidade. **Revista Jurídica Consulex**. Ano VIII, nº 169, 31 de janeiro de 2004, pp. 24-26.

partidária, estado de saúde, situação econômico-financeira, preferência sexual, crenças e sentimentos –, com o fim de proteger os usuários da rede de investidas criminosas e diminuir a incidência dos *cybercrimes*. Discute-se como o Estado poderia impedir a publicação de *blogs*[207] e a participação em comunidades virtuais como o *Orkut*, em que pessoas comuns e notórias, de livre e espontânea vontade, expõem informações sensíveis abertamente, declaram-se portadora de doenças estigmatizantes, simpatizantes ou não simpatizantes de certos grupos de pessoas, integrantes ou não de determinadas agremiações políticas ou religiosas, além de fornecerem dados pessoais como endereço e telefones para contato.

Apenas à própria pessoa cabe o julgamento de se expor ou de não se expor e, ainda mais importante, até que limite deseja se expor; competindo ao Estado apenas o dever de alertar para os perigos decorrentes de tal conduta, como a maior vulnerabilidade em relação a estelionatários, a chantagistas, a seqüestradores ou a outros tipos de criminosos. O indivíduo poderá – seguindo a teoria alemã das esferas (*Sphärentheorie*) – abrir para conhecimento de terceiros fatos de sua esfera privada (*Privatsphäre*), de sua esfera de intimidade em sentido lato (*Intimsphäre*) ou, até mesmo, de sua esfera de intimidade em sentido estrito (*Geheimsphäre*); não existindo nenhum mecanismo apto ao impedimento de tal devassa, por mais perniciosa que tal atitude se mostre para o próprio titular do direito e para a comunidade em geral.

Sob tal aspecto, a privacidade, e aí se inclui a "liberdade de divulgação de fatos íntimos", destaca-se como um mecanismo de extrema relevância para a construção de uma *sociedade pluralista* baseada na tolerância e no respeito mútuo entre os diferentes grupos de pessoas – conjunto de indivíduos com características comuns descobertas a partir da revelação de informações pessoais por parte de seus membros. Criar identidade com outras pessoas supõe a exposição de aspectos íntimos da própria personalidade; a aceitação das diferenças e a formação de uma sociedade pluralista pressupõem a liberdade dos indivíduos de exporem as próprias idiossincrasias. Deve-se abandonar, portanto, a concepção ortodoxa e paternalista – tão comum nos regimes ditatoriais – em que ao Estado cabe decidir "o que" e "em que medida" é bom para os indivíduos, impondo-se a observância de certos "direitos" que mais se identificam com "deveres".

[207] *Blog* é um diário virtual, com conexões cronologicamente atualizadas, em que as pessoas escrevem sobre seus sentimentos, crenças, experiências e passatempos; compartilhando com os outros internautas diversas informações de caráter pessoal.

Gomes Canotillho e Jónatas Machado – em estudo a respeito do problema da privacidade na sociedade contemporânea – alertam que expressões como "intimidade" e "vida privada" devem ser interpretadas na sua dependência contextual pelo caráter variável e passível de mudanças no tempo e no espaço. Dependendo da evolução da mentalidade em uma época, da identidade das pessoas envolvidas, de seu papel social e do estilo de vida dos interessados; o conceito de privacidade pode adquirir maior ou menor elasticidade, o que não recomenda qualquer interferência estatal. Uma pessoa que decide tornar públicos comportamentos normalmente protegidos pelo direito à privacidade não está a renunciar o exercício desse direito; mas apenas a exercê-lo autonomamente de acordo com suas próprias preferências. Nesse sentido, a privacidade deve ser analisada sob a concepção do próprio titular do direito e não de acordo com uma visão unidimensional e heterônoma que ignore as antagônicas e incomensuráveis visões de mundo características das sociedades pluralistas[208].

Também reverbera na teoria geral do direito constitucional a questão em torno da possibilidade ou não de se renunciar os direitos da personalidade, considerando-se que tais direitos se definem como espécie de direitos fundamentais. Parte dos constitucionalistas prega que os direitos fundamentais são *irrenunciáveis* porque – na condição de expressão do *princípio da dignidade da pessoa humana* – formam o *estatuto axiológico* de todo o ordenamento jurídico, vinculando entes públicos e privados. Segundo essa corrente doutrinária – à semelhança dos civilistas – a irrenunciabilidade de tais preceitos não impede, todavia, a *limitação temporária de exercício*, desde que não seja afetado o *núcleo essencial* do direito fundamental. Nesse sentido, o cidadão pode decidir não invocar um direito fundamental em uma determinada circunstância fática, ou, até mesmo, recusar o seu exercício, desde que não se reduza à condição de objeto, mitigando a dignidade da pessoa humana – o que produziria reflexos para toda a coletividade. A outra corrente doutrinária prega que os direitos fundamentais são renunciáveis pelo próprio titular, não se estabelecendo qualquer distinção entre a decisão de *renúncia* e a *limitação temporária de exercício*.

Estes são os ensinamentos de Gomes Canotilho a respeito do tema:

> Se a Constituição só permite restrição através de lei e nos casos nela expressamente previstos, seria fácil eliminar a força dirigente dos direitos fundamentais, imanente a esta reserva, se a vontade individual se sobrepusesse ao sentido constitucional da reserva e transformasse os direitos, liberdades e

[208] CANOTILHO, José Joaquim Gomes; MACHADO, Jónatas E. M.. **Reality Shows e liberdade de programação**. Coimbra: Coimbra Editora, 2003, pp. 55-57.

> garantias em direitos totalmente disponíveis, suscetíveis, inclusive, de renúncia. (...) O princípio da autonomia contratual justificava, à semelhança do princípio *volenti non fit injuria*, uma redução do alcance do princípio da reserva da lei restritiva. De qualquer modo, a renúncia a direitos fundamentais, mesmo a admitir-se, pressupõe sempre como *conditio sine qua* que o titular do direito dispunha sobre a sua posição jurídica de forma livre e autodeterminada. (...) O problema vai entroncar na questão, já estudada, da eficácia *erga omnes* dos direitos fundamentais, e no problema, há muito tratado pela doutrina de renúncia aos direitos da personalidade. A orientação deve ser fundamentalmente diferenciada: (1) é irrenunciável qualquer direito medularmente inerente à dignidade da pessoa humana (...); (2) os direitos fundamentais, como totalidade, são irrenunciáveis, devendo distinguir-se entre renúncia ao núcleo substancial do direito (constitucionalmente proibida) e limitação voluntária ao exercício (aceitável sob certas condições) de direitos. (...) Poderá, assim, existir uma disposição individual acerca de posições de direitos fundamentais, mas o "o uso negativo" de um direito não significa renúncia a esse mesmo direito.[209]

Jorge Miranda formula uma hipótese que exemplifica a *limitação temporária de exercício* a critério do próprio titular do direito fundamental: "*No âmbito de relações contratuais de direito privado e na perspectiva (há pouco apontada a propósito da vinculação de entidades privadas), de escolha de bens ou interesses em presença (v.g., obter um emprego e ter de fixar residência em certo local, em vez de ficar livre para escolher qualquer outro)*"[210]. Gomes Canotilho, embora também rejeite a idéia de renúncia aos direitos fundamentais, afirma que "*no cerne dos direitos, liberdades e garantias, encontra-se a idéia de que os mesmos se caracterizam pela sua densidade subjetiva autônoma, no sentido de que cabe ao seu titular a tomada de decisões fundamentais nesse domínio*"[211], ou seja, admite uma limitação temporária do exercício por decisão do próprio titular.

O indivíduo – no uso do seu direito ao livre desenvolvimento da personalidade – deve deter o poder de autodeterminar-se e de conduzir seus projetos de vida. Essa regra, contudo, alcança um limite: o sujeito não pode promover uma auto-restrição que implique a violação da garantia mínima do preceito, que afete a dignidade da pessoa humana – o axioma antropológico que atua como premissa para que se resguardem todos os direitos fundamentais. Em nome de sua própria liberdade, o indivíduo não pode reduzir-se à condição de objeto, de não-pessoa – nestes casos, o bem jurídico deve ser considerado indisponível. Assim, deve-se aceitar a auto-restrição,

[209] CANOTILHO, José Joaquim Gomes. **Direito constitucional e teoria da Constituição**. Op. cit., pp. 463-465. Grifos nossos.
[210] MIRANDA, Jorge. **Manual de direito constitucional**. Op. cit., p. 356.
[211] CANOTILHO, José Joaquim Gomes; MACHADO, Jónatas E. M. Op. cit., p. 107.

desde que essa liberdade não prejudique intoleravelmente a idéia de dignidade da pessoa humana[212].

Para se avaliar a auto-restrição, classificá-la como pertinente ou não, deve-se aferir também – além da afetação do núcleo essencial da garantia, ou seja, o preceito da dignidade da pessoa humana – a *existência da autonomia do indivíduo no momento da deliberação da restrição.* A autonomia revela a capacidade de o sujeito determinar o próprio comportamento individual e de governar as relações jurídicas que lhes são próprias, ou seja, *de decidir de forma livre e autodeterminada*. Essa autonomia, entretanto, não se confunde com a verificação da igualdade ou da desigualdade material das partes, uma vez que, mesmo em situação de extrema desigualdade material e de poder, ainda assim, pode restar preservada a autonomia dos envolvidos. Errônea, portanto, a adoção de um critério geral de que sempre que houver desigualdade material ou de poder entre as partes, deverá ser mitigado o nível de influência da autonomia privada, devendo-se verificar o grau de *autonomia real* da partes[213].

José Carlos Vieira de Andrade arrola algumas hipóteses em que se observa a inexistência de autonomia de uma das partes da relação jurídica, isto é, a ausência de liberdade e de poder de autodeterminação: (a) quando os grupos ou organizações exercem poder sobre os seus membros, à semelhança das relações típicas de direito administrativo, como ocorre em sindicatos, associações e organizações religiosas; (b) quando a entidade dispõe de um poder social ou econômico que atinja até os não membros como empresas monopolistas ou em situação de quase monopólio; (c) quando uma das partes exerce poder normativo ou institucional sobre a outra, como se verifica em federações desportistas[214]. *Nesses casos, após a verificação de ausência de autodeterminação no momento da deliberação a respeito do ato ou negócio jurídico, deve o Judiciário promover a devida anulação e determinar o pagamento de indenização pelos danos decorrentes da restrição indevida ao direito fundamental pela parte mais fraca. Inexistindo autonomia na decisão de auto-restrição ao direito fundamental, o ato ou o negócio jurídico em questão deve ser considerado inválido por vício de vontade de uma das partes da relação jurídica*.

---

[212] ANDRADE, José Carlos Vieira de. **Os direitos fundamentais na Constituição Portuguesa de 1976**. 3ª ed. Coimbra: Almedina, 2006, pp. 273-276.
[213] SILVA, Virgílio Afonso da. Op. cit., pp. 157-158.
[214] ANDRADE, José Carlos Vieira de. Op. cit., pp. 263-266.

Pelo exposto, verifica-se que, tanto para os civilistas quanto para grande parte dos constitucionalistas, os direitos da personalidade são irrenunciáveis. Essa irrenunciabilidade não impede, todavia, a *limitação temporária de exercício, a critério do próprio titular* – no uso do seu direito ao livre desenvolvimento da personalidade – ou por d*eterminação do Legislativo e do Judiciário nos estritos limites da Constituição – para resolução dos conflitos com outros direitos fundamentais ou com outros valores constitucionalmente protegidos* como, por exemplo, para administração da Justiça e manutenção da ordem pública.

A decisão de auto-restrição do próprio titular do direito será válida, desde que, observados os seguintes requisitos: (a) a restrição não pode afetar o *núcleo essencial* do direito fundamental, ou seja, aquela parcela mínima necessária à preservação da *dignidade da pessoa humana*, sob pena de total descaracterização do preceito; (b) a limitação deve ser *temporária,* sendo inconstitucional a limitação permanente, pois isto representaria renúncia à própria titularidade do direito e não apenas ao seu exercício; (c) ainda que exista assimetria de forças na relação jurídica, esta desigualdade material não pode implicar a ausência de *autonomia real* da parte mais fraca, porque sua decisão tem que ser tomada de forma *livre* e *autodeterminada.*

Esses critérios serão utilizados para uma breve análise da questão da restrição à privacidade nos denominados *reality shows* e nos contratos de trabalho.

Reality shows são programas de televisão que expõem a vida real de seus participantes em troca de prêmios em dinheiro ou outros tipos de vantagem. Destaque-se como o mais evidente o *Big Brother*, programa inspirado no livro *1984*, do autor George Orwell, em que o escritor narra a história de uma sociedade em permanente vigilância. Aquele que deseja participar do programa assina um contrato com a emissora, comprometendo-se não apenas a permanecer confinado de forma ininterrupta em uma casa monitorada e devassada por câmaras que acompanham em tempo integral qualquer movimento nos recintos desse ambiente, bem como a participar de diversas tarefas até ser eliminado pelos demais concorrentes ou triunfar como o grande vencedor do concurso. Em um outro programa, que se intitula *O Aprendiz*, os participantes se propõem a enclausurar-se em um hotel de luxo, a fim de cumprir tarefas que testam habilidades profissionais, cabendo ao vencedor um emprego em uma corporação de renome e salário anual acima do valor de mercado.

Alguns juristas criticam veementemente os referidos programas, sustentando a necessidade de intervenção estatal para interrupção da transmissão sob fundamento de violação

da dignidade dos participantes ao restringirem a privacidade da pessoa humana em prol de um ganho de caráter exclusivamente patrimonial. Outros defendem a liberdade de programação, alertando para a proibição da censura[215] e a necessidade de proteção de outros direitos fundamentais dos participantes como a livre expressão da atividade artística e o livre exercício de qualquer trabalho, ofício ou profissão[216].

Em relação aos participantes de programas de *reality shows*, constata-se que o comportamento desses indivíduos preenche os pressupostos de fato, tanto do *direito à privacidade* como do *direito à liberdade de expressão da atividade artística e de profissão*. Vive-se, portanto, um típico caso de *concorrência de direitos fundamentais*. Nas palavras de Gomes Canotilho:

> Concorrência de direitos fundamentais existe quando um comportamento do mesmo titular preenche os pressupostos de fato de vários direitos fundamentais. (...) Uma das formas de concorrência de direitos é, precisamente, aquela que resulta do cruzamento de direitos fundamentais: o mesmo comportamento de um titular é incluído no âmbito de proteção de vários direitos, liberdades e garantias. O conteúdo destes direitos tem, em certa medida e em certos sectores limitados, uma "cobertura" normativa igual. (...) Outro modo de concorrência de direitos verifica-se com a acumulação de direitos: aqui não é um comportamento que pode ser subsumido no âmbito de vários direitos que se entrecruzam entre si; um determinado "bem jurídico" leva à acumulação, na mesma pessoa, de vários direitos fundamentais[217].

Para solucionar essa *concorrência de direitos fundamentais*, credite-se preponderância ao direito fundamental sujeito a menos restrições pela própria Constituição, como forma de garantir a máxima efetividade das normas constitucionais. Como o direito à privacidade tem seus limites expressamente regrados por vários dispositivos constitucionais, conforme se detalha nos itens 2.8 e 2.10, deve-se conferir prevalência ao direito à liberdade de expressão da atividade artística e de profissão, admitindo-se que o indivíduo exponha sua vida íntima e privada, inclusive para fins econômicos, no exercício de sua profissão ou expressão artística. Por outro lado, apesar de permitida a restrição do direito à privacidade pelo próprio titular, tal ato não pode implicar sua

---

[215] "*Art. 220. A manifestação do pensamento, a criação, a expressão e a informação, sob qualquer forma, processo ou veículo não sofrerão qualquer restrição, observado o disposto nesta Constituição. (...) § 2º - É vedada toda e qualquer censura de natureza política, ideológica e artística*.". In BRASIL. **Constituição da República Federativa do Brasil de 1988**. Op. cit.

[216] "*Art. 5º IX - é livre a expressão da atividade intelectual, artística, científica e de comunicação, independentemente de censura ou licença; XIII - é livre o exercício de qualquer trabalho, ofício ou profissão, atendidas as qualificações profissionais que a lei estabelecer*;". In BRASIL. **Constituição da República Federativa do Brasil de 1988**. Op. cit.

[217] CANOTILHO, José Joaquim Gomes. **Direito constitucional e teoria da Constituição**. Op. cit., p. 1268. Grifos nossos.

renúncia total, pois isto, sim, afrontaria o *núcleo essencial*[218] desse preceito fundamental, a ponto de, para o titular, esse direito perder o significado, além de violar o princípio da dignidade da pessoa humana.

Gomes Canotilho e Jónatas Machado – em estudo específico sobre o tema, encomendado pela Alta Autoridade para Comunicação Social da República Portuguesa – afirmam que não há como se falar em violação da dignidade da pessoa humana em programas de *reality shows*, tendo em vista que não se evidenciam sinais de danos psicológicos ou físicos causados pelos referidos programas aos concorrentes. Ressaltam que, quanto a esse aspecto, os denominados *reality shows* transformam pessoas vulgares, como pedreiros, estudantes, *disk-jockeys,* balconistas em figuras públicas conhecidas e adoradas do país. Ao invés de degradarem as capacidades física, moral e psicológica dos participantes; proporcionam oportunidades sociais, culturais, profissionais e econômicas que dificilmente seriam obtidas nas circunstâncias em que tais pessoas se encontravam antes de se proporem a participar do programa[219].

Além de não violarem o princípio da dignidade da pessoa humana, os *reality shows* também não acarretam uma restrição permanente ao direito à privacidade, já que os participantes podem, voluntariamente, abandonar a casa a qualquer momento, implicando tal conduta única e exclusivamente na desclassificação do concurso. Trata-se, portanto, de uma *limitação temporária e revogável* a qualquer tempo, a critério do próprio titular do preceito. Em relação à *autonomia* da decisão de restrição ao direito fundamental em discussão, verifica-se que o concurso abre suas inscrições para pessoas que manifestem interesse de submeter-se ao processo de seleção para participação no programa. Embora as emissoras exibam irrefutável poderio econômico diante dos participantes, não se constata relação de subordinação entre as partes, demonstrando-se, assim, que se preserva a liberdade dos concorrentes na deliberação de se exporem para o público durante um determinado período de tempo. Nesse sentido, a participação nos chamados *reality shows* não acarreta renúncia ao direito à privacidade; trata-se de mera limitação temporária de exercício revogável a qualquer momento por decisão do próprio titular.

---

[218] Com relação ao conceito de núcleo essencial e seu objeto, duas teorias se defrontam: a teoria objetiva e a teoria subjetiva. Para a teoria objetiva, o objeto do núcleo essencial refere-se à proteção geral e abstrata prevista na norma, a fim de evitar que a disposição de um direito fundamental seja tal que este perca toda a importância para todos os indivíduos ou para a maior parte deles, ou, em geral, para toda a vida social. Para a teoria subjetiva, o objeto do núcleo essencial refere-se à proteção do direito fundamental do particular de tal modo que, em caso de sacrifício, o direito subjetivo de um homem não deixe de ter significado para ele mesmo. Para as duas teorias, o núcleo essencial é um mínimo de valor inatacável, trazendo uma proibição absoluta. In FARIAS, Edilsom. **Liberdade de expressão e comunicação**: teoria e proteção constitucional. São Paulo: Editora Revista dos Tribunais, 2004, pp. 42 e ss.

[219] CANOTILHO, José Joaquim Gomes; MACHADO, Jónatas E. M. Op. cit., p. 70.

Quanto à restrição à privacidade nas relações empregatícias, faz-se necessária uma rigorosa análise da relação jurídica eminentemente assimétrica que se instala, já que a uma das partes contratantes nega-se autonomia em relação à própria conduta. Conforme expôs José Carlos Vieira de Andrade, quando a organização exerce poder normativo ou institucional – à semelhança das relações típicas de direito administrativo – não há autonomia em relação aos empregados, aos quais resta apenas a possibilidade de invocar no Judiciário a invalidação dos atos jurídicos e a solicitação de indenização dos danos causados pela entidade[220]. Na resolução do conflito, o juiz deverá considerar os dois interesses em jogo: de um lado, o direito da pessoa jurídica à propriedade, à autogestão e à livre-iniciativa; de outro, o direito à privacidade de seus membros ou empregados.

Recentemente, uma estatística realizada nos EUA constatou que mais de um terço das empresas interceptam todas as mensagens de seus funcionários, sob a alegação de que os recursos tecnológicos devem ser controlados para que não sejam utilizados em prática de condutas imorais ou ilícitas[221]. Alguns doutrinadores defendem que não existe privacidade no ambiente de trabalho, porque os empregados – no exercício de suas atribuições – estão sujeitos ao poder de direção dos empregadores. Sustentam que as empresas podem – para fins de implementação de um efetivo controle – monitorar todas as comunicações de seus empregados, não havendo qualquer óbice em relação a tal conduta, já que os recursos tecnológicos utilizados são de propriedade da organização. Renato Opice Blum expõe os argumentos favoráveis ao rastreamento das comunicações dos empregados pelos empregadores: (a) os recursos tecnológicos são de propriedade da empresa; (b) há necessidade de controle diante do risco de responsabilização do empregador pelos atos dos empregados com fundamento no inciso II do art. 932 do CC[222]; e (c) o poder de direção do empregador inclui organização, controle e disciplina[223].

Tal entendimento foi adotado pelo Tribunal Superior do Trabalho – TST, que se manifestou pela legalidade tanto do monitoramento quanto do rastreamento das comunicações eletrônicas dos empregados pelos empregadores. O relator para o acórdão, ministro João Oreste

---

[220] ANDRADE, José Carlos Vieira de. Op. cit., pp. 263-266.

[221] WHITAKER, Reg. **El fin de la privacidad**: como la vigilancia total se está convirtiendo en realidad. Tradução de Luis Prat Clarós. Barcelona: Paidós, 1999, p. 133.

[222] "*Art. 932. São também responsáveis pela reparação civil: (...) III - o empregador ou comitente, por seus empregados, serviçais e prepostos, no exercício do trabalho que lhes competir, ou em razão dele*;" In BRASIL. **Lei nº 10.406, de 10 de janeiro de 2002**. Op.cit.

[223] OPICE BLUM, Renato M. S. **O monitoramento de e-mails e a decisão do TST**. [s.l.]: [s.n.], [200-?]. Publicado no sítio do Instituto Brasileiro de Política e Direito da Informática. Disponível em < http://www.ibdi.org.br /index.php?secao=&id_noticia=452&acao=lendo>. Acesso em 30 jan. 2007.

Dalazen, entendeu que o direito à privacidade limita-se à proteção das comunicações pessoais e não atinge as comunicações profissionais, porque, para estas últimas o empregado se vale do computador e do provedor de acesso à internet de propriedade da empresa, além de utilizar um endereço eletrônico associado ao nome da organização. Em complemento, firmou posicionamento no sentido de que os empregados não devem alimentar expectativa de privacidade no ambiente de trabalho, podendo o empregador, inclusive, investigar o conteúdo das mensagens eletrônicas encaminhadas por seus empregados. Destaque-se a seguinte passagem do acórdão, *verbis*:

> EMENTA. PROVA ILÍCITA. "E-MAIL" CORPORATIVO. JUSTA CAUSA. DIVULGAÇÃO DE MATERIAL PORNOGRÁFICO.
> 1. Os sacrossantos direitos do cidadão à privacidade e ao sigilo de correspondência, constitucionalmente assegurados, concernem à comunicação estritamente pessoal, ainda que virtual ("e-mail" particular). Assim, apenas o e-mail pessoal ou particular do empregado, socorrendo-se de provedor próprio, desfruta da proteção constitucional e legal de inviolabilidade.
> 2. Solução diversa impõe-se em se tratando do chamado "e-mail" corporativo, instrumento de comunicação virtual mediante o qual o empregado louva-se de terminal de computador e de provedor da empresa, bem assim do próprio endereço eletrônico que lhe é disponibilizado igualmente pela empresa. Destina-se este a que nele trafeguem mensagens de cunho estritamente profissional. Em princípio, é de uso corporativo, salvo consentimento do empregador. Ostenta, pois, natureza jurídica equivalente à de uma ferramenta de trabalho proporcionada pelo empregador ao empregado para a consecução do serviço.
> 3. A estreita e cada vez mais intensa vinculação que passou a existir, de uns tempos a esta parte, entre Internet e/ou correspondência eletrônica e justa causa e/ou crime exige muita parcimônia dos órgãos jurisdicionais na qualificação da ilicitude da prova referente ao desvio de finalidade na utilização dessa tecnologia, tomando-se em conta, inclusive, o princípio da proporcionalidade e, pois, os diversos valores jurídicos tutelados pela lei e pela Constituição Federal. A experiência subministrada ao magistrado pela observação do que ordinariamente acontece revela que, notadamente o "e-mail" corporativo, não raro sofre acentuado desvio de finalidade, mediante a utilização abusiva ou ilegal, de que é exemplo o envio de fotos pornográficas. Constitui, assim, em última análise, expediente pelo qual o empregado pode provocar expressivo prejuízo ao empregador.
> 4. Se se cuida de "e-mail" corporativo, declaradamente destinado somente para assuntos e matérias afetas ao serviço, o que está em jogo, antes de tudo, é o exercício do direito de propriedade do empregador sobre o computador capaz de acessar à INTERNET e sobre o próprio provedor. Insta ter presente também a responsabilidade do empregador, perante terceiros, pelos atos de seus empregados em serviço (Código Civil, art. 932, inc. III), bem como que está em xeque o direito à imagem do empregador, igualmente merecedor de tutela constitucional. Sobretudo, imperativo considerar que o empregado, ao receber uma caixa de "e-mail" de seu empregador para uso corporativo, mediante ciência prévia de que nele somente podem transitar mensagens profissionais, não tem

> razoável expectativa de privacidade quanto a esta, como se vem entendendo no Direito Comparado (EUA e Reino Unido).
> 5. Pode o empregador monitorar e rastrear a atividade do empregado no ambiente de trabalho, em "e-mail" corporativo, isto é, checar suas mensagens, tanto do ponto de vista formal quanto sob o ângulo material ou de conteúdo. Não é ilícita a prova assim obtida, visando a demonstrar justa causa para a despedida decorrente do envio de material pornográfico a colega de trabalho. Inexistência de afronta ao art. 5º, incisos X, XII e LVI, da Constituição Federal.
> 6. Agravo de Instrumento do Reclamante a que se nega provimento.[224]

Mário Antônio Lobato de Paiva, de forma veemente, critica esse posicionamento do TST. Para o autor, o simples fato de uma linha telefônica e aparelhos pertencerem a uma empresa não confere à organização o direito de interceptação das ligações de seus empregados sem autorização judicial, devendo-se adotar igual entendimento quanto às comunicações eletrônicas, que não podem ser monitoradas sob a alegação tanto da titularidade do contrato com o provedor de acesso à internet quanto da propriedade dos recursos eletrônicos. O monitoramento dos *e-mails* dos empregados impede o exercício de outros direitos fundamentais além do direito à privacidade, como o direito à liberdade de expressão, à crítica e até de reflexão sobre as condições de trabalho. Ademais, observa-se que o poder de direção e a necessidade de controle de tráfego de informações da empresa podem ser implementados recorrendo-se a outros recursos menos invasivos à privacidade, sendo desnecessário o rastreamento de todas as mensagens dos empregados[225].

Entende-se que a decisão do TST, acima transcrita, representa um perigoso retrocesso no estudo da teoria geral dos direitos fundamentais, e, em especial, do direito à privacidade. Diante de um típico conflito entre dois direitos fundamentais – direito à propriedade, à imagem e à livre iniciativa da empresa, em contraposição ao direito à privacidade dos empregados – o Tribunal sequer ventilou os princípios basilares aceitos pela doutrina e pelas Cortes Constitucionais de todo o mundo para resolução de referidas colisões, quais sejam: *princípio da unidade da Constituição; princípio da concordância prática ou da harmonização;* e *princípio da proporcionalidade em sentido amplo*.

---

[224] BRASIL. Tribunal Superior do Trabalho. RR nº 613/2000. Relator para o Acordão: João Oreste Dalazen. Brasília, DF, 18 de maio de 2005. **Diário da Justiça da República Federativa do Brasil**, Brasília, DF, 10 jun. 2005, p. 013. Disponível em <http://www.tst.gov.br/>. Acesso em: 30 jan. 2007. Grifos nossos.

[225] PAIVA, Mário Antônio Lobato de; SILVEIRA NETO, Antônio. **A privacidade do trabalhador no meio informático.** [s.l.]: [s.n.], [2003]. Publicado no sítio do Instituto Brasileiro de Política e Direito da Informática. Disponível em <http://www.ibdi.org.br/index.php?secao=&id_ noticia=125&acao=lendo>. Acesso em 30 jan. 2007.

De acordo com o *princípio da unidade da Constituição,* não existem dispositivos constitucionais antagônicos, devendo a Constituição ser aplicada como um todo unitário; o que exige do intérprete a tarefa de tentar conciliar os dispositivos em conflito, buscando *concordância prática ou harmonização.* Trata-se de medida essencial para a garantia da máxima efetividade da Constituição, conforme expõe Konrad Hesse na obra intitulada *A força normativa da Constituição*[226]. Não sendo possível a preservação, no caso concreto, dos dois princípios em colisão, deve-se aplicar o *princípio da proporcionalidade em sentido amplo* e seus três subprincípios: adequação, necessidade e proporcionalidade em sentido estrito. O *subprincípio da adequação* exige que a restrição a um direito fundamental seja adequada à preservação do outro direito fundamental ou do outro valor constitucional em jogo. Pelo *subprincípio da necessidade,* investiga-se a inexistência de outro meio menos gravoso à preservação do interesse contraposto. E pelo *subprincípio da proporcionalidade em sentido estrito* equaciona-se uma ponderação entre os dois valores em conflito, não se permitindo, em nenhuma hipótese, a nulificação de nenhum deles.

Considerando-se que o rastreamento das mensagens dos empregados se insere no âmbito de proteção do direito à propriedade, à autogestão e à livre-iniciativa da empresa e, ainda, que se configura como um meio *adequado* para se garantir a proteção da imagem da organização, o *subprincípio da necessidade* se impõe como o próximo passo a se analisar, a fim de perquirir-se a existência de outros meios menos invasivos à privacidade dos empregados, resguardando-se, ao mesmo tempo, os direitos da empresa. Existindo outros meios, o direito à privacidade não poderia ter sido desconsiderado pelo Tribunal. Quanto a esse aspecto, observa-se que a empresa, na qualidade de proprietária dos recursos computacionais e gestora de todas as atividades, tem condições de aferir a produtividade de seus empregados, bem como a vinculação de sua imagem, utilizando-se de meios menos invasivos, tais como a auditoria periódica de todos os equipamentos, considerando-se que estes guardam registros de todos os *sites* acessados pelos empregados. Pode-se ventilar, ainda, a adoção de uma política interna de conscientização de todos os empregados a respeito do uso correto do correio eletrônico, demonstrando-se que os abusos decorrentes do mau uso dessa ferramenta de trabalho implicarão na aplicação de penalidades.

[226] HESSE, Konrad. *A força normativa da Constituição*. Tradução de Gilmar Ferreira Mendes. Porto Alegre: Sergio Antonio Fabris, 1991.

Ainda que tal meio se oferecesse como *adequado* e *necessário* como se fosse o único veículo apto a garantir a proteção da pessoa jurídica, descamba-se para uma *desproporcionalidade em sentido estrito*, no que se refere à medida, diante do rastreamento generalizado das comunicações de todos os empregados e não apenas daqueles em relação aos quais se identificou suspeita de má conduta dentro da empresa. O Tribunal, diante da colisão entre os direitos fundamentais dos empregadores e os da empresa, sequer aplicou o princípio da proporcionalidade, aniquilando o núcleo essencial do direito à privacidade, ao consolidar o posicionamento de que não se permite sequer "expectativa de privacidade no ambiente de trabalho".

Ainda que o contrato de trabalho ou a norma interna da empresa previsse a possibilidade de se efetuar o rastreamento de todas as comunicações de seus empregados sob a alegação de existência de prévio alerta a respeito da permanente vigilância, o negócio ou ato jurídico em discussão seria de constitucionalidade, no mínimo, questionável. Isto porque, conforme a melhor doutrina, permite-se a auto-restrição ou a limitação de direitos fundamentais nas relações privadas apenas, em circunstâncias em que tal medida seja temporária, específica e deliberada com liberdade pelas partes. Assim, a relação jurídica, ainda que materialmente assimétrica, deve preservar a *autonomia real* das partes contratantes, sob pena da auto-restrição pela parte mais fraca ser considerada nula. Nos casos de contratos de trabalho, os empregados subordinam-se ao poder de direção do empregador e ao cumprimento dos atos normativos emanados no âmbito da organização, o que lhes retira a *autonomia real*, sendo inconstitucional a limitação de direito fundamental que afete o núcleo essencial da garantia.

O posicionamento que se elege espelha, inclusive, a jurisprudência do STF que, em sede de RE interposto pelas empregadas da empresa De Millus, manifestou-se incidentalmente sobre o tema. O relator para o acórdão, Sepúlveda Pertence, embora não tenha dado provimento ao recurso – tendo em vista o trânsito em julgado para a acusação da pena imposta à empresa por constrangimento ilegal – em seu voto *"lamentou não ter podido enfrentar o mérito da questão e condenou o exacerbado privalismo do acórdão do Tribunal de Alçada Criminal do Rio de Janeiro"* que reformou a decisão do juiz de primeiro grau. Em primeira instância, foi considerada inconstitucional a norma interna da empresa que determinava a submissão das operárias à humilhante revista íntima no momento da saída da fábrica. Embora existisse previsão de tal procedimento no contrato de trabalho e na norma da empresa, o juiz de primeiro grau considerou

ofensiva à dignidade e à imagem das operárias a revista íntima – uma vez que tal medida expunha as trabalhadoras a uma "constante e infundada suspeita de conduta ilícita" – deferindo o pedido de perdas e danos por constrangimento ilegal, o que foi reformado pelo Tribunal e mantido pelo STF por questões meramente processuais, *verbis*:

> EMENTA. I. Recurso extraordinário: legitimação da ofendida - ainda que equivocadamente arrolada como testemunha -, não habilitada anteriormente, o que, porém, não a inibe de interpor o recurso, nos quinze dias seguintes ao termino do prazo do Ministério Público, (STF, Sums. 210 e 448).
> II. Constrangimento ilegal: submissão das operárias de indústria de vestuário a revista íntima, sob ameaça de dispensa; sentença condenatória de primeiro grau fundada na garantia constitucional da intimidade e acórdão absolutório do Tribunal de Justiça, porque o constrangimento questionado a intimidade das trabalhadoras, embora existente, fora admitido por sua adesão ao contrato de trabalho: questão que, malgrado a sua relevância constitucional, já não pode ser solvida neste processo, dada a prescrição superveniente, contada desde a sentença de primeira instância e jamais interrompida, desde então.[227]

Ainda resta ressaltar a artificialidade da distinção entre comunicação pessoal e comunicação profissional, pois atualmente o trabalho humano, em âmbito cada vez mais virtual, já oferece a possibilidade de realização das tarefas em domicílio ou em qualquer outro ambiente, tendo em vista o advento do teletrabalho[228] e a possibilidade de utilização de recursos tecnológicos, como telefones celulares, *notebooks* e acesso remoto à empresa pela internet[229], sendo extremamente complexo distinguir quando o empregado se encontra em um ambiente institucional e quando se encontra em um ambiente privado – argumento utilizado pelo relator do acórdão do TST.

---

[227] BRASIL. Supremo Tribunal Federal. RE nº 160222/RJ. Recorrente: Ana Paula Muniz e outros. Relator: Sepúlveda Pertence. Brasília, DF, 11 de abril de 1995. **Diário da Justiça da República Federativa do Brasil**, Brasília, DF, 01 set. 1995, p. 27402. Disponível em <http://www.stf.gov.br/jurisprudencia/nova/pesquisa.asp> Acesso em: 30 jan. 2007. Grifos nossos.

[228] Teletrabalho é a prestação laboral realizada com subordinação jurídica fora das instalações da empresa e com a utilização de recursos de tecnologia da informação fornecidos por esta. Vantagens do teletrabalho: evita deslocamento; reduz a poluição e o congestionamento nas cidades; permite a redução do espaço físico nas empresas; proporciona maior quantidade de empregos em áreas de difícil acesso; aumenta a produtividade em cerca de 30% tendo em vista a maior flexibilidade de horários e o ambiente não competitivo; proporciona a inovação tecnológica da família; facilita a contratação de pessoas com problema de locomoção. Desvantagens: é meio de marginalização daqueles que não têm acesso a computador e internet; estimula o controle virtual pelo empregador; enfraquece os movimentos sindicais; em situação de primeiro emprego dificulta a aprendizagem com demais colegas; maior dificuldade de realizar a distinção entre as esferas privada e profissional do teletrabalhador. In ESTRADA, Manuel Martin Pino. Tele-trabalho suas perspectivas e novidades. In: IBDE, INSTITUTO BRASILEIRO DE DIREITO ELETRÔNICO; UNAMA, UNIVERSIDADE DA AMAZÔNIA. **II Congresso Internacional de Direito Eletrônico**. Belém, 2 a 6 out. 2006.

[229] ALVES, Ricardo de Paula. Vida pessoal do empregado, liberdade de expressão e direitos fundamentais do trabalhador: considerações sobre a experiência do direito francês. In: MARTINS, Ives Gandra; PEREIRA JÚNIOR, Antonio Jorge (coordenadores). **Direito à privacidade**. São Paulo: Centro de Extensão Universitária, 2005, p. 369.

Considerando que em grandes centros urbanos, as pessoas passam mais de 10 (dez) horas por dia envolvidos em atividades de trabalho, seria pueril considerar que durante esse longo período os empregados não transmitirão *e-mails* com assuntos pessoais, ainda que forma breve e razoável. O monitoramento generalizado de todas as correspondências eletrônicas encaminhadas por meio dos recursos computacionais da empresa, atinge não apenas indivíduos envolvidos em atividades ilícitas como a pornografia, mas também empregados dedicados, com alto nível de produtividade e que muitas vezes sacrificam sua vida pessoal, afastando-se do convívio familiar, para dedicarem-se em tempo praticamente integral aos assuntos de interesse da empresa.

Ademais, verifica-se que a Constituição não estabelece distinção entre comunicação de caráter pessoal e comunicação de caráter profissional, resguardando o sigilo em ambos os casos, pois o que se objetiva proteger não se restringe ao conteúdo da comunicação propriamente dito e muito menos ao meio utilizado e, sim, a intimidade e a vida privada dos interlocutores ou dos destinatários das comunicações.

Apenas como elemento ilustrativo, destaquem-se trechos da Recomendação da Comissão Nacional de Protecção de Dados da República Portuguesa a respeito da privacidade no ambiente de trabalho, documento aprovado em sessão plenária de 29 de outubro de 2002, que espelha a forma como está sendo resolvida essa questão no âmbito da União Européia – UE, *verbis*:

> PRINCÍPIOS SOBRE A PRIVACIDADE NO LOCAL DE TRABALHO
> O tratamento de dados em centrais telefónicas, o controlo do e-mail e do acesso à Internet. Considerando que (...)
> A CNPD RECOMENDA que as entidades empregadoras observem os seguintes princípios na utilização das novas tecnologias (...)
> 3. Princípios gerais relativos à utilização e controlo do e-mail e Internet
> 1. Perante a massificação dos meios de comunicação é ilógico, irrealista e contraproducente que, no contexto da relação de trabalho, se proíba – de forma absoluta – a utilização do correio electrónico e o acesso à Internet para fins que não sejam estritamente profissionais.
> 2. A entidade empregadora deverá analisar todos os factores – a salvaguarda da liberdade de expressão e de informação, a formação, o livre desenvolvimento e iniciativa do trabalhador, a sua sensibilização para acesso às redes públicas, os custos para a empresa, as políticas de segurança, de privacidade e o grau de utilização destes meios, o tipo de actividade e grau de autonomia dos seus funcionários, bem como as suas necessidades concretas e pessoais – para definir regras claras e precisas em relação à utilização do correio electrónico e da Internet para fins privados.
> 3. Estas regras – que não podem ser desenquadradas da prática institucionalizada e das necessidades particulares dos trabalhadores – devem assentar nos princípios da adequação, da proporcionalidade, da mútua colaboração e da confiança recíproca.

4. Estas regras devem ser submetidas à consideração dos trabalhadores e dos seus órgãos representativos, sendo claramente publicitadas por forma a que seja assegurada uma informação clara sobre o grau de tolerância, o tipo de controlo efectuado e, mesmo, sobre as consequências do incumprimento daquelas determinações (cf. art. 10º nº 1 da Lei 67/98).
5. É desejável que a entidade empregadora permita que os trabalhadores utilizem, com moderação e razoabilidade, os meios que esta colocou à sua disposição.
6. A entidade empregadora que permite a utilização do e-mail para fins privados e que não põe limitações à utilização da Internet, que não pretende estabelecer limites à sua utilização e, em consequência, se recusa a efectuar qualquer tipo de controlo dos trabalhadores está dispensada de notificar aqueles "registos de comunicações" (tratamentos) à CNPD.
7. O administrador de sistema está vinculado à obrigação de segredo profissional, não podendo revelar a terceiros os dados privados dos trabalhadores de que tenha tomado conhecimento em consequência das acções de monitorização dos seus postos de trabalho.

3. 1. Princípios específicos em relação ao e-mail

1. O facto de a entidade empregadora proibir a utilização do e-mail para fins privados não lhe dá o direito de abrir, automaticamente, o e-mail dirigido ao trabalhador.
2. A entidade empregadora – enquanto responsável pelo tratamento (cf. art. 3.º al. d) da Lei 67/98) – tem legitimidade para tratar os dados, na sua vertente de «registo, organização e armazenamento», com fundamento no disposto no artigo 6º al. a) da Lei 67/98.
3. As condições de legitimidade do tratamento – na vertente de «acesso» – devem obedecer à previsão do artigo 6º al. e) da Lei 67/98, a qual aponta para a necessidade de ser feita uma ponderação entre os "interesses legítimos do responsável" e os "interesses ou os direitos liberdades e garantias do titular dos dados".
4. Os poderes de controlo da entidade empregadora – que não podem ser postos em causa – devem ser compatibilizados com os direitos dos trabalhadores, assegurando-se que devem ser evitadas intrusões. A entidade empregadora deve, por isso, escolher metodologias de controlo não intrusivas, que estejam de acordo com os princípios previamente definidos e que sejam do conhecimento dos trabalhadores.
5. A entidade empregadora não deve fazer um controlo permanente e sistemático do e-mail dos trabalhadores. O controlo deve ser pontual e direccionado para as áreas e actividades que apresentem um maior "risco" para a empresa.
6. O grau de autonomia do trabalhador e a natureza da actividade desenvolvida, bem como as razões que levaram à atribuição de um e-mail ao trabalhador devem ser tomadas em conta, decisivamente, em relação à forma como vão ser exercidos os poderes de controlo. O segredo profissional específico que impende sobre o empregado (vg. sigilo médico ou segredo das fontes) deve ser preservado.
7. As razões determinantes da entrada na caixa postal dos empregados, com fundamento em ausência prolongada (férias, doença), devem ser claramente explicitadas e do seu conhecimento prévio.
8. Deve ser claramente diferenciado o grau de exigência e de rigor em relação ao controlo dos e-mails expedidos e recebidos, sendo facultados ao trabalhador

> meios expeditos e eficazes para assegurar a eliminação imediata dos e-mails recebidos e cuja entrada na sua caixa de correio ele não pode controlar.
> 9. O controlo dos e-mails – a realizar de forma aleatória e não persecutória – deve ter em vista, essencialmente, garantir a segurança do sistema e a sua performance.
> 10. Para assegurar estes objectivos a entidade empregadora pode adoptar os procedimentos necessários para – sempre com o conhecimento dos trabalhadores – fazer uma «filtragem» de certos ficheiros que, pela natureza da actividade desenvolvida pelo trabalhador podem indiciar, claramente, não se tratar de e-mails de serviço (vg. ficheiros «.exe», .mp3 ou de imagens).
> 11. A necessidade de detecção de vírus não justifica, só por si, a leitura dos e-mails recebidos.
> 12. À constatação da utilização desproporcionada deste meio de comunicação – que será comparada com a natureza e tipo de actividade desenvolvida – deve seguir-se um aviso do trabalhador e, se possível, o controlo através de outros meios alternativos e menos intrusivos.
> 13. Eventuais controlos fundamentados na prevenção ou detecção da divulgação de segredos comerciais deve ser direccionado, exclusivamente, para as pessoas que têm acesso a esses segredos e apenas quando existam fundadas suspeitas.
> 14. Os prazos de conservação dos dados de tráfego devem ser limitados em função de razões relacionadas com a organização da actividade e gestão da correspondência e nunca em razão de quaisquer objectivos de controlo ou organização de perfis comportamentais dos trabalhadores.
> 15. O acesso ao e-mail deverá ser o último recurso a utilizar pela entidade empregadora, sendo desejável que esse acesso seja feito na presença do trabalhador visado e, de preferência, na presença de um representante da comissão de trabalhadores. O acesso deve limitar-se à visualização dos endereços dos destinatários, o assunto, a data e hora do envio, podendo o trabalhador – se for o caso – especificar a existência de alguns e-mails de natureza privada e que não pretende que sejam lidos pela entidade empregadora.
> 16. Perante tal situação a entidade empregadora deve abster-se de consultar o conteúdo do e-mail, em face da oposição do trabalhador. (...) [230]

Diante desse cenário, estabelecem-se alguns parâmetros que podem orientar as empresas quanto o uso de correio eletrônico por seus empregados: (a) os recursos computacionais da empresa devem ser utilizados, prioritariamente, para o desempenho de atividades profissionais, admitindo-se o uso para fins pessoais, desde que, de forma razoável; (b) as empresas não devem monitorar, de forma generalizada, todas as comunicações enviadas pelos empregados por meio de seus recursos computacionais, implicando tal conduta na violação da privacidade desses indivíduos, uma vez que, essas organizações dispõem de outros mecanismos menos invasivos aptos à aferição da produtividade e ao exercício do poder de direção e de controle; (c) a fim de

[230] PORTUGAL. Comissão Nacional de Protecção de Dados. **Princípios sobre a privacidade no local de trabalho**: o controlo do correio electrónico, dos acessos à internet e das chamadas telefónicas dos trabalhadores. Lisboa, 29 out. 2002. Disponível em <http://www.cnpd.pt/bin/orientacoes/principiostrabalho.htm>. Acesso em: 30 jan. 2007. Grifos nossos.

evitar a vinculação do nome da empresa a atividades diferentes daquelas previstas em seu estatuto social, deve ser permitido aos empregados o acesso remoto às suas contas de e-mail particulares – tais como *ig, yahoo, gmail* e tantas outras – o que lhes possibilitará o envio de mensagens pessoais, sem que essas sejam vinculadas à imagem da organização; (d) as pessoas jurídicas, na qualidade de proprietárias dos recursos computacionais disponibilizados aos seus empregados, têm a prerrogativa de realizar auditorias periódicas em todos os equipamentos de forma a aferir como estes são utilizados; (e) no intuito de promover a utilização consciente dos recursos tecnológicos, as empresas podem estabelecer políticas de bom uso dessas ferramentas, práticas aplicáveis tanto na vida profissional como na vida pessoal dos empregados, considerando a complexidade da tarefa de distinguir a esfera pessoal da esfera profissional na sociedade da informação, tendo em vista o advento do teletrabalho, do telefone celular, do *notebook* e tantos outros artefatos que permitem a pessoa trabalhar em qualquer ambiente; (f) quaisquer medidas restritivas de direitos fundamentais de empregados – tais como do direito à privacidade, à liberdade de expressão, à crítica e até de reflexão – devem ser submetidas à apreciação de suas entidades representativas por meio de Convenção Coletiva de Trabalho – CCT ou instrumentos congêneres, considerando-se que as referidas garantias somente são passíveis de limitação em relações jurídicas privadas em que reste preservada a autonomia real de ambas as partes envolvidas, o que não é o caso dos contratos de trabalho que expressam vínculos eminentemente assimétricos e de preponderância dos empregadores; (g) em situações excepcionais, admite-se o monitoramento individualizado das comunicações de determinado empregado, desde que, exista prévia autorização judicial, indício da utilização desarrazoada de tais recursos computacionais ou fundada suspeita da prática de condutas ilícitas, preservando-se nesse caso o sigilo das comunicações em relação a pessoas não envolvidas na investigação e apuração das infrações; (h) em caso de necessidade de preservação de segredos comerciais da empresa, admitir-se-á o monitoramento e controle das comunicações, desde que, essas atividades se restrinjam apenas às pessoas que têm acesso a essas informações e em caso de fundadas suspeitas de quebra de sigilo.

Diante de todo o exposto, conclui-se pela inconstitucionalidade do monitoramento generalizado de todas as comunicações dos empregados realizadas por meio de recursos computacionais da empresa, ainda que tal previsão exista na norma interna e no contrato de

trabalho, por violação ao inciso XII do art. 5º da CF[231]. Este dispositivo resguarda o sigilo das comunicações sem estabelecer qualquer distinção entre comunicação profissional e comunicação pessoal; permitindo a interceptação apenas por ordem judicial e para fins de investigação criminal ou instrução processual penal, hipótese na qual não se encaixa a auto-restrição em contrato de trabalho – relação jurídica assimétrica em que sequer existe liberdade do empregado na decisão de limitação do direito da personalidade.

2.7 Âmbito de proteção de direitos fundamentais

Alguns direitos têm alcance tão amplo que se torna praticamente impossível que o exercício ou a proteção desses direitos não implique em colisão com outros direitos ou com outros valores protegidos pela Constituição; já outros têm alcance tão estreito que dificilmente tais direitos entrarão em conflito com outras garantias. Conhece-se esse "alcance" como *âmbito de proteção* do direito fundamental. A delimitação do âmbito de proteção de um direito fundamental impõe-se como medida de suma importância, pois, além de definir a extensão ou a amplitude da garantia, orienta o intérprete na tentativa de harmonização em caso de colisão com outros valores constitucionalmente protegidos.

Gomes Canotilho denomina de âmbito de proteção de um direito fundamental "o âmbito da vida" ou o "âmbito da realidade", tais como: a vida humana no que ser refere ao direito à vida; a arte referente ao direito à liberdade de criação artística; a comunicação escrita, oral, telefônica e "internética" referente ao direito ao sigilo das comunicações[232]. Assim, o âmbito de proteção de um direito fundamental compreende as realidades da vida asseguradas pelo dispositivo constitucional, indicando os bens assegurados e a extensão da proteção efetuada pela norma que consagra o preceito. Para o autor, o âmbito de proteção não oferece, todavia, uma garantia jurídica definitiva ao direito fundamental, pois só diz respeito àquilo que é conferido pela norma, sem levar em conta as restrições eventualmente impostas pela própria Constituição. Nesse

[231] "*Art. 5º XII - 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;".* In BRASIL. **Constituição da República Federativa do Brasil de 1988.** Op. cit.
[232] CANOTILHO, José Joaquim Gomes. **Direito constitucional e teoria da Constituição**. Op. cit., pp. 448-449.

sentido, o jurista distingue "âmbito de proteção" de "âmbito de garantia efetiva": o primeiro significa o bem jurídico protegido pelo direito fundamental; o segundo, a extensão da garantia, em que se consideram todas as eventuais intervenções restritivas legítimas e o balanceamento com os outros valores constitucionais conflitantes[233].

Gilmar Ferreira Mendes afirma que o *âmbito de proteção de um direito fundamental abrange não apenas os pressupostos fáticos contemplados na norma, ou seja, o bem jurídico protegido pela garantia fundamental; mas também os tipos de agressão ou de restrição contra os quais se outorga a proteção*. Quanto mais amplo o âmbito de proteção de um direito fundamental, maior a probabilidade de se caracterizar como restrição qualquer ato do Estado; ao revés, quanto mais restrito for o âmbito de proteção de um direito fundamental, menor a possibilidade de se qualificar como restrição um ato do Estado. Esse entendimento, ao qual a autora deste trabalho se filia, diferencia-se do anterior por espelhar uma concepção mais estreita do conceito de âmbito de proteção, na medida em que tal conceito pode ser delimitado somente após a confrontação do direito fundamental com os outros valores constitucionais e observadas as restrições impostas ao preceito. Segundo Gilmar Ferreira Mendes, primeiramente se identifica o bem jurídico protegido e a amplitude dessa proteção, confrontando-o com outros valores constitucionais; em seguida, faz-se a verificação das restrições expressas e das reservas legais de índole restritiva – processo que exige uma interpretação sistemática da Constituição[234].

Para efeitos didáticos, efetiva-se a interpretação de um direito fundamental apresentando-a em duas etapas: primeiro afere-se o que se quer proteger, ou seja, o bem jurídico a ser tutelado pela norma; em seguida, identificam-se as restrições impostas ao direito fundamental, estejam estas previstas na própria Constituição (expressa restrição constitucional) ou apenas autorizadas pela mesma Carta (reserva legal de índole restritiva). Superadas essas etapas, tem-se o *âmbito de proteção sob a concepção estreita.* Edilsom Farias esclarece a distinção entre *âmbito de proteção sob a concepção estreita* e *âmbito de proteção sob a concepção ampla*:

> A concepção de âmbito de proteção, que abarca todas as formas de exercício de um direito fundamental, previstas no texto ou programa da norma *iusfundamental* (norma de direito fundamental) pode ser denominada de conceito amplo de âmbito de proteção. Contrapõe-se ao conceito estreito, que propõe a exclusão *a priori* de determinadas hipóteses práticas de exercício do direito fundamental do âmbito de proteção. Por exemplo, a distinção entre os dois conceitos revela-se mais clara quando se analisa o caso de um artista que

[233] CANOTILHO, José Joaquim Gomes. **Estudos sobre direito fundamentais**. Op. cit., p. 199.
[234] MENDES, Gilmar Ferreira. **Os direitos individuais e suas limitações**. Op. cit., pp 210-212.

> deseja pintar um quadro no cruzamento de ruas de tráfego urbano de movimento. A ação do pintor estaria *prima facie* tutelada pelo âmbito de proteção da liberdade de expressão artística conforme o conceito amplo supramencionado; porém, tal ação estaria previamente excluída do âmbito de proteção consoante o conceito estreito aludido. (...) Embora em alguns casos práticos as duas concepções possam apresentar resultados iguais, a vantagem do conceito amplo de âmbito de proteção é oferecer uma fundamentação mais clara e racional das restrições dos direitos fundamentais.[235]

Diante do exposto, observa-se que ainda persiste certa divergência doutrinária quanto à extensão do conceito de âmbito de proteção em relação aos direitos fundamentais. Alguns autores, dentre os quais Gomes Canotilho e Pereira Farias, defendem a adoção de um conceito amplo de âmbito de proteção: diz respeito àquilo que é conferido pela norma sem levar em conta as restrições eventualmente impostas ao direito fundamental. Outros autores, como Gilmar Ferreira Mendes, defendem um conceito estreito de âmbito de proteção: este abrange os pressupostos fáticos contemplados na norma e também as restrições a que está sujeito o direito fundamental. Neste trabalho, opta-se pelo conceito estreito de âmbito de proteção, analisando-se a questão das restrições no item 2.9.

2.8 Âmbito de proteção do direito à privacidade

Peter Häberle ressalta a importância de toda a comunidade participar da delimitação do *âmbito de proteção* dos direitos fundamentais, pois, em uma sociedade livre e aberta de intérpretes da Constituição, tal atividade hermenêutica não deve ficar restrita aos intérpretes jurídicos e aos atores formais do processo constitucional, devendo ser exercida por todos os destinatários das normas constitucionais[236].

Nesse contexto, entende-se de crucial importância a delimitação do âmbito de proteção do direito à privacidade na sociedade contemporânea – garantia aplicável a todos os indivíduos e essencial para o desenvolvimento da personalidade humana. Adotando-se um *conceito estreito de âmbito de proteção*, torna-se possível identificar, em um primeiro passo, a realidade da vida ou o

[235] FARIAS, Edilsom. **Liberdade de expressão e comunicação**. Op. cit., pp. 34-35. Grifos nossos.
[236] HÄBERLE, Peter. **Hermenêutica constitucional. A sociedade aberta dos intérpretes da Constituição**: contribuição para a interpretação pluralista e "procedimental" da Constituição. Tradução de Gilmar Ferreira Mendes. Porto Alegre: Sergio Antonio Fabris, 2002, pp. 13-15.

bem jurídico protegido pelo direito à privacidade; em seguida, em um segundo passo, o alcance ou extensão desse direito fundamental ao confrontá-lo com outros valores também previstos na Constituição.

Quanto ao "âmbito da vida" ou "âmbito da realidade" abrangido pelo preceito, observa-se que o direito à privacidade compreende a *intimidade*, a *vida privada*, o *domicílio*, a *correspondência*, as *comunicações* e os *dados pessoais* a respeito de uma determinada pessoa, resguardando o indivíduo contra quaisquer intromissões alheias nas três esferas descritas pela doutrina alemã: privada (*Privatsphäre*); de intimidade em sentido lato (*Intimsphäre*); e de intimidade em sentido estrito (*Geheimsphäre*). Conforme exposto no item 1.3, a *intimidade* corresponde à esfera em que se esconde o âmago do indivíduo – denominada pela cultura ocidental consciência e pela cultura oriental coração – local onde se recolhem os pensamentos do indivíduo. A *vida privada* abrange, por sua vez, todo ato ou fato externo ao indivíduo, mas que se deseja preservar da divulgação a terceiros, ou seja, informações que devem ater-se a um círculo limitado de pessoas. Por *domicílio*, entende-se todo e qualquer lugar delimitado e reservado que o indivíduo ocupa com exclusividade, seja sua residência, escritório, quarto de hotel.

Maior detalhamento merece a expressão *correspondência.* Questiona-se o que se entende por correspondência; se um *e-mail* pode ou deve ser incluído no âmbito de correspondência. Alguns doutrinadores, adotando uma interpretação restritiva, entendem que *e-mail* não é correspondência, pelo simples fato de não estar previsto no rol do § 1º do art. 7º da Lei nº 6.538, de 22 de junho de 1978, que dispõe sobre os serviços postais:

> Art. 7º. Constitui serviço postal o recebimento, expedição, transporte e entrega de objetos de correspondência, valores e encomendas, conforme definido em regulamento.
> § 1º - São objetos de correspondência:
> a) carta;
> b) cartão-postal;
> c) impresso;
> d) cecograma;
> e) pequena-encomenda.

Apesar de a lei em referência ainda estar em vigor, observa-se que o rol desse ato normativo especifica o que se entende por correspondência apenas para fins de delimitação do serviço postal, conforme se lê no *caput* do dispositivo citado. Ademais, entende-se que esse ato normativo deva ser interpretado dinamicamente, segundo os novos parâmetros da *sociedade da informação*, sendo incabível a adoção de uma interpretação estática de dispositivo legal redigido

na década de 70, quando a internet sequer existia. Uma interpretação mais adequada abrange, portanto, no conceito de correspondência, as mensagens veiculadas em meio eletrônico, vulgarmente conhecidas por *e-mail*. Tal entendimento foi, inclusive, adotado pelo Tribunal Europeu dos Direitos do Homem, que interpreta o conceito "correspondência" constante no art. 8º, nº 1, da Convenção Européia dos Direitos do Homem[237] no sentido de abranger todos os tipos de comunicação, incluindo telecomunicações, pensamento que já se reflete no art. 7º da Carta de Direitos Fundamentais da União Européia[238] – documento que, apesar de ainda não produzir valor jurídico vinculativo, por não ter sido incorporado em tratado internacional, tem indiscutível valor doutrinário e político, uma vez que reúne, pela primeira vez, em um único texto, os direitos civis e políticos tradicionais, bem como os direitos econômicos e sociais, como forma adequada para orientar os tribunais e os juristas da UE[239].

Por fim, quanto à proteção de *dados pessoais*, apesar de não existir expressa previsão na Constituição brasileira acerca de proteção a essas informações – como ocorre nas constituições de Portugal, Eslovênia, Rússia e Espanha, conforme se observou no item 2.4.2.4.2 ao se tratar do direito à privacidade como um direito a prestação, em especial do direito à autodeterminação informativa – a referida garantia pode ser considerada acobertada pelo inciso X do art. 5º que menciona, de forma genérica, a proteção da intimidade e da vida privada do indivíduo. Demonstra-se, desta forma, a vasta abrangência do direito à privacidade no ordenamento jurídico nacional, incluindo-se, no rol de proteção desse preceito, a intimidade, a vida privada, o domicílio, a correspondência, as comunicações e os dados pessoais.

Aspecto que ainda merece atenção quanto à amplitude do âmbito de proteção do direito à privacidade diz respeito à constatação do caráter eminentemente elástico e variável dessa garantia. O tempo, o espaço e o titular podem atuar como elementos determinantes em relação ao grau de abrangência dessa garantia. Quanto ao tempo, verifica-se que em décadas passadas a proteção de dados pessoais não se destacava tão relevante diante da inexistência de recursos tecnológicos aptos à interconexão dessas informações. Quanto ao espaço, observa-se que certas

---

[237] "*Artigo 8.º 1- Qualquer pessoa tem direito ao respeito da sua vida privada e familiar, do seu domicílio e da sua correspondência*". In CONSELHO DA EUROPA. **Convenção para a Proteção dos Direitos do Homem e das Liberdades Fundamentais**. Op. cit.

[238] "*Artigo 7º Respeito pela vida privada e familiar Todas as pessoas têm direito ao respeito pela sua vida privada e familiar, pelo seu domicílio e pelas suas comunicações*". In UNIÃO EUROPÉIA. **Carta de Direitos Fundamentais da União Européia**. 07 de dezembro de 2000. Disponível em <http://europa.eu/scadplus/leg/pt/lvb/l33501.htm> Acesso em: 30 jan. 2007.

[239] CORREIA, Miguel Pupo. O caso Echelon: aspectos jurídicos. In: ASCENSÃO, José de Oliveira (Org.). **Direito da sociedade da informação**. Coimbra: Coimbra Ed., 2003, vol. IV, p. 337.

condutas, perniciosas à privacidade em determinadas comunidades, em outras recebem tratamento sem reações adversas, o que leva à constatação de que tal garantia é passível de flexibilização conforme evidenciem adequação ou não aos costumes adotados pelos grupos sociais. A proteção do isolamento pessoal, lembre-se, não é resguardada em comunidades indígenas. Por fim, quanto ao titular da garantia, verifica-se maior elasticidade de aplicação do preceito quando a questão envolve pessoa pública ou notória, tendo em vista o interesse da coletividade em conhecer a vida íntima, as opiniões, as crenças e os sentimentos das referidas pessoas, o que reduz consideravelmente a distância entre vida privada e mundo exterior.

Conforme leciona Luís Roberto Barroso, a privacidade de políticos, artistas e atletas se sujeita a parâmetros de aferição menos rígidos do que a privacidade de pessoas anônimas, em razão da necessidade de auto-exposição e de promoção pessoal daqueles indivíduos. Menciona-se ainda o caso das pessoas que adquirem notoriedade de forma eventual em razão de uma fatalidade ou circunstância negativa, como envolvimento em determinado acidente ou crime, o que também desperta interesse público[240]. Paulo José da Costa Júnior enfrenta a referida questão, alertando que a esfera da vida privada depende basicamente do *status* do indivíduo: quando a pessoa se destaca como figura pública ou célebre, o âmbito de proteção de sua privacidade reduz-se de forma sensível[241].

Assim, quanto maior a amplitude da projeção da pessoa pública ou notória, menor a possibilidade de se vetarem intromissões alheias em sua vida privada, pois o interesse público sobreeleva-se invadindo a intimidade do indivíduo. A dificuldade consiste em se traçar uma fronteira entre a vida privada e a vida pública da pessoa célebre, uma vez que mesmo aos homens públicos se deve conceder o direito à privacidade. Em tais casos, deve-se sopesar, de um lado, o interesse público pelo conhecimento da notícia e, de outro, a privacidade do protagonista[242] – conflito de direitos fundamentais a ser solucionado à luz do *princípio da proporcionalidade*.

Nesse balanceamento entre os diferentes interesses em jogo, o direito à reserva – apesar de passível de mitigação, jamais pode ser anulado – devendo-se adotar alguns parâmetros no processo de decisão de publicação ou não da notícia. *Um dos requisitos para restrição do direito*

---

[240] BARROSO, Luís Roberto. Colisão entre liberdade de expressão e direitos da personalidade. Critérios de ponderação. Interpretação constitucionalmente adequada do Código Civil e da Lei de Imprensa. **Revista de Direito Administrativo**, Rio de Janeiro, n. 235, pp. 1-36, jan./mar. 2004, p. 14.
[241] COSTA JÚNIOR, Paulo José da. Op. cit., p. 38.
[242] JABUR, Gilberto Haddad. A dignidade e o rompimento da privacidade. In: MARTINS, Ives Gandra; PEREIRA JÚNIOR, Antonio Jorge (coordenadores). **Direito à privacidade**. São Paulo: Centro de Extensão Universitária, 2005, pp. 287-288.

à privacidade é que a notícia apresente-se como de genuíno interesse público – que não se confunde com mera curiosidade – e nos termos e na medida da necessidade de se dar a conhecer com o mínimo desnudamento possível do indivíduo[243]. A notícia, além de *adequada* à preservação do interesse público, deve ser de *necessário* conhecimento da coletividade, expondo o mínimo possível a intimidade da pessoa célebre ou notória, sem anular em completude sua privacidade, em obediência ao *princípio da proporcionalidade em sentido estrito*.

Assim, o direito de informar deve prevalecer apenas em relação ao direito à privacidade se a informação for indispensável e verdadeiramente inarredável para compreensão da informação a ser publicada. Não basta o desejo que manifesta um veículo de comunicação de revelar aspectos ou detalhes íntimos porque entende essencial. *A divulgação requer a existência do efetivo interesse público na informação e a incontornável necessidade de se desnudar a privacidade para coerência e completude da notícia*[244]. *Como terceiro requisito, relacione-se a necessidade de preservação de uma parcela de intimidade da pessoa pública ou notória;* aspectos de sua vida privada que devem ser mantidos em segredo e não devem ser revelados para terceiros sem prévia autorização do titular. Observa-se, portanto, que, embora seja mais restrito o âmbito de proteção do direito à privacidade das pessoas públicas e notórias, mesmo em relação a tais pessoas deve ser preservada uma parcela de confidencialidade necessária ao desenvolvimento de sua personalidade e à manutenção de sua paz interior.

Após tais considerações, importa aferir a extensão do âmbito de proteção do direito à privacidade, quando confrontado com outros direitos fundamentais (*colisão em sentido estrito*) ou com outros valores resguardados pela Constituição (*colisão em sentido amplo*). Na primeira hipótese, o conflito decorre do exercício dos direitos fundamentais por diferentes titulares, como ocorre em situações que envolvem, *privacidade* e *livre acesso à informação*. Na segunda, o conflito se instala com outros valores que tenham por escopo a proteção da coletividade como nos casos de conflito entre *privacidade* e *segurança pública*.

A respeito da colisão de direitos fundamentais, leciona Edilsom Farias:

> Tem-se a colisão de direitos fundamentais em sentido estrito, ou colisão entre os próprios direitos fundamentais, quando o exercício de um direito fundamental por parte de um titular tem repercussões negativas sobre direitos fundamentais de outro titular. Em outros termos: quando o pressuposto de fato ou âmbito de proteção de um direito interceptar o pressuposto de fato de outro direito

[243] JABUR, Gilberto Haddad. **A dignidade e o rompimento da privacidade**. Op. cit., p. 99.
[244] JABUR, Gilberto Haddad. **Liberdade de pensamento e direito à vida privada**. Op. cit., pp. 339-340.

> fundamental. (...) Verifica-se, dessa forma, a colisão em sentido amplo, ou a colisão entre os direitos fundamentais e outros valores constitucionais, quando os direitos fundamentais contrapõem-se a interesses da comunidade, reconhecidos também pela Constituição, tais como: saúde pública, família, segurança pública, patrimônio cultural, entre outros.[245]

Normalmente, a privacidade entra em colisão com o *direito à liberdade de expressão e de comunicação*, resguardado pelos incisos IV e IX do art. 5º e pelo *caput* e § 2º do art. 220 da CF[246]. A proteção da *liberdade de expressão* compreende a manifestação pública de pensamentos, idéias, opiniões, juízos de valor e críticas; enquanto a *liberdade de comunicação* abrange a divulgação pública de imagens, fatos e notícias de interesse para a sociedade. Quando se exerce ilegitimamente a primeira forma de liberdade, afronta-se o *direito à honra* que tutela a reputação e a boa fama do indivíduo contra falsas e desabonadoras imputações independentemente da forma de expressão. Quando o ilícito se instala no exercício da liberdade de comunicação, afronta-se o *direito à privacidade* que protege a imagem do indivíduo e suas informações de caráter pessoal contra a revelação ou divulgação a terceiros, independentemente do meio de comunicação utilizado.

Luís Roberto Barroso arrola alguns parâmetros que devem nortear o órgão julgador na resolução do conflito entre *liberdade de expressão e de comunicação* e *privacidade*, dentre os quais os seguintes: (a) a veracidade do fato: a informação que goza de proteção constitucional é a informação verdadeira, por isso os veículos de comunicação têm o dever de apurar com boa fé a correção do fato, devendo ser responsabilizados quando houver clara negligência ou dolo na difusão da falsidade; (b) a licitude do meio empregado na obtenção da informação: não se admite a divulgação de informação obtida por meios ilícitos como interceptação telefônica clandestina, violação de domicílio, tortura e outros; (c) os fatos ocorridos em locais reservados têm maior proteção do que os ocorridos em locais públicos; (d) os fatos que são notícia – independentemente das pessoas envolvidas – como desastres naturais, acidentes e crimes

[245] FARIAS, Edilsom. **Liberdade de expressão e comunicação**. Op. cit., pp. 46-47. Grifos nossos.

[246] "*Art. 5º IV - é livre a manifestação do pensamento, sendo vedado o anonimato; IX - é livre a expressão da atividade intelectual, artística, científica e de comunicação, independentemente de censura ou licença; Art. 220. A manifestação do pensamento, a criação, a expressão e a informação, sob qualquer forma, processo ou veículo não sofrerão qualquer restrição, observado o disposto nesta Constituição. (...) § 2º - É vedada toda e qualquer censura de natureza política, ideológica e artística*". In BRASIL. **Constituição da República Federativa do Brasil de 1988**. Op. cit.

merecem ser divulgados, devendo o interessado na não divulgação demonstrar as razões para a censura[247].

Um interessante caso que se pode mencionar a respeito da colisão entre o direito à privacidade e o direito à liberdade de comunicação foi julgado pelo STJ, em sede de RESP. Maria Aparecida de Almeida Padilha, alegando violação ao seu direito à privacidade, interpôs recurso contra decisão denegatória de indenização por danos morais diante da divulgação pela imprensa de uma foto em que aparecia de *topless* em praia pública. No mérito, o STJ manteve a decisão recorrida, que resguardava o direito à liberdade de comunicação, uma vez que a recorrente, de livre e espontânea vontade, expôs-se desnuda em cenário público, não sendo ilícita ou indevida a mera reprodução de sua imagem pela imprensa em notícia não sensacionalista de interesse para a coletividade. Destaca-se este trecho do voto do relator, ministro Cesar Asfor Rocha, *verbis:*

> Não se pode cometer o delírio de, em nome do direito de privacidade, estabelecer-se uma redoma protetora em torno de uma pessoa para torná-la imune de qualquer veiculação atinente a sua imagem. (...) Na espécie, a recorrida divulgou fotografia, sem chamada sensacionalista, de imagem da recorrente praticando *topless* "numa praia lotada em pleno feriado" (fl. 196). Isto é, a própria recorrente optou por revelar sua intimidade, ao expor o peito desnudo em local público de grande movimento, inexistindo qualquer conteúdo pernicioso na veiculação, que se limitou a registrar sobriamente o evento sem sequer citar o nome da autora. Assim, se a demandante expõe sua imagem em cenário público, não é ilícita ou indevida sua reprodução sem conteúdo sensacionalista pela imprensa, uma vez que a proteção à privacidade encontra limite na própria exposição realizada. Portanto, *in casu,* não há qualquer ofensa moral. Ante o exposto, não conheço do recurso.[248]

No caso retro-mencionado, como a divulgação pela imprensa já havia ocorrido, discutia-se apenas a respeito do cabimento ou não da indenização por danos morais decorrentes de violação à privacidade no exercício da liberdade de comunicação. Situação mais complexa ocorre quando o Judiciário é provocado antes da divulgação da notícia, invocando o protagonista da matéria a ser noticiada uma ordem de proibição de publicação. Essa questão foi levantada pelo

---

[247] BARROSO, Luís Roberto. **Colisão entre liberdade de expressão e direitos da personalidade. Critérios de ponderação. Interpretação constitucionalmente adequada do Código Civil e da Lei de Imprensa**. Op. cit., pp. 25-28.

[248] BRASIL. Superior Tribunal de Justiça. RESP nº 595600/SC. Recorrente: Maria Aparecida de Almeida Padilha. Relator: Cesar Asfor Rocha. Brasília, DF, 18 de março de 2004. **Diário da Justiça da República Federativa do Brasil**, Brasília, DF, 13 set. 2004, p. 259. Disponível em <http://www.stj.gov.br/SCON/jurisprudencia>. Acesso em: 30 jan. 2007. Grifos nossos.

ministro do STF, Gilmar Ferreira Mendes, na análise da colisão entre o direito à privacidade e o direito à liberdade de expressão e comunicação:

> Não é verdade, ademais, que o constituinte concebeu a liberdade de expressão como direito absoluto, insuscetível de restrição, seja pelo Judiciário, seja pelo Legislativo. (...) É fácil ver, pois que o texto constitucional não excluiu a possibilidade de que introduzissem limitações à liberdade expressão e de comunicação, estabelecendo, expressamente, que o exercício dessas liberdades haveria de ser fazer com observância do disposto na Constituição. Não poderia ser outra a orientação do constituinte, pois, do contrário, outros valores, igualmente relevantes, quedariam esvaziados diante de um direito avassalador, absoluto e insuscetível de restrição.[249]

O jurista complementa sua exposição alertando para a regra do § 1º do art. 220 da CF, segundo a qual "*nenhuma lei conterá dispositivo que possa constituir embaraço à plena liberdade de informação jornalística em qualquer veículo de comunicação social, observado o disposto no art. 5º, IV, V, X, XIII e XIV*". Ao final, conclui que tal dispositivo autoriza o legislador a disciplinar o exercício da atividade de imprensa, tendo em vista a proibição do anonimato e a inviolabilidade da intimidade, da vida privada, da honra e da imagem das pessoas, o que permite o estabelecimento de restrições ao direito à liberdade de comunicação[250].

Edilsom Farias, ao analisar o âmbito de proteção da liberdade de comunicação, ressalta que essa garantia não abrange a divulgação de informações relacionadas à vida privada, intimidade e honra das pessoas, compreendendo apenas a difusão de notícias de transcendência para todo o corpo social e de genuíno interesse público, *verbis*:

> Na sociedade democrática, a presunção é de que todos os fatos da atualidade ligados aos problemas relevantes com que se defrontam os cidadãos na vida social podem ser objeto de divulgação. Entretanto, essa regra apresenta exceções. (...) O âmbito de proteção da liberdade de comunicação tutela preferencialmente a difusão de notícias que têm transcendência pública, ou seja, que digam respeito a fatos culturais, econômicos, políticos, científicos, educacionais, ecológicos, dentre outros, e que são relevantes para a participação dos cidadãos na vida social, bem como para a formação da opinião pública pluralista. As informações que não afetam o bem comum e que são relacionadas com a vida privada, a intimidade e a honra das pessoas amiúde estão excluídas do âmbito de proteção da liberdade de comunicação.[251]

Luís Roberto Barroso, em sentido contrário, demonstra certa preferência pela proteção da liberdade de expressão e de comunicação quando se constata colisão de tais garantias com outros

---

[249] MENDES, Gilmar Ferreira. **Direitos fundamentais e controle de constitucionalidade**. Op. cit., p. 90. Grifos nossos.
[250] MENDES, Gilmar Ferreira. **Direitos fundamentais e controle de constitucionalidade**. Op. cit., p. 91.
[251] FARIAS, Edilsom. **Liberdade de expressão e comunicação**. Op. cit., pp. 84-85. Grifos nossos.

direitos fundamentais, dentre os quais o direito à privacidade. Ressalta que a liberdade de expressão e de comunicação serve de fundamento para o exercício de outras liberdades, o que justifica uma posição de preponderância em tese, embora não de superioridade. Segundo o autor, esse posicionamento foi consagrado pela Suprema Corte americana, pelo Tribunal Constitucional Espanhol e pelo Tribunal Constitucional Federal alemão, resultando na adoção do *princípio da excepcionalidade da proibição prévia de publicações*, reservando-se a referida medida apenas para os casos em que não seja possível posterior composição do dano por reparação[252].

Data venia, discorda-se do posicionamento do jurista, já que, da mesma forma que o direito à liberdade de expressão e de comunicação serve de fundamento para o exercício de outros direitos fundamentais; o direito à privacidade serve de fundamento para o exercício da própria liberdade de expressão. Conforme exposto no item 1.1, não há como exercer com tranqüilidade a liberdade de consciência, de crença e de expressão sem a proteção de um espaço reservado em que o indivíduo possa voltar-se para si mesmo livre de censuras, para despir-se das máscaras e dos condicionamentos impostos pela sociedade. De outro, ressalte-se que não se estabelece hierarquia entre os direitos fundamentais – tendo em vista o *princípio da unidade da Constituição* – e, ainda, caso se adotasse a teoria minoritária da *hierarquização de princípios constitucionais*, não seria possível concordar com o jurista, pois, em eventual escalonamento de direitos fundamentais, deveria ser dada preponderância aos preceitos que decorrem diretamente do *princípio da dignidade da pessoa humana* – valor superlativo de todo o ordenamento jurídico – que é o caso do direito à privacidade.

Quanto à adoção do *princípio da excepcionalidade da proibição prévia de publicações* – reservando-se essa medida apenas para os casos em que não seja possível posterior composição do dano por reparação – convém ter em mente que a indenização sempre será devida quando comprovado o dano moral e/ou material acarretado pela publicação da matéria. Ainda que verdadeiro o fato noticiado, a indenização por divulgação de informação relacionada à vida privada ou intimidade de alguém que não seja de interesse público será devida, conforme dispõe o *caput* e o § 1º do art. 49 da Lei de Imprensa:

> Art. 49. Aquêle que no exercício da liberdade de manifestação de pensamento e de informação, com dolo ou culpa, viola direito, ou causa prejuízo a outrem, fica obrigado a reparar:

[252] BARROSO, Luís Roberto. **Colisão entre liberdade de expressão e direitos da personalidade. Critérios de ponderação. Interpretação constitucionalmente adequada do Código Civil e da Lei de Imprensa**. Op. cit., p.20.

> I - os danos morais e materiais, nos casos previstos no art. 16, números II e IV, no art. 18 e de calúnia, difamação ou injúrias;
>
> II - os danos materiais, nos demais casos.
>
> § 1º Nos casos de calúnia e difamação, a prova da verdade, desde que admissível na forma dos arts. 20 e 21, excepcionada no prazo da contestação, excluirá a responsabilidade civil, salvo se o fato imputado, embora verdadeiro, diz respeito à vida privada do ofendido e a divulgação não foi motivada em razão de interêsse público.[253]

Outro conflito possível ocorreria entre o direito à privacidade e o *direito de livre acesso à informação,* previsto nos incisos XIV e XXXIII do art. 5º, no inciso II do § 3º do art. 37 e no § 2º do art. 216 da CF[254]. O livre acesso à informação decorre do *princípio da publicidade* da administração pública, que consagra o dever do Estado de manter plena transparência de seus atos aos administrados; resguardando-se o direito de acesso às informações não só *de interesse particular*, mas também *de interesse coletivo ou geral*. Quando há acesso a informações de interesse particular, não há que se falar em conflito com o direito à privacidade, pois tais informações são fornecidas ao próprio titular, estando resguardada sua intimidade e vida privada. Entretanto, em relação às informações *de interesse coletivo ou geral*, pode-se estabelecer uma colisão quando revelarem aspectos relacionados à intimidade ou à vida privada de outrem. Nesta hipótese, apesar de as informações constarem nos registros públicos, não poderão ser divulgadas a terceiros, devendo ser consideradas sigilosas.

Na doutrina diz-se que o princípio da publicidade – também denominado princípio do *open file* ou dos arquivos abertos – tem dupla função: de um lado, proteger o administrado das decisões administrativas relacionadas a sua própria pessoa, munindo-o dos documentos necessários à defesa dos seus direitos; de outro, conferir maior transparência aos atos administrativos e incrementar a participação cívica da coletividade nos projetos da administração. Todavia, este princípio deve ser cotejado com o *princípio da confidencialidade* das informações

---

[253] BRASIL. Lei de Imprensa. **Lei nº 5.250, de 09 de fevereiro de 1967**. Disponível em: <https://www.planalto.gov.br/ccivil_03/Leis/L5250.htm>. Acesso em: 30 jan. 2007.

[254] "*Art. 5º XIV - é assegurado a todos o acesso à informação e resguardado o sigilo da fonte, quando necessário ao exercício profissional; XXXIII - todos têm direito a receber dos órgãos públicos informações de seu interesse particular, ou de interesse coletivo ou geral, que serão prestadas no prazo da lei, sob pena de responsabilidade, ressalvadas aquelas cujo sigilo seja imprescindível à segurança da sociedade e do Estado; Art. 37 § 3º A lei disciplinará as formas de participação do usuário na administração pública direta e indireta, regulando especialmente:(...) II - o acesso dos usuários a registros administrativos e a informações sobre atos de governo, observado o disposto no art. 5º, X e XXXIII; Art. 216 § 2º - Cabem à administração pública, na forma da lei, a gestão da documentação governamental e as providências para franquear sua consulta a quantos dela necessitem*." In BRASIL. **Constituição da República Federativa do Brasil de 1988**. Op. cit.

pessoais de terceiros, podendo-se exigir dois requisitos para a autorização de acesso aos registros públicos: demonstração do legítimo interesse, e reconhecimento pela administração de que o documento não tem informação relacionada à intimidade ou à vida privada de outrem[255].

A própria Constituição explicita no inciso LX do art. 5º que "*a lei só poderá restringir a publicidade dos atos processuais quando a defesa da intimidade ou o interesse social o exigirem*", consagrando uma exceção à publicidade dos atos administrativos para preservação do direito à privacidade. Mais expressivo, ainda, no que tange ao acesso às informações detidas pela administração pública, o disposto na parte final do inciso II do § 3º do art. 37, segundo o qual lei regulará "*o acesso dos usuários a registros administrativos e a informações sobre atos de governo, observado o disposto no art. 5º, X e XXXIII*", ou seja, garante-se o direito de livre acesso à informação, desde que preservado o direito à privacidade. Desta forma, são consideradas originariamente sigilosas as informações relacionadas com a intimidade ou com a vida privada de alguém, não podendo ser franqueado tal acesso ao público em geral.

Outra colisão bem comum que se pode mencionar ocorre entre o direito à privacidade e o valor segurança pública (*colisão em sentido amplo*), citando-se um interessante julgado do Tribunal Constitucional Federal alemão. A Corte, em 03 de março de 2004, prolatou decisão (*BverfGe 109, 279 – Lauschangriff*) sobre ato normativo que regula a "escuta secreta" por parte de agentes do Estado. Em 1998, foram inseridos limites significativos ao direito fundamental à privacidade do domicílio com o objetivo de incrementar a segurança pública diante do crescimento vertiginoso da ameaça terrorista e do crime organizado na Alemanha. O ato normativo, apreciado pelo Tribunal, previa a possibilidade de utilização de minúsculos microfones e micro-câmeras no interior do domicílio de suspeitos de crimes, sem o conhecimento do morador – titular do direito fundamental à inviolabilidade do domicílio. *O Tribunal julgou a reclamação parcialmente procedente, manifestando-se no sentido de proteção da dignidade da pessoa humana em detrimento da segurança pública sempre que a vigilância acústica conduzir ao levantamento de informações provenientes do núcleo absolutamente protegido da vida privada – esfera de intimidade em sentido estrito (Geheimsphäre).* Segundo o Tribunal, o direito à privacidade domiciliar – à época em que foi criado – impunha-se contra a intromissão física de agentes públicos no interior do domicílio dos cidadãos; hoje, com os novos artefatos tecnológicos, deve ter seu âmbito de proteção estendido para abranger outras formas de

[255] MARQUES, Garcia; MARTINS, Lourenço. **Direito da informática**. Coimbra: Almedina, 2000, pp. 226-228.

intromissão. Nesse contexto, a observação de um indivíduo, mediante procedimento sigiloso do Estado, não viola, em si, o direito ao respeito, mas devem ser traçados alguns limites, por serem invioláveis as expressões decorrentes dos processos internos das pessoas, como pensamentos, pontos de vista e experiências personalíssimas, bem como a sexualidade. *Assim, a vigilância acústica e por imagem para fins de segurança pública viola a dignidade da pessoa humana e a privacidade quando o núcleo da conformação da vida privada não é respeitado*[256].

Diante de todo o exposto, conclui-se que o âmbito de proteção do direito à privacidade é flexível e variável. É reduzido parcialmente – preservando-se uma parcela de confidencialidade – no caso de pessoas públicas e notórias, visto o maior interesse da coletividade em tomar conhecimento de sua intimidade e vida privada; e também quando a pessoa resolve se expor, já que esta garantia constitucional protege o indivíduo contra intromissões não desejadas pelo autor, e não contra a exposição voluntária. A análise, entretanto, só se faz completa ao se confrontar esse direito com outros valores previstos na Magna Carta, quando se percebe a sua verdadeira extensão. Dependendo do caso concreto, pode ter prevalência em relação ao direito à liberdade de expressão e de comunicação e ao direito ao livre acesso à informação. Entre os bens protegidos se incluem a imagem, o nome, a correspondência, o domicílio, os dados pessoais e toda e qualquer informação íntima a respeito de uma determinada pessoa, bem como o seu recato pessoal ou afastamento do mundo exterior.

2.9 Restrições a direitos fundamentais e limites ao poder de restrição

Os direitos fundamentais, pelo caráter relativo que ostentam, sujeitam-se às denominadas restrições. Restrição consiste na compressão ou na diminuição do "alcance" ou da "extensão" de um direito fundamental, para que sua proteção possa adequar-se à garantia de outros valores constitucionais. Algumas vezes os direitos fundamentais são expressamente restringidos pela própria Constituição; outras vezes são limitados pelo Legislativo ou pelo Judiciário, como forma de garantir o exercício de outros valores protegidos pela Magna Carta.

[256] MARTINS, Leonardo (Org.). Op. cit., pp. 688-718.

Conforme exposto no item 2.7, caso se adote um c*onceito amplo de âmbito de proteção*, diz-se que a restrição é a compressão do próprio âmbito de proteção, que significa o bem da vida protegido pelo direito fundamental; caso se adote um *conceito estreito de âmbito de proteção*, a restrição integra o âmbito de proteção do direito fundamental, significando apenas a diminuição de seu "alcance". Todavia, em um e em outro caso, a restrição reconduz à mesma idéia: trata-se de uma afetação desvantajosa ao direito fundamental, seja integrante ou não de seu âmbito de proteção.

Adotando-se um *conceito estreito de âmbito de proteção,* as restrições, além de complementarem a delimitação do âmbito de proteção do direito fundamental como parte integrante deste; ainda representam uma garantia extra ao cidadão. Isto porque os direitos individuais só podem ser restringidos pela própria Constituição, mediante lei ordinária, após prévia autorização da Constituição ou quando houver autorização implícita à conformação do direito com outros valores também protegidos constitucionalmente. Assim, apesar de representarem uma afetação desvantajosa ao direito fundamental, as restrições configuram-se também como uma garantia contra intromissões do Judiciário, do Legislativo e do Executivo que excederem aos parâmetros constitucionais, o que implicará a constatação de inconstitucionalidade do ato jurídico.

Gomes Canotilho menciona que a restrição pode ser feita por meio de *lei restritiva* de direito, liberdade e garantia; ou mediante *carga coativa imposta no caso concreto* como ocorre em situações de sentença privativa de liberdade, de ato expropriatório de propriedade e de decisão administrativa de proibição de uma determinada manifestação. Nestas hipóteses, fala-se em *restrição jurídico-pública*. Outra modalidade de restrição diz respeito à *restrição privada*, que ocorre quando a afetação ao direito, à liberdade e à garantia ou ao direito da personalidade parte de um particular, seja ela lícita ou ilícita[257].

Konrad Hesse, focando as *restrições jurídico-públicas,* ressalta que tais condições se impõem como limitações necessárias à *concordância prática* entre direitos fundamentais em conflito, ou seja, são afetações essenciais à *coordenação proporcional* de direitos fundamentais para que ambos atinjam *eficácia ótima*. Alerta que a restrição nunca deve privar o direito fundamental mais do que o necessário para proteção do bem jurídico contraposto, devendo ser

[257] CANOTILHO, José Joaquim Gomes. **Estudos sobre direito fundamentais**. Op. cit., pp. 197-198.

adequada para produzir a proteção do mesmo bem, *necessária* e finalmente *proporcional em sentido estrito*[258].

Nesse sentido, infere-se que a imposição de restrições aos direitos fundamentais – enquanto mecanismo de resolução dos conflitos nos casos concretos – deve observar sempre o *princípio da proporcionalidade em sentido amplo* e seus três subprincípios: adequação, necessidade e proporcionalidade em sentido estrito. Conforme já exposto, pelo *subprincípio da adequação* se exige que a restrição a um direito fundamental seja adequada à preservação do outro direito fundamental ou do outro valor constitucional em jogo; pelo *subprincípio da necessidade* verifica-se a inexistência de outro meio menos gravoso à preservação do interesse contraposto; e pelo *subprincípio da proporcionalidade em sentido estrito* estabelece-se uma ponderação entre os dois valores em conflito, não se permitindo a nulificação de nenhum deles, mas apenas uma limitação.

Quanto às restrições impostas por atos normativos, estas decorrem: (a) da própria Constituição (restrições constitucionais diretas); (b) de lei autorizada expressamente pela Constituição (reserva de lei restritiva); ou (c) de lei, mas sem autorização expressa da Constituição (restrições não expressamente autorizadas)[259]. A constitucionalidade do ato jurídico que impõe a restrição requer a observância ao *princípio da proporcionalidade em sentido amplo* e também a preservação *do núcleo essencial* do direito fundamental.

A garantia do *núcleo essencial* protege os direitos fundamentais contra o esvaziamento de seu conteúdo, representando a essência ou substância da proteção que não pode ser afetada, sob pena de declaração de inconstitucionalidade da medida restritiva. Visualizam-se, portanto, dois círculos concêntricos: o interior, formado por elementos essenciais sem os quais o direito perderia sua identidade; e o exterior, constituído por elementos acidentais cujo desaparecimento não afetaria a instituição. O legislador pode restringir o círculo exterior; só não pode adotar medidas que impliquem o desaparecimento, a anulação ou a destruição da parte nuclear[260].

Konrad Hesse afirma que o *núcleo essencial* do direito fundamental protege-o contra o aproveitamento abusivo ou excessivo das reservas legais, ou seja, contra sua desvalorização furtiva pelo poder público, denominada, pelo jurista, de *escavação interna do direito*

[258] HESSE, Konrad. **Elementos de direito constitucional da República Federal da Alemanha**. Op. cit., pp. 255-256.
[259] CANOTILHO, José Joaquim Gomes. **Direito constitucional e teoria da Constituição**. Op. cit., p. 450.
[260] GAVARA DE CARA, Juan Carlos. Op. cit., pp. 229-230.

fundamental[261]. Essa *escavação interna* ocorre mediante edição de atos normativos que impõem restrições em desconformidade com o previsto na própria Constituição. A Lei Fundamental de Bonn, no art. 19, § 2º, expressamente prevê a proteção ao núcleo essencial dos direitos fundamentais: "*Em hipótese nenhuma um direito fundamental poderá ser afetado em sua essência*"[262].

Günter Dürig identifica o *núcleo essencial* dos direitos fundamentais com o *princípio da dignidade da pessoa humana*, significando que o titular de um direito fundamental não pode ser considerado um objeto da atividade estatal. Segundo o autor, a proteção do núcleo essencial impede que o legislador, valendo-se da permissão das reservas legais, aniquile o direito fundamental subordinando-o a intromissões estatais. A dificuldade de se adotar este posicionamento de Dürig reside na forma como tal posicionamento delimita o conceito de dignidade da pessoa humana, como um conceito principiológico que dependerá da avaliação do caso concreto. Outra crítica diz respeito à existência de direitos fundamentais que não constituem expressão da dignidade da pessoa humana[263]. Todavia, verifica-se a importância do posicionamento do jurista, no que concerne à imposição de limites às restrições aos direitos fundamentais mediante proteção de seu núcleo essencial, conforme detalhado no item 2.8.

Duas teorias a respeito do *núcleo essencial* dos direitos fundamentais merecem atenção. De acordo com a *teoria absoluta*, após a identificação do núcleo essencial de um direito fundamental, este limite torna-se aplicável em qualquer caso concreto, ou seja, seu efeito é geral, independentemente da restrição que se queira efetivar. O núcleo essencial, de acordo com a teoria absoluta, apresenta-se como medida preestabelecida e fixa, como parte autônoma do direito fundamental. Pela *teoria relativa*, a identificação do núcleo essencial de um direito fundamental vale tão-somente para aquele caso concreto com que se identifica, uma vez que originário da própria norma do direito fundamental, em conexão com a justificativa da respectiva intervenção[264].

Filia-se a autora desta dissertação à *teoria relativa*, segundo a qual o núcleo essencial é variável conforme o caso concreto, desde que sejam impostos limites às restrições aos direitos fundamentais e seja observado o *princípio da proporcionalidade*. Salvo melhor juízo, parece que

[261] HESSE, Konrad. **Elementos de direito constitucional da República Federal da Alemanha**. Op. cit., p. 264.
[262] ALEMANHA**. Constituição da Alemanha de 1949**. Op. cit.
[263] GAVARA DE CARA, Juan Carlos. Op. cit., pp. 218-225.
[264] GAVARA DE CARA, Juan Carlos. Op. cit., pp. 272-273.

o legislador pátrio também aderiu à teoria relativa ao permitir a realização de aborto em caso de estupro. Caso adotasse a teoria absoluta, o aborto seria vedado mesmo nessas circunstâncias por representar uma violação ao direito à vida de titularidade do feto.

Além da necessidade de observância ao *princípio da proporcionalidade* e da vedação de violação do *núcleo essencial* do direito fundamental, Gilmar Ferreira Mendes menciona um terceiro parâmetro para averiguar a constitucionalidade das leis restritivas: *a proibição de conteúdo casuístico ou discriminatório*. As leis restritivas, para serem consideradas constitucionais, precisam atender aos requisitos da generalidade e da abstração, evitando-se a afronta ao *princípio da igualdade* que proíbe tratamento discriminatório ou arbitrário e edição de leis que mais se assemelham a atos administrativos[265].

Diante de todo o exposto, conclui-se que os direitos fundamentais – pelo caráter relativo de que se revestem – estão sujeitos às restrições impostas pelo próprio constituinte originário (restrições diretamente constitucionais) e às impostas pelo Legislativo e pelo Judiciário (restrições indiretamente constitucionais). Por restrição, entende-se a afetação desfavorável ao direito fundamental, a mitigação da proteção como forma de garantir o exercício de outros direitos protegidos pela Constituição. Todavia, tais restrições não podem ser ilimitadas, sob pena de esvaziamento do próprio conteúdo do direito fundamental, daí falar-se em imposição de *limites ao poder de restrição* – também denominados *limites dos limites* ou *limites imanentes.* Esses limites decorrem da própria Constituição e se relacionam com a necessidade de observância do *princípio da proporcionalidade em sentido amplo*, na resolução dos conflitos entre valores constitucionais; com a preservação do *núcleo essencial* do direito fundamental; e com a *clareza, abstração e generalidade das restrições impostas*.

2.10 Restrições expressas e restrições implícitas ao direito à privacidade

Conforme exposto no item anterior, as restrições aos direitos fundamentais podem ser *expressas* ou *implícitas*. No primeiro caso, a própria Constituição limita o direito fundamental ou prevê a possibilidade de restrição de tais garantias por ato normativo emanado do Legislativo; no

[265] MENDES, Gilmar Ferreira. **Direitos fundamentais e controle de constitucionalidade**. Op. cit., p. 73.

segundo, a restrição é imposta mesmo sem expressa previsão constitucional, por ser uma medida essencial à conformação do direito fundamental com outros valores constitucionais. Nesta hipótese, a restrição decorre da atividade do hermeneuta, que, diante do conflito entre valores constitucionais, busca a preservação do *princípio da unidade da Constituição*, interpretando as normas constitucionais de forma sistemática e não isolada, o que implica eventual mitigação de um dos direitos em colisão.

As *restrições expressas* se distribuem em classes: restrições diretamente constitucionais e restrições indiretamente constitucionais. As *restrições diretamente constitucionais* são estabelecidas pelo próprio texto da Constituição que, ao mesmo tempo, assegura e restringe diretamente o direito fundamental. As *restrições indiretamente constitucionais* – também chamadas *reservas de lei restritiva* – não se encontram definidas no próprio texto constitucional, que se limita a autorizar o legislador a estabelecê-las mediante lei infraconstitucional. Neste caso, a autorização ao Legislativo pode ocorrer de duas formas: *reserva legal simples*, quando a Constituição não determina requisitos ou qualificações para a lei; e *reserva legal qualificada*, quando a Constituição fixa requisitos objetivos que deverão constar na lei regulamentadora da garantia[266].

As *restrições implícitas* – também denominadas *restrições não expressamente autorizadas* ou *restrições tácitas* – são impostas, mesmo sem expressa autorização da Constituição, configurando-se como medidas necessárias à resolução dos conflitos com outros direitos fundamentais (colisão de direitos fundamentais em sentido estrito) ou com outros valores constitucionalmente protegidos (colisão de direitos fundamentais em sentido amplo). Nestes casos, a conformação não é normativa, ou seja, a restrição não se encontra prevista no próprio ordenamento jurídico, e depende da atuação do intérprete.

Partindo-se para a análise do direito fundamental à privacidade, observam-se *restrições expressas* nas modalidades *diretamente constitucionais* e *indiretamente constitucionais*, e também *restrições implícitas*. Há *restrição diretamente constitucional* à privacidade das comunicações nas alíneas "b" e "c" do inciso I do § 1º do art. 136 e no inciso III do art. 139 [267]. A

[266] FARIAS, Edilsom. **Liberdade de expressão e comunicação**. Op. cit., pp. 36-38.

[267] "*Art. 136. O Presidente da República pode, ouvidos o Conselho da República e o Conselho de Defesa Nacional, decretar estado de defesa para preservar ou prontamente restabelecer, em locais restritos e determinados, a ordem pública ou a paz social ameaçadas por grave e iminente instabilidade institucional ou atingidas por calamidades de grandes proporções na natureza. § 1º - O decreto que instituir o estado de defesa determinará o tempo de sua duração, especificará as áreas a serem abrangidas e indicará, nos termos e limites da lei, as medidas coercitivas a*

Constituição prevê que, em situações de vigência do *estado de defesa,* poderão ser restringidos os direitos de reunião, *de sigilo de correspondência e de sigilo de comunicação telegráfica e telefônica* em locais restritos e determinados, para fins de se preservar ou prontamente restabelecer a ordem pública ou a paz social. Durante *estado de sítio*, em razão tanto de comoção grave de repercussão nacional quanto de declaração de estado de guerra, também haverá *restrição ao sigilo das comunicações,* por expressa determinação da Constituição, além das limitações à liberdade de locomoção, à liberdade de imprensa, radiodifusão e televisão, ao direito de reunião e ao direito à propriedade.

Em relação à privacidade do domicílio, a restrição também é *diretamente constitucional* ao prever-se no inciso XI do art. 5º que "*a casa é asilo inviolável do indivíduo, ninguém nela podendo penetrar sem consentimento do morador, salvo em caso de flagrante delito ou desastre, ou para prestar socorro, ou, durante o dia, por determinação judicial*". Assim, a Constituição, mais uma vez, prevê a garantia e, simultaneamente, limita-a de forma expressa ao permitir a invasão "durante o dia por ordem judicial" ou "a qualquer hora em caso de flagrante delito ou desastre, ou para prestar socorro".

A técnica da *restrição indiretamente constitucional* foi adotada na forma de *reserva legal qualificada* no inciso XII do art. 5º, que garante a privacidade das comunicações, ao dispor ser "*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*". O dispositivo, ao mesmo tempo em que garante o sigilo das comunicações, limita-o expressa e indiretamente, identificando tais limites a partir da expressão "nas hipóteses e na forma que a lei estabelecer". Neste caso, a Constituição fixou o requisito objetivo para a lei restritiva, ou seja, "para fins de investigação criminal ou instrução processual penal" e, dessa forma, limitou a discricionariedade do legislador ordinário para impor restrições à privacidade das comunicações.

---

vigorarem, dentre as seguintes: I - restrições aos direitos de: a) reunião, ainda que exercida no seio das associações; b) sigilo de correspondência; c) sigilo de comunicação telegráfica e telefônica (...) ; Art. 139. Na vigência do estado de sítio decretado com fundamento no art. 137, I, só poderão ser tomadas contra as pessoas as seguintes medidas: (...) III - restrições relativas à inviolabilidade da correspondência, ao sigilo das comunicações, à prestação de informações e à liberdade de imprensa, radiodifusão e televisão, na forma da lei (...) Parágrafo único. Não se inclui nas restrições do inciso III a difusão de pronunciamentos de parlamentares efetuados em suas Casas Legislativas, desde que liberada pela respectiva Mesa." In BRASIL. **Constituição da República Federativa do Brasil**. Op. cit. Grifos nossos.

Ada Pellegrini Grinover sustenta que o inciso XII do art. 5º não reproduz o texto aprovado pela Assembléia Constituinte de 1988, o que poderia acarretar a declaração de inconstitucionalidade do referido dispositivo por vício formal, caso a jurisprudência brasileira admitisse a existência de *normas constitucionais inconstitucionais*. Segundo a processualista, a redação original votada e aprovada pelo constituinte originário permitia a restrição do sigilo das comunicações telefônicas para fins de "investigação criminal e instrução processual" abrangendo, portanto, as instruções processuais cíveis e penais – texto alterado pela Comissão de Redação e Revisão[268].

Além das restrições expressamente previstas, observa-se que o direito à privacidade – nas suas diversas modalidades (física, das comunicações, do domicílio, *decisional* e *informacional*) – também se submete a *restrições implícitas* quando entra em conflito com direito fundamental de outro cidadão ou com outro valor também previsto constitucionalmente. Isto decorre da amplitude do âmbito de proteção dessa garantia, que, por ser tão extenso, acaba entrando em colisão com outras previsões constitucionais, especialmente com dispositivos que amparam o direito à liberdade de expressão e de comunicação, o direito de livre acesso à informação e a segurança pública, conforme se verificou no item 2.8.

Uma hipótese de restrição implícita, prevista na jurisprudência do STF, refere-se à possibilidade de gravação de conversa telefônica por um dos interlocutores ou com sua autorização, sem a ciência do outro e sem autorização judicial, quando este último estiver praticando alguma investida criminosa como ameaça, extorsão ou estelionato. Apesar de a Constituição não ter previsto a possibilidade de violação do sigilo das comunicações telefônicas sem autorização judicial, o Tribunal considera prova lícita a gravação nesses casos, conforme se pode observar nos seguintes acórdãos:

> EMENTA. *HABEAS CORPUS*. PROVA. LICITUDE. GRAVAÇÃO DE TELEFONEMA POR INTERLOCUTOR.
> É lícita a gravação de conversa telefônica feita por um dos interlocutores, ou com sua autorização, sem ciência do outro, quando há investida criminosa deste último. É inconsistente e fere o senso comum falar-se em violação do direito à privacidade quando interlocutor grava diálogo com seqüestradores, estelionatários ou qualquer tipo de chantagista. Ordem indeferida.[269]

[268] GRINOVER, Ada Pellegrini. Interceptação de dados telemáticos. In: IBDE, INSTITUTO BRASILEIRO DE DIREITO ELETRÔNICO; UNAMA, UNIVERSIDADE DA AMAZÔNIA. *II Congresso Internacional de Direito Eletrônico*. Belém, 2 a 6 out. 2006.

[269] BRASIL. Supremo Tribunal Federal. HC nº 75338/RJ. Impetrante: José Mauro Couto de Assis. Relator: Nelson Jobim. Brasília, DF, 11 de março de 1998. **Diário da Justiça da República Federativa do Brasil**, Brasília, DF, 25

> EMENTA: "*HABEAS CORPUS*". UTILIZAÇÃO DE GRAVAÇÃO DE CONVERSA TELEFÔNICA FEITA POR TERCEIRO COM A AUTORIZAÇÃO DE UM DOS INTERLOCUTORES SEM O CONHECIMENTO DO OUTRO QUANDO HÁ, PARA ESSA UTILIZAÇÃO, EXCLUDENTE DA ANTIJURIDICIDADE.
> Afastada a ilicitude de tal conduta - a de, por legítima defesa, fazer gravar e divulgar conversa telefônica ainda que não haja o conhecimento do terceiro que está praticando crime -, é ela, por via de conseqüência, lícita e, também conseqüentemente, essa gravação não pode ser tida como prova ilícita, para invocar-se o artigo 5º, LVI, da Constituição com fundamento em que houve violação da intimidade (art. 5º, X, da Carta Magna). "*Habeas corpus*" indeferido.[270]

Outra hipótese de restrição implícita digna de registro refere-se à questão da violação do sigilo de correspondência de presos. A Constituição previu a inviolabilidade do sigilo de correspondência, admitindo restrição apenas ao sigilo das comunicações telefônicas e de dados (reserva legal qualificada do inciso XII do art. 5º da CF). A Lei de Execução Penal, Lei nº 7.210, de 11 de julho de 1984, dispõe no parágrafo único do art. 41, sobre a possibilidade de suspensão ou de restrição pelo diretor do presídio do direito de correspondência do preso, desde que a decisão seja motivada: "*Art. 41 - Constituem direitos do preso: (...) XV - contato com o mundo exterior por meio de correspondência escrita, da leitura e de outros meios de informação que não comprometam a moral e os bons costumes. (...) Parágrafo único. Os direitos previstos nos incisos V, X e XV poderão ser suspensos ou restringidos mediante ato motivado do diretor do estabelecimento*". Apesar de a Lei ser anterior à Constituição de 1988, a jurisprudência pacificou o entendimento de que o sigilo de correspondência de presos pode ser restringido para preservação da segurança pública e garantia da disciplina prisional, tendo sido este dispositivo recepcionado pela Magna Carta, conforme se observa no seguinte julgado do STJ:

> EMENTA: *HABEAS CORPUS* - ESTRUTURA FORMAL DA SENTENÇA E DO ACÓRDÃO - OBSERVÂNCIA - ALEGAÇÃO DE INTERCEPTAÇÃO CRIMINOSA DE CARTA MISSIVA REMETIDA POR SENTENCIADO - UTILIZAÇÃO DE CÓPIAS XEROGRÁFICAS NÃO AUTENTICADAS - PRETENDIDA ANÁLISE DA PROVA - PEDIDO INDEFERIDO.
> - A estrutura formal da sentença deriva da fiel observância das regras inscritas no art. 381 do Código de Processo Penal. O ato sentencial que contém a

---

set. 1998, p. 00011. Disponível em <http://www.stf.gov.br/jurisprudencia/nova/pesquisa.asp>. Acesso em: 30 jan. 2007. Grifos nossos.

[270] BRASIL. Supremo Tribunal Federal. HC nº 74678/SP. Impetrante: Miguel Reale Júnior e outros. Relator: Moreira Alves. Brasília, DF, 10 de junho de 1997. **Diário da Justiça da República Federativa do Brasil**, Brasília, DF, 15 ago. 1997, p. 37036. Disponível em <http://www.stf.gov.br/jurisprudencia/nova/pesquisa.asp>. Acesso em: 30 jan. 2007. Grifos nossos.

> exposição sucinta da acusação e da defesa e que indica os motivos em que se funda a decisão satisfaz, plenamente, as exigências impostas pela lei.
> - A eficácia probante das cópias xerográficas resulta, em princípio, de sua formal autenticação por agente público competente (CPP, art. 232, parágrafo único). Peças reprográficas não autenticadas, desde que possível a aferição de sua legitimidade por outro meio idôneo, podem ser validamente utilizadas em juízo penal. A administração penitenciária, com fundamento em razões de segurança pública, de disciplina prisional ou de preservação da ordem jurídica, pode, sempre excepcionalmente, e desde que respeitada a norma inscrita no art. 41, parágrafo único, da Lei nº 7.210/84, proceder a 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.
> - O reexame da prova produzida no processo penal condenatório não tem lugar na ação sumaríssima de *habeas corpus*.[271]

Jorge Reis Novais, em aprofundado estudo a respeito das restrições implícitas aos direitos fundamentais, esclarece a respeito da impossibilidade de se considerar absolutamente irrestringível pelo legislador direitos consagrados na Constituição sem reserva expressa porque essas garantias acabam por colidir de forma inevitável com direitos fundamentais de outros cidadãos. Todo direito fundamental é limitável tanto pelo juiz – para resolução do caso concreto – como também pelo legislador ordinário. O legislador constituinte originário ou de revisão não tem condições de prever todas as vicissitudes que, ao longo do tempo, marcarão a necessária convivência dos direitos fundamentais com os demais valores dignos de tutela jurídica. As normas constitucionais de direitos fundamentais não podem ser interpretadas como regras, mas como princípios; o que exige a imposição de limitações ou de restrições não consagradas expressamente pela Constituição[272].

Duas teorias rejeitam a proibição absoluta de limitações aos direitos fundamentais não expressamente previstas pela Constituição: a doutrina da *concepção restritiva da previsão normativa dos direitos fundamentais* e a doutrina dos *limites imanentes*. A *concepção restritiva da previsão normativa dos direitos fundamentais* pretende excluir da proteção de um direito fundamental aquilo que só aparentemente nele está incluído, podendo, desta forma, classificar como constitucional ou inconstitucional uma restrição não expressamente autorizada pela Constituição. No primeiro caso, diz-se que se estabelece uma restrição apenas aparente, porque o

[271] BRASIL. Superior Tribunal de Justiça. HC nº 70814/SP. Impetrante: Ulisses Azevedo Soares. Relator: Celso de Mello. Brasília, DF, 01 de março de 1994. **Diário da Justiça da República Federativa do Brasil**, Brasília, DF, 24 jun. 1994, p. 16649. Disponível em <http://www.stj.gov.br/SCON/jurisprudencia>. Acesso em: 30 jan. 2007. Grifos nossos.
[272] NOVAIS, Jorge Reis. Op. cit., pp. 367 e ss..

direito fundamental não inclui determinada conduta em seu âmbito de proteção. Exemplificando: a norma que impõe vacinação a crianças em idade escolar não viola a *privacidade física* que protege a incolumidade do corpo, porque o referido direito fundamental não oferece tal extensão[273].

A doutrina dos *limites imanentes* defende que os direitos fundamentais resguardam limites implícitos não escritos e residentes *ab initio* em seu interior. A teoria em questão foi adotada pela jurisprudência alemã a partir da década de 50, sob a fundamentação de que os direitos fundamentais têm que ser compatibilizados com outros valores também originariamente integrantes da Constituição, garantindo-se a liberdade e a dignidade de todos. Essa corrente doutrinária tenta resolver o problema das restrições não expressamente autorizadas, objetando que, se a restrição apresentar-se como decorrência natural dos limites imanentes do direito fundamental, ela será considerada constitucional; se a restrição extravasar os limites imanentes, ela será inconstitucional. Logo, o ato legislativo, ainda que aparente uma afetação desvantajosa ao direito fundamental, seria uma mera revelação dos limites imanentes necessários à compatibilização do direito fundamental com outros valores igualmente dignos de proteção constitucional[274].

No caso da interceptação de correspondência de presos, observa-se a adoção da doutrina dos *limites imanentes*, entendendo-se que o sigilo das comunicações desses indivíduos pode ser restringido para se resguardar o valor da segurança pública, também garantido pela Constituição. As pessoas submetidas a *relações especiais* – presidiários, militares e determinadas categorias de funcionários públicos – podem sofrer redução do âmbito de proteção de um ou mais de seus direitos fundamentais, como forma de garantir a ordem e a disciplina nessas relações que se estabelecem. Jorge Reis Novais afirma que a *relação especial de pode*r – também denominada *estatuto especial* ou *relação jurídica especial* – abrange o conjunto de situações em que, por razões atinentes às necessidades de prosseguimento dos fins das respectivas instituições do Estado, o indivíduo encontra-se em uma situação de sujeição ou de dependência, se comparada com a chamada *relação geral de poder*, ou seja, a relação comum Estado/cidadão. Nesses casos, sendo omisso o constituinte, poderá o legislador impor limites a alguns direitos fundamentais e na estrita medida das exigências da situação especial[275].

[273] NOVAIS, Jorge Reis. Op. cit., pp. 396 e ss.
[274] NOVAIS, Jorge Reis. Op. cit., pp. 438 e ss.
[275] NOVAIS, Jorge Reis. Op. cit., pp. 510 e ss.

Ressalte-se, entretanto, que, mesmo nos casos das relações especiais de poder, devem ser traçados limites às restrições, sendo inconstitucional a afetação do núcleo essencial do direito fundamental de presos, de militares e de funcionários especiais do Estado. Segundo Konrad Hesse, a primeira premissa a ser adotada é que, mesmo nessas relações, só podem ser adotadas limitações com base na própria Constituição, o que impõe – da mesma forma que nas relações de status cívico-geral – a tarefa da concordância prática. Outra premissa a destacar diz respeito à limitação, que pode ser imposta tão-somente quando os direitos fundamentais dificultarem a vida nesse regime de ordem especial, ou seja, quando for indispensável a limitação dessas garantias ao estabelecimento e à continuidade do regime especial de poder, que exige forma diferenciada de disciplina e obediência às ordens hierárquicas[276].

Em relação aos presidiários, constata-se que o sigilo de sua correspondência contém *ab initio*, em seu interior, o limite implícito e não escrito "segurança pública"; o que pode determinar tratamento mais flexível à questão da privacidade de suas comunicações escritas, que, mesmo sem ordem judicial podem ser interceptadas por determinação do próprio diretor do presídio, conforme demonstra a jurisprudência. O mesmo entendimento poderia ser adotado para interceptação das comunicações telefônicas dos presos, em especial quando houver utilização de telefonia celular dentro dos estabelecimentos prisionais que não se mostram aptos a controlar a entrada desses aparelhos. Nesse sentido, poderiam ser instalados, nos presídios, recursos tecnológicos que possibilitassem a escuta de todas as comunicações que ocorrem no interior da edificação prisional; como forma de garantir a ordem nessas relações especiais de poder, a segurança pública e, de modo mais imediato, o desmantelamento de organizações criminosas comandadas por detentos que se encontram confinados nesses estabelecimentos prisionais.

[276] HESSE, Konrad. **Elementos de direito constitucional da República Federal da Alemanha**. Op. cit., pp. 259-263.

PARTE II

CAPÍTULO 3 A PRIVACIDADE NA SOCIEDADE DA INFORMAÇÃO

3.1 Explicação inicial

Após o estudo do direito à privacidade no âmbito da *teoria geral dos direitos fundamentais*, passa-se à análise desse mesmo direito no contexto da *sociedade da informação*. Objetiva-se, nesta investigação, obter os fundamentos sociológicos e filosóficos para melhor compreensão da privacidade diante do novo cenário mundial que se instalou, caracterizado pelo extraordinário avanço da *tecnologia da informação* e pela supervalorização da *informação*.

O tema ganha relevância com a disseminação do uso de redes abertas e o incremento do poder computacional. O avanço tecnológico, ao propiciar o cruzamento de dados pessoais e o monitoramento eletrônico de indivíduos e empresas, agiganta-se como uma ameaça ao direito à privacidade. EUA e Europa monitoram as comunicações ao redor do mundo por meio dos projetos *Echelon* e *Enfopol*, respectivamente; câmeras de vigilância instaladas por toda parte observam as pessoas que sob seu foco transitam; difunde-se a "cultura da auto-exposição" em meio eletrônico. Quando o tema *privacidade na sociedade da informação* entra em discussão, a doutrina jurídica nacional ainda não oferece respostas aprofundadas. Impõe-se, portanto, sensibilizar juristas e estudiosos do direito para uma reflexão a respeito do impacto que a tecnologia impinge à privacidade para que os recursos computacionais sejam utilizados de maneira mais consciente. A tecnologia da informação, dependendo do uso que dela se faça, pode-se tornar uma grande aliada na defesa do direito fundamental à privacidade.

Primeiramente, sob o viés da sociologia, traçar-se-ão os contornos da sociedade da informação, apresentando-se o seu conceito e principais características. A seguir, sob um enfoque de caráter mais filosófico, discorre-se sobre o panoptismo de Michel Foucault, as origens da disciplina e do controle do comportamento dos indivíduos enquanto mecanismo de exercício do poder. Em seguida, apresenta-se a temática do panoptismo na sociedade da informação,

abordando-se questões como o exercício do poder disciplinar e controle por meio da tecnologia, e vigilância eletrônica. Na terceira parte do capítulo, delineiam-se os riscos que a internet causa à privacidade, discutindo-se a polêmica questão do anonimato na *web*. Por fim, estudam-se as questões da intromissão estatal na intimidade e na vida privada das pessoas e da espionagem por meio dos novos artefatos tecnológicos.

3.2 Conceito de sociedade da informação

A *era da informação* foi vislumbrada nos tecnocentros dos EUA e do Japão na década de 80[277], com a explosão da indústria da computação (*software* e *hardware*). Em 1993, o mundo toma conhecimento da expressão *sociedade da informação*, utilizada pela primeira vez em caráter oficial, pelo então presidente da Comissão Européia, Jacques Delors, no Conselho da Europa de Copenhague, para definir o crescente uso da *tecnologia da informação* no intuito de reforçar a economia, melhorar a prestação dos serviços públicos e incrementar a qualidade de vida dos cidadãos[278].

A expressão sociedade da informação define uma nova forma de organização social[279], *política e econômica que recorre ao intensivo uso da tecnologia da informação para coleta, produção, processamento, transmissão e armazenamento de informações.* Por *tecnologia da informação* entende-se a microeletrônica, a computação (*software* e *hardware*), as telecomunicações, a optoeletrônica[280], a engenharia genética e todos os processos tecnológicos

[277] GERMAN, Christiano. **O caminho do Brasil rumo à era da informação**. São Paulo: Konrad-Adenauer, 2000, p. 16.
[278] MARQUES, Garcia; MARTINS, Lourenço. Op. cit., p. 43.
[279] Pode-se questionar que a expressão *sociedade da informação* define uma nova forma de organização social, pois, a rigor, o mundo continua organizado segundo o modo de produção capitalista. Há criação de um novo paradigma, tendo em vista o fato da informação, de *per si*, ter assumido maior relevância para a geração de riquezas, utilizando-se a tecnologia da informação enquanto mecanismo facilitador de sua geração, processamento, transmissão e toda espécie de tratamento. Assim, embora a informação e a tecnologia da informação tenham assumido posição de destaque nesse novo cenário, configurando-se como verdadeiras mercadorias, não alteraram intrinsecamente as relações econômicas entre os diversos atores sociais, dinamizando apenas o já conhecido modo de produção capitalista.
[280] Optoeletrônica é o ramo da eletrônica voltado para o estudo e a concepção de dispositivos eletrônicos para emissão, modulação, transmissão e captação da luz. In HOUAISS, Antônio. **Dicionário eletrônico Houaiss da língua portuguesa**. Editora Objetiva Ltda, 2001. O conteúdo do programa corresponde à edição integral do Dicionário Houaiss da língua portuguesa.

interligados por uma interface e linguagem comuns, na qual a informação é gerada, armazenada, recuperada, processada e transmitida[281]. *Informação* consiste em um dado[282] ou conjunto de dados, processado ou não, em qualquer suporte, capaz de produzir conhecimento. Nesse sentido, informação pode ser uma imagem, um som, um documento físico ou eletrônico, ou, até mesmo, um dado isolado.

A *informação* contém em si o principal ativo da *sociedade da informação*, ou seja, sua principal riqueza, sendo indispensável ao desempenho de qualquer atividade – o que explica a nomenclatura atribuída pela doutrina a essa nova forma de organização social, política e econômica. O trabalho, a educação, a saúde, o lazer, a política, a economia, enfim, tudo depende de informação. Após a supervalorização da terra na época da revolução agrícola e o predomínio dos bens de produção na revolução industrial, o que prepondera agora é a *informação.* Na qualidade de principal matéria-prima desse novo modelo capitalista, a informação se impõe como condição determinante para o desenvolvimento econômico e cultural da sociedade, daí o intensivo uso da *tecnologia da informação* – enquanto mecanismo facilitador da coleta, produção, processamento, transmissão e armazenamento – o que acarreta avassaladoras mudanças no mundo.

Diz-se que hoje se vivencia a chamada *revolução da tecnologia da informação*, um fenômeno que, embora evidencie importância semelhante à revolução industrial do século XVIII, supera-a exponencialmente, porque induz a todos e a tudo a um padrão de descontinuidade nas bases materiais da economia, da sociedade e da cultura e, diferentemente de qualquer outra revolução, abala, na mais plena amplitude, os domínios da vida, não como fonte exógena de impacto, mas como elemento nuclear de um tecido que, desse elemento destituído, atualmente já não logra desenvolver-se. Um aspecto adicional que se levanta em relação à revolução da tecnologia da informação é que, ao contrário das demais revoluções que ocorreram em uma área geográfica limitada do planeta, com lenta expansão para outras regiões, esta revolução se difundiu celeremente por todo o globo em menos de duas décadas[283].

---

[281] CASTELLS, Manuel. **A sociedade em rede**. Tradução de Roneide Venancio Majer; Colaboração de Klauss Brandini Gerhardt; Prefácio de Fernando Henrique Cardoso. São Paulo: Paz e Terra, 2003, p. 67.

[282] Dado é o elemento inicial de qualquer processo de conhecimento, apresentado de forma direta e imediata à consciência servindo de base ou pressuposto no processo cognitivo e capaz de ser processado por um computador. In HOUAISS, Antônio. Op. cit.

[283] CASTELLS, Manuel. **A sociedade em rede**. Op. cit., pp. 67-70.

Hermínia Campuzano Tomé expõe como a revolução da tecnologia da informação produziu impactos na área científica, cultural, econômica, jurídica e social:

> Como punto de partida en el examen de tal fenómeno, debe destacarse el hecho de que el desarrollo y la universalización de las nuevas tecnologías de la información y las comunicaciones, si bien provocan un revolución técnica en el estado de la ciencia, no agotan ahí sus efectos. Su impacto es también cultural, económico, legal y social. (...) El carácter universal y más accesible que los últimos años han adquirido los recursos informáticos, unido al desarrollo de las nuevas tecnologías, ha propiciado el que la informatización de la sociedad, anunciada desde finales de los años setenta, se haya convertido en una realidad que se concreta en una nueva forma de organización social. Este fenómeno engendra una revolución que, a decir de algunos, tendrá una incidencia equivalente a la que tuvo la revolución industrial hace un siglo. Las nuevas tecnologías configuram la información como uno de los valores fundamentales de nuestra sociedad. Estamos caminando desde una forma de vida asentada en los bienes físicos hacia una centrada en el conocimiento y la información.[284]

Nesse sentido, a *sociedade da informação* chancela-se com as marcas vigorosas do progresso, pelo fortalecimento das ciências, especialmente da tecnologia da informação; pela substituição da informação ao capital e ao trabalho, como recurso estratégico da economia, e pela expansão dos riscos de base tecnológica. Impõe-se como uma sociedade cujos valores imateriais, dado, informação, conhecimento científico e tecnológico, constituem a força motriz da formação e desenvolvimento sociais. Surgem daí *a indústria e os serviços de informação* que abrangem atividades de educação, pesquisa científica, fabricação de equipamentos e sistemas de informação e de comunicações, mercados e serviços financeiros, bibliotecas e bancos de dados eletrônicos, biotecnologia e indústria farmacêutica. Mas a grande novidade dessa nova forma de organização reside na expansão do próprio conceito de *informação* que abrange a imagem, a voz e todo e qualquer dado em formato digital[285].

Diante desse cenário, criam-se utopias tanto positivas como negativas. Essa nova forma de organização social, denominada de *sociedade da informação,* segundo alguns estudiosos, configura-se como uma oportunidade histórica de realização dos direitos de cidadania, especialmente das liberdades tanto de informação quanto de expressão. As possibilidades técnicas de informação e de comunicação permitem aos cidadãos desfrutar, em plenitude, direitos e liberdades, na medida em que esses indivíduos dispõem de mais e de melhores meios de

[284] CAMPUZANO TOMÉ, Hermínia. **Vida privada y datos personales**: su protección jurídica frente a la sociedad de la información. Madrid: Tecnos, 2000, pp. 19 -20.
[285] GONÇALVES, Maria Eduarda. **Direito da informação**: novos direitos e modos de regulação na sociedade da informação. Coimbra: Almedina, 2003, pp. 27-29.

expressão, criação, participação e interação – o que amplia a participação democrática. Outros autores afirmam que a *sociedade da informação* agrava o risco de se ampliarem as desigualdades sociais, pelas condições de acesso ou não à informação, aumentando o fosso entre as classes sociais mais pobres e os economicamente favorecidos; além de representar um perigo de reforço da vigilância por parte dos *aparelhos de Estado*[286] sobre os indivíduos[287].

Quanto a esse aspecto, Manuel Castells ressalta que a tecnologia da informação deveria ser utilizada para fortalecimento das democracias, ampliando a participação dos cidadãos na gestão dos recursos públicos. Ao invés de os governos utilizarem a internet para vigiar as pessoas, as pessoas deveriam utilizar a rede para vigiar os governos – o que, de fato, representa um direito desses indivíduos, já que teoricamente o povo é o soberano. Os governos deveriam disponibilizar na *web* um amplo espectro das informações não sigilosas de interesse da coletividade, abrir um canal para solicitação de serviços públicos e possibilitar a fácil comunicação entre o povo e seus representantes. Entretanto, a maioria dos estudos e relatórios descreve um quadro melancólico e, com a possível exceção de alguns países escandinavos, prevalece a aplicação dos recursos tecnológicos para vigilância e controle dos indivíduos, enquanto mecanismo de poder do Estado e não como um instrumento de fortalecimento da democracia participativa[288]. Essa temática da vigilância mediante utilização de recursos tecnológicos será desenvolvida especialmente no item 3.5, que traz como título *panoptismo na sociedade da informação*.

3.3 Características da sociedade da informação

Conforme já exposto, a característica básica da *sociedade da informação* incide no fato de a *informaçã*o atuar como a matéria-prima por excelência do desenvolvimento social, político e

[286] Entende-se por *aparelhos de Estado*, também conhecidos por *aparelhos ideológicos de Estado*, a superestrutura de poder integrada por instituições distintas e especializadas como a igreja, a escola, a família, a imprensa e o Estado, propriamente dito. In ALTHUSSER, Louis. **Aparelhos ideológicos de Estado**: nota sobre os aparelhos ideológicos de Estado (AIE). Tradução de Walter José Evangelista e Maria Laura Viveiros de Castro e introdução crítica de José Augusto Guilhon Albuquerque. Rio de Janeiro: Edições Graal, 1985, p. 68.
[287] GONÇALVES, Maria Eduarda. Op. cit, pp. 30-32.
[288] CASTELLS, Manuel. **A galáxia da internet**: reflexões sobre a internet, os negócios e a sociedade. Tradução de Maria Luiza X. de A. Borges, Revisão de Paula Vaz. Rio de Janeiro: Jorge Zahar Ed., 2003, p. 128.

econômico. Todo avanço tecnológico impulsiona-se tanto pela busca de uma gestão mais eficiente das informações já disponíveis, quanto pela necessidade de incremento das comunicações, para que mais e mais informações sejam acessadas e transmitidas entre os diferentes atores. De outro lado – como em uma relação simbiótica – a tecnologia também agrega mais valor à informação. Nas palavras de Maria Eduarda Gonçalves, o desenvolvimento tecnológico transformou, de uma vez por todas, o desempenho da informação nas diversas atividades humanas e sociais:

> Não há dúvida que foi o desenvolvimento do computador, com a sua capacidade de tratar e de guardar vastas quantidades de informação, e do sistema de comunicações que transformaram o papel da informação, de meramente auxiliar, num papel central em diversas actividades humanas e sociais. Os computadores convertem qualquer tipo de informação num formato digital que as redes de telecomunicações transmitem entre diferentes terminais de computador. A informação aparece-nos sob diversas formas e diferentes conteúdos. No contexto da sociedade da informação e devido ao uso das novas tecnologias, formas inovadoras de tratamento de informação tornaram possível organizar e apresentar sob formatos diversos um maior quantidade de dados e/ou conhecimentos. (...) Numa economia de mercado, a informação pode ser objecto de produtos transacionáveis ou de serviços. São exemplos dos primeiros as edições profissionais especializadas, as bases de dados; exemplos dos segundos os serviços de acesso à Internet e à informação *on-line*.[289]

A informação atualmente assume, diante do capitalismo, a posição que o petróleo exercia no início do século passado. Todavia, a informação não se apresenta com a pretensão de substituir velhos recursos, mas apenas alterar o antigo modo de produção de riquezas. Hoje, a linha de produção realiza-se de forma enxuta, e, particularmente, a área de *marketing* – pelo aumento da concorrência – requer cada mais profissionais habilitados não apenas na coleta, mas também na análise das informações, fator essencial à garantia de êxito nessa nova fase de desenvolvimento econômico[290]. E se a informação anuncia-se o novo "petróleo", as bases de dados públicas denunciam-se como seu principal "jazigo". A iniciativa privada busca no setor público os mais diversos tipos de informação, o que faz surgir a preocupação com a necessidade de se "limitar e gerir o uso das informações" constantes nos bancos de dados públicos, sabendo-se que tais medidas produzirão reflexos diretos na economia, na política e na sociedade[291].

[289] GONÇALVES, Maria Eduarda. Op. cit., pp. 17-18.
[290] WHITAKER, Reg. Op. cit., p. 91.
[291] PEREIRA, Alexandre Dias. Op. cit., pp. 246-254.

Essa necessidade de se promover uma "gestão mais eficiente das informações" faz surgir uma nova especialidade denominada *segurança da informação*[292]. Trata-se da área responsável por assegurar a disponibilidade, a integridade, a autenticidade e a confidencialidade das informações. Por *disponibilidade* entende-se a possibilidade de acesso e utilização oportunos de informações por indivíduos e sistemas autorizados. *Integridade* significa que a informação não foi modificada, inclusive quanto à origem e ao destino. *Autenticidade* quer dizer que a informação foi produzida, expedida, recebida, modificada ou destruída por determinado indivíduo ou sistema. Por fim, *confidencialidade* significa acesso ou divulgação restritos, ou seja, sigilo. Hoje, a *segurança da informação* está sendo implementada tanto pelo setor privado – como forma garantir a continuidade do negócio, minimizar os riscos e maximizar os investimentos – como pelo setor público – especialmente para garantir a disponibilidade e a integridade dos documentos públicos, para controlar o acesso às informações sigilosas e para incrementar as atividades de governo eletrônico.

Essa supervalorização da informação acarreta uma cisão global entre países "ricos em informação" e países "pobres em informação", conforme relatório da Organização das Nações Unidas – ONU, de julho de 1999, intitulado *Globalization with human*. Os países que produzem conhecimento pela pesquisa e conseguem aproveitar esse *know-how* na implementação de novos produtos e serviços integram o clube dos chamados "ricos em informação"[293]. De outro lado, há os países denominados "pobres em informação", aqueles que, por não serem desenvolvidos tecnologicamente, apenas "consomem" as pesquisas, produtos e serviços fornecidos pelos países mais avançados por meio de conglomerados ou *redes de empresas* com grande capacidade tecnológica. Conforme expõe Manuel Castells, pela primeira vez na história, a unidade básica da organização econômica não se vale mais do sujeito individual (empresário ou família empresarial), nem do coletivo (classe capitalista, empresa ou Estado), a unidade hoje contempla uma *rede de empresas*, formada por organizações de diferentes culturas que mudam a todo instante, à medida que a tecnologia se desenvolve[294].

---

[292] A *segurança da informação* está regulamentada em âmbito nacional por diversas normas técnicas, destacando-se as seguintes: ABNT NBR ISO/IEC 17799:2005, de 31 de agosto de 2005; e ABNT NBR ISO/IEC 27001, de 31 de março de 2006. No âmbito da Administração Pública Federal, a *segurança da informação* está regulamentada pelo Decreto nº 3.505, de 13 de junho de 2000.

[293] MARTIN, Willian J. The global information society. Brookfield/Vermont, 1995, p. 3 apud GERMAN, Christiano. Op. cit., p. 15.

[294] CASTELLS, Manuel. **A sociedade em rede**. Op. cit., pp. 257-258.

Outro aspecto negativo da sociedade da informação diz respeito ao surgimento de uma nova classe de desempregados: integrantes de classes sociais proeminentes eliminados do mercado em conseqüência das inovações tecnológicas[295], a exemplo do crescente uso de *agentes inteligentes*[296] e da possibilidade de "produção à distância" com o teletrabalho. Esses profissionais – apesar de qualificados, "digitalmente alfabetizados" e "virtualmente conectados" – são dispensados diante do crescente uso de recursos computacionais e da possibilidade de "contratação a distância" de profissionais capacitados, disponíveis em países que oferecem mão-de-obra mais barata – o que torna desnecessária a transferência da empresa ou a abertura de filiais.

Outra característica marcante da sociedade da informação se ostenta no intensivo uso de aparatos tecnológicos pelo setor privado. As corporações utilizam a rede como principal meio de comunicação e processamento de informações, transformando a prática empresarial. Além disso, surgem as chamadas empresas ponto com (*empresas.com*) – entidades privadas responsáveis pela infra-estrutura da internet; pelo fornecimento dos canais de comunicação; pela fabricação dos equipamentos e programas de computador; por consultorias em tecnologia da informação; pela prestação de serviços de montagem de sítios e portais; pelo comércio eletrônico; e pela publicidade na *web*[297].

No âmbito público, os governos também canalizam vultosos investimentos em tecnologias como forma de modernizar o Estado, diminuir a burocracia, reduzir custos, conferir maior transparência aos gastos públicos, melhorar a prestação dos serviços públicos e incrementar o relacionamento entre os cidadãos e a administração pública. Algumas atividades implementadas pelo *governo eletrônico*[298] se materializam no fornecimento *on-line* de certidões; na tramitação eletrônica de documentos públicos; na criação de portais com informações úteis sobre serviços públicos relevantes; na orientação dos cidadãos pela internet, utilizando as denominadas FAQ (*frequently asked questions* ou perguntas freqüentes); no ensino à distância;

---

[295] GERMAN, Christiano. Op. cit., pp. 25-32.

[296] Por *agente inteligente*, entende-se qualquer sistema computacional ou meio eletrônico automatizado, que tem capacidade de decisão, sem qualquer intervenção humana; capacidade de comunicação de alto nível com outros agentes ou indivíduos; desempenhando por si só todas as funções para as quais foi projetado de forma autônoma e proativa, sem necessidade de revisão. In MASSENO, Manuel Davi. Direito e inteligência artificial In: IBDE, INSTITUTO BRASILEIRO DE DIREITO ELETRÔNICO; UNAMA, UNIVERSIDADE DA AMAZÔNIA. **II Congresso Internacional de Direito Eletrônico**. Belém, 2 a 6 out. 2006.

[297] CASTELLS, Manuel. **A sociedade em rede**. Op. cit., pp. 191-192.

[298] No Brasil, as atividades relacionadas ao governo eletrônico estão regulamentadas pelo Decreto s/nº, de 18 de outubro de 2000. Mais informação podem ser obtida no *site* <www.governoeletronico.gov.br>.

no diário oficial eletrônico; no peticionamento eletrônico; no pagamento e consulta *on-line* ao fisco; no pregão eletrônico; na integração dos órgãos por rede de comunicação de voz, de dados e de imagens em alta velocidade.

Observa-se também o crescente uso dos recursos de tecnologia da informação pelo Estado para controle e gestão das denominadas *infra-estruturas críticas* do país tais como energia, água, transporte, telefonia e saneamento urbano. Entretanto, a ampla utilização de recursos computacionais no gerenciamento das atividades relacionadas à prestação desses serviços implica temerárias *vulnerabilidades*[299], isto é, a possibilidade de exploração das falhas dos sistemas por indivíduos mal intencionados. Hoje, um ataque cibernético interromperia o fornecimento de água, de telefone ou de energia elétrica atingindo cidades inteiras, isto sem mencionar a infra-estrutura de transporte aéreo, controlada integralmente por computadores sujeitos às mais diversas falhas e a diferentes ameaças por indivíduos mal intencionados.

Nesse contexto, um conflito se estabelece na esteira da política de supervalorização da informação enquanto mecanismo de poder e de geração de riquezas, conduzindo à possibilidade da *guerra informacional* e, de maneira mais geral, ao surgimento de uma nova doutrina de segurança apropriada à *era da informação*. A capacidade de se obter uma informação crítica, poluir bancos de dados ou devastar sistemas-chave de comunicação torna-se uma arma nesse novo ambiente tecnológico. Quanto mais um governo e uma sociedade dependem de sua rede de comunicação, maior sua exposição a ataques de *hackers*[300], de *crackers*[301] e de organizações criminosas[302]. Cresce, portanto, a incidência dos denominados *cybercrimes*, ou seja, crimes cometidos em meio eletrônico. Além dos ataques às infra-estruturas críticas e aos sistemas informatizados dos organismos de defesa – característicos da *guerra informacional* ou *guerra cibernética* – tornam-se cada vez mais comuns os ilícitos praticados em meio digital materializados tanto no acesso indevido a informações armazenadas em bancos de dados ou transmitidas por meio de sistemas informatizados (violação da *confidencialidade*); quanto na

[299] Vulnerabilidade é uma fragilidade presente ou associada a um ativo que se for explorada pode gerar um incidente de segurança. As vulnerabilidades por si sós não acarretam incidentes, necessitando de um agente causador ou condição favorável, denominada de ameaça. In: SÊMOLA, Marcos. **Gestão da segurança da informação**: gestão executiva da segurança da informação. Rio de Janeiro: Elsevier, 2003, p. 48.
[300] Hacker é a pessoa que acessa sistemas informatizados sem autorização. In PEREIRA, Joel Timóteo Ramos. **Compêndio jurídico da sociedade da informação**: notas práticas, legislação e jurisprudência. Lisboa: Quid Juris, 2004, p. 1035.
[301] Craker é a pessoa que acessa sistemas informatizados sem autorização com a finalidade de alterar ou remover dados. In PEREIRA, Joel Timóteo Ramos. Op. cit., p. 1032.
[302] CASTELLS, Manuel. **A galáxia da internet**. Op. cit., pp. 130-131.

alteração de dados armazenados em bancos de dados ou transmitidos por sistemas de comunicação eletrônica (violação da *integridade*); sem falar na falsificação de identidade e de dados (violação da *autenticidade*); estelionatos eletrônicos (*phishing scams*); na pornografia infantil; no racismo e na xenofobia; no atentado à propriedade intelectual e aos direitos conexos; nos danos por difusão de vírus; na invasão de privacidade; e na violação de sigilo industrial.

Segundo Bruce Schneier, pesquisador e consultor na área de segurança, as ameaças do mundo virtual espelham as ameaças do mundo real: estelionato, furto, invasão de privacidade, extorsão, pornografia infantil, jogos, fraudes, danos materiais e morais, enfim, tudo o que ocorre no mundo analógico pode ocorrer no digital. Apesar da atuação configurar-se de forma diferente, na manipulação de conexões digitais e entradas de sistemas ao invés de arrombamento de ambientes físicos constata-se que os objetivos e os resultados não diferem entre si; todavia, o rastreamento, a captura e a condenação desses criminosos revelam-se muito mais complexos, destacando-se este traço como o grande diferencial que distingue os crimes cometidos no mundo real daqueles cometidos no mundo virtual. Os atacantes dispensam a proximidade física de suas presas – o criminoso pode situar-se tanto em um recinto contíguo ao ocupado pela vítima quanto em um país milhares de milhas distante e atacar computadores onde quer que estejam – o que complica sobremaneira a investigação e também a punição[303].

Ainda, como característica da sociedade da informação, ressalta-se o extraordinário avanço na infra-estrutura da comunicação com o advento da internet. A rede permite a troca de informações de forma surpreendentemente simples, rápida e com plena interatividade entre as pontas. Enquanto o serviço de radiodifusão baseia-se na transmissão de informações de um emissor para vários destinatários sem qualquer interatividade[304], e o serviço de telefonia restrinja a transmissão de informações de um único emissor para um único destinatário apenas; a *web* permite a troca de informações de muitos usuários para muitos outros ao mesmo tempo, e com total interatividade, o que revoluciona todo o sistema de comunicação[305], conforme se verá no item 3.6.

A internet constitui-se das chamadas *auto-estradas da informação*, ou seja, de meios de comunicação de massa que ultrapassam as fronteiras nacionais e compõem uma rede mundial. As

---

[303] SCHNEIER, Bruce. ***Segurança.com***: segredos e mentiras sobre a proteção na vida digital. Tradução de Daniel Vieira. Rio de Janeiro: Campus, 2001, pp. 27-33.
[304] A implantação da TV digital agregará interatividade ao serviço de radiodifusão.
[305] ASCENSÃO, José de Oliveira. A sociedade da informação. In: _____(Org.). **Direito da sociedade da informação**. Coimbra: Coimbra Ed., 1999. vol. I, p. 164.

redes locais se interligam até formar redes nacionais, as redes nacionais também se unem para formar a rede internacional que, ao multiplicar-se, corporifica a *infra-estrutura global de informação*[306]. Pierre Levy denomina *cyberspace* o conjunto integrado pela *infra-estrutura global de informação* (internet), pelo universo oceânico de informações que ela abriga, e pelos usuários, cientistas e técnicos responsáveis pela sua manutenção e desenvolvimento[307]. A *web* – principal expressão do *cyberepaço* – difere-se dos demais meios de comunicação de massa por sua intangibilidade e estruturação descentralizada, o que permite a comunicação de todos para todos e o amplo acesso a informações em escala global, quebrando as barreiras de tempo e de espaço.

Um exemplo desse amplo acesso a informações em escala global, de forma fácil e rápida, pode ser observado no *site Google*. A notável diversidade de acesso a buscas por meio desse recurso, em tantos idiomas diferentes, confere a esse motor de busca uma força niveladora de inefável competência. Nunca antes na história do mundo, tanta gente, por conta própria, usufruiu a possibilidade de encontrar tantas informações sobre assuntos e pessoas tão diversas. Independentemente da localização física, todas as pessoas, cada uma de *per si*, dispõem das mesmas ferramentas, do mesmo acesso básico a dados gerais de pesquisa, podendo consultar informações a respeito do assunto armazenadas no mundo todo. A expectativa da empresa é que, em um futuro próximo, a qualquer pessoa se possibilite o acesso a informações da internet por meio de *palmtops*[308], *ipods*[309] ou telefones celulares, ou seja, o conhecimento estará literalmente dentro do bolso[310].

Além do *Google*, outro fenômeno que se oferece no mundo virtual como portal de relacionamento denomina-se *Yahoo!Groups,* que viabiliza a constituição de comunidades virtuais para troca de informações entre pessoas conhecidas ou não. Hoje, já há mais de 300 (trezentos) milhões de usuários e 4 (quatro) milhões de grupos ativos acessados por cerca de 13 (treze) milhões de pessoas do mundo inteiro. Essa ferramenta proporciona uma plataforma virtual para encontros privados, semiprivados ou públicos, independentemente de fatores geográficos ou temporais. Alguns grupos só existem em ambiente virtual; outros refletem comunidades já

[306] ASCENSÃO, José de Oliveira. Op. cit., p. 165.
[307] LÉVY, Pierre. **Cybercultura.** Tradução de Carlos Irineu da Costa. São Paulo: Editora 34, 1999, p. 17.
[308] *Palmtop* é um mini-computador que cabe na palma da mão.
[309] *Ipod* é um aparelho de áudio eletrônico projetado e vendido pela *Apple Computer* com capacidade de armazenamento de dados como imagem, som e documentos.
[310] FRIEDMAN, Thomas. **O mundo é plano**: uma breve história do século XXI. Tradução de Cristina Serra e S. Duart. Rio de Janeiro: Objetiva, 2005, pp. 176-180.

existentes no mundo real que agregam mais esse instrumento para comunicação e troca de informações[311].

Na sociedade da informação não se estabelecem, portanto, fronteiras físicas, traçadas em nível jurídico, político e territorial; o fluxo de informações é intenso e transnacional. Diante da dificuldade de se traçarem limites geográficos no mundo virtual, enfraquece-se até mesmo a soberania dos Estados, que não conseguem mais regulamentar nem controlar de forma individualizada os serviços de comunicação. Alguns países proíbem a comercialização interna de recursos criptográficos utilizados para garantir o sigilo das comunicações, a fim de evitar que organizações criminosas se valham desses meios, o que acabaria com a possibilidade de acesso ao conteúdo das comunicações interceptadas pelos organismos estatais. Entretanto, acessando-se a própria rede esses recursos podem ser adquiridos de forma gratuita ou onerosa. Assim, diz-se que os Estados já se vêem inermes, impossibilitados de evitar, de forma isolada, os efeitos produzidos pela nova infra-estrutura global de informação.

A respeito do caráter desterritorializante do ciberespaço e do enfraquecimento da soberania dos Estados, expõe Pierre Levy:

> De fato, o ciberespaço é desterritorializante por natureza, enquanto o Estado moderno baseia-se, sobretudo, na noção de território. Pela rede, bens informacionais (programas, dados, informações, obras de todos os tipos) podem transitar instantaneamente de um ponto a outro do planeta digital sem serem filtradas por qualquer tipo de alfândega. Os serviços financeiros, médicos, jurídicos, de educação a distância, de aconselhamento, de pesquisa e desenvolvimento, de processamento de dados também podem ser prestados aos locais por empresas ou instituições estrangeiras (ou vice-versa) de forma instantânea, eficaz e quase invisível. O Estado perde, assim, o controle sobre uma parte cada vez mais importante dos fluxos econômicos e informacionais transfronteiros. Além disso, as legislações nacionais obviamente só podem ser aplicadas dentro das fronteiras dos Estados. Ora, o ciberespaço possibilita que as leis que dizem respeito à informação e à comunicação (censura, direitos autorais, associações proibidas etc.) sejam contornadas de forma muito simples. De fato, basta que um centro servidor que distribua ou organize a comunicação proibida seja instalado em qualquer 'paraíso de dados', nos antípodas ou do outro lado da fronteira, para estar fora da jurisdição nacional. Como os sujeitos de um Estado podem conectar-se a qualquer servidor do mundo, contanto que tenham um computador ligado à rede telefônica, é como se as leis nacionais que dizem respeito à informação e à comunicação se tornam inaplicáveis.[312]

Traçadas essas primeiras considerações, ressalte-se que, após a revolução agrícola e a revolução industrial, a *revolução da tecnologia da informação* se eleva como a terceira grande

[311] FRIEDMAN, Thomas. Op. cit., p. 184.
[312] LÉVY, Pierre. Op. cit., p. 204.

transformação da humanidade. Todas as *infra-estruturas críticas* passaram a ser controladas por meio de recursos computacionais; massificaram-se os meios de comunicação com o advento da microeletrônica; o Estado e a iniciativa privada aderiram à internet, utilizando-a para prestar serviços; recursos humanos foram substituídos por *agentes inteligentes* em linhas de produção específicas; o fluxo de informações assumiu escala global, enfraquecendo tradicionais limites territoriais; surgiu uma nova especialidade denominada *segurança da informação* com intuito de gerenciar de forma mais eficiente as informações; enfim, consagrou-se um novo paradigma denominado *sociedade da informação*.

3.4 O panoptismo de Michel Foucault

3.4.1 O exercício do poder disciplinar

A história da humanidade expõe o *exercício do poder disciplinar* que se materializa na manipulação e no uso de informações em benefício de certas elites, capazes de processá-las e armazená-las, fazendo desses repositórios fontes seguras de fiscalização, de repressão e de controle dos indivíduos. Esse modelo remonta aos mosteiros medievais e à Igreja que, dominando a escrita, elaboraram arquivos não apenas sobre orientação religiosa, como também a respeito dos hábitos, crenças, práticas e costumes das comunidades que ameaçavam seu poderio. Os arquivos da Inquisição nada mais evidenciam do que relatos detalhados sobre inclinação sexual e intelectual, saúde, ascendência e descendência, círculo de amizade e costumes dos indivíduos. A sofisticação adquiria tais contornos que já se praticava cruzamento de informações, especialmente no que concerne aos considerados "hereges", o que demonstra que as perseguições e os julgamentos pelos tribunais não se efetivavam aleatoriamente[313].

No século XIX, essa invasão de privacidade, desde há muito tempo arraigada nas organizações religiosas, passou a ser adotada também pelos Estados, que organizaram seus

[313] PIZZOLANTE, Francisco Eduardo Orcioli Pires e Albuquerque. **Habeas data e bancos de dados**: privacidade, personalidade e cidadania no Brasil atual. Rio de Janeiro: Lumen Juris, 2002, pp. 51-53.

primeiros arquivos para exercitar seu poder disciplinar. Em estudos, especialmente em *Vigiar e punir,* publicado em 1975, o pensador e filósofo francês Michel Foucault descreve como se exerce o poder disciplinar e quais os reflexos desse mecanismo para o indivíduo e para a coletividade – tema da maior relevância para a compreensão dos fundamentos filosóficos do exercício da vigilância na sociedade contemporânea, ou seja, na *sociedade da informação*.

Segundo o autor, o objetivo da disciplina perseguia a meta de tornar o corpo mais obediente e mais útil por meio de uma política de coerção e de manipulação do comportamento humano. A disciplina se impunha como um mecanismo utilizado para controlar de maneira minuciosa o corpo, impondo-lhe uma relação de docilidade-utilidade. Assim, tinha por fim reduzir a força política e maximizar a utilidade do indivíduo. Fábricas, escolas, hospitais, hospícios e prisões se estruturavam e, como lógica de funcionamento, norteavam-se por técnicas disciplinantes[314]. A disciplina era exercida recorrendo-se a pequenas astúcias, arranjos sutis, dispositivos que procuravam impor a coerção sem demonstrar a gravidade do controle. Havia cálculo do infinitamente pequeno, descrição das características mais tênues dos indivíduos. Enfim, a disciplina impunha-se como uma anatomia política do detalhe, integrava a "microfísica" do poder[315].

Durante séculos as ordens religiosas destacaram-se como mestras da disciplina, monitorando o ritmo e o tempo. No século XIX, entretanto, o controle em relação ao tempo foi levado às escolas. Tentou-se construir um tempo integralmente útil, anulando-se tudo que perturbasse e distraísse o aluno dos estudos. O tempo medido e pago aos empregados também deveria ser de boa qualidade e por isso precisava ser fiscalizado nas oficinas e nas fábricas[316]. Assim, no ambiente laboral, o controle passou a ser intenso e contínuo durante todo o processo de trabalho. Não se restringia mais ao processo de produção, o comportamento dos empregados também passou a ser monitorado. Tornou-se necessária a formação de um pessoal especializado na "arte de vigiar". A vigilância ganhou status de operador econômico, na medida em que se tornava peça essencial no aparelho de produção e na engrenagem do poder disciplinar[317].

---

[314] MAIA, Antônio C. Sobre a analítica do poder de Foucault. **Tempo Social – Revista de sociologia da USP**. São Paulo: Universidade de São Paulo, n. 7(1-2), out. 1995, pp. 93-94.
[315] FOUCAULT, Michel. **Vigiar e punir**: nascimento da prisão. Tradução de Raquel Ramalhete. Petrópolis: Vozes: 1987, p. 120.
[316] FOUCAULT, Michel. **Vigiar e punir**. Op. cit., pp.127-129.
[317] FOUCAULT, Michel. **Vigiar e punir**. Op. cit., pp. 146-151.

Na Idade Média, o poder do Estado funcionava essencialmente por meio de símbolos e de taxas, na forma de impostos, pilhagens e guerras. Com o passar do tempo, tornou-se mais complexo, estruturando-se sobre uma "tecnologia de controle" sobre os corpos. A disciplina passou a funcionar como uma rede que atravessava os corpos; um instrumento ou mecanismo do poder estatal. Os indivíduos deveriam agrupar-se espacialmente nos ambientes de suas atividades rotineiras; exercendo-se controle não mais em relação ao seu passado, mas em relação ao futuro, ou seja, o comportamento ainda em fase de desenvolvimento[318].

Essa mudança na forma de exercício do poder pelo Estado produziu efeitos até no ambiente da criminalidade. A denominada "criminalidade de sangue" aos poucos foi sendo substituída pela "criminalidade da fraude". O desenvolvimento da produção, o aumento das riquezas, a maior valorização jurídica da propriedade, o policiamento mais estreito da população, o advento de técnicas mais modernas de descoberta e captura de informações; tudo isso levou ao deslocamento da delinqüência da morte para a da vigarice. A violência física aos corpos gradualmente arrefeceu-se, enquanto crescia a criminalidade das bordas e das margens, reservada a um grupo de profissionais bem treinados e experientes em fraudes[319].

Nesse contexto, tornou-se necessária a implantação de novo método de vigilância pelo Estado. O aparelho disciplinar originário das organizações religiosas foi reformulado. Construíram-se observatórios humanos com capacidade de, em um único olhar, tudo ver permanentemente: *olho perfeito a que nada escapa e em direção para o qual todos os olhares convergem.* A tecnologia, unida à física e à cosmologia, preparava, em surdina, um saber novo a respeito do homem sobre o qual se acumulavam mais e mais mecanismos de sujeição[320].

Traçadas essas primeiras considerações, verifica-se que a disciplina – enquanto método de controle do comportamento dos indivíduos – surgiu no âmbito das organizações religiosas, sendo depois incorporada pelas instituições de ensino e pelas fábricas, para incremento da produtividade. Verificada a eficiência da implantação desse mecanismo de sujeição, o Estado absorveu tais dispositivos a fim de controlar o comportamento das pessoas ainda em fase de desenvolvimento; vigiando não apenas o passado, mas também o futuro desses indivíduos. Diante de tal cenário, cresceu o número de instituições disciplinares, passou-se a investir cada vez mais

[318] MAIA, Antônio C. Op. cit., pp. 95-96.
[319] FOUCAULT, Michel. **Vigiar e punir**. Op. cit., pp. 64-74.
[320] FOUCAULT, Michel. **Vigiar e punir**. Op. cit., pp. 143-146.

em tecnologias de controle, centradas no comportamento humano, enfim, a vigilância tornou-se o principal operador econômico da sociedade.

3.4.2 O modelo panóptico

Jeremy Bentham, no final do século XVIII, editou o livro *Panopticon*. A obra, entretanto, permaneceu desconhecida até ser apresentada por Michel Foucault, nos anos 70, como um acontecimento na história do espírito humano[321]. O modelo arquitetural panóptico foi descrito pelo irmão de Bentham que, ao visitar a Escola Militar de Paris em 1751, percebeu que os dormitórios do prédio eram envidraçados, o que permitia o controle dos alunos até mesmo no período noturno, como forma de evitar qualquer contato entre os colegas. Diante da descrição desse cenário, Bentham atribuiu a denominação "Panóptico" a esse modelo arquitetural utilizado para resolver os problemas de vigilância[322].

O princípio panóptico consiste em construir na periferia da construção um anel e, no centro, uma torre de forma a garantir constante vigilância. Assim descreve Foucault:

> A construção periférica é dividida em celas, cada uma ocupando toda a largura da construção. Estas celas têm duas janelas: uma abrindo-se para o interior, correspondendo às janelas da torre; outra, dando para o exterior, permite que a luz atravesse a cela de um lado a outro. Basta então colocar um vigia na torre central e em cada cela trancafiar um louco, um doente, um condenado, um operário ou um estudante. Devido ao efeito de contraluz, pode-se perceber da torre, recontando-se na luminosidade, as pequenas silhuetas prisioneiras nas celas da periferia. Em suma, inverte-se o princípio da masmorra; a luz e o olhar de um vigia captam melhor que o escuro que, no fundo, protegia.[323]

Adotando-se a figura arquitetural panóptica, observa-se que aqueles que se encontram confinados, mais que sofrer pelo encarceramento, devem imbuir-se da condição de eterna vigilância a que se encontram expostos e, mais, a esses mesmos encarcerados não se concede sequer o recíproco direito de observar quem os vigia e quando os vigia; *são esses indivíduos objetos de informação, mas nunca sujeitos de comunicação*. Assim, o efeito mais importante do

[321] FOUCAULT, Michel. **Microfísica do poder**. Organização e tradução de Roberto Machado. Rio de Janeiro: Edições Graal, 1979, p. 209.
[322] FOUCAULT, Michel. **Microfísica do poder**. Op. cit., p. 211.
[323] FOUCAULT, Michel. **Microfísica do poder**. Op. cit., p. 210.

panóptico é o processo de indução a que se recorre, uma vez que o detento deve estar ciente do estado de permanente exposição à visibilidade, medida que assegura o funcionamento automático do poder; fazer que a vigilância seja ininterrupta, independentemente de seu exercício. Mais importante do que ser vigiado propriamente é saber que pode estar sendo vigiado. *Para ser eficiente, o panóptico deve ser "visível" e "inverificável"; o indivíduo não precisa saber que está sendo observado, mas precisa ter certeza que poderá sê-lo a qualquer momento*[324].

Outro efeito do panóptico traduz-se na possibilidade de constituir um saber sobre os indivíduos vigiados. Esse saber pode ser utilizado para classificar as pessoas, a fim de determinar se elas se conduzem ou não da maneira "correta", se são ou se não são indivíduos "normais", se cumprem ou não as ordens dadas[325]. Trata-se de um equívoco, porque se baseia na crença de que as pessoas se tornarão virtuosas e "normais" por saberem que estão sendo vigiadas[326]. Conforme descreve Michel Foucault: "*o panóptico é uma utopia de uma sociedade e de um tipo de poder que é, no fundo, a sociedade que atualmente conhecemos*"[327]. O *panoptismo* evidencia-se como traço característico das sociedades contemporâneas, por permitir ao Estado a vigilância individual e contínua dos cidadãos. Segundo Jeremy Bentham, esse modelo de organização do poder baseado no controle mediante punição, correção e recompensa, isto é, fundamentado na formação e na transformação dos indivíduos sujeitos a certas normas, nada mais é do que uma sociedade *panóptica*, sociedade em que reina o *panoptismo*[328].

Para finalizar, ressalta-se que o panóptico não se apresenta apenas como um modelo arquitetural que permite constante e detalhada vigilância de loucos, doentes, condenados, operários, militares e estudantes. Michel Foucault destaca a importância do método panóptico enquanto meio de exercício do poder: *quanto maior o número de informações em relação aos indivíduos, maior a possibilidade de controle do comportamento desses mesmos indivíduos*. A vigilância é "visível", mas "inverificável", ou seja, o "detento" sabe que pode estar sendo observado, embora não tenha certeza. Esse mecanismo de permanente visibilidade assegura o funcionamento automático do poder, daí a sua incorporação pelas sociedades contemporâneas, enquanto mecanismo de fortalecimento dos *aparelhos de Estado*.

---

[324] FOUCAULT, Michel. **Vigiar e punir**. Op. cit., pp. 166-167.
[325] FOUCAULT, Michel. **A verdade e as formas jurídicas**. Tradução de Roberto Cabral de Melo Machado e Eduardo Jardim. 3ª Ed. Rio de Janeiro: NAU Editora, 2003, p. 88.
[326] FOUCAULT, Michel. **Microfísica do poder**. Op. cit., p. 225.
[327] FOUCAULT, Michel. **A verdade e as formas jurídicas**, Op. cit., p. 87.
[328] FOUCAULT, Michel. **A verdade e as formas jurídicas**, Op. cit., p. 103.

3.4.3 O controle dos indivíduos enquanto mecanismo de poder

Segundo Jeremy Bentham, o problema do panóptico consiste no olhar dominador e vigilante a que nada escapa. A questão da vigilância, no caso, não privilegia a punição; a preocupação do panóptico se concentra no propósito de o encarcerado nunca se entregar a comportamentos que o poder julga inadequados, ao se sentir mergulhado em um campo de visibilidade absoluta. *O que há de diabólico nessa idéia, assim como em todas as suas concretizações, é que a força não é dada inteiramente a alguém e este alguém não a exerce de forma isolada*. O panóptico se traduz em uma máquina que abrange todas as pessoas, tanto aquelas que exercem o poder como aquelas sobre os quais o poder se exerce. *Essa é a característica das sociedades que se instauram no século XIX, o poder não é identificado com um indivíduo, ele é uma maquinaria de que ninguém é titular sendo, portanto, mais difícil limitá-lo*[329].

Sob essa ótica, Foucault impõe um deslocamento em relação ao Estado, ao identificar a existência de uma série de relações de poder na sociedade atual, que exorbita o âmbito estatal e que não pode, de maneira alguma, ser analisada em termos de soberania, de proibição ou de imposição de uma lei como, a relação homem-mulher, a relação familiar, a relação entre um que sabe e outro que não sabe, a relação entre patrão e empregado. Tais relações não se restringem a projeções do poder do Estado, estendem-se além de tais limites. O Estado, com todo o seu aparato, mostra-se incapaz de ocupar todo o campo de poder, já que oferece somente a superestrutura[330].

O poder não emana de um ponto centralizado, ele se estrutura em uma rede que permeia todo o corpo social, articulando e integrando os diferentes focos que se apóiam uns nos outros, tais como escola, prisão, hospital, asilo, família, fábrica, vila operária. O poder se estabelece mediante relações mais ou menos coordenadas; sendo, portanto, móveis e fragmentadas[331]. Segundo Foucault, essa rede institucional de poder que permeia todo o campo social é intra-estatal e baseada em um poder epistemológico – um poder de saber sobre os indivíduos submetidos a um olhar incessante: "*Vemos assim nascer, ao lado desse saber tecnológico,*

[329] FOUCAULT, Michel. **Microfísica do poder**. Op. cit., pp. 215-219.
[330] MAIA, Antônio C. Op. cit., p. 87.
[331] MAIA, Antônio C. Op. cit., p. 88.

próprio a todas as instituições de seqüestro, um saber de observação, um saber de certa forma clínico, do tipo da psiquiatria, da psicologia, da psico-sociologia, da criminologia"[332].

A individualidade entra em um campo documentário. O resultado de exames escolares e médicos expõe um arquivo inteiro com detalhes e minúcias. São criados métodos para documentação e registro. Surgem os códigos para classificar as informações: código físico para qualificação, código médico dos sintomas, código dos comportamentos. *É a primeira "formalização" do individual dentro de relações de poder; a pessoa passa a ser objeto descritível, analisável e submetido ao permanente controle*[333].

Com base no que foi exposto, observa-se o notável incremento do poder disciplinar a partir do século XIX. A vigilância constante e detalhada passou a ser utilizada como mecanismo de poder, tanto pelo Estado como pelas instituições de caráter privado, estruturando-se como uma rede de controle que permeia todo o campo social. Diante da complexidade dessa estrutura, as pessoas ficaram expostas a uma visibilidade universal e constante – característica das sociedades panópticas. Além de permanentemente observados, os indivíduos são ainda classificados, registrando-se nos mínimos detalhes suas características e condutas. A grande pretensão consiste em se prever se os indivíduos inseridos em tal sociedade adotarão comportamentos considerados "normais" e "adequados" à superestrutura pelo fato de saberem que se encontram sujeitos a uma visibilidade absoluta.

3.5 Panoptismo na sociedade da informação

3.5.1 Poder disciplinar e controle por meio da tecnologia

Apresentados os fundamentos sociológicos do paradigma da *sociedade da informação,* e delineado o modelo *panóptico*, descrito pelo filósofo francês Michel Foucault, analisa-se a configuração do *panoptismo na sociedade da informação* no que concerne ao exercício do poder

[332] FOUCAULT, Michel. **A verdade e as formas jurídicas.** Op. cit., p. 122.
[333] FOUCAULT, Michel. **Vigiar e punir**. Op. cit., pp. 157-158.

disciplinar e controle utilizando a tecnologia. Diante desse novo cenário social, político e econômico em que a principal riqueza é a informação; destaca-se o intensivo uso da tecnologia da informação para supervisão e para fiscalização dos indivíduos. São dois os principais mecanismos utilizados: formação de arquivos com informações pessoais e vigilância do comportamento das pessoas.

Na Idade Média, o poder disciplinar foi instaurado pela Igreja, adotando-se a técnica de formação de arquivos contendo informações pessoais a respeito das comunidades que ameaçavam seu poderio. Com o passar dos anos, esse método foi adotado também pelo Estado por revelar-se um excelente instrumento de controle dos indivíduos. Trata-se de uma tecnologia de poder, chamada por Foucault *biopolítica*, objetivando-se transformar toda a população para para impulsionar a evolução da sociedade e o fortalecimento do Estado[334].

Assim, a vigilância, antes exercida pela família e pela Igreja, aos poucos é transferida para o Estado diante da maior complexidade da sociedade e da necessidade de gerenciamento das informações[335]. Conforme expõe Reg Whitaker, o método passou a ser utilizado pelos governos para facilitar o desempenho de diversas atividades tais como arrecadação tributária; criação de um arquivo central com a classificação dos cidadãos de acordo com suas atividades produtivas, patrimônio e outros dados relevantes; manutenção da lei e da ordem pública por meio da vigilância de grupos de oposição; elaboração de estatísticas; dentre outras[336]. A intromissão do Estado na privacidade dos cidadãos por meio da coleta de informações pessoais e uso de recursos tecnológicos configura-se, neste contexto, como um mecanismo de poder necessário para benefício da população.

No século XIX, a disciplina foi implantada em oficinas e em fábricas para fiscalização do processo de trabalho, e também nas escolas, hospitais e presídios para supervisão do comportamento dos indivíduos. No final do século XX, o avanço da tecnologia da informação intensificou o exercício do poder disciplinar, ao permitir a coleta, o cruzamento e o

---

[334] REVEL, Judith. **Michel Foucault**: conceitos essenciais. Tradução de Maria do Rosário Gregolin, Nilton Milanez e Carlos Piovesani. São Carlos: Claraluz, 2005, pp. 26-28.

[335] GRAY, Susan H. Eletronic data bases and privacy: policy for the 1990s. In: **Science, Technology, & Human Values**, n. 3, vol. 14, verão 1989, pp. 242-257, p. 252: *Societies have always had surveillance and information systems. In small-scale tradition-based societies, the family or the village was responsible for surveillance and information management. The local church may have been involved as well. As societies has grown more complex, the social-control responsibilities fo the family and organize religion have diminished and the state's responsibility has increased* (Tradução Livre).

[336] WHITAKER, Reg. Op. cit., pp. 57-58.

armazenamento de dados pessoais a baixos custos e de forma facilitada, além de ter incrementado a *vigilância eletrônica* – tema a ser explorado no próximo item.

Hoje, a formação de arquivos pessoais não se impõe como mais um privilégio exclusivo da Igreja e do Estado. Empresas coletam informações de caráter pessoal de forma desautorizada e depois cruzam essas mesmas informações com dados provenientes de prestadoras de serviço telefônico, provedores de acesso à internet, administradoras de cartão de crédito, bancos, enfim, toda e qualquer organização que possa contribuir para o processo de delineamento do perfil das pessoas. O mecanismo utilizado para facilitar a coleta recorre à persuasão para convencer o próprio titular das informações; sua privacidade se transforma em moeda de troca na *era da informação*. Trocam-se informações pessoais por serviços personalizados, brindes, direito de participar de sorteios, acesso gratuito à *web*, produtos e financiamentos *online*[337]. Empresas oferecem "cartões promocionais de fidelidade" apenas para coletar dados que denunciam as tendências de compras de seus clientes[338]. A Blockbuster – maior rede de locação de filmes do mundo – armazena registros eletrônicos que contêm dados identificadores de dia e de horário para que usuários possam receber "descontos"[339].

Mas as grandes vilãs se identificam como *empresas.com*, ou seja, as empresas que prestam serviços pela internet. Como as principais fontes de rendimento dessas companhias advêm de publicidade e de *marketing*, essas empresas monitoram seus clientes, compram e vendem informações de caráter pessoal, enfim, utilizam as mais diversas artimanhas para traçar o perfil de seus consumidores[340]. Apenas a título exemplificativo, resgata-se o caso da empresa *Geocities*, grande e poderoso provedor que, como condição para disponibilizar páginas gratuitas na internet, exigia que seus usuários preenchessem formulários com dados pessoais, tais como endereço, salário, formação educacional, sexo, estado civil, profissão, áreas de interesse. A partir desses dados, criava o perfil de seus usuários e vendia tais dados para empresas de *marketing*[341]. Noticia-se que nos EUA, 92% (noventa e dois por cento) dos *websites* coletam dados pessoais de seus usuários e os processam segundo interesses comerciais próprios[342]. Apesar da intervenção do governo norte-americano com intermediação da *Federal Trade Commission,* a prática tem

[337] FORTES, Débora. A morte da privacidade. **Revista Info Exame**. São Paulo: Ed. Abril, ano 15, pp. 30-40, jun. 2000.
[338] SCHNEIER, Bruce. Op. cit., p. 31.
[339] SCHNEIER, Bruce. Op. cit., p. 45.
[340] CASTELLS, Manuel. **A galáxia da internet**. Op. cit., pp. 66-67.
[341] SANTOS, Antonio Jeová. Op. cit., p. 188.
[342] CASTELLS, Manuel. **A galáxia da internet**. Op. cit., p. 143.

crescido exponencialmente, sendo adotada pelo *Yahoo!Groups, Google, Aol,* conforme expõe David Freedman:

> *Google, Yahoo* e outras empresas precisam saber quem você é; onde você está; o que você compra; o que você assiste e lê; com quem você divide seu tempo; e até o que você diz para seus amigos. Mas nenhuma empresa quer ser pega espionando seus clientes, então, essas companhias importunam-nos e seduzem-los literalmente a cada dígito teclado, até que concordem com a coleta de informações necessárias à publicidade personalizada. Devemos aceitar essa situação? Uma vez que a história de sua vida cotidiana está nos bancos de dados do *Google* e de outras empresas, você simplesmente tem que ter confiança que não será disponibiliza para organismos públicos de execução da lei, sua esposa, seu chefe, extorsionários ou qualquer pessoa que esteja trabalhando contra seus interesses. E por mais que essas companhias sejam confiáveis, elas não terão como evitar o acesso por *hackers* e outras espécies de criminosos.[343]

Assim, o ciberespaço põe em risco a privacidade dos usuários diante da excessiva acumulação de informações de caráter pessoal. Poucos serviços prestados pela *web* dispensam a coleta, o armazenamento, o tratamento e a difusão de dados relacionados com a intimidade e com a vida privada dos internautas. Qualquer acesso à rede deixa gravados registros do usuário, ainda que de forma indireta: o seu espectro de relações, as suas opiniões e gostos, os hábitos de consumo, o nível social, entre outros. O problema reside no fato de a coleta de dados ser feita tanto de forma transparente para finalidades explícitas e autorizadas pelo titular, como também de forma velada e contra os interesses da pessoa em questão[344].

Em ambiente de trabalho, exerce-se o poder disciplinar por meio da instalação de câmeras de vigilância e do monitoramento das comunicações dos empregados, conforme visto no item 2.6. Além desses mecanismos, as empresas ainda controlam a utilização dos sistemas de informática pelos empregados, recorrendo a *softwares* que registram e arquivam, *pari passu*, a movimentação e as consultas virtuais realizadas por esses indivíduos. Objetiva-se controlar o

---

[343] FREEDMAN, David H. Why privacy won´t matter. **Newsweek Magazine**. New York: MSNBC. pp. 38-42, 3 abr. 2006: "*Google, Yahoo and others need to know who you are; where you are, what you buy, watch and read; who you spend time with, and even what you say to your friends. No business wants to be caught spying on its customers, of course; these companies plan to nudge and seduce us, literally bit by bit, into agreeing to let them gather the information advertisers needed for tailored pitches. (...) Should we put up with it? (...) Once the story of your day-to-day life is on file at Google and other companies, you will simply have to take it on faith that they won't let it get into the hands of law-enforcement agencies, your spouse, your boss, extortionists and anyone else who might be working against your interests. And no matter how trustworthy these companies turn out to be, they might not be able to stop criminal and hackers from lifting the data anyway*" (Tradução Livre).

[344] GONÇALVES, Maria Eduarda. Op. cit., pp. 173-174.

tempo e a produtividade do empregado, o modo como desenvolve suas atividades, seu *know-how* e conhecimentos utilizados para cumprimento das tarefas[345].

Diante do exposto, observa-se que – a espelho do que ocorria no século XIX – o Estado não utiliza essa arquitetura de poder de forma isolada. O *panóptico da era da informação* abrange todo aquele que se coloca em situação de supremacia – como empresas em relação aos consumidores e empregados – limitando a privacidade e a autodeterminação dos subjugados. Verifica-se, ademais, que as tecnologias utilizadas pelo Estado para controle e espionagem foram quase que na sua totalidade desenvolvidas pela iniciativa privada.

A *Electronic Frontier Foundation* – EFF[346], um grupo de defesa dos direitos civis, com sede em São Francisco (Califórnia), descobriu, no ano de 2005, que os serviços secretos dos EUA codificam dia e hora em que documentos são impressos por equipamentos da Cannon e da Xerox. O governo admitiu a existência de um acordo com as fabricantes de impressoras, mas essas empresas asseguraram que as informações rastreadas seriam utilizadas unicamente para investigações relacionadas com a falsificação de equipamentos. Os códigos instalados nas impressoras conferem ao governo norte-americano – com a colaboração da indústria – a faculdade de registrar todos os documentos impressos com dia e hora, por mais absurdo que isso possa parecer[347].

A respeito da parceria entre Estado e iniciativa privada na organização desse sistema de permanente controle, elucida Manuel Castells:

> A grande ironia histórica é que uma das instituições capitais na defesa da liberdade, a livre empresa, é o ingrediente essencial na construção desse sistema de vigilância – apesar da boa vontade geral e da ideologia libertária da maior parte das companhias da Internet. Sem ajuda delas, os governos não teriam o know-how e, mais fundamentalmente, a possibilidade de intervir na Internet: tudo depende da capacidade de agir sobre provedores de serviços da Internet e redes específicas por toda parte. (...) Por que empresas de tecnologia da informação colaboram com tanto entusiasmo na reconstrução do velho mundo do controle e da repressão? Há duas razões principais, afora atitudes oportunistas ocasionais. A primeira que diz respeito, sobretudo às firmas *ponto.com*, é que elas precisam quebrar a privacidade de seus clientes para poder vender. A segunda é que elas precisam de apoio do governo para preservar seus direitos de propriedade na economia baseada na Internet.[348]

[345] JABUR, Gilberto Haddad. **A dignidade e o rompimento da privacidade**. Op. cit., pp. 102-103.
[346] Mais informações disponíveis no sítio <http://www.eff.org>. Acesso em: 30 jan. 2007.
[347] CUIDADO: sua impressora espiona você. 20 out. 2005. Disponível em <http://tecnologia.terra.com.br/interna/0,,OI717103-EI4801,00.html>. Acesso em: 30 jan. 2007.
[348] CASTELLS, Manuel. **A galáxia da internet**. Op. cit., pp. 148-149. Grifos nossos.

Observa-se, pois, uma certa dependência dos governos em relação à iniciativa privada na implementação desse mecanismo de permanente vigilância, especialmente no que concerne à invenção e fabricação de novos equipamentos utilizados para controle da população. Isto, de um lado, representa a fragilidade do Estado no exercício do poder disciplinar; de outro, demonstra sua fortaleza, já que na atualidade a superestrutura de poder permeia todo o campo social e em escala global. Estabelecem-se parcerias, tanto com o empresariado quanto com a comunidade científica ao redor de todo o mundo; isto sem mencionar os convênios entre agências de inteligência de diferentes países, conforme será visto no item 3.7.1.

Os governos passam a agir de maneira coordenada para incrementar a vigilância. A primeira vítima desse controle é o Estado, que sofre limitações à sua própria soberania ao se obrigar a uma atuação de forma conjunta com outros países para garantir eficácia no combate à criminalidade na rede; além de se sujeitar a padrões tecnológicos comuns. A segunda vítima é a liberdade de expressão, já que, o tráfego de comunicações pode ser interceptado por agências de inteligência de vários países que se encontram interconectadas, o que expõe a vida das pessoas de forma implacável. Essa visibilidade permanente, como no modelo panóptico de Jeremy Bentham, induz as pessoas a agirem de maneira diversa do que agiriam se não estivessem sendo observadas. É o mundo da dissimulação, da falsidade, dos subterfúgios cada vez mais elaborados para disfarçar o ego e encobrir as condutas. Entretanto, conforme descreve Foucault, tudo não passa de um equívoco, porque as pessoas não se tornarão virtuosas simplesmente por saberem que estão sendo vigiadas.

Manuel Castells descreve como a vigilância e a espionagem em meio eletrônico influenciam o comportamento dos indivíduos:

> O aspecto mais atemorizante é, de fato, a ausência de regras explícitas de comportamento, de previsibilidade das conseqüências de nosso comportamento exposto, segundo os contextos de interpretação, e de acordo com critérios usados para julgar nosso comportamento por uma variedade de atores atrás da tela de nossa casa de vidro. Não é o Big Brother, mas uma multidão de irmãzinhas, agências de vigilância e processamento de informações que registram nosso comportamento para sempre, enquanto bancos de dados nos rodeiam ao longo da nossa vida – a começar, dentro em breve, com nosso DNA e características pessoais (nossa retina, nosso datilograma, na forma de marcas digitalizadas). Nas condições vigentes nos Estados autoritários, essa vigilância pode afetar diretamente nossas vidas (essa é de fato a situação da maioria esmagadora da humanidade). Mas mesmo em sociedades democráticas, em que os direitos civis são respeitados, a transparência de nossas vidas moldará decisivamente as nossas atitudes. Ninguém jamais foi capaz de viver numa sociedade transparente. Se esse sistema de vigilância e controle da Internet se desenvolver

> plenamente, não poderemos fazer o que nos agrada. Talvez não tenhamos nenhuma liberdade, e nenhum lugar onde nos esconder.[349]

Em contrapartida, cresce o número de recursos tecnológicos utilizados para neutralizar esse controle por parte do Estado, a exemplo da criptografia[350], empregada na cifragem do conteúdo das comunicações. Essas tecnologias – denominadas *tecnologias de liberdade* – são produzidas e comercializadas por empresas que encontram um novo nicho de mercado; em outros casos, são inventadas por combatentes resolutos de movimentos sociais em defesa da liberdade, a exemplo da EFF. A criptografia não assegura o anonimato total do emissor, pois a origem da mensagem pode ser identificada por meio do IP (*internet protocol*)[351], ou seja, o número atribuído ao computador quando este se conecta à rede, mas garante o sigilo do conteúdo da comunicação. Este tema será explorado com detalhes no item 3.6.1.

Pierre Lévy, estudioso da internet, ressalta a resistência do Estado diante das *tecnologias de liberdade,* como a criptografia, justamente por dificultarem o exercício da vigilância operada pela interceptação das comunicações:

> Os Estados vêem evidentemente na 'democratização" de poderosos instrumentos de criptografia um atentado à sua soberania e segurança. Por isso o governo dos Estados Unidos tentou impor com padrão um sistema de criptografia cuja chave seria conhecida por suas agências de informação. (...) Diversos governos, entre os quais o francês e o chinês, requerem autorização prévia (muito difícil de conseguir) para o uso das tecnologias de criptografia. A lei considera os milhares de franceses que usam o PGP sem autorização oficial possuem armas de guerra e poderiam atentar contra a segurança do Estado. (...) Observemos, enfim, para concluir esse assunto, que a proibição dos instrumentos de

[349] CASTELLS, Manuel. **A galáxia da internet**. Op. cit., pp. 148-149. Grifos nossos.

[350] "*A palavra criptografia tem origem grega e significa a arte de escrever em códigos, de forma a esconder a informação na forma de um texto incompreensível. A cifragem ou processo de codificação, é executada por um programa de computador que realiza um conjunto de operações matemáticas e transformam um texto claro em um texto cifrado, além de inserir uma chave secreta na mensagem. O emissor do documento envia o texto cifrado, que será reprocessado pelo receptor, transformando-o, novamente, em texto legível, igual ao emitido, desde que tenha a chave correta. Existem dois tipos de criptografia: simétrica e assimétrica. A criptografia simétrica é baseada em algoritmos que dependem de uma mesma chave, denominada chave secreta, que é usada tanto no processo de cifrar quanto no de decifrar o texto. Para a garantia da integridade da informação transmitida é imprescindível que apenas o emissor e o receptor conheçam a chave. O problema da criptografia simétrica é a necessidade de compartilhar a chave secreta com todos que precisam ler a mensagem, possibilitando a alteração do documento por qualquer das partes. A criptografia assimétrica utiliza um par de chaves diferentes entre si, que se relacionam matematicamente por meio de um algoritmo, de forma que o texto cifrado por uma chave, apenas seja decifrado pela outra do mesmo par. As duas chaves envolvidas na criptografia assimétrica são denominadas chave pública e chave privada. A chave pública pode ser conhecida pelo público em geral, enquanto que a chave privada somente deve ser de conhecimento de seu titular*". Disponível em <http://www.iti.br/twiki/bin/view/Certificacao/PerguntasFrequentes>. Acesso em: 30 jan. 2007.

[351] IP é a abreviatura da palavra *internet protocol*. É o principal protocolo da internet, responsável pela identificação das máquinas e redes e pelo encaminhamento correto das mensagens. In PEREIRA, Joel Timóteo Ramos. Op. cit., p. 1036.

> criptografia em um país não impede de forma alguma seu uso em toda parte pelo terrorismo e crime organizado, que, não se importando com uma ilegalidade, podem muito facilmente conseguir tais instrumentos, sobretudo através da rede.[352]

Outra forma de exercício de poder disciplinar na era da informação estabelece-se mediante o controle da própria internet pelos EUA. Na administração Clinton, o Congresso e a administração dos EUA se armaram para monitorar a rede. Para isso, valeram-se do argumento de que a *web* precisava ser regulada para proteger as crianças das perversidades sexuais que vagavam pela rede. A Suprema Corte, em 26 de junho de 1997, proibiu o controle e garantiu o "direito constitucional ao caos da rede", sob fundamento da liberdade de expressão. Em 1998, houve nova tentativa do Congresso por meio da *Child On-line Protection Act,* também derrubada pela Suprema Corte[353].

Diante desse impasse com o Judiciário, o governo dos EUA desenvolveu novas tecnologias que possibilitam não apenas a identificação das rotas de comunicação, mas também a monitoração de todas as informações que circulam na rede por meio de aplicações de *software* que se superpõe em camadas e protocolos. Utilizou-se o argumento da necessidade de identificação das comunicações para facilitar a prestação de serviços personalizados, bem como a proteção de direitos de propriedade intelectual. Na realidade, essas tecnologias foram adotadas como forma de recuperação de poder que o governo estava perdendo. Contudo, novas *tecnologias de liberdade* dia a dia surgem para se opor ao controle, a sociedade civil se arma e o Judiciário oferece relativa proteção diante dos flagrantes abusos[354], enfim, incrementam-se as disputas pela liberdade na era de informação, a mais fascinante dentre todas as épocas.

Entretanto, a disputa pelo controle da *web*, que se perpetua desde a sua criação como um projeto militar na década de 60, ainda não se concluiu. A *governança da internet* foi inclusive o tema mais palpitante discutido na segunda fase da Cúpula Mundial da Sociedade da Informação realizada em Túnis, capital da Tunísia, entre os dias 16 e 18 de novembro de 2005. Pelo caráter descentralizado da rede mundial de computadores, é de se esperar que nenhum país a controle. Por outro lado, não se pode perder de vista que, para que um usuário acesse a internet de forma "amigável", localizando um determinado ponto de rede mesmo sem saber sua exata identificação;

[352] LÉVY, Pierre. Op. cit., pp. 205-206.
[353] CASTELLS, Manuel. **A galáxia da internet**. Op. cit., pp. 139-140.
[354] CASTELLS, Manuel. **A galáxia da internet**. Op. cit., pp. 140-141.

faz-se necessário incumbir alguma autoridade da administração de certos aspectos técnicos, tais como a vinculação de determinados endereços de IP a nomes de domínio[355].

Atualmente, esse controle se sustenta no poder de veto que o Departamento de Comércio Norte-Americano detém sobre as atividades estratégicas da ICANN (*Internet Corporation for Assigned Names and Numbers*). A ICANN, uma associação norte-americana sem fins lucrativos, tem a chave tecnológica por meio da qual são distribuídos os nomes de domínio ou "endereços" na internet, possibilitando a comunicação entre os computadores. Outorga-se um poder inimaginável a essa corporação, ao permitir-lhe tomada de decisões que oscilam de escalas relativamente limitadas, como desconectar qualquer endereço da rede, até atingir dimensões globais, como desconectar um país inteiro e isolá-lo do resto do mundo[356].

Na Cúpula Mundial da Sociedade da Informação, países como Brasil, China, Índia e, mais recentemente, a União Européia, contestaram o controle norte-americano sobre a internet, sob o argumento de que esse conglomerado de redes se tornou uma ferramenta de comunicação e motor do crescimento econômico em escala mundial, não podendo ser dirigida por um único país. Após infindáveis discussões, decidiu-se que a gestão técnica da rede continuará sob domínio dos EUA, que não cederam à pressão da comunidade internacional para um compartilhamento do controle das numerações e dos domínios da *net* que passaria a ser dirigido por um organismo intergovernamental[357].

Entre 30 de outubro e 02 de novembro de 2006, o tema *governança da internet* foi novamente discutido em Atenas (Grécia), em foro convocado pelo Secretário Geral das Nações Unidas, quando se debateram questões envolvendo liberdade de expressão na internet; livre circulação de informações na rede; segurança da infra-estrutura; formulação de políticas públicas relacionadas à *web*; conectividade; e custos. Os EUA assumiram o compromisso de o Departamento de Comércio Norte-Americano não interferir mais nas atividades da ICANN até 2009, quando se encerrará a vigência do memorando de entendimento entre essas entidades. O

---

[355] No Brasil, esses aspectos técnicos são atribuição do *Núcleo de Informação e Coordenação do Ponto BR - NIC.br* vinculado ao *Comitê Gestor da Internet no Brasil*. O *NIC.br*, dentre outras atividades, é responsável pelos registros de nomes de domínio, pela administração e pela publicação do DNS (*domain name server* ou servidor de nome de domínio) para o domínio <.br>, e pelos serviços de distribuição e de manutenção de endereços na internet no Brasil; o que é realizado através do Registro.br hospedado no site <http://www.registro.br/>. Para maiores informações consultar o sítio do Comitê Gestor da Internet no Brasil, disponível em <http://www.cgi.br/>. Acesso em: 30 jan. 2007.

[356] Disponível em <http://www.icann.org>. Acesso em: 30 jan. 2007.

[357] ONU quer internet em todo mundo até 2015. 18 nov. 2005 Disponível em: <http://www.prodatasystems.com.br/noticias/view.asp?id=15>. Acesso em: 30 jan. 2007.

próximo fórum ocorrerá em novembro de 2007, no Rio de Janeiro – RJ, mas até o presente momento nenhuma definição se estabeleceu a respeito da questão do controle da rede mundial de computadores[358].

Pelo exposto, observa-se como a tecnologia contribuiu para o incremento do poder disciplinar enquanto mecanismo de controle dos indivíduos. Informações pessoais contidas em diferentes bancos de dados são interconectadas como forma de facilitar a manipulação de consumidores. Recorrem-se a variados dispositivos tecnológicos para monitorar o comportamento das pessoas e, desta forma, garantir o funcionamento automático do poder. É o *panoptismo* na sociedade da informação – superestrutura formada pela combinação de esforços dos governos e iniciativa privada que, juntos, desenvolvem novos artefatos de vigilância e de espionagem. De outro lado, cresce o número de pessoas preocupadas com o desenvolvimento de tecnologias de liberdade, a exemplo da criptografia, além do maior envolvimento dos países em torno do tema *governança da internet* – controle e monitoramento da rede – nada mais do que a antiga questão enfrentada por Foucault na década de 70: *quem vigia o vigia*?

3.5.2 Vigilância eletrônica

Conforme exposto no item anterior, as duas principais formas de exercício de poder disciplinar são a formação de arquivos com informações a respeito dos indivíduos controlados e a vigilância do comportamento das pessoas. Incrementou-se a primeira com a criação de *softwares*, que, automaticamente, cruzam informações armazenadas em diferentes bancos de dados; e com o advento da internet, que facilitou a coleta, o tratamento e a difusão dos dados pessoais. A vigilância sobre o comportamento das pessoas – apesar de ser uma prática que remonta à Idade Média – também sofreu extraordinário avanço com a invenção de aparatos tecnológicos que permitem o permanente controle dos indivíduos. Câmeras de segurança em locais públicos; circuitos internos de televisão em ambientes privados; rastreamento de indivíduos mediante sinais emitidos por celular; cartões magnéticos e pulseiras com *chips* que permitem o monitoramento

[358] INTERNET Governance. Disponível em: <http://ec.europa.eu/information_society/policy/internet_gov/index_en.htm>. Acesso em: 30 jan. 2007.

dos usuários; enfim, inúmeros artefatos garantem a transparência do comportamento humano na sociedade, tolhendo a privacidade daqueles que estão expostos à permanente vigilância.

Entende-se por *vigilância eletrônica* qualquer espécie de vigilância realizada a distância mediante dispositivos tecnológicos utilizados para rastreamento, monitoramento e controle. A *videovigilância* se materializa como a espécie mais comum de vigilância eletrônica e também a mais noticiada nos meios de comunicação de massa, embora existam outros mecanismos mais avançados. Implementa-se tal dispositivo para se captarem imagens por meio de circuitos internos de televisão (*closed-circuit television* – CCTV) integrados a câmeras de segurança que se encontram estrategicamente instaladas tanto espaços públicos quanto privados. Diversas funções se atribuem a tais mecanismos, sendo mais comum a utilização para controlar o fluxo de trânsito nas grandes cidades, proteger pessoas e bens e facilitar a supervisão e o monitoramento permanente de crianças e adolescentes por pais e professores, o que pode acarretar sérios distúrbios de personalidade.

Em Londres, tendo-se como referência apenas espaços públicos, estima-se a existência de 2,5 milhões de câmeras de segurança; sendo que a imagem de um cidadão britânico médio é capturada cerca de 300 (trezentas) vezes em um mesmo dia. Em Nova York, circunscrita apenas à cidade de Manhattan, identificaram-se 2.397 (duas mil trezentos e noventa e sete) câmeras instaladas para o mesmo fim[359]. David Freedman afirma, em matéria publicada na revista *Newsweek* chamada *Why Privacy Won't Matter*, que, nos EUA, no ano de 2006, já havia mais de 25 (vinte e cinco) milhões de câmeras de segurança espalhadas pelos locais públicos, estimando-se um aumento de dois milhões de câmeras em um único ano[360], o que torna os americanos o segundo povo mais vigiado do mundo, perdendo apenas para os ingleses.

Em matéria publicada na revista Veja, em 2004, um relatório do governo inglês revela que as câmeras só previnem delitos leves contra o patrimônio, não produzindo nenhum impacto quanto ao número de homicídios, seqüestros e outros crimes graves[361]. Em outra matéria jornalística, publicada na revista Isto É, a população é alertada para os perigos das câmeras de vigilância. Especialistas em segurança revelam que, assim como as páginas da internet, essas câmeras têm um endereço eletrônico na rede, sendo possível o rastreamento e o acesso às

[359] CASTRO, Catarina Sarmento. Op. cit., pp. 122-123.
[360] FREEDMAN, David H. Op. cit.
[361] FERRANTE, Daniel. O Big Brother é inglês. **Revista Veja.** São Paulo: Ed. Abril, Edição 1848, ano 37, n. 14, 7abr.2004, p. 60.

imagens filmadas por qualquer internauta, exceto em casos de proteção por mecanismos especiais de cifragem[362]. Essa atividade de busca de imagens capturadas via internet por circuitos internos de televisão e câmeras de segurança localizados em locais públicos ou privados denomina-se *videorraspagem*[363]. O problema se intensifica em razão de a população em geral aprovar a utilização de tais dispositivos que conduzem à perda da privacidade, sob a justificativa de que se impõe o incremento da segurança pública para proteção do cidadão e do patrimônio, apesar do relatório do governo inglês revelar que o emprego desse método produz um impacto mínimo em relação aos crimes mais graves.

Na Inglaterra, a preocupação em torno da videovigilância e outras formas de invasão utilizando modernos aparatos tecnológicos deu origem a uma organização não-governamental em defesa do direito à privacidade, chamada *Privacy Internacional*, com sede em Londres e filial em Washington. A organização já conta com membros filiados de mais de trinta países e tem atuado em diversas áreas, como direito, comunicação, publicidade e estatística. Pesquisas da *Privacy Internacional* revelam que os países que mais utilizam a vigilância – enquanto mecanismo de controle do comportamento das pessoas – são Inglaterra, EUA, Rússia e China; pessoas negras se expõem como cidadãos mais vigiados, em proporção três vezes maior em relação àqueles que se distinguem pela cor branca; tornam-se alvo única e exclusivamente por pertencerem a alguma minoria 40% (quarenta por cento) das pessoas vigiadas, ou seja, a vigilância se materializa como mais um mecanismo de repressão à diversidade e de exercício da discriminação[364].

Para minimizar os impactos da videovigilância estatal e privada, alguns países, como Portugal, regulamentaram a atividade e passaram a exigir, dentre outros requisitos, que se colocasse um alerta, em local visível, em áreas monitoradas por câmeras, para que as pessoas tomassem conhecimento da vigilância mediante filmagem a que se expunham ao transitarem por esses espaços monitorados. Na França, a Lei de Orientação e de Programação da Segurança Francesa determina que o público deve ser informado não só da existência da vigilância, como também da autoridade responsável por ela; permitindo-se ao filmado em local público o acesso às suas próprias imagens para defesa de interesses pessoais. O diploma português que regula a

[362] PINHO, Cláudia; MENCONI, Darlene. Tá tudo vigiado. **Revista Isto É**. São Paulo: Editora Três, n. 1848, 16mar.2005, pp. 69-70.
[363] SOUZA, Carlos Afonso Pereira. O progresso tecnológico e a tutela jurídica da privacidade. In: **Informática e internet**: aspectos legais internacionais. Tarcísio Queiroz Cerqueira, Erick Iriarte, Márcio Morena (organizadores). Rio de Janeiro: Esplanada, 2001, p. 69.
[364] Mais informações disponíveis no sítio <http://www.privacyinternational.org/index.shtml>. Acesso em: 30 jan. 2007.

utilização de câmeras de vídeo pelas forças e pelos serviços de segurança em locais públicos também contempla mecanismos para o exercício do direito de acesso à imagem por quem está sendo filmado, devendo o responsável, antes de promover o acesso, excluir a imagem de terceiros, para que não ocorra a violação da privacidade desses mesmos terceiros[365].

Em Portugal, a lei que regulamenta a videovigilância em locais públicos[366] fixa o prazo máximo de conservação das imagens em trinta dias, o que obriga a destruição das imagens findo esse lapso temporal. Na Bélgica, as imagens gravadas em espaços públicos podem ser conservadas apenas durante vinte e quatro horas; na Dinamarca, trinta dias; na Finlândia, três dias; na França, trinta dias; na Grécia, quinze dias; na Espanha, trinta dias; na Suécia, trinta dias; no Reino Unido, o período varia conforme o tipo de local. Em todos esses países, o prazo é suspenso ou estendido quando a imagem estiver sendo utilizada em investigação criminal ou em processo judicial[367].

Diante desse contexto – constatada a irreversibilidade da utilização da videovigilância enquanto mecanismo de monitoramento de áreas públicas e privadas e controle do comportamento das pessoas – ressalte-se a necessidade de regulamentação dessa atividade, definindo-se questões tais como: dever de informação de que a área sofre monitoração por câmeras; direito de acesso às imagens pelos próprios filmados; dever de apagamento das imagens de terceiros no momento do acesso por algum dos filmados; prazo de conservação das imagens; dever de acesso limitado às imagens por funcionários devidamente treinados; obrigação de utilização de mecanismos de segurança que garantam o sigilo das imagens durante o período de seu armazenamento como, a cifragem dos dados; a proibição de comunicação das imagens a terceiros sem prévia autorização judicial; a proibição de instalação de câmeras em banheiros, em vestiários e em outros locais em que possa ocorrer ofensa à dignidade da pessoa humana; dentre outras.

Catarina Sarmento ressalta que, além da necessidade de regulamentação da videovigilância, deve ser observado, no exercício dessa atividade, o *princípio da proporcionalidade*. A captação de imagens deve ser pertinente e não excessiva relativamente às finalidades para as quais são recolhidas. As câmeras de vigilância que pertencem a edifícios não podem ser colocadas com a finalidade de captar a imagem das pessoas que circulam na rua ou na

[365] CASTRO, Catarina Sarmento. Op. cit., pp. 145-148.
[366] Lei Orgânica n. 2, de 12 de maio de 2004.
[367] CASTRO, Catarina Sarmento. Op. cit., pp. 148-149.

calçada, focando apenas as áreas de acesso e os espaços interiores. Aplica-se ainda o princípio no próprio uso em si do recurso, sendo admitido apenas diante da não existência de mecanismos menos invasivos à privacidade do cidadão, ou seja, impõe-se que o mecanismo seja necessário além de adequado. Afere-se a proporcionalidade em sentido estrito pela utilização, mediante análise do número de câmeras, a sua localização e correspondente capacidade técnica, especialmente para *zoom*[368].

Mais além da videovigilância, existem outras espécies de *vigilância eletrônica* não baseadas no tratamento de imagens como, a vigilância mediante o uso de radiofreqüência (*radio frequency identification* – RFID) utilizada em "pulseiras eletrônicas". Trata-se de um conjunto de equipamentos e de aplicações informáticas que permite detectar, a distância, a presença ou a ausência de determinada pessoa em determinado local, mediante emissão de um sinal de rádio emitido pela "pulseira" colocada no pulso ou no tornozelo da pessoa que se vigia, sendo os sinais captados pelo centro de controle[369]. Algumas escolas da Califórnia adotam essa tecnologia para localizar com exatidão os estudantes dentro do campus, em cujos limites todos que ali estudam são obrigados a portar um dispositivo com *chip* que emite sinais de rádio. Bibliotecas dos EUA também recorrem a essa tecnologia para rastrear os livros emprestados, que dispõem de *chips* acoplados; a conseqüência lógica evidencia um outro universo, o do monitoramento dos próprios leitores, o que pode afetar não apenas o direito à privacidade como também a liberdade de pensamento, de crença e de expressão em decorrência das opções de leitura a que os estudantes se inclinam, o que preocupa os integrantes do movimento social em defesa da liberdade EFF[370].

Bruce Schneier, especialista em segurança, cita outras formas de exercício da *vigilância eletrônica* como a instalação de microfones minúsculos, microcâmeras, rastreamento via satélite de usuários de celular, reconhecimento de rosto e de voz, dentre outros dispositivos tecnológicos descritos pelo autor:

> Microfones direcionais poderosos podem pegar conversas a centenas de metros de distância. No resultado da tomada da embaixada japonesa no Peru pelo grupo terrorista MRTA (1997), os noticiários descreveram insetos de áudio escondidos nos botões das camisas, permitindo aos policiais detectarem o local de cada um. Dispositivos Van Eck podem ler o que está no monitor do seu computador desde a metade da sua rua. (...) Câmeras minúsculas – agora sendo vendidas em catálogos de produtos eletrônicos – podem se ocultar nos menores lugares;

[368] CASTRO, Catarina Sarmento. Op. cit., p. 150.
[369] CASTRO, Catarina Sarmento. Op. cit., p. 122.
[370] RADIO Frequency Identification. 4 abr. 2005. Disponível em: <http://www.eff.org/Privacy/Surveillance/RFID/>. Acesso em: 30 jan. 2007.

> câmeras de satélite podem ler a placa do seu carro desde a órbita da terra. E o Departamento de Defesa está construindo protótipos de micro veículos aéreos, do tamanho de pequenos pássaros ou borboletas, que podem passar por vigias inimigos, localizar reféns em prédios ocupados ou espiar praticamente qualquer pessoa. (...) Em 1993, o chefão da droga colombiano Pablo Escobar foi identificado parcialmente rastreando-o através do uso do telefone celular: uma técnica conhecida por *pinpointing* (localização com precisão). (...) A tecnologia para procurar negociações de drogas em conversas telefônicas aleatórias, comportamento suspeito em imagens de satélite ou rostos de criminosos em "lista de procurados" a partir de câmeras na rua ainda não é comum, mas isso é apenas uma questão de tempo. O reconhecimento de rosto poderá selecionar pessoas individuais em uma multidão. O reconhecimento de voz poderá analisar milhões de ligações telefônicas, ouvindo uma pessoa em particular; ele já pode procurar palavras ou frases suspeitas e apanhar conversas em uma multidão.[371]

Uma outra espécie de *vigilância eletrônica*, bem comum, denuncia-se pelo sistema de posicionamento global por satélite (*global positioning system* – GPS) que indica a latitude, a longitude e a altitude – coordenadas geodésicas – do objeto ou da pessoa a ser localizada. O sistema foi criado e é controlado pelo Departamento de Defesa dos EUA, e pode ser utilizado por qualquer pessoa, gratuitamente, necessitando-se apenas de um receptor que capte os sinais emitidos por satélites. Além das aplicações na aviação e na navegação, aplica-se o referido sistema para localização de veículos automotores, como carros e caminhões que se deseja proteger. Transmissores instalados nos veículos indicam sua localização controlada por um computador central que monitora esses veículos por onde quer que circulem.

Mas a grande descoberta em termos de vigilância consiste em um *chip* batizado de *Digital Angel,* lançado em 2001, nos Estados Unidos[372]. Trata-se de um biossensor de identificação, integrado à internet, que possibilita o monitoramento das pessoas por sistema de satélites, podendo ser instalado em doentes, em condenados, enfim, em qualquer pessoa que se deseje controlar. O *chip* inserido no corpo do indivíduo franqueia a um monitor instalado a distância a localização do portador onde quer que se encontre, em qualquer parte do mundo; além de registrar batimentos cardíacos, pressão arterial e outros dados considerados importantes. O dispositivo foi criado com o propósito de monitorar animais em rebanhos; com o passar dos anos passou a ser utilizado para preservar a saúde e a vida de pessoas, o que merece aplausos. Todavia, o uso dessa tecnologia para finalidades alheias a tal mister torna-se temerário pela inimaginável capacidade humana de adaptar instrumentos para adequá-los a interesses muitas vezes escusos.

---

[371] SCHNEIER, Bruce. Op. cit., pp. 42-43. Grifos nossos.
[372] Disponível em <http://www.digitalangelcorp.com> Acesso em: 30 jan. 2007.

Quando o assunto diz respeito ao direito à privacidade, o *Digital Angel* condensa em si a exata expressão do panoptismo em vigor na sociedade da informação. Muito mais preciso do que o modelo arquitetural de Jeremy Bentham, o *chip* permite a construção de um detalhado saber sobre aquele que é vigiado, além de garantir absoluta visibilidade do vigiado por meio de satélites que rastreiam o indivíduo onde quer que se encontre. O sujeito se torna mero objeto de informação, é mergulhado em um campo de visibilidade ilimitada, seus comportamentos e o funcionamento de seu organismo são permanentemente supervisionados por aqueles responsáveis por seu monitoramento – sejam estes médicos, carcereiros, empregadores ou qualquer outra pessoa em situação de vigilância.

Diante do exposto, observa-se o impacto produzido pelo desenvolvimento da tecnologia da informação na prática medieval da vigilância. Esse mecanismo para exercício do poder disciplinar – utilizado pela Igreja e depois pelo Estado e pelas empresas segundo o modelo arquitetural do Panóptico, conforme expôs Michel Foucault – exacerbou-se com a revolução tecnológica e com a criação de diversos dispositivos utilizados para rastreamento, monitoramento e controle a distância; daí falar-se em vigilância eletrônica. A espécie mais comum é a videovigilância – operada por meio de circuitos internos de televisão e câmeras de segurança que captam as imagens das pessoas, a fim de influenciar seu comportamento e incrementar a segurança. O uso indiscriminado desses dispositivos tem preocupado juristas e ativistas de organizações não governamentais de defesa das liberdades públicas ao redor de todo o mundo, o que levou a sua regulamentação em diversos países, a exemplo de Portugal, Espanha, França, Bélgica, Dinamarca, Suécia, Finlândia e Grécia. Outras formas de vigilância, comuns na sociedade da informação, destacam a vigilância mediante o uso de radiofreqüência (*radio frequency identification* - RFID); o rastreamento via satélite de usuários de celular; o GPS; e a utilização de *chips* integrados à internet como o biossensor *Digital Angel*.

3.6 Riscos da internet à privacidade

A internet é conseqüência da fusão de conhecimentos de estratégia militar, cooperação científica e iniciativa tecnológica. Surgiu no auge da Guerra Fria, quando a extinta União das

Repúblicas Socialistas Soviéticas – URSS lançou o primeiro satélite ao espaço. Os EUA, em resposta, investiram em um projeto de criação de um sistema de comunicação que se mostrasse invulnerável a ataques dos países inimigos. O trabalho – coordenado pela Agência de Projetos de Pesquisa Avançada (*Advanced Research Projects Agency* – ARPA) do Departamento de Defesa norte-americano – foi denominado ARPAnet. O objetivo consistia em criar uma rede de comunicação independente, cujos dispositivos gerissem-se por si sós, sem prenderem-se a uma fonte central, ou seja, uma rede capaz de tornar todos os pontos de conexão equivalentes e autônomos. Assim, eventual bombardeio pela ex-URSS em um determinado ponto da rede norte-americana não comprometeria a conexão entre os demais dispositivos.

Com base na tecnologia de comunicação de troca de mensagens por pacotes, criou-se uma rede capaz de transmitir sons, imagens e dados sem se recorrer a um centro de controle. O sistema entrou em funcionamento em 1969, com a participação de militares e de cientistas. Em 1983, ocorreu uma divisão do projeto em duas vertentes: a ARPAnet, dedicada a fins científicos; e a MILnet, orientada para aplicações militares. Em meados de 1980, a tecnologia do projeto ARPAnet passou a ser utilizada por pesquisadores e por acadêmicos das universidades americanas para troca de informações, contribuindo, cada vez mais, para o desenvolvimento de uma "interface amigável". Em 1990, os serviços da ARPAnet foram encerrados, e a *National Science Foundation* – NSFNET assumiu o desenvolvimento da rede. Em 1995, após fortes pressões comerciais, o governo norte-americano privatizou a rede, outorgando seu controle a uma instituição sem fins lucrativos denominada *Internet Society*[373]. Aos poucos foram surgindo inúmeros provedores de acesso que disseminaram a tecnologia para o restante da população. Assim, criada inicialmente para fins militares, milhões de pessoas em todo o mundo atualmente usufruem os benefícios que o acesso à internet oferece.

Vale ressaltar que a internet não consiste apenas em uma rede informática internacional, mas em uma interconexão de várias redes por meio do denominado protocolo TCP/IP (*transmission control protocol/internet protocol*) – uma espécie de língua comum que permite a comunicação entre as redes, quaisquer que sejam as suas características tecnológicas. Destaque-se, como expediente importante, o denominado *request for comments* – RFC, um canal em que investigadores da comunidade científica depositam idéias e solicitam comentários de outros pesquisadores – o que comprova que a *net* emerge da cooperação científica e da iniciativa

[373] CASTELLS, Manuel. **A sociedade em rede**. Op. cit., pp. 82-83.

tecnológica. A *world wide web* (www) destaca a área em que se colocam páginas com informações em texto, som e imagem; permitindo-se o compartilhamento desses dados entre usuários ao redor de todo o mundo. A *internet relay chat* – IRC possibilita a comunicação em tempo real entre os assinantes e o intercâmbio de informações[374].

Configurando-se como uma interconexão de várias redes de comunicação, a internet aumentou sobremaneira o acesso às informações, além de ter permitido a troca de dados nos mais diversos formatos entre pessoas e organizações ao redor de todo o mundo. Por trás desse desenvolvimento científico e tecnológico, surgiu uma nova economia chamada por Manuel Castells *economia informacional, global e em rede,* para identificar suas características fundamentais e enfatizar sua interligação. É *informacional* porque tanto a produtividade quanto a competitividade, seja de empresas, seja de nações, dependem basicamente da respectiva capacidade de produzir, processar e aplicar de forma eficiente as informações e de gerar conhecimentos. É *global* porque as atividades produtivas, o consumo e a circulação de seus componentes (capital, trabalho, matéria-prima, informação, tecnologia e mercados) organizam-se em escala global. É *em rede*, pois as condições históricas, a produtividade e a concorrência conectam-se diretamente[375].

Essa excessiva valorização da informação de per si na *economia informacional, global e em rede* aliada à pressão do mercado por maior produtividade permitiu que as empresas – organizadas em rede – passassem a explorar, desmesuradamente, a intimidade e a vida privada de seus clientes, esquadrinhando informações pessoais para, desta forma, personalizar o *marketing* e oferecer maior eficiência nos serviços oferecidos. Nesse contexto, a *web* – enquanto fenômeno dessa nova forma de organização social, política e econômica denominada sociedade da informação – atua como uma ameaça à privacidade de seus usuários.

Reconhecendo-se não apenas a revolução política, econômica e social promovida pelo advento da internet, mas também a extraordinária ampliação do acesso a informações, e, ainda, o incremento da liberdade de expressão responsável pelo fortalecimento dos movimentos contraculturais e da democracia, tendo em vista, igualmente, a maior eficiência na administração dos órgãos públicos e das empresas, dentre tantos outros benefícios proporcionados pela rede;

[374] MARQUES, Garcia; MARTINS, Lourenço. Op. cit., pp. 50-53.
[375] CASTELLS, Manuel. **A sociedade em rede**. Op. cit., p. 119.

pretende-se tão-somente alertar para os riscos à privacidade que tais avanços podem oferecer, como forma de contribuir para o uso mais consciente desse notável meio de comunicação.

Conforme já exposto, a *net* revelou-se um meio propício de invasão à privacidade ao facilitar o intercâmbio de informações pessoais entre os diversos *prestadores de serviço da sociedade da informação*, em especial as *empresas.com*. Bancos de dados, antes *off-line,* integraram-se à rede, sendo transformados em bancos de dados *on-line*; o que implica a possibilidade de interconexão de maior número de *informações pessoais identificáveis*. Esses dados, conforme já exposto, são posteriormente utilizados para atividades de *marketing,* tais como o envio de *spam*[376] ou para outros fins obscuros e não autorizados pelo titular das referidas informações[377].

Além disso, a *web* facilita o monitoramento das condutas virtuais das pessoas, registradas nos bancos de dados dos provedores de acesso por sistemas informáticos automatizados. O monitoramento ocorre por meio da leitura do número de IP, ou seja, do número de registro que identifica cada computador quanto a máquina se conecta à rede. Cruzando-se o IP com os *logs*[378] – também conhecidos como *diários de navegação* – o provedor consegue identificar o computador utilizado, a data e o lapso de tempo de cada conexão, os destinatários das mensagens enviadas por meio daquele computador, os *sites* visitados, dentre outras informações técnicas[379]. A invasão à privacidade se caracteriza ainda mais grave quando se submetem os *logs* registrados nos bancos de dados dos provedores à análise de *agentes inteligentes*[380], que, então, classificam os internautas em diversas categorias, conforme os assuntos pesquisados, produtos ou serviços consumidos, faixa etária, classe social e outras informações relevantes que interessem a determinados setores de publicidade ou que se destinem a qualquer outra finalidade não autorizada pela titular das informações.

---

[376] *Spam* consiste em toda e qualquer correspondência eletrônica não solicitada. PEREIRA, Joel Timóteo Ramos. Op. cit., p. 1042.
[377] PEREIRA, Joel Timóteo Ramos. Op. cit., p. 465.
[378] *Log* é o termo utilizado para descrever o processo de registro de eventos relevantes em um sistema computacional. In CARTILHA de Segurança para Internet. Versão 3.1. São Paulo: **Comitê Gestor da Internet no Brasil**, 2006, p. 60.
[379] CASTRO, Catarina Sarmento. Op. cit., p. 159.
[380] Agentes inteligentes consistem em sistemas computacionais capazes de raciocinar e de resolver problemas a partir de informações incompletas. Possuem aptidão para aprendizagem, resolução de problemas, articulação de ações, previsão de conseqüências, percepção de fatos ambíguos; além de criatividade e de capacidade para comunicação. In ROVER, Aires José. **Informática no direito**: inteligência artificial. Curitiba: Juruá, 2001.

Outro inconveniente da utilização da *net* esconde-se sob a falsa sensação de privacidade. Embora se apresente como um ambiente eminentemente público, a intangibilidade do mundo virtual induz os internautas a uma exposição incauta em relação às próprias comunicações. Esse fenômeno se constata na *internet relay chat* (IRC)[381] quando se tem acesso a um diálogo em tempo real, podendo tal comunicação ser realizada entre vários internautas que participam de grupos abertos ou fechados mediante sua conexão com o servidor[382] de uma rede de IRC. Cada participante desse "bate-papo" se identifica mediante um pseudônimo ou *nickname*, garantindo seu *anonimato*, mas, com o decorrer do tempo, a freqüência dos diálogos induz as pessoas a confidências e à identificação. Outros internautas, menos cautelosos, além de se identificarem, revelam informações íntimas que deveriam ficar restritas à vida pessoal e familiar – dados relevantes que fomentam a prática de delitos não só no mundo virtual, como estelionato e outras fraudes, mas também no mundo real, como extorsão mediante seqüestro e outras condutas de grave potencial ofensivo.

Outra prática muito comum de exposição da privacidade em rede ocorre em situações de utilização de *blogs*, ou seja, sítios da internet nos quais as pessoas – em especial adolescentes – publicam um *diário eletrônico*, em que se desnudam ao expor características e experiências mais íntimas[383]. Idêntica situação se verifica nos denominados *sites* de relacionamento, como o *Orkut* e o *ParPerfeito*. O *Orkut* se apresenta como uma rede social filiada ao *Google*, criada em 19 de janeiro de 2004 pelo projetista turco Orkut Büyükkokten, com o objetivo de oferecer aos seus membros um meio de comunicação facilitador para o estabelecimento de novas amizades e relacionamentos[384]. Por meio dessa rede, as pessoas criam comunidades virtuais para estabelecer comunicações entre indivíduos que comungam interesses comuns. Ao se inserir nessa rede de relacionamentos, o indivíduo descreve seu perfil pessoal e/ou profissional, com o objetivo de se tornar *visível* para outras pessoas. A base de dados pode ser utilizada livremente por qualquer usuário cadastrado na rede, e a busca pode ser feita pelo nome ou pelo detalhamento do perfil da pessoa a ser encontrada. O *ParPerfeito* foi projetado para facilitar o encontro entre pessoas que

[381] *Internet Relay Chat* (*IRC*) é um protocolo de comunicação bastante utilizado na internet por permitir a interação simultânea de vários internautas. Usado basicamente para bate-papo (*chat*) e troca de arquivos, permitindo a conversação em grupos abertos ou fechados. PEREIRA, Joel Timóteo Ramos. Op. cit., p. 1037.
[382] Servidor é um sistema de computação que fornece serviços a uma rede de computadores. Normalmente é ligado à internet. PEREIRA, Joel Timóteo Ramos. Op. cit., p. 1041.
[383] In CARTILHA de Segurança para Internet. Op. cit., p. 29.
[384] Disponível em <http://www.orkut.com>. Acesso em: 30 jan. 2007.

buscam um relacionamento amoroso[385]. O internauta, ao se cadastrar, disponibiliza seu perfil e descreve a "pessoa ideal" segundo suas afinidades. Os usuários mais empolgados fornecem fotos e imagens pessoais, revelam a renda e o patrimônio – tudo isso na esperança de encontrar a "pessoa ideal". Após a interconexão dessas informações por *softwares*, o *site* disponibiliza os contatos das pessoas com perfis semelhantes, facilitando o "encontro amoroso" entre indivíduos solitários ao redor do mundo.

Cria-se a *cultura da auto-exposição* na *web.* Para se sentirem "digitalmente incluídas" na sociedade da informação, algumas pessoas colocam-se em evidência de forma temerária, alimentando o firme propósito de serem "localizadas" na rede mundial de computadores por meio de motores de busca[386] como o *Google*, *Yahoo* e *Cadê*, que levam às páginas nas quais detalhadas informações revelam seu perfil. Enfim, a internet, além de facilitar a violação da privacidade por terceiros, induz o usuário inconsciente à auto-exposição exagerada. Nas palavras de Paulo José da Costa Júnior, "*a tecnologia acoberta, estimula e facilita o devassamento da vida privada; (...) as pessoas condicionadas pelos meios de divulgação da era tecnológica (...) sentem-se compelidas a renunciar à própria intimidade*"[387].

Victor Drummond, ao discorrer sobre as comunicações na internet, estabelece alguns critérios para separar a esfera pública da esfera privada no ambiente virtual:

> a) identificação do destinatário da mensagem: a mensagem cujo destinatário for indeterminado será uma mensagem pública, já a mensagem cujo destinatário for determinado poderá ser pública ou privada, dependendo dos demais critérios;
> b) ciência das demais pessoas envolvidas na comunicação: a mensagem será privada se o emissor tiver conhecimento das pessoas envolvidas na comunicação e será pública se não tiver conhecimento dos destinatários;
> c) existência de intimidade entre os interlocutores: a mensagem será privada se o grupo for coeso e formado por amigos ou pessoas que tenham qualquer outra estreita relação, a mensagem será pública se o grupo for formado por pelo menos um estranho.[388]

O autor conclui que se caracteriza como violação à intimidade a utilização da internet que implique em deslocamento de dados ou de informações de um ambiente de comunicação privada para um ambiente de comunicação pública; ou o deslocamento de dados ou informações de um ambiente de comunicação privada, compartilhado pelo usuário, para outro ambiente, igualmente

[385] Disponível em <http://www.parperfeito.com>. Acesso em: 30 jan. 2007.
[386] Motores de busca ou máquinas de busca são programas utilizados para encontrar qualquer informação na *web*, apresentando os resultados de forma organizada e rápida. Entre as maiores empresas se encontram o *Google*, o *Yahoo*, o *Lycos*, o *Cadê*, o *Donavera* e, mais recentemente, a *Amazon.com*.
[387] COSTA JÚNIOR, Paulo José da. Op. cit., pp. 19-20.
[388] DRUMMOND, Victor. **Internet, privacidade e dados pessoais**. Rio de Janeiro: Lumen Juris, 2003, p. 27.

de comunicação privada, mas do qual o mesmo usuário não compartilhe[389]. Tal fato se constata quando uma pessoa expõe, em rede, fotografias que recebe de terceiro por *e-mail*, em que se expõe a intimidade de ambos; também ocorre violação à privacidade quando um participante anônimo revela, em *chat*, informações íntimas de terceiros que sequer têm conhecimento do fato porque não participam dessa conversação simultânea.

Além da proliferação dos bancos de dados *on line*, do monitoramento eletrônico por meio do número de IP, da disseminação da *cultura da auto-exposição*, mencionem-se os *cookies* como mais uma ameaça à invasão da privacidade. *Cookies* consistem em pequenos programas que servem para coletar informações e agilizar a navegação em rede. Operam, usualmente, sem o consentimento e sem o conhecimento do usuário, podendo apresentar-se em dois tipos: os que são gravados diretamente no computador do internauta, objetivando-se facilitar um futuro acesso ao mesmo sítio cibernético; e aqueles que só servem para coletar dados do visitante, cujo destino é inevitavelmente o banco de dados do prestador de serviço da sociedade da informação. O usuário da *net* recebe um número que proporciona a identificação do computador e a conexão à rede e, a partir desse momento, são registrados pelos *cookies* o navegador utilizado, o sistema operacional, o período de conexão e as páginas acessadas, dentre outras informações. Essas informações são depois cruzadas com outros dados do internauta, tais como nome, telefone, endereço, número e fatura do cartão de crédito. Por esse motivo, muitas pessoas se surpreendem ao receber correspondência eletrônica de empresas com as quais jamais estabeleceu contato, mas que detém conhecimentos detalhados de seu perfil e de sua vida particular.

No segundo semestre de 1999, a justiça americana condenou a empresa *DoubleClick* por ameaça à privacidade em decorrência da utilização de *cookies*. Combinavam-se os perfis anônimos dos internautas – colhidos por meio dos *cookies* – com as informações pessoais retiradas de bancos de dados de *marketing* direto sem o prévio consentimento do usuário. Indiscutível, portanto, o fato de os *cookies* atuarem como meio de violação da privacidade ao propiciarem não apenas a identificação do perfil do internauta, mas também o mapeamento da navegação que o indivíduo realiza pela internet[390].

Em abril de 2003, no Canadá, colocaram-se os *cookies* novamente em evidência diante da decisão tomada pelo Comissário para a Proteção da Privacidade (*Privacy Comissioner*), em

[389] DRUMMOND, Victor. Op. cit., p. 28.
[390] GUERRA, Sidney. Op. cit, pp. 107-108.

processo administrativo aberto em decorrência de reclamação de um visitante de *site* de companhia aérea. Como fundamento, o queixoso alegou basicamente: (a) que lhe foi negado acesso ao *website* porque o seu programa de navegação (*browser*) estava configurado para desabilitar os *cookies*; e (b) que a companhia se utilizava tanto de *cookies* permanentes como de temporários para coletar informações pessoais sem o conhecimento e sem o consentimento dos visitantes do *site*. A página estruturava-se de tal forma que, uma vez desabilitados os *cookies* permanentes, ao internauta se negava acesso às páginas seguintes. Assim que tomou conhecimento da reclamação, a companhia adotou providências para reconfiguração do *site*, a fim de permitir a navegação por páginas internas, mesmo quando desativados os *cookies*. Conclui-se que a conduta da companhia aérea feriu o princípio da privacidade, que proíbe a coleta de informações pessoais sem a autorização do titular[391].

A Directiva 2002/58/CE, do Parlamento Europeu e do Conselho da Europa, dispõe que os usuários devem dispor do arbítrio de recusar a instalação de *cookies* ou de dispositivos similares em seu computador. No preâmbulo da Directiva, reconhece-se que os *cookies* – espécies de coordenadas eletrônicas – podem atuar como um instrumento legítimo e útil, nomeadamente para a oferta de produtos ou de serviços análogos por parte da mesma empresa; desde que aos usuários se forneçam informações claras e precisas acerca de sua finalidade, cabendo aos interessados a oportunidade de aceitar ou de recusar a instalação de tais dispositivos no seu computador[392]. A questão se torna mais complexa em caso de acesso de usuários diversos por meio de um mesmo computador, ou de acesso automático mediante um *click* pelo internauta que deseja ignorar as extensas e complexas regras que regulam o sítio, tal como ocorre na página da empresa *Amazon.com,* que já define como "de sua propriedade" os dados pessoais de clientes armazenados durante da transação, bastando, então, a esse usuário anuir, o que se consuma mediante um *click* com o *mouse*, para "admitir" a violação à sua privacidade[393].

---

[391] REINALDO FILHO, Demócrito. **Uso de cookies pode infringir a privacidade do internauta**: decisão do Comissário para a Proteção de Dados do Canadá. [s.l.]: [s.n.], [200-?]. Publicado no Portal Infojus. Disponível em <http://www.infojus.com.br/webnews/noticia.php?id_noticia=1717&s>. Acesso em: 30 jan. 2007.

[392] "*(41) No contexto de uma relação comercial existente, é razoável permitir a utilização de coordenadas electrónicas do contacto para a oferta de produtos ou serviços análogos, mas apenas por parte da mesma empresa que obteve os elementos da comunicação junto do cliente em conformidade com a Directiva 95/46/CE. Sempre que sejam obtidas coordenadas electrónicas do contacto, o cliente deverá ser informado de forma clara e distinta sobre a sua futura utilização para fins de comercialização directa, e deve-lhe ser dada a oportunidade de recusar essa utilização. Deverá continuar a ser-lhe dada gratuitamente essa oportunidade em todas as subseqüentes mensagens de comercialização directa, excepto no que diz respeito a eventuais custos para a transmissão dessa recusa*". In UNIÃO EUROPÉIA. **Directiva 2002/58/CE do Parlamento Europeu e do Conselho da Europa**. Op. cit.

[393] PEREIRA, Joel Timóteo Ramos. Op. cit., pp. 465-467.

Outro artefato tecnológico utilizado para violação à privacidade é o chamado *trojan* ou cavalo de tróia. *Trojan* consiste em um programa de computador normalmente recebido como um "presente" (cartão virtual, álbum de fotos, protetor de tela, jogo e outros) que, além de realizar a função para o qual foi projetado, executa atividades maliciosas sem o conhecimento do usuário, podendo causar sérios prejuízo, tais como: (a) furto de senhas e outras informações sensíveis como, por exemplo, números de cartões de crédito; (b) instalação de programas chamados *keyloggers*[394], que permitem a gravação das teclas digitadas pelo usuário do computador, como o texto de um *e-mail*, dados digitados na declaração de imposto de renda e outras informações sensíveis; (c) instalação de programas que permitem não apenas a coleta de dados pessoais, mas também a monitoração de computadores denominados *spywares*[395]; (d) alteração, destruição e cópia de documentos armazenados no computador; (e) instalação de *backdoors*[396], que oferecem ao atacante acesso a todas as informações armazenadas no computador, permitindo-lhe pleno controle dos dados ali contidos.

Em 23 de maio de 2005, a Câmara de Representantes dos EUA aprovou punições para usuários da *net* que disseminassem *spywares*. Por 395 (trezentos e noventa e cinco) votos a 1 (um), decidiu-se que aquele que recorresse a tal tipo de programa sofreria pena até dois anos de prisão e pagaria multa de até US$ 3 (três) milhões por infração, e todo usuário que recorresse a esse mesmo estratagema com a finalidade de se apossar de dados pessoais de outrem poderia ter a pena aumentada em cinco anos. Ainda para coibir os *spywares*, o Departamento de Justiça Americano aprovou uma proposta para destinar um montante de US$ 10 (dez) milhões anuais até o ano de 2009 para combater essa espécie de delito[397].

Alguns técnicos da área de informática argumentam que a informática é neutra, podendo servir-se de avançados processos técnicos para contribuir para o reforço da segurança e para a

---

[394] *Keylogger* é um programa de computador do tipo *spyware* cuja finalidade é monitorar tudo o que a vítima digita, a fim de descobrir suas senhas de banco, números de cartão de crédito e afins. In CARTILHA de Segurança para Internet. Op. cit., p. 73.

[395] *Spyware* consiste em um *software* que monitora as atividades de um sistema e envia essas informações a terceiros, normalmente sem o conhecimento e o consentimento do usuário do computador. Os *spywares* são desenvolvidos por empresas para monitorar os costumes dos internautas para fins de *marketing* e para acessar dados confidenciais dos usuários como senhas e documentos. In CARTILHA de Segurança para Internet. Op. cit., p. 70.

[396] *Backdoor* (porta dos fundos) é um trecho de código mal-intencionado que cria uma ou mais falhas de segurança para dar acesso ao sistema operacional a pessoas não autorizadas, sem que essas precisem recorrer novamente aos métodos utilizados na primeira invasão. Esta falha de segurança criada é análoga a uma porta dos fundos por onde a pessoa mal intencionada pode entrar (invadir) o sistema. In CARTILHA de Segurança para Internet. Op. cit., p. 72.

[397] MCGUIRE, David. House approuves spyware penalties. *Washington Post*. Tuesday, May 24, 2005. Disponível em <http://www.washingtonpost.com/wp-dyn/content/article/2005/05/23/AR2005052302000.html>. Acesso em 30 jan. 2007.

preservação das garantias individuais, não se configurando como uma real ameaça à privacidade. Outros vão mais além, afirmando que os riscos da internet evidenciam o preço a se pagar por todos os benefícios que se recebe em outras áreas. O primeiro argumento não procede porque, ao mesmo tempo em que a informática coloca à disposição dos usuários recursos técnicos para maior salvaguarda da privacidade, constata-se, nos últimos anos, a proliferação de aparatos tecnológicos utilizados para o incremento da vigilância. Quanto ao segundo, observa-se que a revolução tecnológica e os benefícios que oferece não podem servir de justificativa para violação desse valor essencial ao ser humano que é o direito de preservar a sua privacidade[398].

Diante desse cenário, ressalta-se a necessidade de conscientização dos internautas quanto aos riscos que a rede pode ocasionar à privacidade, para que o usuário se preocupe em se proteger dos programas maliciosos, utilizando o computador de forma mais segura, sem se sujeitar à exagerada auto-exposição proporcionada pelos novos recursos tecnológicos. Destaque-se a periculosidade dos bancos de dados *on-line* que permitem a interconexão de informações pelos prestadores de serviço da sociedade da informação; o risco de monitoramento eletrônico por meio do IP; a massificação dos *chats*, *blogs* e comunidades virtuais; a existência dos maliciosos *cookies,* que permitem a coleta de informações sobre a navegação do internauta, e a disseminação de *trojans, keyloggers, spywares* e outros programas desenvolvidos para executar ações maliciosas na internet.

3.6.1 O anonimato na internet

Após a apresentação de um panorama acerca dos riscos da internet à privacidade, impõe-se breve análise a respeito da polêmica questão do anonimato na rede. O maior pesquisador em sociologia da internet, Barry Wellman, afirma que a *web* favorece a comunicação desinibida, especialmente no que tange a minorias e a grupos sociais oprimidos, em debates de conotação política, e em outros assuntos, justamente por favorecer o anonimato. Movimentos que surgiram para defender causas femininas, direitos humanos e preservação ambiental fazem uso da *net*, como ferramenta essencial para a disseminação e para a troca de informações, diante do caráter

[398] MARQUES, Garcia; MARTINS, Lourenço. Op. cit., p 82.

aberto desse meio de comunicação[399]. Assim, a internet demonstra seu extraordinário potencial para o fortalecimento da liberdade de expressão e de comunicação.

Bruce Schneier, outro pesquisador a respeito do tema, alerta para a importância da preservação do anonimato na *web*, considerando-se o benefício que oferece a alcoólatras, a portadores de doenças graves, como a AIDS (síndrome de imunodeficiência adquirida), a psicóticos, a vítimas de crimes graves, a sobreviventes de abusos sexuais e a outros que se valem largamente desse meio de comunicação. Ressalta o mesmo autor, ainda, a relevância do anonimato *on-line* no campo político, relatando que, em 1999, habitantes do Kosovo, da Sérvia e de outras localidades, capturados na guerra dos Bálcãs, anonimamente enviaram para o restante do mundo notícias a respeito do conflito, sem se exporem ao risco de morte que a revelação da própria identidade poderia desencadear[400].

Ressalte-se a relevância da preservação do anonimato na internet, permitindo-se, dessa forma, a liberação, sem constrangimentos, de emoções aprisionadas, especialmente por pessoas discriminadas, que podem expor suas vidas sem revelar sua "real" identidade. Os tradicionais "disque-denúncias" – serviços oferecidos à população tão-somente por telefone até o advento da internet – atualmente contam com mais esse canal de comunicação, facilitando a delação anônima de vítimas e de testemunhas de crimes. O anonimato *on-line* fortalece, ainda, a liberdade de expressão e de comunicação. A manifestação pública de pensamentos, idéias, opiniões, juízos de valor e críticas (liberdade de expressão) é incrementada na *web*, em razão de esse mesmo veículo atuar como um canal que se abre para acolher a todos os grupos e a todos os movimentos sociais. De outro lado, a divulgação de acontecimentos e de notícias de interesse da sociedade (liberdade de comunicação) se enriquece também com a rápida difusão, em nível global, de fatos culturais, econômicos, políticos, científicos, ecológicos, dentre outros de interesse coletivo. Fica, inclusive, mais difícil o exercício da censura pelo Estado, tendo em vista o caráter transnacional da rede, embora o controle seja tecnicamente possível e implementado por alguns países como a China, a Coréia do Norte, o Irã, e a Arábia Saudita – países que monitoram todo o conteúdo das informações veiculadas em seus domínios. Enfim, o anonimato na internet favorece a construção de uma sociedade pluralista, base para a consolidação de um autêntico regime democrático.

[399] CASTELLS, Manuel. **A sociedade em rede**. Op. cit., pp. 446-448.
[400] SCHNEIER, Bruce. Op. cit., pp. 73-74.

Por outro lado, o anonimato *on-line* dificulta a apuração de ilícitos praticados no mundo virtual como a violação da honra e da imagem de pessoas, o dano por difusão de vírus, a pornografia infantil, o racismo, a xenofobia, o atentado à propriedade intelectual, a ameaça, o estelionato, dentre tantos outros. Além disso, facilita as comunicações entre terroristas e membros de organizações criminosas que se escondem sob o manto do sigilo oferecido pela rede. Por isso, governos de alguns países discutem a questão da preservação do anonimato na *web*, e também a regulamentação do uso de recursos criptográficos capazes de garantir o sigilo absoluto do conteúdo das comunicações telefônicas e telemáticas. Entidades responsáveis pela persecução penal dizem que o anonimato e o sigilo favorecem a impunidade; assim, defendem a aprovação de leis que prevejam: (a) procedimentos "menos burocráticos" para interceptação das comunicações telefônicas e telemáticas; (b) proibição de acesso à *web* por usuários não cadastrados; e (c) proibição de uso de "criptografia forte", ou seja, de recursos criptográficos com algoritmos[401] de melhor qualidade, capazes de impedir a "quebra" da mensagem ou da comunicação cifrada, o que torna sem efeito a interceptação pela impossibilidade de acesso ao conteúdo.

Diante desse cenário, lança-se a seguinte questão: realmente existe anonimato na internet? Bruce Schneier expõe que existem dois tipos de anonimato: o *anonimato completo*, em que a pessoa é completamente desconhecida, não havendo como obter tal identificação; e o *pseudoanonimato*, em que a pessoa pode ser conhecida por diversos meios, apesar de não ter revelado seu nome ou outra forma de "autenticação direta". O especialista em segurança sustenta que o *verdadeiro anonimato* ou *anonimato completo* não existe mais no mundo virtual, porque a infra-estrutura em rede facilita a identificação do usuário mediante números de série atribuídos às máquinas, interconexão de informações coletadas por meio de *cookies* e de dados cadastrais, e rastreamento do IP[402].

Conforme visto no item anterior, o IP armazenado nos provedores de acesso e concessionárias de serviço de comunicação destaca-se como uma das formas de se identificar um internauta. Atribui-se o referido número a cada conexão à rede, identificando-se o computador, a data, a hora exata de conexão, o tempo de navegação e o fuso horário do sistema. Existem dois

[401] A palavra *algoritmo* tem origem no sobrenome, Al-Khwarizmi do matemático persa Mohamed ben Musa que viveu no século IX. Em informática, significa conjunto de regras e procedimentos lógicos perfeitamente definidos que levam à solução de um problema em um número finito de etapas, ou seja, são os passos necessários para realizar uma tarefa. In HOUAISS, Antônio. Op. cit.
[402] SCHNEIER, Bruce. Op. cit., p. 74.

tipos de IP: o *estático*, não sujeito a alterações por um determinado período de tempo, sendo mais comum seu uso por pessoas jurídicas; e o *dinâmico*, que é aleatoriamente atribuído a cada conexão à rede, sendo mais comum sua utilização por *cybercafés*[403], *lan-houses*[404] e usuários domésticos[405]. Utiliza-se o protocolo *dinâmico* cada vez que o usuário se conecta à rede por meio de um provedor de acesso, e seu computador recebe aleatoriamente um endereço IP diferente. Durante a conexão, seu computador retém aquele IP que não pode ser atribuído a nenhum outro internauta. Quando o assinante encerra a conexão, o protocolo fica novamente disponível, podendo ser atribuído a outro usuário. Assim, quando o IP é dinâmico, este pode associar-se a diversos internautas, sendo que a identificação do usuário só é possível se o provedor de acesso registrar a data, a hora exata de conexão, o tempo de navegação e o fuso horário em que o protocolo estava sendo utilizado por determinado computador.

No ordenamento jurídico nacional, o IP e os *logs* (diários de navegação) são acobertados pelo *sigilo dos dados telemáticos*, podendo ser fornecidos pelos provedores de acesso e pelas concessionárias de serviço de comunicação apenas mediante ordem judicial e para fins de investigação criminal ou instrução processual penal, conforme regulamentação da Lei nº 9.296/96. Promovida a quebra de sigilo desses dados telemáticos, ainda se impõe a identificação do usuário do IP em uma determinada data e horário. Seja o IP estático ou dinâmico, o autor dos delitos pode ser identificado mediante perícia forense computacional e outros meios de prova. Nesse caso, diz-se que ocorre apenas um *pseudoanonimato*, uma vez que, apesar de o internauta não se identificar diretamente, poderá ser conhecido.

Há *verdadeiro anonimato* ou *anonimato completo* quando o internauta, mesmo após perícia técnica, não puder ser conhecido. Isto ocorre com maior freqüência nos seguintes casos: (a) quando o IP é dinâmico e usado por *cybercafés* e *lan-houses* que não registram os usuários das máquinas por data e horário, tornando praticamente impossível identificar o internauta responsável pelo uso do computador em que foram praticados os ilícitos; (b) quando se utiliza o método indireto de acesso à rede por meio de *servidores proxy* – também denominados sistemas de computação "substitutos" – que oculta o verdadeiro IP do internauta, redirecionando toda a

[403] *Cybercafé* é um local que, além de funcionar com bar ou lanchonete, oferece aos clientes acesso à internet mediante pagamento de um preço, normalmente cobrado por minutos ou horas de conexão.
[404] *Lan-house* é um estabelecimento comercial em que as pessoas vão para acessar a internet e participar de jogos em rede, desfrutando de computadores de última geração em um ambiente *hi-tech*.
[405] CRIMES Cibernéticos: manual prático de investigação. São Paulo: **Comitê Gestor da Internet no Brasil e Ministério Público Federal**, 2006, item 4.1.7.

sua navegação, transmissão e recepção de mensagens[406]; (c) quando se acessa a rede recorrendo-se a sistemas de transmissão sem fio (*wireless* ou *wi-fi*)[407] – muito comum em aeroportos, shoppings, hotéis e faculdades – tendo em vista a dificuldade de identificação das pessoas que transitam na área de abrangência das ondas emitidas pelo ponto de acesso em determinada data e horário[408].

Para resolver o problema da impossibilidade de identificação dos autores de delitos cibernéticos praticados em *cybercafés, lan-houses, cyber offices*[409] e congêneres, o Estado de São Paulo – SP publicou lei obrigando os estabelecimentos desse tipo lá sediados a criarem e manterem cadastro atualizado de todos os seus usuários, contendo as seguintes informações: nome completo, data de nascimento, endereço completo, telefone e número de identidade[410]. A questão ainda não foi resolvida nos outros estados e nem no plano federal. Quanto ao acesso à internet por meio de *servidores proxy* e sistemas de transmissão sem fio (*wireless* ou *wi-fi*), a dificuldade de identificação dos usuários é tanto técnica quanto jurídica, não existindo qualquer regulamentação até o presente momento no ordenamento jurídico nacional.

---

[406] CRIMES Cibernéticos. Op. cit., item 4.8.

[407] *Wireless* ou *wi-fi* é um protocolo de comunicação sem fios projetado com o objetivo de criar redes de alta velocidade capazes de transmitir dados por ondas de rádio e radiação infravermelha. Para se ter acesso à internet através de uma rede *wi-fi* (também conhecida como *wlan*) deve-se estar no raio de ação de um ponto de acesso (normalmente conhecido por *hotspot*) ou local público onde opere uma rede sem fios e usar um dispositivo móvel, como um computador portátil ou um assistente pessoal digital com capacidades de comunicação *wireless*. Essas redes ganharam grande popularidade pela mobilidade que provêem aos seus usuários e pela facilidade de instalação e de uso em ambiente domésticos e empresariais. In CARTILHA de Segurança para Internet. Op. cit., p. 49.

[408] CRIMES Cibernéticos. Op. cit., item 4.1.7.

[409] *Cyber offices* são estabelecimentos comerciais em que as pessoas podem acessar a Internet para atividades de estudo ou trabalho.

[410] "*Artigo 1º - São regidos por esta lei os estabelecimentos comerciais instalados no Estado de São Paulo que ofertam a locação de computadores e máquinas para acesso à Internet, utilização de programas e de jogos eletrônicos, abrangendo os designados como "lan houses", cibercafés e "cyber offices", entre outros. Artigo 2º - Os estabelecimentos de que trata esta lei ficam obrigados a criar e manter cadastro atualizado de seus usuários, contendo: I - nome completo; II - data de nascimento; III - endereço completo; IV - telefone; V - número de documento de identidade. § 1º - O responsável pelo estabelecimento deverá exigir dos interessados a exibição de documento de identidade, no ato de seu cadastramento e sempre que forem fazer uso de computador ou máquina. § 2º - O estabelecimento deverá registrar a hora inicial e final de cada acesso, com a identificação do usuário e do equipamento por ele utilizado. § 3º - Os estabelecimentos não permitirão o uso dos computadores ou máquinas: 1. a pessoas que não fornecerem os dados previstos neste artigo, ou o fizerem de forma incompleta; 2. a pessoas que não portarem documento de identidade, ou se negarem a exibi-lo; § 4º - As informações e o registro previstos neste artigo deverão ser mantidos por, no mínimo, 60 (sessenta) meses. § 5º - Os dados poderão ser armazenados em meio eletrônico. § 6º - O fornecimento dos dados cadastrais e demais informações de que trata este artigo só poderá ser feito mediante ordem ou autorização judicial. § 7º - Excetuada a hipótese prevista no § 6º, é vedada a divulgação dos dados cadastrais e demais informações de que trata este artigo, salvo se houver expressa autorização do usuário*". In SÃO PAULO (Estado). **Lei nº 12.228, de 11 de janeiro de 2006**. Disponível em: <http://www.legislacao.sp.gov.br/legislacao/index.htm>. Acesso em: 30 jan. 2007.

Objetivando combater os delitos cibernéticos, em novembro de 2006, apresentou-se na Comissão de Constituição e Justiça – CCJ do Senado Federal, para votação, projeto de lei que, dentre outras medidas, torna obrigatória a identificação direta do internauta pelos provedores de acesso, por meio de senha ou de outro identificador, nome completo, data de nascimento, endereço completo e outros dados. Essa regra se complementa com a obrigação de o provedor não apenas conferir o acesso tão-somente após a autenticação do usuário; mas também de armazenar, pelo prazo de três anos, os dados relacionados às conexões (*logs* ou diários de navegação). Por fim, o projeto prevê pena de dois a quatro anos de prisão e multa tanto para usuários quanto para provedores que não procederem à identificação prévia ao acesso à internet de forma direta (nome, endereço e demais dados). Aquele que se identificar mediante pseudômino ou nome de terceiro tem a pena aumentada de sexta parte. Assim, o projeto criminaliza tanto o anonimato como o uso de pseudônimos na internet, o que gerou duras críticas por parte da sociedade civil, tendo sido retirado da pauta de votação da CCJ por tempo indeterminado[411].

Conforme já exposto, a Constituição resguarda a privacidade das comunicações e também a liberdade de expressão e de comunicação, conforme dispõe os incisos IV e IX do art. 5o: "*IV - é*

---

[411] "***Art.1º*** *Esta Lei altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal), o Decreto-Lei nº 1.001, de 21 de outubro de 1969 (Código Penal Militar), a Lei nº 9.296, de 24 de julho de 1996, Decreto-Lei nº 3.689, de 3 de outubro de 1941 (Código do Processo Penal), a Lei nº 10.446, de 8 de maio de 2002, e a Lei nº 8.078, de 11 de setembro de 1990 (Código do Consumidor), para tipificar condutas realizadas mediante uso de sistema eletrônico, digital ou similares, de rede de computadores, ou que sejam praticadas contra dispositivos de comunicação ou sistemas informatizados e similares, e dá outras providências. (...)* ***Art. 3º*** *O Título I da Parte Especial do Código Penal fica acrescido do Capítulo VII-A, assim redigido: "Capítulo VII-A DA VIOLAÇÃO DE REDE DE COMPUTADORES, DISPOSITIVO DE COMUNICAÇÃO OU SISTEMA INFORMATIZADO Acesso indevido a rede de computadores, dispositivo de comunicação ou sistema informatizado* ***Art. 154-A****. Acessar indevidamente, rede de computadores, dispositivo de comunicação ou sistema informatizado: Pena – reclusão, de 2 (dois) a 4 (quatro) anos, e multa. § 1º Nas mesmas penas incorre quem, indevidamente, permite, facilita ou fornece a terceiro meio não autorizado de acesso a rede de computadores, dispositivo de comunicação ou sistema informatizado. § 2º Somente se procede mediante representação, salvo se o crime é cometido contra a União, Estado, Município, empresa concessionária de serviços públicos, agências, fundações, autarquias, empresas públicas ou sociedade de economia mista e suas subsidiárias. § 3º A pena é aumentada de sexta parte, se o agente se vale de nome suposto ou da utilização de identidade de terceiros para a prática de acesso. § 4º Nas mesmas penas incorre, o responsável pelo provedor de acesso à rede de computadores, dispositivo de comunicação ou sistema informatizado, que permite o acesso a usuário sem a devida identificação e autenticação ou que deixa de exigir, como condição de acesso, a necessária, identificação e regular cadastramento do usuário. § 5º No crime previsto no caput ou na hipótese do § 4º deste artigo, se o crime é culposo: Pena – detenção de seis meses a um ano e multa. (...)". (...)* ***Art. 20.*** *Todo aquele que acessar uma rede de computadores, local, regional, nacional ou mundial, deverá identificar-se e cadastrar-se naquele provedor que torna disponível este acesso. Parágrafo único. Os atuais usuários terão prazo de cento e vinte dias, após a entrada em vigor desta Lei, para providenciarem ou revisarem sua identificação e cadastro junto ao provedor que torna disponível o acesso*". [Substitutivo ao PLS 76/2000 que tramita em conjunto com o PLC nº 89/2003 e o PLS nº 137/2000. Para maiores informações sobre a tramitação de referido projeto de lei, consultar sítio do Senado Federal, disponível em <http://www.senado.gov.br/sf/atividade/Materia/>].

livre a manifestação do pensamento, sendo vedado o anonimato; (...) IX - é livre a expressão da atividade intelectual, artística, científica e de comunicação, independentemente de censura ou licença;". Segundo Edilsom Farias, *o princípio da vedação do anonimato – aplicável tanto à liberdade de expressão como à liberdade de comunicação – tem âmbito de aplicação bem restrito, significando apenas a ocultação maliciosa do próprio nome para fugir à responsabilidade pela divulgação de matérias que possam causar prejuízos a terceiros.* O objetivo é evitar que os autores de mensagens apócrifas permaneçam imunes quando provocarem danos à honra, à intimidade, à vida privada e à imagem de terceiros, bem como quando forem responsabilizados por condutas que violem os valores de segurança e bem-estar da sociedade. Todavia, o princípio em discussão não impõe que seja inscrito, em qualquer manifestação do pensamento, o nome de seu autor, pois tal inscrição atentaria contra a liberdade de expressão e de comunicação. *Basta que exista uma forma de se identificar a autoria quando isto for solicitado pela Justiça para investigação de crimes, sendo permitido inclusive o uso de pseudônimos de forma a ocultar a verdadeira identidade de quem se vale desse direito para exercício de atividades lícitas*[412].

Observa-se, pois, a inconstitucionalidade de referido projeto de lei, ao criminalizar de forma generalizada a não identificação dos usuários da internet e o uso de pseudônimos, já que a vedação do anonimato prevista na Magna Carta coíbe tão-somente a ocultação do próprio nome para a prática de delitos e não para o regular exercício da liberdade de expressão e de comunicação. Verifica-se, ainda, que o projeto vai de encontro à tendência dos ordenamentos jurídicos de países mais avançados em termos direito da sociedade da informação – também denominado direito da tecnologia da informação ou direito da informática –, que expressamente prevêem a preservação do anonimato na internet. Em Portugal, por exemplo, considera-se a limitação do anonimato na *web* uma violação à privacidade, sendo permitida a utilização de pseudônimos em *chats*, *blogs* e até em certificados digitais[413], desde que os prestadores de serviço mantenham um cadastro atualizado com os dados relacionados à verdadeira identidade do

[412] FARIAS, Edilsom. **Liberdade de expressão e comunicação**. Op. cit., pp. 182-185.

[413] "*O Certificado Digital funciona como uma espécie de carteira de identidade virtual que permite a identificação segura de uma mensagem ou transação em rede de computadores. O processo de certificação digital utiliza procedimentos lógicos e matemáticos bastante complexos para assegurar confidencialidade, integridade das informações e confirmação de autoria. O Certificado Digital é um documento eletrônico, assinado digitalmente por uma terceira parte confiável, que identifica uma pessoa, seja ela física ou jurídica, associando-a a uma chave pública. Um certificado digital contém os dados de seu titular como, por exemplo, nome, e-mail, CPF, chave pública, bem como o nome e a assinatura da Autoridade Certificadora que emitiu o certificado*". Disponível em <http://www.iti.br/twiki/bin/view/Certificacao/PerguntasFrequentes>. Acesso em: 30 jan. 2007.

usuário, que só podem ser revelados a terceiros com autorização judicial[414]. Tal análise é importante, pois, considerando-se o caráter transnacional da rede, chega-se à conclusão de que ainda que o projeto fosse aprovado e julgado constitucional em eventual Ação Direta de Inconstitucionalidade – ADIN, tal ato normativo ofereceria impacto de pouca expressividade em relação aos delitos cibernéticos, acarretando a mera migração de usuários responsáveis por crimes para provedores de acesso localizados em países que não imponham obrigação de prévia autenticação do internauta e proibição de uso de pseudônimos.

No âmbito da UE, em 1999, por meio de uma Recomendação, o Conselho da Europa enunciou princípios a serem observados em matéria de proteção da privacidade tanto pelos usuários quanto pelos fornecedores de serviços na internet, destacando-se o *anonimato* e a *confidencialidade das informações circuladas*. Ressaltou-se a importância desses princípios para a proteção da intimidade e da vida privada das pessoas, diante dos riscos das denominadas auto-estradas da informação, o que levou à sua qualificação como *fair privacy practice*. Enfatizou-se a necessidade de os internautas se socorrerem dos melhores dispositivos tecnológicos de criptografia disponíveis para garantir o sigilo de suas comunicações e de salvaguardarem seu anonimato, apontando-se para a preocupação que deve guiar o internauta para a manutenção da própria privacidade. Os prestadores de serviço da sociedade da informação, de outro lado, são encorajados a obedecerem aos "clássicos princípios de proteção de dados pessoais"[415] – princípios a serem descritos no item 4.5.

Em 2006, regulamentou-se, com a publicação da Directiva 2006/24/CE, do Parlamento Europeu e do Conselho da Europa, de 15 de março de 2006, a guarda de dados relacionados com a prestação de serviços de comunicação, com orientações para que tais dados estivessem disponíveis para fins de detecção e investigação de crimes graves. Nos considerandos da Directiva, destaca-se "*a necessidade de coleta e armazenamento desses dados para preservação da segurança nacional, segurança pública, defesa da ordem, prevenção de infrações criminais e proteção das liberdades de terceiros, visto que a conservação dos dados facilita as investigações e o controle do crime organizado e do terrorismo*"[416].

---

[414] PEREIRA, Joel Timóteo Ramos. Op. cit., pp. 21-22.
[415] GONÇALVES, Maria Eduarda. Op. cit., pp. 179-180.
[416] "*O PARLAMENTO EUROPEU E O CONSELHO DA UNIÃO EUROPEIA, (...) Considerando o seguinte: (...) (9) Nos termos do artigo 8.o da Convenção Europeia dos Direitos do Homem (CEDH), qualquer pessoa tem direito ao respeito da sua vida privada e da sua correspondência. As autoridades públicas só podem interferir no exercício deste direito nos termos previstos na lei e, quando essa ingerência for necessária, numa sociedade democrática,*

A Directiva obriga os Estados-membros a adotarem medidas legislativas com o objetivo de impor aos provedores de acesso e às concessionárias de serviço de comunicação o dever de registrarem e de conservarem os dados relacionados aos serviços de telefonia e conexão à internet para tornar possível a identificação de usuários responsáveis por condutas ilícitas. *São os denominados "dados de tráfego" e "dados de localização" – informações relacionadas ao serviço de comunicação que revelam quem é o usuário, com quem ele está se comunicando, quando e onde*. Segundo a Directiva 2006/24/CE, quando o serviço diz respeito à telefonia fixa ou móvel devem ser registradas as seguintes informações: número de telefone de origem da chamada; nome e endereço do usuário do serviço; número do destinatário da chamada; data e hora do início e fim da chamada; localização dos equipamentos utilizados por ambos os interlocutores durante a chamada; serviço de telefonia utilizado. Quando o serviço é de correio eletrônico ou comunicação telefônica pela internet, devem ser armazenadas as seguintes informações: código de identificação do usuário atribuído pela prestadora de serviço; nome e endereço do usuário do protocolo IP estático ou dinâmico; data e hora do início (*log-in*) e do fim (*log-off*); serviço de internet utilizado; linha de assinante ou qualquer outro identificador do terminal utilizado[417].

---

designadamente, para a segurança nacional ou para a segurança pública, a defesa da ordem e a prevenção das infracções penais, ou a protecção dos direitos e das liberdades de terceiros. Visto que a conservação de dados se tem revelado um instrumento de investigação necessário e eficaz de repressão penal em vários Estados-Membros, nomeadamente em matérias tão graves como o crime organizado e o terrorismo, é necessário assegurar que as autoridades responsáveis pela aplicação da lei possam dispor dos dados conservados por um período determinado, nas condições previstas na presente directiva. A aprovação de um instrumento de conservação de dados que obedeça aos requisitos do artigo 8.o da CEDH é, pois, uma medida necessária. (10) Em 13 de Julho de 2005, na sua Declaração condenando os ataques terroristas em Londres, o Conselho reafirmou a necessidade de aprovar o mais rapidamente possível medidas comuns relativas à conservação de dados de telecomunicações. (11) Tendo em consideração a importância dos dados de tráfego e dos dados de localização para a investigação, detecção e repressão de infracções penais, é necessário, como os trabalhos de investigação e a experiência prática em vários Estados-Membros o demonstram, garantir a nível europeu a conservação durante um determinado período dos dados gerados ou tratados, no contexto da oferta de comunicações, pelos fornecedores de serviços de comunicações electrónicas publicamente disponíveis ou de uma rede pública de comunicações, nas condições previstas na presente directiva". In UNIÃO EUROPÉIA. Directiva 2006/24/CE do Parlamento Europeu e do Conselho da Europa, de 15 de março de 2006, relativa à conservação de dados gerados ou tratados no contexto da oferta de serviços de comunicações electrónicas publicamente disponíveis ou de redes públicas de comunicações, e que altera a Directiva 2002/58/CE. **Jornal Oficial da União Européia**. Portugal, 13 abr. 2006. nº L 105, pp. 54-63.

417 "*Artigo 5.oCategorias de dados a conservar 1. Os Estados-Membros devem assegurar a conservação das categorias de dados seguintes em aplicação da presente directiva: a) Dados necessários para encontrar e identificar a fonte de uma comunicação: 1) no que diz respeito às comunicações telefónicas nas redes fixa e móvel: i) o número de telefone de origem, ii) o nome e endereço do assinante ou do utilizador registado; 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 telefónica pública, iii) o nome e o endereço do assinante ou do utilizador registado, a quem o endereço do protocolo IP, o código de identificação de utilizador, ou*

Os dados devem ser registrados e arquivados pelos prestadores de serviços de comunicação, para fins de identificação dos usuários responsáveis pela prática de ilícitos criminais, com a ressalva de serem disponibilizados tão-somente para as autoridades autorizadas, devendo ser armazenados, transmitidos e destruídos de forma segura. Verifica-se, pois, que a Directiva facilita a identificação dos internautas envolvidos em organizações criminosas e em atividades terroristas, mas não proíbe, em nenhum dispositivo, o anonimato na internet ou o uso de pseudônimos, ao contrário do projeto de lei discutido recentemente no Congresso Nacional.

Diante de todo o exposto, ressalte-se a importância da preservação do anonimato na internet, mecanismo essencial para o exercício do direito à liberdade de expressão e de comunicação e também à preservação da privacidade dos internautas. Destaque-se a necessidade de identificação apenas dos usuários responsáveis pela prática de atividades ilícitas mediante o

---

o número de telefone 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 telefónicas nas redes fixa e móvel: i) o(s) número(s) marcados (o número ou 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 registado; 13.4.2006 PT Jornal Oficial da União Europeia L 105/57 2) no que diz respeito ao correio electrónico 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 telefónica através da internet, ii) o(s) nome(s) e o(s) endereço(s) do(s) subscritor(es), ou do(s) utilizador(es) registado(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 telefónicas 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 electrónico através da internet e às comunicações telefónicas 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 registado, ii) a data e a hora do início e do fim da ligação ao serviço de correio electrónico através da internet ou de comunicações telefónicas 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 telefónicas nas redes fixa e móvel: o serviço telefónico utilizado; 2) no que diz respeito ao correio electrónico através da internet e às comunicações telefónicas 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 telefónicas na rede fixa os números de telefone de origem e de destino; 2) no que diz respeito às comunicações telefónicas 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 carácter anónimo, a data e a hora da activação inicial do serviço e o identificador da célula a partir da qual o serviço foi activado; 3) No que diz respeito ao acesso à internet, ao correio electrónico através da internet e às comunicações telefônicas através da internet: i) o número de telefone que solicita o acesso por linha telefónica, 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 directiva, não podem ser conservados quaisquer dados que revelem o conteúdo das comunicações". In UNIÃO EUROPÉIA. **Directiva 2006/24/CE do Parlamento Europeu e do Conselho da Europa**. Op. cit.

uso desse meio de comunicação, o que pode ser feito pelo rastreamento do IP e cruzamento dessa informação com os dados armazenados pelos prestadores de serviços de telefonia e conexão à internet ou outra forma de identificação do protocolo, e desde que exista prévia autorização judicial para a realização da perícia forense computacional.

3.7 Intromissão estatal na privacidade

Delineados os principais riscos à privacidade na sociedade da informação com o advento da internet, examina-se, neste item, a questão da intromissão do Estado na esfera privada dos indivíduos. Conforme já exposto, apresentam-se como formas mais comuns de intervenção estatal na intimidade a coleta de dados pessoais e a vigilância por meio dos sistemas de inteligência – tema a ser tratado no próximo item.

A coleta de informações pessoais é imprescindível ao desempenho das atividades estatais. O problema reside na quantidade e qualidade dos dados coletados, muitas vezes desproporcionais quando se compara com os fins perseguidos; e na forma de armazenamento, transmissão e interconexão dos mesmos dados entre os diferentes entes públicos. Uma vez coletados – seja para fins de censo, estatística, pagamento de tributos, investigação e combate à criminalidade ou prestação de serviços públicos – tais dados devem receber um *tratamento*[418] adequado e seguro, de forma a garantir sua integridade[419], autenticidade[420] e sigilo[421].

---

[418] Entende-se por *tratamento*, a recepção, produção, reprodução, utilização, acesso, transporte, transmissão, distribuição, armazenamento, eliminação e controle de informações.

[419] *Integridade* significa que a informação não foi modificada, inclusive quanto à origem e ao destino. Definição no ordenamento jurídico nacional: "*Art. 4º Para os efeitos deste Decreto, são estabelecidos os seguintes conceitos e definições: (...) VIII - integridade: incolumidade de dados ou informações na origem, no trânsito ou no destino*;" In BRASIL. **Decreto nº 4.553, de 27 de dezembro de 2002**. Disponível em: <http://www.planalto.gov.br/ccivil_03/decreto/2002/D4553.htm>. Acesso em: 30 jan. 2007.

[420] *Autenticidade* quer dizer que a informação foi produzida, expedida, recebida, modificada ou destruída por determinado indivíduo ou sistema. Definição no ordenamento jurídico nacional: "*Art. 4º Para os efeitos deste Decreto, são estabelecidos os seguintes conceitos e definições: I - autenticidade: asseveração de que o dado ou informação são verdadeiros e fidedignos tanto na origem quanto no destino;"* In BRASIL. **Decreto nº 4.553, de 27 de dezembro de 2002**. Op. cit.

[421] *Sigilo* significa acesso ou divulgação restritos. Definição no ordenamento jurídico nacional: "*Art. 4º Para os efeitos deste Decreto, são estabelecidos os seguintes conceitos e definições: (...) XVI - sigilo: segredo; de conhecimento restrito a pessoas credenciadas; proteção contra revelação não-autorizada; e*". In BRASIL. **Decreto nº 4.553, de 27 de dezembro de 2002**. Op. cit.

Na área denominada *segurança da informação*[422], diz-se que as informações sigilosas, dentre as quais os dados pessoais, só podem ser acessados por quem tenha *necessidade de conhecer* tais informações para o exercício de cargo, função, emprego ou atividade. Trata-se de uma norma fundamental, conhecida na doutrina norte-americana como *need to know*. Podem-se, então, identificar pelo menos três princípios que devem nortear o poder público nas atividades relacionadas à gestão de dados pessoais: da proporcionalidade da quantidade e qualidade dos dados coletados aos fins perseguidos; do acesso restrito a pessoas que tenham necessidade de conhecer; e da preservação da segurança em todas as fases do tratamento da informação. Este tema será aprofundado no capítulo 4.

Com o surgimento dos sistemas automatizados, cresceu a preocupação em relação à coleta de dados pessoais pelo Estado, tendo em vista a capacidade de interconexão das informações armazenadas em diferentes bancos de dados, o que facilita a perda de controle em relação à gestão dessas mesmas informações. Susan Gray relata que, desde 1970, mais de 80% (oitenta por cento) dos dados pessoais coletados por agências governamentais norte-americanas já se encontravam armazenados em sistemas automatizados total ou parcialmente[423]. No ano de 1982, o governo americano já dispunha de mais de 500 (quinhentos) programas para interconexão de informações de caráter pessoal[424].

O armazenamento dos dados em sistemas automatizados facilita o cruzamento de informações, permitindo ao Estado a descoberta das mais diversas modalidades de fraude, como aquelas que se comete contra a previdência e contra o fisco, o que traz grande economia aos cofres públicos. Também agiliza processos de produção de conhecimento. Uma vez interconectadas por recursos computacionais, as informações são analisadas por especialistas para elaboração de estatísticas e prospecção de cenários, o que facilita a formulação de políticas públicas mais eficientes. Conhecendo as deficiências do setor sob sua gestão, o administrador pode formular e implementar programas de melhor qualidade, produzindo reflexos positivos nas áreas social, política e econômica.

---

[422] Ver item 3.3.

[423] GRAY, Susan H. Op. cit, p. 243: *Even as long ago, from a technological standpoint, as the mid-1070s, more than 80% of the personal data records maintanined by U.S. federal agencies were either partially or fully in automated systems* (Tradução Livre).

[424] GRAY, Susan H. Op. cit., p. 249: *Marx and Reichman (...) point out that by 1982, approximately 500 computer matching programs, except for those used for reasons consistent with the purposes for which the information was originally gathered, this exception has been interpreted very broadly for government-initiated searches, particularly by the Reagan administration* (Tradução Livre).

Entretanto, o uso generalizado desse mecanismo de interconexão de informações pessoais armazenadas em diferentes bancos de dados públicos tem despertado preocupações em relação ao direito à privacidade, tendo em vista a crescente violação da autodeterminação dos indivíduos diante do constante monitoramento por parte do Estado. Steven C. Carlson e Ernest D. Miller expõe essa questão:

> Os governos têm incrementado seus sistemas de detecção de fraudes e diminuído os custos por meio de programas de cruzamento de dados. (...) A interconexão dos dados acarreta preocupações em relação ao direito à privacidade, pois o governo utiliza essas informações de modo irrestrito para monitorar e vigiar os indivíduos. A autonomia destes é violada quando seus dados são usados para propósitos diversos daqueles para os quais foram coletados. Indubitavelmente, identifica-se uma colisão entre o direito individual à privacidade e o interesse publico de que os administradores decidam de forma acertada, implementando políticas públicas eficientes.[425]

No mesmo sentido manifesta-se Hermínia Campuzano Tomé:

> Hasta hace pocos anõs podíamos decidir cómo, a quién y en qué circuntancias queríamos que nuestros datos personales fueran objeto de difusión. Aceptábamos que en determinadas ocasiones era obligado proporcionar información personal a determinados organismos públicos, pero podíamos negarnos a facilitarlos cuando consderábamos que no existia una razón justificada para ello. La realidad actual resulta bien distinta; la excesiva, incontrolada y, en algunos casos, injustificada recolección automatizada de los datos de carácter personal, asi como el mal uso que en determinadas ocasiones los organismos públicos y privados pueden hacer de ellos, origina que el individuo pueda ver totalmente cercenado su derecho a la vida privada.[426]

Além da indiscriminada coleta e interconexão de informações pessoais por sistemas informatizados, a privacidade pode ser ainda mais devassada caso aos bancos de dados se agreguem pesquisas, como a do Projeto Genoma. Destinado a mapear o código genético humano, esse projeto, de um lado, revoluciona o tratamento de diversas patologias; de outro lado, pode gerar graves danos, caso as informações sejam utilizadas para fins espúrios como, no caso de servir como meio para se promover exclusão de indivíduos do mercado de trabalho. A

---

[425] CARLSON, Steven C.; MILLER, Ernest D. Public Data and Personal Privacy. **Santa Clara Computer & High Technology Law Journal**. Santa Clara: HeinOnline, 2000, vol. 16, pp. 83-109: *Governments have improved their fraud detection systems and have generated significant cost savings through data matching programs. (...) Data matching gives rise to numerous concerns over privacy interests and substantive rights. Privacy concerns generally stem from a fear of the government having unrestricted power to employ its data in the monitoring and surveillance of individuals, and from a notion that the personal autonomy of individuals is violated when their personal data is used for purposes other than those for which the data was originally disclosed. Without a doubt, an individual's interest in informational privacy is in tension with the public interest in accurate decision making and efficient policy implementation* (Tradução Livre).

[426] CAMPUZANO TOMÉ, Hermínia. Op. cit., p. 58. Grifos nossos.

preocupação com a preservação do direito à privacidade, assim, coloca em plano menor o simples direito ao isolamento, para cumprir outra função ainda mais importante, qual seja a de reagir contra políticas de discriminação baseadas em opiniões políticas, opções religiosas e sexuais e toda sorte de informações de caráter privado, como a predisposição genética a determinadas doenças[427].

Há risco ainda em relação às potenciais cópias por terceiros, porque, uma vez que a informação integra um banco de dados, torna-se difícil identificar a organização que originariamente a coletou. Um dado coletado por uma agência governamental pode ser facilmente corrigido e atualizado na origem, mas provavelmente permanecerá inalterado em outros sistemas. Essa contradição entre cadastros afetos ao mesmo indivíduo pode comprometer direta ou indiretamente interesses pessoais desse mesmo indivíduo.

Assim, o recente dilema dos Estados democráticos e liberais é que, de um lado necessitam de cada vez mais informações detalhadas e personalizadas sobre os cidadãos para exercício de diversas atividades, como investigação de evasão tributária, diminuição e combate à criminalidade, formulação de políticas públicas, dentre tantas outras; de outro têm que impor alguns limites e controles ao uso das informações de caráter pessoal para evitar abusos e excessiva intromissão na intimidade das pessoas. A tensão entre a proteção das informações confidenciais dos cidadãos e o impulso de coletar e armazenar cada vez mais dados pessoais é permanente. O problema se evidencia na constatação de que os responsáveis pela proteção de dados pessoais encontram-se politicamente posicionados sempre de forma desvantajosa em relação aos burocratas encarregados de coletar tais informações[428].

Mesmo na UE, em que é obrigatória a instituição, pelos Estados-membros, de uma Agência de Proteção de Dados Pessoais ou designação de uma autoridade de controle por força do artigo 28 da Directiva 95/46/CE do Parlamento Europeu e do Conselho da Europa[429], há prevalência das entidades responsáveis pela coleta de dados pessoais, justamente por serem atividades mais rentáveis ao Estado, tanto em termos políticos como econômicos. Por esse motivo, a própria Directiva ressalta que essas entidades responsáveis pela proteção de dados pessoais deverão se beneficiar de total independência no exercício de suas competências, a fim de

[427] DONEDA, Danilo César Maganhoto. **Considerações iniciais sobre os bancos de dados informatizados e o direito à privacidade**. Op. cit.
[428] WHITAKER, Reg. Op. cit., pp. 158-159.
[429] UNIÃO EUROPÉIA. **Directiva 95/46/CE do Parlamento Europeu e do Conselho da Europa**. Op. cit.

garantir imparcialidade em suas decisões. Na maior parte dos países da Europa, os integrantes dessas entidades têm mandato de 2(dois) a 4(quatro) anos para evitar que sofram pressão de autoridades de outros organismos públicos. São técnicos e especialistas em segurança, membros do MP e do Judiciário.

Nesse contexto, verifica-se, de um lado, a importância da coleta e da interconexão de informações pessoais pelos governos, como forma de combater fraudes e fornecer melhores serviços aos cidadãos; de outro, a necessidade de adoção de precauções mínimas para segurança dessas informações e preservação da privacidade dos cidadãos. Reconhece-se que, para um bom funcionamento da máquina estatal, é necessário que o Estado exerça certo controle em relação aos administrados, que têm obrigação de fornecer informações pessoais aos órgãos públicos, notadamente no tange aos dados criminais, tributários, de saúde pública, e afins, mas alguns limites devem ser impostos ao poder estatal.

Recomenda-se a especificação, por meio de normas, dos dados pessoais que podem ser coletados e aqueles que são proibidos de coleta. O impasse entre o direito à privacidade e o poder estatal surge quando há tratamento de *dados sensíveis*, tais como aqueles referentes à origem racial ou étnica, às opiniões políticas, às convicções religiosas ou filosóficas, à saúde, ao código genético, à vida sexual e ao patrimônio do indivíduo. Aos titulares se deveria conceder o direito ao controle exclusivo em relação a tais informações, por revelarem aspectos relacionados a sua intimidade; permitindo-se a coleta apenas em casos excepcionais e por organismos que adotassem procedimentos rigorosos de segurança. Steven C. Carlson e Ernest D. Miller observam:

> Os governos coletam uma variedade de dados pessoais. Alguns dados como registros fiscais e médicos, por exemplo, são extremamente sensíveis, tendo sido reconhecidos há muito tempo como fonte de preocupação na preservação da privacidade dos cidadãos. Outras espécies de informação são inofensivas, desde que coletadas de forma razoável, apesar de também poderem ser consideradas invasivas quando compiladas e cruzadas de forma a criar perfis mais abrangentes dos indivíduos.[430]

Algumas questões, então, surgem em relação à intervenção estatal na privacidade dos cidadãos. A primeira delas discute se os governos podem utilizar dados pessoais para fins

[430] CARLSON, Steven C.; MILLER, Ernest D. Op. cit: *Governments collect a vast array of personal data. Some data, such as tax and medical records, are extremely sensitive and have long been recognized as sources of concern for the privacy interests of individuals. Other sources of personal information are quite innocuous when considered in discrete amounts, although they can be compiled and matched to create broader profiles of individuals that are invasive of personal privacy* (Tradução Livre).

diversos daqueles para os quais se procedeu à coleta sem a autorização de seus titulares. Se a resposta for afirmativa, indaga-se se devem existir restrições em relação ao compartilhamento de dados sensíveis entre os diversos órgãos públicos ou entre estes e entes privados.

Em regra, os cidadãos não podem negar informações ao Estado, quando essas mesmas são solicitadas para fins de recolhimento de tributos, identificação civil, vacinação, exercício de direitos eleitorais e outras atividades relacionadas ao poder de fiscalização. Uma vez coletadas, essas informações são armazenadas em bancos de dados públicos, podendo ser utilizadas para as mais diversas finalidades. O problema reside na utilização dessas informações para finalidades diversas daquelas para as quais foram coletadas sem que tenha havido autorização prévia de seus titulares. Os bancos de dados públicos provavelmente falhariam se os indivíduos tivessem oportunidade de controlar o uso das próprias informações. Além de aumentar os custos de processamento, tal procedimento contribuiria para ampliar a burocracia, desnecessária, prejudicando o bom funcionamento da máquina estatal. Mas algumas restrições devem ser estabelecidas em relação ao compartilhamento de dados sensíveis entre os diversos órgãos públicos.

No ordenamento jurídico brasileiro, a Lei dos Arquivos Públicos, ao regulamentar a parte final do inciso XXXIII do art. 5º da CF, assim determina:

> Art. 23. Decreto fixará as categorias de sigilo que deverão ser obedecidas pelos órgãos públicos na classificação dos documentos por eles produzidos.
> § 1º Os documentos cuja divulgação ponha em risco a segurança da sociedade e do Estado, bem como aqueles necessários ao resguardo da inviolabilidade da intimidade, da vida privada, da honra e da imagem das pessoas são originariamente sigilosos.
> § 2º O acesso aos documentos sigilosos referentes à segurança da sociedade e do Estado será restrito por um prazo máximo de 30 (trinta) anos, a contar da data de sua produção, podendo esse prazo ser prorrogado, por uma única vez, por igual período.
> § 3º O acesso aos documentos sigilosos referentes à honra e à imagem das pessoas será restrito por um prazo máximo de 100 (cem) anos, a contar da sua data de produção.[431]

A Lei nº 11.111, de 05 de maio de 2005, por sua vez, prevê no art. 7º que "*os documentos públicos que contenham informações relacionadas à intimidade, vida privada, honra e imagem de pessoas, e que sejam ou venham a ser de livre acesso poderão ser franqueados por meio de*

[431] BRASIL. **Lei nº 8.159, de 8 de janeiro de 1991**. Disponível em <http://www.planalto.gov.br/ccivil_03/Leis/L8159.htm >. Acesso em: 30 jan. 2007. Grifos nossos.

certidão ou cópia do documento que expurgue ou oculte a parte sobre a qual recai o disposto no inciso X do art. 5º da CF"[432].

Ainda no sentido de preservação do direito à privacidade, o Decreto nº 5.584, de 18 de novembro de 2005, *verbis*:

> Art. 1º Os documentos arquivísticos públicos produzidos e recebidos pelos extintos Conselho de Segurança Nacional - CSN, Comissão Geral de Investigações - CGI e Serviço Nacional de Informações - SNI, que estejam sob a custódia da Agência Brasileira de Inteligência - ABIN, deverão ser recolhidos ao Arquivo Nacional, até 31 de dezembro de 2005, observados os termos do § 2º do art. 7º da Lei nº 8.159, de 8 de janeiro de 1991.
> (...)
> Art. 10. Recolhidos ao Arquivo Nacional, os documentos referidos no art. 1º deverão ser disponibilizados para acesso público, resguardadas a manutenção de sigilo e a restrição ao acesso de documentos que se refiram à intimidade da vida privada de pessoas ou cujo sigilo seja imprescindível à segurança da sociedade e do Estado, nos termos do Decreto nº 4.553, de 2002.[433]

Analisada a legislação vigente, observa-se que os dados sensíveis, por se relacionarem à intimidade, à vida privada, à honra e à imagem dos indivíduos, são sempre sigilosos. Por isso qualquer espécie de tratamento que se ofereça a esses mesmos dados pelos órgãos públicos, tais como a coleta, armazenamento, alteração, recuperação, consulta, utilização e transmissão, requer a adoção de procedimentos de segurança para evitar a interceptação e posterior utilização por terceiros não autorizados. Além disso, deve ser adotado, em relação ao compartilhamento de dados sensíveis por agentes públicos, o princípio da doutrina norte-americana do *need to know* (necessidade de conhecer), previsto no ordenamento jurídico nacional no inciso XIII do art. 4º e no inciso I do art. 37 do Decreto nº 4.553/02[434]. Conforme já exposto, esse princípio determina que só pode ter conhecimento de uma informação sigilosa aquele que demonstrar a indispensabilidade dessa para o exercício de suas funções.

Em conclusão, os cidadãos têm obrigação de fornecer certas informações pessoais ao Estado, que pode utilizá-las para as mais diversas finalidades, e não apenas para aquelas

---

[432] BRASIL. **Lei nº 11.111, de 05 de maio de 2005**. Disponível em <http://www.planalto.gov.br/ccivil_03/_Ato2004-2006/2005/Lei/L11111.htm>. Acesso em: 30 jan. 2007.

[433] BRASIL. **Decreto nº 5.584, de 18 de novembro de 2005**. Disponível em <http://www.planalto.gov.br/ccivil_03/_Ato2004-2006/2005/Decreto/D5584.htm>. Acesso em: 30 jan. 2007. Grifos nossos.

[434] "*Art. 4º Para os efeitos deste Decreto, são estabelecidos os seguintes conceitos e definições: (...) XIII - necessidade de conhecer: condição pessoal, inerente ao efetivo exercício de cargo, função, emprego ou atividade, indispensável para que uma pessoa possuidora de credencial de segurança, tenha acesso a dados ou informações sigilosos; (...) Art. 37. O acesso a dados ou informações sigilosos em órgãos e entidades públicos e instituições de caráter público é admitido: I - ao agente público, no exercício de cargo, função, emprego ou atividade pública, que tenham necessidade de conhecê-los;*". In BRASIL. **Decreto nº 4.553, de 27 de dezembro de 2002**. Op. cit.

ventiladas no momento da coleta. Assim, não se aplica em relação aos órgãos públicos o direito de o titular vedar a utilização de seus dados para fins diversos daqueles para os quais foram fornecidos, ao contrário do que ocorre em relação a entidades privadas. Entretanto, essa maior liberalidade conferida ao Estado em razão do seu poder de fiscalização e controle, deve ser cotejada com a obrigação de conferir-se segurança a esses dados em todas as fases de seu tratamento, a fim de se garantir integridade, autenticidade e sigilo – os principais pilares da área denominada segurança da informação. Assim, recomenda-se a edição de ato normativo regulamentado a atividade de coleta e compartilhamento de informações pessoais entre os diferentes entes públicos, para coibir os abusos e a excessiva intromissão estatal na intimidade dos cidadãos.

3.7.1 Espionagem estatal: Echelon e outros artefatos tecnológicos

A vigilância mediante sistemas de inteligência remonta à Antiguidade, mas apenas no século XX, em razão da Guerra Fria, foi sistematizada, ganhou caráter científico, e assumiu importante papel na política nacional e internacional. A espionagem se apóia em uma aquisição sistemática de informações sensíveis, no intuito de produzir o conhecimento necessário à decisão de questões estratégicas de interesse do Estado ou de determinados grupos políticos e econômicos. Obtidas as informações – pelos mais variados meios, dentre os quais, a infiltração de agentes, o monitoramento à distância de determinados indivíduos e a interceptação de comunicações – estas são analisadas e interpretadas por pessoal qualificado, produzindo-se informes a serem enviados ao mais alto escalão. Esses informes, uma vez digitalizados e transformados em *documentos eletrônicos*[435], são classificados e protegidos por meio da adoção de medidas e procedimentos de segurança, dentre os quais, o uso da criptografia para garantir sua autenticidade, integridade e sigilo.

[435] O *documento eletrônico* se apresenta como uma seqüência de bits, elaborada mediante processamento eletrônico de dados, destinada a reproduzir um pensamento, fato ou informação. São características do documento eletrônico. a) não se prende a nenhum meio físico; b) traduzido por sistemas computacionais; c) pode ser alterado sem deixar vestígios, caso não seja assinado digitalmente através do uso da criptografia; d) assume formas diversificadas como, por exemplo, a escrita, imagem (foto), som, vídeo; e) pode ser copiado infinitas vezes, sem perder a característica de original.

Assim, à medida que vão surgindo novos meios de comunicação, a inteligência desenvolve artefatos e mecanismos mais sofisticados de interceptação, cifragem e proteção de informações. Hoje, agências de inteligência de diversos países interceptam comunicações realizadas por meio de telefone, fax, rádio, telex e até internet; o que suscita preocupações em relação ao direito à privacidade, uma vez que na maior parte dos casos sequer existe autorização judicial. Isto sem falar no uso generalizado de micro-câmeras e de minúsculos microfones que captam imagens e sons a longa distância, o que pode representar uma afronta à intimidade dos indivíduos monitorados, caso não sejam impostos limites à espionagem estatal e observado o *princípio da proporcionalidade*. Conforme exposto no item 2.8 – quando se tratou do âmbito de proteção do direito à privacidade – o uso desses novos artefatos tecnológicos viola a dignidade da pessoa humana e a privacidade, quando são levantadas informações provenientes do núcleo absolutamente protegido da vida privada, ou seja, da intimidade em sentido estrito – conhecida na doutrina alemã por *Geheimsphäre*.

Em 1890, o norte-americano Herman Hollerith inventou uma máquina eletromecânica que lia uma série de dados perfurados em cartões. A máquina organizava, catalogava, distribuía e armazenava todos os dados desejados, a partir da efetivação de furos em cartões em que restavam preestabelecidas as informações coletadas. Diante da engenhosidade do sistema – que permitia identificar um indivíduo, dentre milhões, por meio das perfurações operadas nos cartões – a invenção recebeu por parte de Edwin Black a definição de *código de barras do século XIX para seres humanos*. O sistema Hollerith foi utilizado pelo governo dos EUA no censo de 1890, resultando no barateamento da operação, na maior rapidez dos resultados e em um arquivo com multiplicidade de informações sobre os americanos. Alguns anos depois foi introduzido na Rússia, pelo czar Nicolau II, que armazenou diversas informações a respeito de 120 (cento e vinte) milhões de pessoas. Posteriormente, foi incrementado e utilizado pelo III Reich, na Alemanha, para identificação do povo alemão e dos judeus que precisavam ser eliminados[436].

Comprovada a eficácia da espionagem pela adoção de procedimentos estatísticos; em 1946, o governo norte-americano criou mais um sistema de controle dos cidadãos a partir do cruzamento de informações. O sistema foi batizado de ENIAC (*Electronic Numerical Integrator and Computer* ou Computador e Integrador Numérico Eletrônico). Tratava-se de um computador eletrônico que trabalhava com lógica digital, efetuando 3.500 (três mil e quinhentas)

[436] PIZZOLANTE, Francisco Eduardo Orcioli Pires e Albuquerque. Op. cit., p. 55-57.

multiplicações por segundo, sendo denominado, pelos tecnólogos da época, *o grande cérebro eletrônico*[437].

Mas o grande marco tecnológico da espionagem estatal só ocorreu em meados dos anos 70, no auge da Guerra Fria, quando os EUA e a Inglaterra implementaram o denominado Projeto *Echelon,* com a finalidade de interceptar comunicações militares e diplomáticas da ex-URSS. Após o fim da Guerra, o sistema passou a ser utilizado para espionagem econômica e política, sendo controlado pelas agências de inteligência *National Security Agency* – NSA – americana e pela *Government Communications Headquarters* – GCHQ – britânica.

Ao longo dos anos, outros países aderiram ao projeto, que atualmente conta com a participação de Nova Zelândia, Austrália e Canadá, além dos EUA e Inglaterra. São interceptadas informações relacionadas à área econômica e de desenvolvimento científico e tecnológico, a fim de favorecer grupos e empresas dos países participantes em detrimento de empresas e Estados estrangeiros. O Brasil, cite-se, foi alvo da espionagem concorrencial norte-americana em 1994, quando tentava contratar uma empresa para implementar o projeto Sistema de Vigilância da Amazônia – SIVAM. O *Echelon* foi utilizado para possibilitar a interceptação de comunicações entre funcionários públicos brasileiros e servidores da empresa francesa Thourson. Com fundamento nessas provas, o governo dos EUA ofereceu queixa de corrupção ao governo do Brasil, que acabou contratando uma empresa americana denominada Raytheon; ao final, coube a essa empresa um lucro de US$1,4 bilhões (um bilhão e quatrocentos milhões) de dólares[438].

Outro caso famoso foi o da empresa norte-americana McDonnell-Douglas, que ganhou do consórcio europeu Airbus uma concorrência para a compra de aviões pela Arábia Saudita, faturando 6(seis) bilhões de dólares. Essa transação despertou o interesse do Parlamento Europeu pelo Projeto, que acabou instituindo uma comissão temporária para investigá-lo. Ao final da investigação, concluiu-se que os EUA utilizavam recursos de espionagem contra empresas que participavam de concorrências internacionais – designadas pelo governo norte-americano de "concorrências injustas em países amigos"[439].

Hoje, o *Echelon* tem capacidade global de vigilância, interceptando mais de 3 (três) bilhões de comunicações diariamente, incluindo ligações telefônicas, mensagens de *e-mail*,

[437] PIZZOLANTE, Francisco Eduardo Orcioli Pires e Albuquerque. Op. cit., p. 58.
[438] LEONARDI, Marcel. Vigilância tecnológica, bancos de dados, internet e privacidade. **Jus Navigandi**, Teresina, ano 9, n. 499, 18 nov. 2004. Disponível em <http://jus2.uol.com.br /doutrina/texto.asp?id=5899>. Acesso em: 30 jan. 2007.
[439] PIZZOLANTE, Francisco Eduardo Orcioli Pires e Albuquerque. Op. cit., p. 163-164.

downloads da internet, transmissões por satélite e assim por diante. As comunicações que despertam mais atenção são justamente aquelas que se escondem sob mensagens criptografadas, pois a simples indicação de que as partes não desejam ser gravadas já seria suficiente para se levantar um alarme a respeito da importância do conteúdo. Para tal, recorre-se a um conjunto de antenas, grampos em cabos submarinos e programas de busca na rede[440].

Atualmente, o Projeto conta com mais de 120 (cento e vinte) satélites espiões e 11 (onze) estações terrestres de satélites, bem como com diversas estações de comunicações por cabos submarinos e outros meios de comunicações terrestres. A sua concepção se materializa em estações dispostas por todo o planeta para interceptar o máximo possível de comunicações por satélite, microondas, redes celulares e fibra óptica, mediante utilização de um sistema de busca por palavras-chave; a seguir, as informações captadas são processadas por poderosos computadores, que dispõem de programas de reconhecimento de voz (*voice recognition*), de reconhecimento óptico de caracteres (*optical caracther recognition*), de busca de textos cifrados e de decifração; por fim, as informações captadas são analisadas por funcionários da NSA e da GCHQ[441].

Em 1999, o *Echelon* veio a conhecimento público, sendo criticado por governos de diversos países e por grupos ativistas do direito à privacidade como a EFF[442]. Promoveram-se campanhas contra o Projeto, estimulando que os simpatizantes incluíssem em suas mensagens as palavras-chave mais buscadas pelo sistema, a fim de travar os *softwares* utilizados. Apesar das duras críticas, o *Echelon* continua em funcionamento sob a justificativa de ser um instrumento importante de combate ao terrorismo, ao narcotráfico e ao crime organizado.

Além da potencial violação à privacidade, o *Echelon* apresenta duas características preocupantes: a primeira, a capacidade global de vigilância mediante interceptação sistemática e aleatória de quaisquer comunicações; segundo, a afronta ao *princípio da livre concorrência*, favorecendo grupos econômicos e políticos dos Estados da chamada "Comunidade UKUSA" (EUA, Inglaterra, Nova Zelândia, Austrália e Canadá). Diante desse cenário, em 05 de junho de 2000, o Parlamento Europeu constituiu uma comissão temporária para estudar o caso *Echelon.*

[440] SCHNEIER, Bruce. Op. cit., p. 47.
[441] CORREIA, Miguel Pupo. Op. cit., p. 326-327.
[442] Mais informações disponíveis no sítio <http://www.eff.org>. Acesso em: 30 jan. 2007.

Em 11 de junho de 2001, essa comissão apresentou seu relatório, tendo sido aprovado em sessão do dia 05 de setembro de 2001[443].

Marcel Leonardi traz trechos do relatório elaborado pela comissão do Parlamento Europeu, designada para estudar a compatibilidade do Projeto *Echelon* com o ordenamento jurídico da União Européia, especialmente com relação ao direito fundamental de respeito à vida privada e familiar, previsto no art. 8º da Convenção Européia dos Direitos do Homem:

> No atinente à questão da compatibilidade de um sistema do tipo *Echelon* com o direito da UE, impõe-se estabelecer a seguinte diferenciação: se o sistema for apenas utilizado para fins de informação, não se observa qualquer contradição com o direito da EU (...) Se, pelo contrário, o sistema é objeto de utilização abusiva para espionar a concorrência, é o mesmo contrário à obrigação de lealdade que vincula os Estados-membros e à concepção de um mercado comum em que a concorrência é livre. Se um Estado-membro nele participa, viola, assim a legislação da União. (...) Todas as operações de interceptação de comunicações constituem uma grave ingerência na vida privada da pessoa humana. O art. 8º da Convenção dos Direitos do Homem, que protege a vida privada, apenas permite uma tal ingerência quando esteja em causa garantir a segurança nacional, disposições essas que sejam de acesso geral e estabeleçam em que circunstâncias e condições os poderes públicos a ela podem recorrer. Tais ingerências devem ser proporcionadas, razão pela qual se impõe ponderar os interesses em jogo. Não é suficiente que a intervenção seja meramente oportuna e desejável. Um sistema de comunicações que, aleatória e sistematicamente, interceptasse todas e quaisquer comunicações, infringiria o princípio da proporcionalidade e seria, por conseguinte, contrário à Convenção dos Direitos do Homem. (...) A conformidade com os direitos fundamentais de uma actividade legalmente legitimada de serviços de informações exige, além disso, a existência de suficientes mecanismos de controlo, a fim de equilibrar os riscos inerentes à ação secreta levada a efeito por uma parte do aparelho administrativo.[444]

Observa-se, portanto, que o Projeto *Echelon* – com o pretexto de resguardar a segurança nacional e combater o terrorismo e o crime organizado – tem sido utilizado para defesa de interesses escusos, ao afrontar, à luz dos aspectos político e econômico, os *princípios da livre concorrência e da lealdade,* favorecendo determinadas empresas e grupos dos países financiadores em detrimento de empresas e países estrangeiros; nos aspectos jurídico e social, viola a *privacidade*, tendo em vista a interceptação generalizada e aleatória das comunicações em escala global, ultrapassando as fronteiras de jurisdição e os limites impostos pelo *princípio da proporcionalidade* – princípio basilar exigido na resolução da colisão entre dois valores constitucionais; no caso o direito à privacidade e a segurança pública.

---

[443] CORREIA, Miguel Pupo. Op. cit., p. 328-329.

[444] Relatório do Parlamento Europeu, pp. 139-140, disponível no endereço <http://www.europarl.eu.int> apud LEONARDI, Marcel, Op. cit. Grifos nossos.

Nos Estados Unidos da América, além do Projeto *Echelon,* implementou-se igualmente, no início do ano 2000, o programa *Carnivore,* do *Federal Bureau of Investigation* – FBI[445]. Em julho do mesmo ano, o *Eletronic Privacy Information Center* – EPIC formulou um pedido de informações sobre o *Carnivore*[446]. Diante do indeferimento do pedido, o EPIC ajuizou uma ação judicial para obrigar o FBI a revelar as informações solicitadas quando, então, o sistema se abriu ao conhecimento público.

Trata-se de um sistema de *software* e *hardware* instalado nos computadores dos provedores de acesso à internet, com a finalidade de interceptar, em tempo real, as comunicações via cabo. O FBI grampeia *e-mails*, ligações telefônicas e navegações na *web* realizadas por pessoas suspeitas de atividades ilícitas. O procedimento é menos intrusivo do que o *Echelon*, porque se exige prévia autorização judicial, bem como demonstração da inexistência de outros meios capazes de atender às necessidades da investigação, ou seja, requer-se a observância do *princípio da proporcionalidade* e seus subprincípios (adequação, necessidade e proporcionalidade em sentido estrito). Além disso, todas as informações coletadas pelo sistema são gravadas em formato ininteligível ao usuário comum, ou seja, são criptografadas; sendo permitido o acesso apenas pelos agentes do FBI que detém o conhecimento da chave criptográfica necessária à decifração da informação.

Apesar de o *Carnivore* apresentar-se como um excelente recurso à disposição das autoridades policiais quando utilizado corretamente, o sistema foi criticado pelos próprios provedores de acesso à internet norte-americanos que começaram a perder clientes, já que usuários da rede, localizados em domínios não abrangidos pela jurisdição dos Estados Unidos, estavam sendo interceptados de forma ilegítima. Quando se configura o sistema adequadamente, apenas se registra o tráfego que esteja de acordo com os filtros autorizados pelo juiz. Mas isso não impede que investigadores mal-intencionados mudem o fluxo dos filtros para interceptar terceiros em relação aos quais não se obteve autorização judicial.

Diante dos abusos cometidos por alguns investigadores e das intensas críticas ao sistema, em janeiro de 2005 noticiou-se que o FBI não recorreria mais à utilização do programa *Carnivore.* Aos poucos o denominado *Magic Lantern* substitui o programa anterior. Esse, muito mais avançado, não requer a instalação física de filtros via provedor de acesso, sendo introduzido

[445] Mais informações disponíveis no sítio <http://www.fbi.gov/>. Acesso em: 30 jan. 2007.
[446] Mais informações disponíveis no sítio <http://www.epic.org/>. Acesso em: 30 jan. 2007.

no computador do investigado, via internet, e de forma imperceptível. O *software* (*keylogger*) registra inclusive a seqüência de teclas digitadas pelo usuário no computador, podendo, desta forma, obter senhas passíveis de utilização para leitura e acesso a documentos sigilosos criptografados.

Outro programa utilizado para espionagem pelos EUA desde 2003 é *Matrix*, conforme relata Pedro Doria:

> Desde 2003, o governo norte-americano mantém em funcionamento o *Matrix*, um grande aglomerado de bancos de dados que lhe permite encontrar possíveis terroristas. Tem dados médicos, informação sobre motoristas, antecedentes criminais, relatórios de uso de cartões de crédito. E não só de norte-americanos. Segundo o Epic, Centro de Informação sobre Privacidade Eletrônica, uma das empresas responsáveis pelo *Matrix*, a *ChoicePoint*, tem cadastros de todos os empresários brasileiros, além de uma lista telefônica completa que inclui os números não listados daqui. Parece pouco, mas é só o início. Estão todos no mercado para adquirir os bancos de dados que estiverem à venda. Não demora muito para que qualquer agente de imigração nos EUA tenha acesso a mais dados sobre um cidadão brasileiro – ou mexicano, ou argentino, ou saudita – do que seus governos de origem.[447]

Todavia, a novidade mais recente apresenta-se sob a denominação *TIASystems* (*Total Information Awareness Systems*). O objetivo do sistema consiste em prever os movimentos de todos os potenciais terroristas e prevenir possíveis ações. Representa o mais ambicioso sistema de vigilância já imaginado do mundo, e, para bem cumprir seus objetivos, exibe alcance – a exemplo do *Echelon* – que ignora jurisdição. Sua capacidade de armazenamento de informações é da ordem de *petabytes,* que equivale a 1024 (mil e vinte e quatro) *terabytes* ou um quatrilhão de bytes. Segundo a *DARPA (Defense Advanced Research Projects Agency)*[448], o funcionamento segue um encadeamento lógico que se processa na seguinte seqüência: detectar, classificar, identificar, rastrear, compreender e prevenir. Integrando arquiteturas de tecnologia da informação, os agentes federais norte-americanos pretendem colher toda e qualquer informação proveniente de transações financeiras, viagens, educação, serviços médicos e veterinários, transportes, entrada de estrangeiros no país, comunicações, eventos, movimentação geográfica, hospedagem, uso de recursos de comunicação e internet, e cruzar esses dados com modelos de comportamento preestabelecidos, com o fito de encontrar "pessoas com tendências para a prática

[447] DORIA, Pedro. Era uma vez a privacidade. **No Mínimo Ibest**, Rio de Janeiro, nov. 2005. Disponível em: <http://nominimo.ibest.com.br/notitia/servlet/newstorm.notitia.presentation.NavigationServlet?publicationCode=1&pageCode=54&textCode=19591&date=currentDate&contentType=html>. Acesso em: 30 jan. 2007.

[448] Mais informações sobre a DARPA (Agência de Pesquisas em Projetos Avançados de Defesa) podem ser encontradas no sítio <http://www.darpa.mil/>. Acesso em: 30 jan. 2007.

de atividades ilícitas". O sistema trabalha formulando hipóteses e propondo teorias. O objetivo do programa é alcançar, em 5 (cinco) anos, "*a reinvenção total das tecnologias de armazenamento e acesso de informação*"[449].

Apesar de os EUA se destacarem como os grandes precursores da espionagem estatal por meio de recursos tecnológicos; as agências de inteligência dos países da UE também adotam esse mecanismo de controle e vigilância. Por volta de 1995, foi criado o programa *Enfopol* ou *Enforcement Police* com objetivo de padronizar os procedimentos adotados pelas polícias dos diversos países de interceptação de dados e comunicações por telefone, fax e internet. O programa também não é reconhecido pelas autoridades européias.

Diante desse cenário, ressalte-se o crescimento vertiginoso da espionagem estatal em meio eletrônico, em detrimento da preservação da privacidade dos indivíduos sob alegação da necessidade de se combater a criminalidade e de se preservar da segurança pública, conforme expõe Stephen A. Oxman:

> De um lado, os Estados membros precisam ter capacidade de garantir a segurança nacional e conduzir as investigações criminais de forma eficiente, e a exigência de obter autorização do titular dos dados para o processamento dessas informações poderia obstar estes esforços. De outro lado, autoridades locais e nacionais com poderes infinitos de restrição ao direito à privacidade, em qualquer hipótese, podem levar a uma situação de vigilância em que os cidadãos fiquem desprotegidos contra as intromissões do governo em suas esferas privadas.[450]

Ainda que justificável a restrição ao direito à privacidade para combate aos mais diversos tipos de condutas ilícitas, destaque-se que tal restrição não pode anular completamente o exercício desse direito fundamental, permitindo-se apenas a compressão de seu âmbito de proteção na exata medida, necessária à preservação do interesse contraposto, em observância ao já mencionado *princípio da proporcionalidade*. Outro problema consiste na prática generalizada de monitoramento e de interceptação das comunicações sem a prévia autorização judicial e

---

[449] PEIXOTO, Rodney de Castro. Vigilância sem fronteiras: tempos difíceis para as liberdades civis. **Revista Consultor Jurídico**, [s.l]: [s.n.], 1 set. 2002. Disponível em <http://conjur.estadao. com.br/static/text/10636,1>. Acesso em: 30 jan. 2007.

[450] OXMAN, Stephen A. Exemptions to the European Union Personal Data Privacy Directive: will they swallow the directive? **Boston College International & Comparative Law Review**, vol. 24, 2000-2001, pp.191-203: *On the one hand, the Member States must be able to protect national security and conduct criminal investigations in an efficient manner, and the need to obtain the subject's consent for all processing of personal data could hinder these efforts. On the other hand, national and local authorities with license to infinitely restrict privacy rights in any case that they choose could lead to a Big Brother situation in which citizens are defenseless against government intrusions into their personal spheres* (Tradução Livre).

delimitação dos indivíduos a serem investigados, adotando-se a premissa de que qualquer pessoa deve ser considerada um suspeito.

Conforme já exposto, no ordenamento jurídico nacional exige-se autorização judicial prévia a qualquer interceptação telefônica, informática ou telemática, em cumprimento ao disposto na Lei nº 9.296/96, devendo o procedimento correr em segredo de Justiça. A Lei veda a interceptação quando não houver indícios razoáveis de autoria ou de participação em infração penal, ou quando a prova puder ser feita por outros meios disponíveis, consagrando-se, portanto, a exigência do *fumus boni juris*. Concede-se autorização judicial apenas nos casos em que o crime é punido com pena de reclusão e a diligência conduzida por autoridade policial, com a ciência do MP. Após o término dos procedimentos, a prova ainda é submetida ao contraditório e à ampla defesa, caso já exista processo criminal em curso[451].

A Lei nº 9.034, de 03 de maio de 1995, ao regular os procedimentos investigatórios que versem sobre ilícitos decorrentes de ações praticadas por quadrilha ou bando ou organizações ou associações criminosas de qualquer tipo, autoriza o acesso a dados, documentos e informações fiscais, bancárias, eleitorais e financeiras; a captação e a interceptação ambiental de sinais eletromagnéticos, óticos ou acústicos, e o registro e a análise, mediante autorização judicial circunstanciada.

Contata-se, portanto, a previsão, no ordenamento jurídico nacional, da interceptação de comunicações por telefone, fax e internet, além da interceptação ambiental de sinais eletromagnéticos, óticos ou acústicos, quando se tratar de crime organizado. O procedimento deve ser conduzido por autoridade policial, sob acompanhamento do MP, e nos estritos limites da lei. *Mas como defender o cidadão comum das interceptações promovidas por outros países ou por agentes de inteligência nacionais?*

Muitos países, sob influência dos EUA, regularam a espionagem em meio eletrônico, permitindo a interceptação das comunicações não só por agentes policiais, mas também por *agentes de inteligência*. Como forma de complementar o controle, proibiram o uso de qualquer tecnologia que dificulte o acesso ao conteúdo das comunicações interceptadas como, a denominada "criptografia forte"[452]. Dado o caráter intrusivo deste tipo de investigação, permite-se tal monitoramento eletrônico do indivíduo tão-somente após autorização judicial, e quando o

[451] MORAIS, Alexandre de. **Direito constitucional**. Op. cit., pp. 86-87.
[452] Ver item 3.6.1.

órgão solicitante – seja a polícia, seja uma agência de inteligência – demonstrar que tal meio representa o único possível para a obtenção da prova. Ainda perseguindo a meta de conter abusos, existe a previsão da possibilidade de fiscalização do monitoramento eletrônico por comissões especiais após a concessão da autorização judicial, visto que o Judiciário não dispõe de um corpo técnico capacitado para avaliar se o mandato está sendo fielmente cumprido. No Brasil, não se estabelece regulamentação semelhante, o que dificulta ainda mais a garantia da preservação da privacidade em meio eletrônico.

Pelo exposto, percebe-se que o próprio Estado representa uma ameaça à privacidade dos cidadãos. Utilizando alta tecnologia, agências de inteligência interceptam mensagens transmitidas por telefone, fax, rádio, telex e até internet. Os países mais desenvolvidos, como Estados Unidos e Inglaterra, além de monitorarem os próprios cidadãos, ainda interceptam mensagem de indivíduos e empresas onde quer que se encontrem, em todo o mundo. Justificam o procedimento alegando necessidade de combate à corrupção, ao terrorismo, ao tráfico de entorpecentes e à lavagem de dinheiro, mas o que se observa é a tentativa de ampliar o já desmesurado poderio econômico daqueles países, que livremente coletam informações privilegiadas sobre transações comerciais e negociações políticas de todos os povos.

CAPÍTULO 4 PROTEÇÃO DE DADOS PESSOAIS NA SOCIEDADE DA INFORMAÇÃO

4.1 Considerações iniciais

Traçada a conformação do direito fundamental à privacidade, e analisados os principais riscos de invasão à intimidade e à vida privada diante dos novos recursos da tecnologia da informação, passa-se a investigar a questão da proteção de dados pessoais na sociedade da informação. Explica-se primeiramente o problema relacionado com o tratamento de dados pessoais, apresentando-se o conceito e as espécies de dados pessoais. A seguir, expõe-se o panorama internacional da proteção de dados pessoais e a legislação nacional relacionada ao tema. Ao final, relacionam-se os princípios reconhecidos pela doutrina referentes à proteção de dados pessoais, com uma proposição para a regulamentação de tal proteção no ordenamento jurídico nacional.

Dado representa uma informação em sua dimensão mais reduzida[453]. Pode dispor de valor intrínseco ou não: no primeiro caso, mesmo de forma isolada, transmite uma mensagem; no segundo caso, impõe-se a condição de agrupar-se com outros dados para se atingir tal fim. A informação pode apresentar-se como numérica, gráfica, fotográfica, acústica, enfim, de qualquer tipo, importa que represente um dado, que já tem significado por si só, ou um conjunto de dados reunidos.

Dado pessoal é o dado relacionado a um indivíduo identificado ou identificável, independentemente do suporte em que se encontre registrado (escrita, imagem, som ou vídeo). Entende-se por identificado, o indivíduo que já é conhecido; e por identificável, a pessoa que pode ser conhecida diretamente pelo próprio possuidor de seus dados, ou indiretamente através de recursos e meios à disposição de terceiros[454]. Um exemplo de dado pessoal é o IP atribuído a um determinado computador quando este se conecta à rede. Apesar de essa informação não conduzir à identificação direta do internauta, tal identificação poderá ser conhecida a partir da

[453] Na computação e na teoria da informação, diz-se que o bit é a menor unidade da informação. Um bit tem um único valor: 0 (zero) ou 1 (um); verdadeiro ou falso; e nesse contexto, quaisquer dos dois valores mutuamente exclusivos.
[454] CASTRO, Catarina Sarmento. Op. cit., pp. 70-71.

interconexão do IP com outros dados armazenados pelo provedor de acesso à internet, *cybercafé, lan-house, cyber office* ou estabelecimento congênere.

Assim, a identificação pode ser feita diretamente pelo próprio possuidor dos dados ou indiretamente por meio de terceiros. Entretanto, para não se resvalar ao absurdo de se classificar aleatoriamente qualquer informação relacionada com alguém como dado pessoal – o que implicaria a necessidade de adoção de procedimentos e de medidas especiais de proteção – *devem-se considerar identificáveis apenas as pessoas físicas e jurídicas que possam ser conhecidas direta ou indiretamente, sem que seja necessário o dispêndio de tempo, custo ou esforço exagerado*[455].

Para melhor compreensão da temática exposta, exponham-se alguns conceitos presentes no art. 2º da Directiva Européia 95/46/CE, de 24 de outubro de 1995:

> *Dados pessoais*, qualquer informação relativa a uma pessoa singular identificado ou identificável (pessoa em causa); é considerado identificável todo aquele que possa ser identificado, directa ou indirectamente, nomeadamente por referência a um número de identificação ou a um ou mais elementos específicos da sua identidade física, fisiológica, psíquica, econômica, cultural ou social;
> *Tratamento de dados pessoais*, qualquer operação ou conjunto de operações efectuadas sobre dados pessoais, com ou sem meios automatizados, tais como a recolha, registro, organização, conservação, adaptação ou alteração, recuperação, consulta, utilização, comunicação por transmissão, difusão ou qualquer forma de colocação à disposição, com comparação ou interconexão, bem como o bloqueio, apagamento ou destruição;
> *Ficheiro de dados pessoais*, qualquer conjunto estruturado de dados pessoais, acessível segundo critérios determinados, quer seja centralizado, descentralizado ou repartido de modo funcional ou geográfico;
> (...)
> *Consentimento da pessoa em causa*, qualquer manifestação de vontade, livre, específica e informada, pela qual a pessoa em causa aceita que dados pessoais que lhe dizem respeito sejam objecto de tratamento[456].

Observa-se que, na sociedade da informação, as pessoas cada vez mais se encontram sujeitas aos bancos de dados controlados por potentes *softwares* de cruzamento e busca de informações. Desde o nascimento, o indivíduo já tem inseridos os respectivos dados pessoais em arquivos informatizados da Secretaria de Registro Civil. Ao longo dos anos, passa a integrar também os arquivos da Secretaria de Segurança Pública, do Conselho Nacional de Trânsito, da Receita Federal, dos conselhos profissionais e outros. Isto sem mencionar os registros de estabelecimentos médicos, de instituições financeiras, de estabelecimentos de ensino, de

[455] GONÇALVES, Maria Eduarda. Op. cit., p. 89.
[456] UNIÃO EUROPÉIA. **Directiva 95/46/CE do Parlamento Europeu e do Conselho da Europa**. Op. cit.

associações, de lojas, de bibliotecas e de tantos outros estabelecimentos. Essas informações, uma vez coletadas, são armazenadas em bancos de dados ligados em rede, o que permite a interconexão dos arquivos e a definição do perfil de seus titulares, medida que se consuma em alta velocidade, com baixo custo e com pequena margem de erro. Neste caso, até os dados mais irrelevantes passam a ter importância. José Afonso da Silva comenta, com propriedade: "*O perigo é tão maior quanto mais a utilização da informática facilita a interconexão de fichários com a possibilidade de formar grandes bancos de dados que desvendem a vida dos indivíduos, sem sua autorização e até sem seu conhecimento*"[457].

A prática de se traçar o perfil de um indivíduo mediante coleta e interconexão dos respectivos dados pessoais armazenados em diferentes bancos de dados já se disseminou tanto no setor privado – para fins de *marketing* e publicidade – como no setor público – para fiscalização, monitoramento e controle. Essa iniciativa se materializa na política adotada pelo governo norte-americano após o atentado terrorista pelo grupo islâmico al-Qaeda, em de 11 de setembro de 2001. Atualmente, qualquer passageiro de vôo destinado aos EUA obriga-se a responder a uma série de perguntas para a companhia aérea – independentemente se americano ou não – perguntas que oscilam de identificação de raça até a refeição a ser servida durante o vôo. Aparentemente tais respostas são irrelevantes, entretanto, uma vez cruzadas com outros dados coletados pela polícia de imigração e pelas agências de inteligência americanas, tem-se revelada a identidade e a personalidade do passageiro.

Assim, antes mesmo que um passageiro entre em uma aeronave, as autoridades dos EUA já tomaram conhecimento a respeito de minuciosos dados a seu respeito, incluindo nome, sobrenome, idade, endereço, número do passaporte e do cartão de crédito, rendimentos mensais, preferências alimentares indicativas da religião do passageiro, viagens precedentes, nomes das organizações das quais a pessoa faz parte, tempo de permanência em cada país nas viagens anteriores, nome dos familiares e amigos mais íntimos, e outros tantos. Essas informações são armazenadas em um dispositivo de filtragem batizado de *Computer Assisted Passenger Pre-screening* (Sistema Assistido por Computador para Controle Preventivo), que analisa as informações e classifica o indivíduo em diferentes níveis de periculosidade: verde para inofensivos; amarelo para casos duvidosos; e vermelho para aqueles que devem ser impedidos de

[457] SILVA, José Afonso da. **Curso de direito constitucional positivo**. 15ª ed. São Paulo: Malheiros, 1998, p. 213.

entrar no avião. Tal prática revela a sensibilidade da atividade de coleta, armazenamento e interconexão de dados pessoais no mundo contemporâneo.

Além de facilitar a definição do perfil dos titulares dos dados pessoais interconectados e a conseqüente classificação dessas pessoas em diferentes categorias – afrontando-se não apenas a prerrogativa da intimidade e da vida privada, mas especialmente o direito à autodeterminação que é próprio a cada cidadão – os bancos de dados manipulados por entes públicos e privados traz ainda outra agravante: o fato de ao titular das informações muitas vezes não ser conferido conhecimento de tal existência. Não lhe sendo permitido acesso aos dados que constam a seu respeito, o cidadão perde a oportunidade de solicitar correção de tais informações, caso não sejam verdadeiras; ou a devida atualização, caso estejam defasadas. Essas informações podem, então, ser utilizadas indevidamente e afetar os interesses particulares do titular dos dados. Ser considerado inadimplente e não conseguir crédito na praça, não obter atendimento médico e nem ter direito a um plano de saúde, ser rejeitado em uma vaga de emprego sem justificativa aparente ilustram apenas alguns problemas que dados incorretos, desatualizados ou propositadamente errados podem causar.

Mesmo que as informações sejam corretas, ainda assim haverá dano, caso os dados sejam divulgados ou acessados indevidamente por terceiros mal intencionados. É recomendável, portanto, que o titular seja informado de que seus dados estão sendo coletados e armazenados em banco de dados, em relação aos quais se permitirá a esse mesmo titular acesso para conhecimento, correção e atualização. Caso os dados sejam transmitidos para terceiros ou utilizados para finalidades diversas daquelas para as quais foram coletados, o interessado deverá ser novamente informado. Em todas as hipóteses, deverá ser garantido ao titular dos dados pessoais o exercício do *direito de oposição* – faculdade de negar o tratamento de seus dados pessoais – bem como do *direito à identidade correta* – a identidade do titular dos dados não pode ser afetada por informações inexatas, incompletas ou desatualizadas[458]. Este tema será detalhado no item 4.5.

Concluindo, são pessoais os dados que dizem respeito a determinado indivíduo identificado ou identificável, seja a identificação direta ou indireta. Independentemente de passarem ou não uma mensagem e estarem ou não diretamente afetos ao sujeito, devem ser protegidos mediante adoção de medidas e procedimentos especiais de segurança. Isto porque,

[458] SAMPAIO, José Adércio. Op. cit., p. 520.

com o incremento da tecnologia da informação, podem ser facilmente cruzados e relacionados por potentes *softwares*, que permitem traçar o perfil dos indivíduos, o que caracteriza uma violação de sua intimidade e vida privada, além da afronta à sua autodeterminação, caso essa pessoas sejam posteriormente classificadas em diferentes categorias pelo sistema informático. Além da invasão à privacidade, o tratamento de dados pessoais ainda pode causar graves danos a seus titulares, caso estes não tenham sequer conhecimento da existência dos bancos de dados, o que inviabiliza a correção de dados incorretos, incompletos e defasados e o exercício do direito de oposição.

4.2 Espécies de dados pessoais

Os dados pessoais podem ser classificados em três espécies: *não sensíveis*; *sensíveis*; e *de tratamento proibido*. Os *dados não sensíveis* pertencem ao primeiro círculo da teoria alemã das esferas (*Sphärentheorie*), correspondendo à esfera privada de seu titular, denominada *Privatsphäre* pelos alemães ou *Sphere of Privacy* pelos norte-americanos. Os *dados sensíveis* pertencem ao segundo círculo denominado *Intimsphäre*, abrangendo os valores atinentes ao âmbito da intimidade ou esfera confidencial, cujo acesso é mais restrito. Os *de tratamento proibido* pertencem à esfera do segredo – *Geheimsphäre* na teoria alemã – abrangendo as manifestações espirituais da pessoa características da vida íntima *strictu sensu*.

Os *dados não sensíveis* podem ser coletados e armazenados sem prévio e expresso consentimento de seu titular ou representante, exemplificando-se pelo nome, sobrenome, sexo, estado civil e outros. Os *dados sensíveis* – por se referirem a aspectos mais íntimos do indivíduo como, por exemplo, à origem racial ou étnica, às opiniões políticas, às convicções religiosas ou filosóficas, à filiação sindical, à saúde e à vida sexual do indivíduo – necessitam da prévia e expressa permissão do titular ou de seu representante para serem tratados; exceto se houver autorização legal, quando será dispensável essa manifestação. Considera-se atividade de risco qualquer espécie de *tratamento* de dados sensíveis – recepção, produção, reprodução, utilização, acesso, transporte, transmissão, distribuição, armazenamento e eliminação – o que implica em

responsabilização objetiva pela divulgação ou acesso indevidos[459]. Por fim, os *dados de tratamento proibido* merecem total e absoluta proteção, devendo existir vedação legal de seu tratamento, por se referirem a aspectos relacionados à dignidade humana de seu titular.

Ressalte-se que, mesmo os *dados não sensíveis* podem necessitar de proteção – garantindo-se sua integridade, autenticidade e confidencialidade [460] – uma vez que, ao serem confrontados com outros dados, podem revelar aspectos que o titular gostaria de manter em sigilo, por afrontarem diretamente seu direito à privacidade. Ainda que certos dados pessoais não deixem transparecer mensagem significativa, quando analisados isoladamente, devem ser submetidos a procedimentos e medidas especiais de proteção, pois, uma vez agrupados, permitem a definição do perfil de seu titular. Daí falar-se que são dados pessoais não apenas aqueles relacionados a uma pessoa identificada, citem-se, nome, endereço, telefone, número de identidade, *e-mail* e filiação; mas também aqueles referentes a uma pessoa identificável mediante associações e cruzamentos como o que ocorre em casos de identificação por DNA, impressão digital e registros médicos.

Hoje, com o avanço da engenharia genética, discutem-se meios que garantam a preservação do sigilo de dados concernentes ao patrimônio genético das pessoas, bem como a disponibilidade dessas informações ao próprio titular, familiares, pessoas mais próximas, organismos públicos e privados. Ao se diagnosticar que um determinado paciente tem propensão para contrair uma doença, questiona-se se ao médico cumpriria o dever de alertar o paciente a respeito do problema, mesmo que o indivíduo se encontrasse sadio no momento em que tal comunicado lhe fosse transmitido. Ao tomar conhecimento de ser portador de gene com predisposição para determinada anomalia, deveria um indivíduo dar ciência desse problema para seu/sua companheiro(a) e descendentes? Dados genéticos coletados por determinado órgão público, a exemplo da polícia ou instituto de pesquisa, poderiam chegar ao conhecimento de outras entidades públicas e privadas? São questões enfrentadas pela área conhecida como bioética[461] e também pelo direito.

---

[459] SANTOS, Antonio Jeová. Op. cit., p. 194.

[460] Os conceitos de integridade, autenticidade e confidencialidade estão descritos no item 3.3.

[461] Bioética é o estudo dos problemas e implicações morais despertados pelas pesquisas científicas em biologia e medicina. A bioética abrange questões como a utilização de seres vivos em experimentos, a legitimidade moral do aborto ou da eutanásia, as implicações profundas da pesquisa e da prática no campo da genética etc. Considera, portanto, a responsabilidade moral de cientistas em suas pesquisas, bem como de suas aplicações. In HOUAISS, Antônio. Op. cit.

Na França, o grupo religioso da Igreja de Jesus Cristo dos Santos do Último Dia (Igreja dos Mórmons) foi objeto de indagação pela CNIL (*Commission Nationale de l'Informatique et des Libertés*)[462] quanto ao compartilhamento dos dados genéticos dos fiéis com o Instituto Americano de Saúde para fins do Projeto Genoma Humano. Esses dados são de extrema importância para o tratamento precoce de doenças graves e para a medicina preventiva; mas, de outro lado, podem conduzir aos horrores da eugenia. Algo semelhante se pode comentar acerca da relevância desses dados para a segurança pública e luta contra o crime, na medida em que proporcionam a fiel identificação de autores de ilícitos penais; mas devem ser protegidos para que não sejam utilizados para finalidades escusas[463].

Hermínia Campuzano Tomé alerta para a gravidade do compartilhamento de dados genéticos, mesmo com o prévio e expresso consentimento do titular, uma vez que o acesso a essas informações afetaria não apenas aquele indivíduo de *per si*, mas todos os membros dessa mesma família. Isso sem falar na possibilidade de essas informações serem utilizadas para fins escusos, como ocorreria em casos de seleção de indivíduos a partir de seu patrimônio genético por seguradoras de saúde ou por outras entidades públicas e privadas. Nas palavras da autora:

> El problema surge cuando el tratamiento de tal información excede de los fines propios para los cuales ha si recolectada, y es utilizada con una finalidad diferente, pudiendo operarse situaciones de verdadera intrusión en la vida privada. En este sentido, una de las actividades que más viene preocupando em los últimos anõs, com consecuencia de los abusos que conlleva y la consiguiente reducción del derecho a la vida privada, es la distribución de información personal para fines de marketing publicitario. La recogida de datos y de información personal acerca de los usuarios, realizada para fines publicitarios o de marketing directo, se ha convertido en un negocio de grandes dimensiones para muchas empresas. (...) En la misma línea, debe ser destacada la grave intromisión que para la vida privada supone la recolección de determinados datos personales relativos a la salud, a los fines de selección de compañías de seguro, de contratación laboral, incluso de identificación policial. Cada vez con más frecuencia resulta práctica extendida, por las compañias de seguros y por determinadas empresas, el solicitar resultados de tests de ADN para eliminar o seleccionar clientes susceptibles de realizar reclamaciones por enfermedades graves, o bien para seleccionar a sus empleados. (...) La información genética permite obtener información tanto de la persona como también de sua familia al

[462] *Commission Nationale de l'Informatique et des Libertés* (CNIL) é a autoridade francesa de controle e de proteção de dados pessoais, criada pela "*Loi n° 78-17 du 6 janvier 1978*" a partir da determinação do artigo 28 da Directiva 95/46/CE do Parlamento Europeu e do Conselho da Europa. Atua a partir da emissão de recomendações, atos normativos e autorização de tratamento de dados pessoais. Para maiores informações acessar o sítio <http://www.cnil.fr/>. Acesso em: 30 jan. 2007.

[463] MARQUES, Garcia; MARTINS, Lourenço. Op. cit., pp. 117-123.

> completo. De esta forma, persona que jamás han dado ningún consentimiento podrán ser afectadas por decisiones a las cuales ellas no conocel el origem.[464]

Considerando-se que os dados genéticos denunciam a filiação do indivíduo, sua predisposição para desenvolver certas doenças, a presença de determinadas características físicas e psicológicas, enfim toda uma gama de informações circunscrita à intimidade ou à esfera confidencial da pessoa (*Intimsphäre*), devem tais informações ser classificadas como *dados sensíveis*. Diante do grave potencial ofensivo do compartilhamento dessas informações – ainda que com o consentimento de seu titular ou representante, tendo em vista pertencerem não apenas ao indivíduo, mas também a toda à família – adotem-se medidas e procedimentos especiais de proteção para tal tratamento. Recomenda-se que se permita coleta e armazenamento desses dados apenas para fins de medicina preventiva, diagnóstico médico, ou fins legais, como ocorre em casos de reconhecimento de paternidade ou de identificação de autores de crimes graves. Enfim, devem ser traçados limites e procedimentos especiais para o tratamento de dados genéticos.

Diante do exposto, conclui-se que os dados pessoais devem ser classificados em três categorias: não sensíveis, sensíveis e de tratamento proibido. Independentemente da espécie em que se enquadre, todo e qualquer dado pessoal deve ser protegido, e a ele assegurada a prerrogativa da integridade, da autenticidade e do sigilo. Em relação aos dados sensíveis – como os dados genéticos, informações relacionadas com a saúde do indivíduo, filiação partidária ou sindical, convicções religiosas ou filosóficas, vida sexual – é importante verificar, ainda, a pertinência da disponibilidade dessas informações para consulta e outras espécies de tratamento, considerando-se que esses dados podem ser utilizados tanto para a defesa de interesses do próprio titular como para sua discriminação ou outras formas de violação de sua dignidade. Quanto, aos dados de tratamento proibido, ressalte-se a necessidade de regulamentação da vedação de seu tratamento, a fim de se evitarem os abusos cometidos por entes públicos e privados que coletam de forma desarrazoada dados relacionados ao aspecto mais íntimo do indivíduo, ou seja, de sua vida íntima *strictu sensu*.

[464] CAMPUZANO TOMÉ, Hermínia. Op. cit., pp. 59-61. Grifos nossos.

4.3 Panorama internacional da proteção de dados pessoais

Considerando-se que as ocorrências de violação ao direito à *privacidade informacional*[465] se instalaram em conseqüência do tratamento automatizado de dados pessoais, detectou-se inicialmente o problema em países que dispunham de um nível de desenvolvimento tecnológico mais avançado, e apenas recentemente tais manifestações se expandiram para países em desenvolvimento, como Chile, Brasil e Argentina. Nesse contexto, destaque-se a experiência internacional referente ao tema, especialmente dos Estados-membros da UE e dos EUA, medida que contribuirá significativamente em posterior análise do ordenamento jurídico nacional.

A *primeira geração* de leis sobre proteção de dados pessoais surgiu na década de 60 (sessenta). Fundava-se no princípio de que poucos e gigantescos centros computacionais controlavam os dados, dominando o armazenamento de informações pessoais; portanto, a ofensa necessariamente partiria dessas grandes empresas. Assim, a tutela da privacidade se restringia à autorização de funcionamento desses grandes centros por um órgão governamental[466].

Diante dos avanços da informática e da redução dos custos de aquisição de computadores, criaram-se novos centros, o que evidenciou a ineficácia dessas leis de *primeira geração*, já que não havia mais grandes centros a serem controlados de forma rígida pelos governos, e sim múltiplos centros de diferentes portes e ampla capilaridade. Além disso, com o aumento da capacidade de processamento dos computadores, esses grandes centros deixaram de controlar todas as informações, que passaram a ser intercambiadas entre os pequenos centros por meio das redes, fazendo surgir, na década de 70 (setenta), a *segunda geração* de leis sobre proteção de dados pessoais. Nestas, o mecanismo de autorização se apresenta diluído e substituído, em muitos casos, por uma mera notificação da sua existência ao órgão governamental[467].

Com a massificação da internet, o risco de violação da privacidade por meio do tratamento de dados pessoais intensificou-se significativamente diante possibilidade de transmissão e de cruzamento dessas informações entre diferentes bancos de dados *on-line*. Além disso, a mera notificação a um órgão governamental realizada pelos centros de diferentes portes –

---

[465] Ver item 1.2.
[466] DONEDA, Danilo César Maganhoto. **Considerações iniciais sobre os bancos de dados informatizados e o direito à privacidade**. Op. cit.
[467] DONEDA, Danilo César Maganhoto. **Considerações iniciais sobre os bancos de dados informatizados e o direito à privacidade**. Op. cit.

característica da *segunda geração* de leis – mostrou-se ineficaz, tendo em vista a ausência de controle dos mecanismos utilizados por esses estabelecimentos para garantia da integridade, da integridade e do sigilo dos dados pessoais submetidos a diferentes espécies de tratamento. Surge, então, a *terceira geração* de leis para regulamentar tanto os princípios relacionados ao tratamento de dados pessoais como também as medidas e os procedimentos de segurança a serem adotados pelos responsáveis durante a coleta e posterior armazenamento dessas informações.

José Adércio Sampaio expõe a evolução das leis de proteção de dados pessoais na Europa:

> De acordo com a evolução legislativa, as leis são classificadas como de primeira, de segunda e de terceira geração. As primeiras (...) apresentavam as seguintes características: a) tratava-se de uma legislação garantista, situada na linha histórica das declarações de direitos; b) pretensamente ampla, única e uniforme para todas as situações; c) cujo instrumento jurídico principal se firmava na autorização, no suposto de se ser possível controlar todos os sistemas tecnológicos de coleta e processamento de dados, a partir de uma necessária autorização prévia para seu funcionamento, acompanhada de um controle a posteriori por parte do institucional; d) de aplicação restrita às pessoas físicas. (...) A experiência decorrente da aplicação dessas leis terminou por demonstrar que o tratamento maniqueísta e pretensamente definitivo e completo, dispensado ao problema, deixou muito a desejar. De uma forma geral os bancos de dados não se mostraram tão demoníacos (...) ensejando a introdução de novas técnicas e modificado conteúdo nas legislações editadas na segunda metade dos anos 70. Com efeito, pode-se registrar: a) essas leis apresentavam (...) maior grau de definição dos institutos, com o estabelecimento de princípios de boas práticas informáticas (...); b) procuravam simplificar os procedimentos exigidos para instalação e operação desses centros (...); c) algumas delas incluíam em seu manto protetor as pessoas jurídicas Na linha evolutiva, vêm a seguir as leis de terceira geração, marcadas pela ampla reflexão crítica sobre a adequação dos modelos e dos instrumentos de tutela até então adotados.[468]

No ano de 1967 foi constituído, no âmbito do Conselho da Europa, uma Comissão Consultiva para estudar os impactos da tecnologia da informação ao direito à privacidade. Alguns anos depois, em 1974, o Comitê de Ministros do Conselho da Europa editou uma resolução para recomendar a todos os países europeus a adoção de precauções contra o abuso e mau emprego da informática diante da proliferação dos bancos de dados, tanto no setor público como no setor privado. Em 1976, o Comitê de Ministros do Conselho da Europa editou nova resolução versando sobre os fluxos internacionais de dados pessoais e a proteção das liberdades individuais[469].

Em nível interno de cada país, essas resoluções foram precedidas por duas leis: a *Lei do Estado alemão de Hesse de 1970*, que regulava os bancos de dados governamentais e instituía a

[468] SAMPAIO, José Adércio. Op. cit., pp. 490-491.
[469] CAMPUZANO TOMÉ, Hermínia. Op. cit., p. 78.

figura do comissário – pessoa responsável pela garantia da segurança dos arquivos estaduais, bem como pela assessoria preventiva relativamente ao impacto da tecnologia sobre os direitos fundamentais; e a *Lei Sueca de 1973*, conhecida como *Datalegen*[470].

Destaca-se também a *Lei Francesa nº 78-17, de 1978*[471], que criou a CNIL, e, por ser bem detalhada, acabou servindo como fonte de inspiração para outros países, especialmente no que concerne aos seguintes princípios: (a) *dever de lealdade na coleta de dados*, sancionando a coleta de dados pessoais de modo fraudulento e ilícito; (b) *respeito à finalidade declarada*, estabelecendo que os dados só poderiam ser utilizados para aquelas finalidades para os quais foram recolhidos, sancionando-se o uso de dados pessoais para fins diversos; (c) *dever de informação às pessoas*, obrigando que fossem prestadas informações aos titulares dos dados coletados a fim de permitir sua retificação; e (d) *dever de proteção de dados sensíveis*, protegendo os dados referentes à origem racial, opiniões políticas, filosóficas ou religiosas, preferências sexuais e outros ligados à intimidade das pessoas.

No âmbito da Organização para a Cooperação e Desenvolvimento Econômico – OCDE o tema *privacidade informacional*[472] vem sendo discutido desde 1977, quando se criou um grupo *ad hoc* de peritos encarregados de elaborar as diretrizes relativas às regras fundamentais sobre os fluxos internacionais de dados pessoais e a proteção das liberdades individuais. Em 23 de setembro de 1980, o Conselho de Ministros da OCDE aprovou o trabalho do grupo consolidado na "Recomendação das Linhas Diretrizes Regulamentadoras da Protecção da Vida Privada e dos Fluxos de Dados Pessoais". Essa Recomendação, apesar de não se apresentar com caráter vinculativo, trazia oito princípios basilares que deveriam nortear a atividade de tratamento de dados pessoais: *princípio da limitação em matéria de coleta*; *princípio da qualidade dos dados*; *princípio da especificação das finalidades*; *princípio da limitação da utilização*; *princípio das garantias de segurança*; *princípio da transparência*; *princípio da participação individual*; e *princípio da responsabilidade*[473]. Tais princípios serão detalhados no item 4.5.

---

[470] SAMPAIO, José Adércio. Op. cit., pp. 480-481.

[471] Esta lei foi modificada pela Lei n. 2004-801, de 6 de agosto de 2004, relativa à proteção das pessoas físicas quanto ao processamento de dados pessoais. A nova lei foi editada em razão da necessidade de transposição, para o direito interno francês, de disposições da Directiva 95/46/CE relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais. In REINALDO FILHO, Demócrito. A imagem de um indivíduo é dado pessoal: a decisão da autoridade francesa de proteção de dados e suas conseqüências. **Revista de Derecho Informático**. [s.l.]: Alfa-Redi, n. 85, ago. 2005. Disponível em <http://www.alfa-redi.org/rdi-articulo.shtml?x=1603>. Acesso: em 30 jan. 2007.

[472] Ver item 1.2.

[473] MARQUES, Garcia; MARTINS, Lourenço. Op. cit., pp. 144-146.

Entretanto, o grande marco normativo dentro da abordagem européia foi a *Convenção 108*, aprovada pelo Conselho da Europa, em Estraburgo, sendo denominada "Convenção para Proteção das Pessoas relativamente ao Tratamento Automatizado de Dados de Caráter Pessoal". O referido documento, baseado na *Lei Francesa de 1978* e na *Recomendação da OCDE de 1980,* foi preparado entre 1976 e 1980, tendo sido aberto à assinatura em 28 de janeiro de 1981, e entrado em vigor em 1º de outubro de 1985. O objetivo era garantir a toda pessoa, de qualquer nacionalidade ou residência, o respeito aos direitos e liberdades fundamentais, especialmente ao direito à privacidade diante do tratamento automatizado de dados de caráter pessoal. Para isso, estabelecia um nível mínimo de proteção aos dados pessoais automatizados; não impedindo, todavia, aos Estados signatários, ascenderem tal proteção para níveis mais elevados. Da mesma forma que a *Lei Francesa de 1978* e a *Recomendação da OCDE de 1980*, também previa princípios basilares para tratamento de dados pessoais[474].

Além de conferir ampla proteção aos titulares de dados pessoais sujeitos ao tratamento automatizado, a *Convenção 108* representou um grande avanço em termos regulatórios, ao permitir que países não europeus também fossem signatários, conforme se observa nos seguintes dispositivos:

> Preâmbulo. Os Estados membros do Conselho da Europa, signatários da presente Convenção: (...) Considerando desejável alargar a protecção dos direitos e das liberdades fundamentais de todas as pessoas, nomeadamente o direito ao respeito pela vida privada, tendo em consideração o fluxo crescente, através das fronteiras, de dados de carácter pessoal susceptíveis de tratamento automatizado; Reafirmando ao mesmo tempo o seu empenhamento a favor da liberdade de informação sem limite de fronteiras; Reconhecendo a necessidade de conciliar os valores fundamentais do respeito pela vida privada e da livre circulação de informação entre os povos, acordaram o seguinte:
> (...)
> Artigo 1º - Objectivos e finalidades. A presente Convenção destina-se a garantir, no território de cada Parte, a todas as pessoas singulares, seja qual for a sua nacionalidade ou residência, o respeito pelos seus direitos e liberdades fundamentais, e especialmente pelo seu direito à vida privada, face ao tratamento automatizado dos dados de carácter pessoal que lhes digam respeito («protecção dos dados»).
> (...)
> Artigo 12º - Fluxos transfronteiras de dados de carácter pessoal e direito interno. 1- As disposições que se seguem aplicam-se à transmissão através das fronteiras nacionais, qualquer que seja o suporte utilizado, de dados de carácter pessoal objecto de tratamento automatizado ou recolhidos a fim de serem submetidos a um tal tratamento.
> (...)

[474] MARQUES, Garcia; MARTINS, Lourenço. Op. cit., pp. 151-154.

> Artigo 23º - Adesão de Estados não membros. 1- Após a entrada em vigor da presente Convenção, o Comité de Ministros do Conselho da Europa poderá convidar qualquer Estado não membro do Conselho da Europa a aderir à presente Convenção mediante decisão tomada pela maioria prevista na alínea d) do artigo 20º do Estatuto do Conselho da Europa e por unanimidade dos representantes dos Estados contratantes com direito de assento no Comité.[475]

Em que pese o grande avanço proporcionado pela *Convenção 108*, até o início da década de 90 (noventa) constatava-se ratificação apenas por alguns Estados-membros da UE, o que dificultava a harmonização legislativa necessária à livre circulação de dados no mercado interno europeu. Além disso, pelo caráter *non self-executing* de que se revestia, dependia de freqüentes remissões aos direitos nacionais, o que também sinalizava como obstáculo para tal aplicação, considerando-se que nem todos os países signatários dispunham de legislação específica a respeito da matéria[476]. Para resolver esse problema, foi aprovada, em 24 de outubro de 1995, a *Directiva 95/46/CE,* do Parlamento Europeu e do Conselho da Europa. A Directiva aprimorou o texto da Recomendação da OCDE de 1980 e da Convenção 108 – que se apresentavam desatualizados por não terem considerado o advento da internet e a proliferação dos bancos de dados *on-line*. Entretanto, os objetivos principais da edição da Directiva, além da atualização tecnológica, centravam-se na harmonização de toda a legislação vigente na Europa sobre proteção de dados pessoais, a fim de facilitar o fluxo internacional dessas informações no mercado interno, e reforçar as medidas e procedimentos de segurança durante o tratamento dos dados pessoais, especialmente no que concerne aos serviços de telecomunicações e de correio eletrônico[477].

---

[475] CONSELHO DA EUROPA. **Convenção nº 108 para a proteção das pessoas relativamente ao tratamento automatizado de dados de caráter pessoal**. Estrasburgo. 28 de janeiro de 1981. Disponível em <http://www.apdt.org/guia/L/Ldados/108.htm>. Acesso em: 30 jan. 2007. Grifos nossos.

[476] MARQUES, Garcia; MARTINS, Lourenço. Op. cit., p. 262.

[477] "(*8) Considerando que, para eliminar os obstáculos à circulação de dados pessoais, o nível de protecção dos direitos e liberdades das pessoas no que diz respeito ao tratamento destes dados deve ser equivalente em todos os Estados-membros; que a realização deste objectivo, fundamental para o mercado interno, não pode ser assegurada unicamente pelos Estados-membros, tendo especialmente em conta a dimensão das divergências que se verificam actualmente a nível das legislações nacionais aplicáveis na matéria e a necessidade do coordenar as legislações dos Estados-membros para assegurar que a circulação transfronteiras de dados pessoais seja regulada de forma coerente e em conformidade com o objectivo do mercado interno nos termos do artigo 7º A do Tratado; que é portanto necessária uma acção comunitária com vista à aproximação das legislações; (9) Considerando que, devido à protecção equivalente resultante da aproximação das legislações nacionais, os Estados-membros deixarão de poder levantar obstáculos à livre circulação entre si de dados pessoais por razões de protecção dos direitos e liberdades das pessoas, nomeadamente do direito à vida privada; que é deixada aos Estadas-membros uma margem de manobra que, no contexto da aplicação da directiva, poderá ser utilizada pelos parceiros económicos e sociais; que os Estados-membros poderão, pois, especificar na sua legislação nacional as condições gerais de licitude do tratamento de dados; que, ao fazê-lo, os Estados-membros se esforçarão por melhorar a protecção actualmente assegurada na*

A falta de homogeneidade da legislação européia sobre proteção de dados pessoais causou prejuízos, especialmente ao comércio eletrônico e às instituições financeiras, pela diversidade de regulamentações sobre procedimentos para processamento e para transmissão dessas informações, o que se tentou resolver com a publicação da *Directiva 95/46/CE*, conforme expõe Stephen A. Oxman:

> Quando a Directiva foi editada, alguns países europeus, como a Alemanha, já tinham regulamentado o processamento dos dados pessoais. A divergência entre as diversas regulamentações, contudo, criou potenciais obstáculos para a transferência de dados pessoais entre os países membros. O objetivo da Directiva, desta forma, foi criar um rol comunitário de direitos ligados à privacidade para remover tais obstáculos e harmonizar a transferência de dados entre os países da Comunidade Européia.[478]

Todavia, ao contrário da Convenção 108, que permitia a adesão de países além-fronteiras da Europa, a Directiva 95/46/CE limitou seus efeitos circunscrevendo-os ao território em referência apenas. Objetivando maior efetividade, os Estados-membros da UE obrigaram-se a promover sua transposição para o respectivo ordenamento jurídico nacional, respeitando um prazo máximo de três anos, conforme o disposto no item 1 do art. 32º [479]. Atualmente, Portugal, Itália, Áustria, França, Grécia, Alemanha, Irlanda, Luxemburgo, Suíça e Inglaterra, dentre outros, possuem legislação específica sobre proteção de dados pessoais – aplicáveis tanto no âmbito

---

respectiva legislação nacional; que, nos limites dessa margem de manobra e em conformidade com o direito comunitário, poderão verficar-se disparidades na aplicação da directiva, o que poderá reflectir-se na circulação de dados quer no interior de um Estado-membro, quer na Comunidade; (...)(46) Considerando que a protecção dos direitos e liberdades das pessoas em causa relativamente ao tratamento de dados pessoais exige que sejam tomadas medidas técnicas e organizacionais adequadas tanto aquando da concepção do sistema de tratamento como da realização do próprio tratamento, a fim de manter em especial a segurança e impedir assim qualquer tratamento não autorizado; que compete aos Estados-membros zelar por que os responsáveis pelo tratamento respeitem estas medidas; que estas medidas devem assegurar um nível de segurança adequado, atendendo aos conhecimentos técnicos disponíveis e ao custo da sua aplicação em função dos riscos que o tratamento implica e a natureza dos dados a proteger; (47) Considerando que, quando uma mensagem que contém dados pessoais é transmitida através de um serviço de telecomunicações ou de correio electrónico cujo único objectivo é a transmissão de mensagens deste tipo, será a pessoa de quem emana a mensagem, e não quem propõe o serviço de transmissão, que será em regra considerada responsável pelo tratamento dos dados pessoais contidos na mensagem; que, contudo, as pessoas que propõesm esses serviços serão em regra consideradas responsáveis pelo tratamento dos dados pessoais suplementares necessários ao funcionamento do serviço;" In UNIÃO EUROPÉIA. **Directiva 95/46/CE do Parlamento Europeu e do Conselho da Europa**. Op. cit.

[478] OXMAN, Stephen A. Op. cit.: *At the time the Directive was passed, some individual European countries such as Germany, already had passed their own legislation regulating the processing of personal data. Disparities among these various regulations, however, created potential obstacles to the free flow of personal data among Member States. The purpose of the Directive, therefore, was to create EU-wide privacy rights that would remove those obstacles and harmonize the transfer of personal data within the EU* (Tradução Livre).

[479] "*Artigo 32º 1. Os Estados-membros porão em vigor as disposições legislativas, regulamentares e administrativas necessárias para dar cumprimento à presente directiva o mais tardar três anos a contar da data da sua adopção*" In UNIÃO EUROPÉIA. **Directiva 95/46/CE do Parlamento Europeu e do Conselho da Europa**. Op. cit.

público como no privado. Na Itália, a Directiva foi transposta pela Lei nº 675, de 31 de dezembro de 1996, que tutela dados pessoais, inclusive nos meios eletrônicos e automatizados. Em Portugal, a Directiva foi incorporada no ordenamento jurídico pela Lei nº 67, de 26 de outubro de 1998, conhecida por Lei de Proteção de Dados Pessoais[480].

Em cumprimento ao disposto na Directiva 95/46/CE, as leis nacionais dos países da Europa apresentam dispositivos comuns no que se refere a princípios relacionados à proteção de dados pessoais; todavia, são variáveis em relação a outros aspectos. Alguns países, dentre os quais, Portugal, Espanha, Bélgica e Suécia, aplicam dispositivos legais de proteção de dados pessoais indistintamente a qualquer entidade, seja esta pública ou privada; outros, tais como Alemanha, França, Países Baixos, Áustria, Finlândia e Itália isentam serviços de comunicação da obrigação de cumprimento de diversas normas[481]. Quanto aos beneficiários, algumas leis são aplicáveis apenas às pessoas físicas, como a da Suécia, da Grã-Bretanha, da Espanha e da França; outras se estendem às pessoas jurídicas como a da Noruega, da Dinamarca, da Áustria e de Luxemburgo. Quanto ao objeto de proteção, verifica-se que algumas legislações regulam apenas os registros automatizados de dados, conforme se constata em leis que vigoram na Suécia, na Grã-Bretanha, em Luxemburgo e na Áustria; enquanto a maioria prevê a proteção não apenas em relação a essa automatização, mas também em relação aos registros manuais, mecanográficos, de imagens e de sons[482].

Na UE, a questão da proteção de dados pessoais encontra-se em fase tão avançada que, após a incorporação da Directiva 95/46/CE ao ordenamento jurídico dos diversos Estados-membros, iniciou-se o *controle pela via administrativa*. Hoje, todos os países da Europa dispõem de uma agência, de uma comissão ou, pelo menos, de um departamento, nos respectivos governos, responsável pela proteção de dados pessoais e pela fiscalização da aplicabilidade da Directiva, em conformidade ao disposto no art. 28 do mesmo ato normativo[483], apesar de serem variáveis suas atribuições de país para país.

---

[480] VASCONCELOS, Pedro Pais de. Proteção de dados pessoais e direito à privacidade. In: ASCENSÃO, José de Oliveira (Org.). **Direito da sociedade da informação**. Coimbra: Coimbra Ed., 1999, vol. I, pp. 241-243.
[481] CAMPUZANO TOMÉ, Hermínia. Op. cit., p. 101.
[482] SAMPAIO, José Adércio. Op. cit., pp. 520-521.
[483] "*Artigo 28º Autoridade de controlo* 1. Cada Estado-membro estabelecerá que uma ou mais autoridades públicas serão responsáveis pela fiscalização da aplicação no seu território das disposições adoptadas pelos Estados-membros nos termos da presente directiva. Essas autoridades exercerão com total independência as funções que lhes forem atribuídas. 2. Cada Estado-membro estabelecerá que as autoridades de controlo serão consultadas quando da elaboração de medidas regulamentares ou administrativas relativas à protecção dos direitos e liberdades das pessoas no que diz respeito ao tratamento de dados pessoais. 3. Cada autoridade de controlo disporá, nomeadamente: - de poderes

Expressiva parte das agências ou comissões, entretanto, enfrenta problemas para custear as próprias investigações, além de lhe ser negada independência funcional dentro do próprio governo, o que dificulta o desenvolvimento dos trabalhos. Para solucionar esses problemas, alguns países – dentre os quais Portugal – criaram entidades administrativas independentes em relação ao governo e às organizações reguladas, não integrando tais entidades a administração ordinária do Estado. Configuram-se como órgãos colegiados, formados por membros eleitos de integridade e mérito reconhecidos, protegidos por mandatos que lhes garantem autonomia e independência em suas decisões. As deliberações dessas entidades administrativas não se subordinam ao controle de mérito pelo governo, mas apenas à revisão pelo Judiciário. Exercem funções consultivas, de decisão administrativa, de investigação, de sanção, de representação internacional, de treinamento e de esclarecimento[484].

Destacam-se as principais atribuições dessas entidades administrativas de proteção de dados pessoais: (a) controlar e fiscalizar o cumprimento das disposições legais e regulamentares em matéria de proteção de dados pessoais; (b) exercer poderes de autoridade, quer ordenando o bloqueio, quer o apagamento ou a destruição de dados, quer proibindo temporária ou definitivamente o tratamento de dados pessoais; (c) advertir ou censurar publicamente o responsável pelo tratamento dos dados pessoais, pelo não-cumprimento das disposições legais; (d) intervir nos processos judiciais que versem sobre tratamento de dados pessoais; (e) denunciar ao MP possíveis infrações penais nessa matéria; (f) assegurar os direitos relacionados com a proteção de dados pessoais[485].

---

de inquérito, tais como o poder de aceder aos dados objecto de tratamento e de recolher todas as informações necessárias ao desempenho das suas funções de controlo; - de poderes efectivos de intervenção, tais como, por exemplo, o de emitir pareceres previamente à execução adequada desses pareceres, o de ordenar o bloqueio, o apagamento ou a destruição dos dados, o de proibir temporária ou definitivamente o tratamento, o de dirigir uma advertência ou uma censura ao responsável pelo tratamento ou o de remeter a questão para os parlamentos nacionais ou para outras instituições políticas; - do poder de intervir em processos judiciais no caso de violação das disposições nacionais adoptadas nos termos da presente directiva ou de levar essas infracções ao conhecimento das autoridades judiciais. As decisões de autoridade de controlo que lesem interesses são passíveis de recurso jurisdicional. (...). 6. Cada autoridade de controlo é competente, independentemente do direito nacional aplicável ao tratamento em causa, para o exercício no território do seu Estado-membro dos poderes que lhe foram atribuídos em conformidade com o nº3. Cada autoridade de controlo pode ser solicitada a exercer os seus poderes por uma autoridade de outro Estado-membro. As autoridades de controlo cooperarão entre si na medida do necessário ao desempenho das suas funções, em especial através do intercâmbio de quaisquer informações úteis. 7. Os Estados-membros determinarão que os membros e agentes das autoridades de controlo fiquem sujeitos, mesmo após a cessação das suas actividades, à obrigação de segredo profissional em relação às informações confidenciais a que tenham acesso". In UNIÃO EUROPÉIA. **Directiva 95/46/CE do Parlamento Europeu e do Conselho da Europa**. Op. cit.

[484] CASTRO, Catarina Sarmento. Op. cit., pp. 323-328.

[485] DRUMMOND, Victor. Op. cit., p. 52.

Além da Directiva 95/46/CE, duas outras regulamentações dizem respeito à matéria de proteção de dados pessoais, sendo o conjunto vulgarmente conhecido por *Privacy Directives*: a *Directiva 97/66/CE*, de 15 de dezembro de 1997, que tem como objeto a regulamentação da proteção da intimidade no setor de telecomunicações, abrangendo a proteção do conteúdo das comunicações, dos registros cadastrais fornecidos no momento da contratação do serviço e ainda a fatura gerada a partir das comunicações estabelecidas[486]; e a *Directiva 2002/53/CE*, de 12 de julho de 2002, que regula o tratamento de dados pessoais no setor de comunicações eletrônicas, tendo por fim garantir, nos diferentes Estados-membros, um nível idêntico de preservação da segurança e da confidencialidade nas comunicações, restringindo-se a identificação das chamadas, as listas de assinantes e as comunicações não solicitadas denominadas SPAM[487].

Mesmo após a edição da *Directiva 2002/53/CE*, o problema de violação à privacidade no setor de comunicações eletrônicas ainda não foi solucionado na Europa e nem no resto do mundo. Isto porque na internet o tratamento de dados pessoais muitas vezes se processa de forma não transparente. Expressiva parcela dos usuários sequer imagina que, toda vez que se conectam ao mundo virtual, sujeita-se, automaticamente, à coleta não autorizada de informações a seu respeito. Assim, por meio da *web*, comete-se a violação de um dos princípios mais importantes em relação à proteção de dados pessoais, que é o *princípio da transparência* e o *princípio da exigência de consentimento expresso* por parte do titular dos dados. Diante dessa questão,

---

[486] "*Artigo 1º Objecto e âmbito 1. A presente directiva prevê a harmonização das disposições dos Estados-membros necessárias para garantir um nível equivalente de protecção dos direitos e liberdades fundamentais, nomeadamente o direito à privacidade, no que respeita ao tratamento de dados pessoais no sector das telecomunicações e para garantir a livre circulação desses dados e de equipamentos e serviços de telecomunicações na Comunidade. 2. Para os efeitos do nº 1, as disposições da presente directiva especificam e complementam a Directiva 95/46/CE. Além disso, estas disposições asseguram a protecção dos legítimos interesses dos assinantes que sejam pessoas colectivas. 3. A presente directiva não é aplicável às actividades que não sejam abrangidas pelo âmbito da legislação comunitária, tais como as referidas nos títulos V e VI do Tratado da União Europeia e, em caso algum, às actividades relacionadas com a segurança pública, a defesa, a segurança do Estado, incluindo o bem-estar económico do Estado quando a actividade se relacione com matérias de segurança do Estado, e as actividades do Estado em matéria de direito penal*". In UNIÃO EUROPÉIA. **Directiva 97/66/CE do Parlamento Europeu e do Conselho da Europa**. Op. cit.

[487] *"Artigo 1º Âmbito e objectivos. 1. A presente directiva harmoniza as disposições dos Estados-Membros necessárias para garantir um nível equivalente de protecção dos direitos e liberdades fundamentais, nomeadamente o direito à privacidade, no que respeita ao tratamento de dados pessoais no sector das comunicações electrónicas, e para garantir a livre circulação desses dados e de equipamentos e serviços de comunicações electrónicas na Comunidade. 2. Para os efeitos do n.o 1, as disposições da presente directiva especificam e complementam a Directiva 95/46/CE. Além disso, estas disposições asseguram a protecção dos legítimos interesses dos assinantes que são pessoas colectivas. (...) Artigo 3º Serviços abrangidos. 1. A presente directiva é aplicável ao tratamento de dados pessoais no contexto da prestação de serviços de comunicações electrónicas publicamente disponíveis nas redes públicas de comunicações da Comunidade (...)*". In UNIÃO EUROPÉIA. **Directiva 2002/58/CE do Parlamento Europeu e do Conselho da Europa**. Op. cit.

constituiu-se, no âmbito da UE, um grupo denominado *Grupo Operativo Internet – Task Force,* cuja principal atribuição consiste no propósito de estimular os fabricantes de *softwares* e de *hardwares* a colocarem no mercado produtos que facilitem a aplicação das Directivas e a conseqüente proteção do direito à privacidade. Objetiva-se, desta forma, implementar medidas de proteção à privacidade na rede, não apenas recorrendo-se a leis, mas também colocando em funcionamento sistemas de tecnologia da informação que garantam a confidencialidade e a segurança nas comunicações[488].

Apesar do maior avanço da UE em termos de proteção de dados pessoais, o tema também tem sido discutido nos EUA desde a década de 70 (setenta). Em 1974, o Subcomitê de Direitos Constitucionais do Senado produziu um relatório denominado *Federal Data Banks and Constitutional Rights*, apontando as inconsistências e os excessos cometidos pelas agências governamentais norte-americanas em relação à coleta de dados pessoais, bem como o descaso administrativo no trato da segurança em relação a informações sigilosas. Em 1º de janeiro de 1975, foi publicado o *Privacy Act of 1974,* com o objetivo de proteger a privacidade dos indivíduos em relação ao tratamento de suas informações pelas agências governamentais. De acordo com esse ato normativo, as agências poderiam coletar informações pessoais tão-somente se demonstrassem a "relevância" dessa coleta e a "necessidade" de tais procedimentos pelo órgão governamental, que ficaria obrigado a garantir a autenticidade, a integridade e a confidencialidade dessas informações mediante instalação de sistemas de segurança[489]. Um outro dispositivo obrigava as agências a conferirem aos titulares dos dados o *direito de acesso* a essas informações para fins de correção. Entretanto, esse ato normativo foi considerado ineficaz pelos especialistas, tendo em vista a dificuldade de exercício dos direitos nele previstos, especialmente o direito de acesso aos bancos de dados pelos titulares[490].

Nas décadas de 70 (setenta) e 80 (oitenta), publicaram-se dispositivos legais relacionados com a proteção de dados pessoais na área de consumo. Em 1984, instituiu-se o *Cable Communications Policy Act of 1984*, que obrigou os prestadores de serviço de comunicações a adotarem, dentre outros, os seguintes procedimentos: solicitação de autorização dos consumidores antes da coleta e do armazenamento de seus dados pessoais; oportunidade para os titulares dos dados recusarem ou aceitarem o uso das informações fornecidas para finalidades

[488] CAMPUZANO TOMÉ, Hermínia. Op. cit., pp. 138-139.
[489] SAMPAIO, José Adércio. Op. cit., pp. 484-485.
[490] GRAY, Susan H. Op. cit, p. 244.

diversas daquelas relacionadas diretamente com a prestação do serviço requisitado; destruição dos dados pessoais dos consumidores ao término do contrato. Vários Estados seguiram o arcabouço principiológico de proteção de dados pessoais previsto no *Cable Communications Policy Act of 1984*; assim o Estado da Califórnia regulamentou as atividades de telefonia, de prestação de serviços de saúde e de finanças. Todavia, ainda se mostra incipiente nos EUA a questão da proteção de dados pessoais, especialmente no que concerne à coleta de informações por prestadores de serviço da sociedade da informação, que disponibilizam produtos e serviços pela internet, violação à privacidade que se agrava dramaticamente com o decorrer do tempo[491]. A situação assumiu contornos mais sérios ainda após o atentado terrorista de 11 de setembro de 2001, que destruiu o *World Trade Center*, em Manhattan, Nova Iorque, diante das novas medidas de vigilância e monitoramento adotadas pela agência de inteligência NSA e pelo FBI, com o apoio da maior parte dos cidadãos norte-americanos, conforme visto no item 3.7.1 quando se tratou da espionagem estatal mediante utilização de artefatos tecnológicos.

Na América Latina, a proteção de dados pessoais encontra-se igualmente em estágio incipiente. Até o presente momento, somente o Chile e a Argentina aprovaram leis específicas sobre proteção de dados pessoais: Lei nº 19.628, de 28 de agosto de 1999; e Lei nº 25.326, de 30 de outubro de 2000, respectivamente. A aprovação de atos normativos de igual conteúdo exige que um país atue de forma coordenada com os demais países, para que não se obstrua a transmissão de dados pessoais entre os integrantes da América Latina e entre esses e o resto do mundo, dada a importância do comércio eletrônico no mundo globalizado[492].

Para atingir tal meta, em 1999 a Organização dos Estados Americanos – OEA elaborou a *Convenção Americana sobre Autodeterminação Informativa* influenciada pelos princípios previstos nas *Privacy Directives*. O documento faz referência à Declaração dos Direitos do Homem de 1948 e, em seguida, reconhece os perigos a que o tratamento automatizado de dados de caráter pessoal expõe a vida privada do usuário de computador, mediante o uso de novos aparatos tecnológicos. Ao final, conclui com um forte argumento de que o modelo de proteção de dados pessoais não pode se diferenciar na Europa e na América Latina, porque os problemas que as novas tecnologias oferecem não respeitam delimitações nacionais, ultrapassam fronteiras,

[491] IMPARATO, Nicholas (coordenador) *et al*. **Public policy and the internet**: privacy, taxes and contract. Stanford: Hoover Institution Press, 2000, pp. 5-6.
[492] PALLAZZI, Pablo A. **La transmisión internacional de datos personales y la protección de la privacidad**: Argentina, América Latina, Estados Unidos e la Unión Europea. Buenos Aires: Editora Ad-Hoc, 2002, pp. 95-96.

exercendo similares efeitos em todo o mundo[493]. Assim, as soluções jurídicas, sejam nacionais, sejam regionais, sejam mundiais, não podem ser muito diferentes, por duas razões básicas: a forte tendência de internacionalização em matéria de direitos humanos, e a comprovação, ao longo de todos esses anos de experiência, de que a regulamentação de temas relacionados à internet se impõe como medida efetiva tão-somente quando considera o caráter transnacional da rede, ou seja, o fluxo *transfronteiriço* das informações na *web*.

Em conclusão, apesar de a quase totalidade dos ordenamentos jurídicos preservar o direito à intimidade e à vida privada, a discussão a respeito da tutela dos dados pessoais mal consegue traçar as diretrizes iniciais. Conforme visto, os maiores avanços ocorreram no continente europeu, onde já se garante proteção tanto pela via legislativa como pela administrativa por meio da criação de agências ou comissões especializadas no tema. Nos EUA, apesar de ter ocorrido grande avanço em termos legislativos nas décadas de 70 (setenta) e 80 (oitenta), atualmente o direito à proteção de dados pessoais não encontra respaldo, especialmente em se tratando de órgãos governamentais, que adotam procedimentos cada vez mais invasivos à privacidade na "luta contra o terrorismo". Na América Latina, a proteção à *privacidade informacional* também se mostra incipiente, existindo legislação específica apenas na Argentina e no Chile. Entretanto, aos poucos, a percepção dos riscos que a tecnologia da informação desencadeia contra a preservação do direito à privacidade se difunde em outros países. Ressalta-se a necessidade de edição de lei especifica sobre a tutela dos dados pessoais que considere o modelo de proteção adotado na Europa – o mais avançado atualmente – bem como o caráter transnacional da rede.

4.4 Panorama nacional da proteção de dados pessoais

O ordenamento jurídico nacional prevê a proteção de dados pessoais de forma indireta. A CF prevê a *inviolabilidade da intimidade, da vida privada* e da imagem das pessoas (art. 5º, inciso X); dispõe sobre a inviolabilidade da correspondência e das comunicações telegráficas, *de dados* e das comunicações telefônicas (art. 5º, inciso XII); garante a todos o direito de receber dos órgãos públicos *informações de seu interesse particular*, ou de interesse coletivo ou geral,

[493] PALLAZZI, Pablo A. Op. cit. pp. 49-52.

ressalvadas aquelas cujo sigilo seja imprescindível à segurança da sociedade e do Estado (art. 5º, inciso XXXIII); e regula o *habeas data* para assegurar o conhecimento e a correção de informações relativas à pessoa do impetrante (art. 5º, inciso LXXII).

A inviolabilidade do sigilo de dados pessoais (CF, art. 5º, inciso XII) resguarda a privacidade do indivíduo em relação a *informações fiscais e bancárias*, independentemente do fato de se encontrarem ou não armazenadas em bancos de dados das instituições financeiras, da Receita Federal ou de qualquer órgão do poder público. O *sigilo bancário* encontra-se regulado pela Lei Complementar nº 105, de 10 de janeiro de 2001, e pelo Decreto nº 4.489, de 28 de novembro de 2002. O *sigilo fiscal* está previsto no art. 198 do Código Tributário Nacional – CTN – instituído pela Lei nº 5.172, de 15 de outubro de 1966 – impondo-se a obrigação de confidencialidade para os agentes do Fisco que, em razão de suas funções, tenham acesso a dados sobre as operações e situações econômicas das pessoas e empresas que fiscalizam[494].

Importante observar que o sigilo bancário e fiscal, enquanto expressão do direito à privacidade, *não tem caráter absoluto*, conforme visto no item 2.3.1. Assim, poderá ser determinada a quebra sempre que se demonstrar a indispensabilidade da medida para a preservação de outro direito fundamental ou de outro valor constitucional; e desde que a decisão seja tomada por autoridade judiciária ou por uma comissão parlamentar de inquérito – CPI, conforme expressa autorização do seguinte dispositivo constitucional:

> Art. 58. O Congresso Nacional e suas Casas terão comissões permanentes e temporárias, constituídas na forma e com as atribuições previstas no respectivo regimento ou no ato de que resultar sua criação.
> .....
> § 3º - As comissões parlamentares de inquérito, que terão poderes de investigação próprios das autoridades judiciais, além de outros previstos nos regimentos das respectivas Casas, serão criadas pela Câmara dos Deputados e pelo Senado Federal, em conjunto ou separadamente, mediante requerimento de um terço de seus membros, para a apuração de fato determinado e por prazo certo, sendo suas conclusões, se for o caso, encaminhadas ao Ministério Público, para que promova a responsabilidade civil ou criminal dos infratores.[495]

Alexandre de Moraes arrola requisitos para quebra de sigilo bancário: indispensabilidade dos dados constantes em determinada instituição financeira; individualização do investigado e do

---

[494] "*Art. 198. Sem prejuízo do disposto na legislação criminal, é vedada a divulgação, por parte da Fazenda Pública ou de seus servidores, de informação obtida em razão do ofício sobre a situação econômica ou financeira do sujeito passivo ou de terceiros e sobre a natureza e o estado de seus negócios ou atividades*". In BRASIL. Código Tributário Nacional. **Lei nº 5.172, de 25 de outubro de 1966**. Disponível em: <http://www.planalto.gov.br/ccivil_03/Leis/L5172.htm>. Acesso em: 30 jan. 2007.

[495] BRASIL. **Constituição da República Federativa do Brasil de 1988**. Op. cit. Grifos nossos.

objeto da investigação; obrigatoriedade de manutenção do sigilo em relação às pessoas estranhas ao procedimento investigatório; utilização restrita dos dados obtidos, e decisão de CPI ou autorização judicial[496].

A jurisprudência do STF é farta de casos interessantes sobre sigilo bancário e fiscal; ressaltando-se seu caráter relativo, bem como a necessidade de emanação da ordem de quebra por autoridade judicial ou CPI, conforme se observa no seguinte acórdão, literalmente:

> E M E N T A. COMISSÃO PARLAMENTAR DE INQUÉRITO - PODERES DE INVESTIGAÇÃO (CF, ART. 58, § 3º) - LIMITAÇÕES CONSTITUCIONAIS - LEGITIMIDADE DO CONTROLE JURISDICIONAL - POSSIBILIDADE DE A CPI ORDENAR, POR AUTORIDADE PRÓPRIA, A QUEBRA DOS SIGILOS BANCÁRIO, FISCAL E TELEFÔNICO - NECESSIDADE DE FUNDAMENTAÇÃO DO ATO DELIBERATIVO - DELIBERAÇÃO DA CPI QUE, SEM FUNDAMENTAÇÃO, ORDENOU MEDIDAS DE RESTRIÇÃO A DIREITOS - MANDADO DE SEGURANÇA DEFERIDO. (...).
> - Não há, no sistema constitucional brasileiro, direitos ou garantias que se revistam de caráter absoluto, mesmo porque razões de relevante interesse público ou exigências derivadas do princípio de convivência das liberdades legitimam, ainda que excepcionalmente, a adoção, por parte dos órgãos estatais, de medidas restritivas das prerrogativas individuais ou coletivas, desde que respeitados os termos estabelecidos pela própria Constituição. O estatuto constitucional das liberdades públicas, ao delinear o regime jurídico a que estas estão sujeitas - e considerado o substrato ético que as informa - permite que sobre elas incidam limitações de ordem jurídica, destinadas, de um lado, a proteger a integridade do interesse social e, de outro, a assegurar a coexistência harmoniosa das liberdades, pois nenhum direito ou garantia pode ser exercido em detrimento da ordem pública ou com desrespeito aos direitos e garantias de terceiros. A QUEBRA DO SIGILO CONSTITUI PODER INERENTE À COMPETÊNCIA INVESTIGATÓRIA DAS COMISSÕES PARLAMENTARES DE INQUÉRITO.
> - O sigilo bancário, o sigilo fiscal e o sigilo telefônico (sigilo este que incide sobre os dados/registros telefônicos e que não se identifica com a inviolabilidade das comunicações telefônicas) - ainda que representem projeções específicas do direito à intimidade, fundado no art. 5º, X, da Carta Política - não se revelam oponíveis, em nosso sistema jurídico, às Comissões Parlamentares de Inquérito, eis que o ato que lhes decreta a quebra traduz natural derivação dos poderes de investigação que foram conferidos, pela própria Constituição da República, aos órgãos de investigação parlamentar. As Comissões Parlamentares de Inquérito, no entanto, para decretarem, legitimamente, por autoridade própria, a quebra do sigilo bancário, do sigilo fiscal e/ou do sigilo telefônico, relativamente a pessoas por elas investigadas, devem demonstrar, a partir de meros indícios, a existência concreta de causa provável que legitime a medida excepcional (ruptura da esfera de intimidade de quem se acha sob investigação), justificando a necessidade de sua efetivação no procedimento de ampla investigação dos fatos determinados

[496] MORAES, Alexandre de. **Direito constitucional**. Op. cit., pp. 92-93.

> que deram causa à instauração do inquérito parlamentar, sem prejuízo de ulterior controle jurisdicional dos atos em referência (CF, art. 5º, XXXV).[497]

Um caso de relevo na jurisprudência do STF enfrentou a polêmica questão a respeito da possibilidade de o MP promover diretamente a quebra do sigilo bancário e fiscal, dispensando-se intervenção judicial. O relator para o acórdão, ministro Carlos Velloso, destacou que, como o sigilo bancário e fiscal encontra-se inserido no âmbito de proteção do direito fundamental à privacidade, essa garantia só poderia sofrer limitação pelo MP caso existisse previsão dessa restrição pela própria Constituição (restrição diretamente constitucional) ou por lei infraconstitucional autorizada expressamente pela Magna Carta (restrição indiretamente constitucional), hipótese que não se sustenta, vedando-se, portanto, ao MP promover diretamente a quebra do sigilo de qualquer pessoa sem prévia autorização judicial, *verbis*:

> EMENTA. CONSTITUCIONAL. MINISTÉRIO PÚBLICO. SIGILO BANCÁRIO: QUEBRA. CF, art. 129, VIII.
> I - A norma inscrita no inc. VIII do art. 129, da CF, não autoriza ao Ministério Público, sem a interferência da autoridade judiciária, quebrar o sigilo bancário de alguém. Se se tem presente que o sigilo bancário é espécie de direito à privacidade, que a CF consagra, art. 5º, X, somente autorização expressa da Constituição legitimaria o Ministério Público a promover, diretamente e sem a intervenção da autoridade judiciária, a quebra do sigilo bancário de qualquer pessoa.
> II - R.E. não conhecido.[498]

Por fim, destaque-se, como requisito para restrição do sigilo bancário e fiscal – além da exigência da individualização do investigado e do objeto da investigação, obrigatoriedade de manutenção do sigilo em relação às pessoas estranhas ao procedimento investigatório, utilização restrita dos dados obtidos, e decisão de CPI ou autorização judicial – a exigência de que a decisão de quebra não apenas se apóie em fundamentação adequada mas também que seja contemporânea ao ato que contenha tal determinação e baseada em fatos idôneos, a fim de se evitar a devassa espúria da intimidade das pessoas. É o que se lê na ementa do seguinte acórdão julgado pelo STF:

---

[497] BRASIL. Supremo Tribunal Federal. MS nº 23452-RJ. Impetrante: Luiz Carlos Barreti Junior. Relator: Celso Mello. Brasília, DF, 16 de agosto de 1999. **Diário da Justiça da República Federativa do Brasil**, Brasília, DF, 12 maio 2000, p. 00020. Disponível em <http://www.stf.gov.br/jurisprudencia>. Acesso em: 30 jan. 2007. Grifos nossos.

[498] BRASIL. Supremo Tribunal Federal. RE nº 215301-CE. Recorrente: Ministério Público Federal. Relator: Carlos Velloso. Brasília, DF, 13 de abril de 1999. **Diário da Justiça da República Federativa do Brasil**, Brasília, DF, 28 maio 1999, p. 00700. Disponível em <http://www.stf.gov.br/jurisprudencia>. Acesso em: 30 jan. 2007. Grifos nossos.

> EMENTA. COMISSÃO PARLAMENTAR DE INQUÉRITO. QUEBRA DE SIGILO BANCÁRIO E FISCAL.
> - Esta Corte, em julgamentos relativos a mandados de segurança contra a quebra de sigilo bancário e fiscal determinada por Comissão de Inquérito Parlamentar (assim, entre outros, nos MS's 23.452, 23.454, 23.851, 23.868 e 23.964), já firmou o entendimento de que tais Comissões têm competência para isso desde que essa quebra tenha fundamentação adequada, que não só há de ser contemporânea ao ato que a ordena, mas também que se baseie em fatos idôneos, para que não seja ela utilizada como instrumento de devassa indiscriminada sem que situações concretas contra alguém das quais possa resultar suspeitas fundadas de suposto envolvimento em atos irregulares praticados na gestão da entidade em causa. No caso, a determinação da quebra de sigilo em causa está fundamentada na forma em que, tratando-se de decretação por parte de CPI, se admite que ela se dê. Mandado de segurança indeferido, cassada a liminar.[499]

Dando-se continuidade ao estudo a respeito da previsão de proteção de dados pessoais no ordenamento jurídico nacional, observa-se a existência de dispositivo constitucional relacionado ao tema no que se refere à possibilidade de se aceder aos dados pessoais armazenados nos órgãos e nas entidades de caráter público, excetuando-se tão-somente o acesso a informações classificadas como sigilosas (CF, art. 5º, inciso XXXIII). O referido dispositivo foi regulamentado pelo § 3º do art. 23 da Lei nº 8.159/91, que dispõe que o acesso a documentos sigilosos referentes à honra e à imagem das pessoas será restrito por um prazo máximo de 100 (cem) anos, a contar da data da sua produção[500]; e pelo parágrafo único do art. 7º da Lei nº 11.111/05, que dispõe que documentos que contenham informações relacionadas à intimidade, à vida privada, à honra e à imagem de pessoas terão acesso restrito à pessoa diretamente interessada ou, em se tratando de morto ou ausente, ao seu cônjuge, aos ascendentes ou aos descendentes[501]. Há, portanto, suficiente regulamentação da questão da *disponibilidade* de dados pessoais aos próprios titulares, cônjuges e parentes; verificando-se, todavia, a carência de atos normativos que versem sobre a obrigatoriedade de adoção de medidas e procedimentos de segurança que garantam a *integridade,* a *autenticidade* e o *sigilo* dessas informações durante o seu *tratamento*, a exemplo da legislação aprovada nos países da UE.

---

[499] BRASIL. Supremo Tribunal Federal. MS nº 23843-RJ. Impetrante: Carlos Augusto Saade Montenegro. Relator: Moreira Alves. Brasília, DF, 10 de outubro de 2001. **Diário da Justiça da República Federativa do Brasil**, Brasília, DF, 01 ago. 2003, p. 00105. Disponível em <http://www.stf.gov.br/jurisprudencia>. Acesso em: 30 jan. 2007. Grifos nossos.
[500] BRASIL. **Lei nº 8.159, de 08 de janeiro de 1991**. Op. cit.
[501] BRASIL. **Lei nº 11.111, de 05 de maio de 2005**. Op. cit.

O *habeas data* (CF, art. 5º, inciso LXXII) foi regulamentado pela Lei nº 9.507, de 12 de novembro de 1997. Essa ação constitucional tem caráter civil, conteúdo e rito sumário, tendo por objeto a proteção do direito líquido e certo do impetrante em conhecer todas as informações relativas à sua pessoa, constantes de registro ou banco de dados de entidades governamentais ou de caráter público; em retificar dados; e em anotar nos seus assentamentos, contestação ou explicação sobre dado verdadeiro, mas justificável ou sob pendência de discussão judicial ou amigável, conforme disposto nos incisos I, II e III do art. 7º[502]. Todavia, o emprego desse "remédio constitucional" figura-se restrito, uma vez que a impetração exige, como pressuposto, a negativa da via administrativa, de maneira que inexistirá interesse de agir a essa ação se não houver relutância do órgão detentor da informação de prestá-la, retificá-la ou efetuar a anotação solicitada. Esse entendimento está previsto no art. 8º da Lei, que prevê que a petição inicial deverá ser instruída com a prova da negativa administrativa[503].

Ressalte-se que o HD pode ser impetrado inclusive para conhecimento, retificação e anotação em relação a *documentos classificados como sigilosos para garantia da segurança da sociedade e do Estado*. Ainda que o acesso a tais documentos possa restringir-se a um lapso de tempo de trinta anos, prorrogável por igual período, não se pode *a priori* negar o conhecimento ao próprio titular. Assim, a ressalva de *segredo do Estado,* prescrita no inciso XXXIII, vale geralmente em relação a terceiros, mas não necessariamente em relação ao titular das informações, uma vez que, caso as informações sejam verdadeiras, provavelmente, o próprio impetrante da ação constitucional a respeito delas já terá conhecimento, todavia, caso sejam falsas, tal retificação não causará nenhum dano à segurança social ou nacional.

Além do disposto nos incisos X, XII, XXXIII e LXXII do art. 5º da CF e das leis que regulamentam esses dispositivos, ainda constituem regras aplicáveis à proteção de dados pessoais aquelas constantes no Código de Proteção e Defesa do Consumidor – CDC, aprovado pela Lei nº 8.078, de 11 de setembro de 1990. O *caput* do art. 43 dispõe que o consumidor terá acesso não apenas às informações existentes em cadastros, em fichas, em registros, mas também a todos os

---

[502] BRASIL. **Lei nº 9.507, de 12 de novembro de 1997**. Disponível em: <http://www.planalto.gov.br/ccivil_03/Leis/L9507.htm >. Acesso em: 30 jan. 2007.

[503] "*Art. 8° A petição inicial, que deverá preencher os requisitos dos arts. 282 a 285 do Código de Processo Civil, será apresentada em duas vias, e os documentos que instruírem a primeira serão reproduzidos por cópia na segunda. Parágrafo único. A petição inicial deverá ser instruída com prova: I - da recusa ao acesso às informações ou do decurso de mais de dez dias sem decisão; II - da recusa em fazer-se a retificação ou do decurso de mais de quinze dias, sem decisão; ou III - da recusa em fazer-se a anotação a que se refere o § 2° do art. 4° ou do decurso de mais de quinze dias sem decisão*". In BRASIL. **Lei nº 9.507, de 12 de novembro de 1997**. Op. cit.

dados pessoais e de consumo arquivados e que a esse consumidor se refiram, bem como às informações a respeito de suas respectivas fontes[504]. Essa norma traduz o *dever de informação*, obrigando que sejam prestados esclarecimentos aos titulares dos dados coletados, a fim de ensejar a oportunidade de retificação, direito que cabe ao titular, segundo princípio expresso na *Lei Francesa de 1978* e na *Recomendação da OCDE de 1980*, conforme visto no item anterior.

O § 1º do art. 43 determina que cadastros e dados de consumidores devem ser objetivos, claros, verdadeiros e em linguagem de fácil compreensão, não podendo conter informações negativas que ultrapassem lapso de tempo superior a cinco anos[505], evitando-se que o devedor fique marcado indefinidamente por uma ocorrência passada. Esse dispositivo refere-se ao *dever de lealdade na coleta de dados*, princípio também previsto na *Lei Francesa de 1978* e na *Recomendação da OCDE de 1980*, além de regular o denominado *direito ao apagamento* – também chamado *direito ao esquecimento* – garantia prevista nas legislações mais avançadas em termos de proteção de dados pessoais, conforme se detalhará no item 4.5.7.

O § 2º do art. 43 dispõe que a abertura de cadastro ou registro de dados pessoais e de consumo deverá ser comunicada por escrito ao consumidor, quando não solicitada por esse interessado[506]. Caso a relação de consumo tenha se estabelecido pela internet, sugere-se a aplicação desse mesmo dispositivo para proteger os consumidores em relação à atividade de coleta desautorizada de dados pessoais desses mesmos titulares, por meio da utilização de *cookies* pelas *empresas.com*, uma vez que esses dispositivos normalmente são instalados de forma velada nos computadores dos internautas, conforme visto no item 3.6.

A seguir, o § 3° do art. 43 garante ao consumidor o direito de exigir correção em registros nos quais se constata inexatidão nos dados e cadastros a seu respeito[507]. Esse dispositivo traduz o *princípio da veracidade* – também denominado *princípio da exatidão e atualização dos dados* – norma prevista na Directiva 95/46/CE, conforme se verá no item 4.5.6.

Na área criminal, o tipo penal 313-A (Inserção de dados falsos em sistema de informações), acrescentado pela Lei nº 9.983/00 ao CP, sanciona a inserção de dados falsos, alteração ou exclusão indevida de dados corretos nos sistemas informatizados ou nos bancos de

[504] BRASIL. Código de Proteção e Defesa do Consumidor. **Lei nº 8.078, de 11 de setembro de 1990**. Disponível em: <http://www.planalto.gov.br/ccivil_03/LEIS/L8078.htm>. Acesso em: 30 jan. 2007.
[505] BRASIL. **Lei nº 8.078, de 11 de setembro de 1990**. Op. cit.
[506] BRASIL. **Lei nº 8.078, de 11 de setembro de 1990**. Op. cit.
[507] BRASIL. **Lei nº 8.078, de 11 de setembro de 1990**. Op. cit.

dados da administração pública, com o fim de obter vantagem indevida para si ou para outrem ou para causar dano[508].

De forma mais específica, protegem-se ainda os dados pessoais, no § 1º-A do art. 153 do CP. Esse dispositivo incrimina a conduta de divulgação de informações sigilosas ou reservadas, contidas ou não nos sistemas de informação ou nos bancos de dados da administração pública[509].

Por fim, o inciso I do art. 325 incrimina a conduta daquele que permite ou facilita, mediante atribuição, fornecimento e empréstimo de senha ou mediante qualquer outro procedimento escuso, o acesso de pessoas não autorizadas a sistemas de informações ou banco de dados da administração pública[510].

Considerando-se que nos registros públicos armazenam-se dados pessoais dos cidadãos – informações referentes à saúde, ao patrimônio e à renda do indivíduo, dentre tantas outras – verifica-se que esses tipos penais, ainda que indiretamente, tutelam a integridade e o sigilo desses mesmos dados tratados por meio de sistemas informatizados ou bancos de dados da administração pública.

Diante do exposto, conclui-se que, embora o ordenamento jurídico nacional não assegure, de forma direta, a proteção de dados pessoais, essa garantia, mesmo assim, emana de dispositivos da própria CF, do CDC, do CTN, do CP e de leis esparsas. Todavia, com o objetivo de conferir maior efetividade ao direito à privacidade informacional, sugere-se a regulamentação dessa garantia por lei específica, conforme será detalhado no item 4.6.

---

[508] "*Art. 313-A. Inserir ou facilitar, o funcionário autorizado, a inserção de dados falsos, alterar ou excluir indevidamente dados corretos nos sistemas informatizados ou bancos de dados da Administração Pública com o fim de obter vantagem indevida para si ou para outrem ou para causar dano: Pena – reclusão, de 2 (dois) a 12 (doze) anos, e multa*." In BRASIL. Código Penal. **Decreto-lei nº 2.848, de 7 de dezembro de 1940**. Disponível em: <http://www.planalto.gov.br/ccivil_03/Decreto-Lei/Del2848.htm>. Acesso em: 30 jan. 2007.

[509] "*Art. 153 § 1º-A. Divulgar, sem justa causa, informações sigilosas ou reservadas, assim definidas em lei, contidas ou não nos sistemas de informações ou banco de dados da Administração Pública: Pena – detenção, de 1 (um) a 4 (quatro) anos, e multa"*. In BRASIL. **Decreto-lei nº 2.848, de 7 de dezembro de 1940**. Op. cit.

[510] "*Art. 325 - Revelar fato de que tem ciência em razão do cargo e que deva permanecer em segredo, ou facilitar-lhe a revelação: Pena - detenção, de seis meses a dois anos, ou multa, se o fato não constitui crime mais grave. § 1º Nas mesmas penas deste artigo incorre quem: I – permite ou facilita, mediante atribuição, fornecimento e empréstimo de senha ou qualquer outra forma, o acesso de pessoas não autorizadas a sistemas de informações ou banco de dados da Administração Pública; II – se utiliza, indevidamente, do acesso restrito. § 2º Se da ação ou omissão resulta dano à Administração Pública ou a outrem: Pena – reclusão, de 2 (dois) a 6 (seis) anos, e multa*". In BRASIL. **Decreto-lei nº 2.848, de 7 de dezembro de 1940**. Op. cit.

4.5 Princípios relacionados ao tratamento de dados pessoais

4.5.1 Explicação inicial

Conforme visto no item 4.3, a *terceira geração* de leis sobre proteção de dados pessoais já trazia em seu bojo os princípios identificados como necessários à garantia dos direitos e das liberdades dos indivíduos no que respeita a *privacidade informacional*. A *Lei Francesa de 1978* e a *Recomendação da OCDE de 1980* foram as primeiras a arrolá-los de forma sistematizada, servindo depois como fonte de inspiração para regulamentações posteriores. Com o desenvolvimento da tecnologia da informação, ao longo dos últimos anos, reconheceram-se novos princípios aplicáveis ao tratamento de dados pessoais em sistemas automatizados. Atualmente, aplicam-se tais princípios a qualquer espécie de tratamento de dados pessoais, para regular as relações jurídicas entre os titulares dos dados e o poder público ou a iniciativa privada.

Nesse contexto, as lições de Paulo Bonavides a respeito da *força normativa dos princípios* merecem consideração. Segundo o autor, a juridicidade dos princípios transitou por três fases bem distintas: a jusnaturalista, a positivista e a pós-positivista. Na fase *jusnaturalista*, os princípios assumiam normatividade praticamente nula, sendo concebidos apenas como "axiomas jurídicos" ou normas estabelecidas pela reta razão, com o objetivo de preencher as lacunas do ordenamento jurídico, formando um conjunto de "verdades objetivas" derivadas das leis divina e humana. Na segunda fase, denominada *positivista* ou *juspositivista,* os princípios ganharam certa força normativa ao integrarem o ordenamento jurídico por derivação das próprias leis. No terceiro período – a fase em que se encontram os ordenamentos jurídicos mais avançados, denominada *pós-positivista* – os princípios assumem ampla normatividade, impondo obrigações ao serem declarados e reconhecidos pela jurisprudência, mesmo quando não se encontram expressamente dispostos em textos de lei[511].

Sob a concepção *pós-positivista* analisem-se os princípios que a seguir se apresentam, ou seja, independentemente de se encontrarem ou não presentes nas leis que integram o ordenamento jurídico, devem tais determinações nortear a jurisprudência, que apenas os

[511] BONAVIDES, Paulo. Op. cit., pp. 259 e ss.

reconhece e os declara. Servem, ainda, como fonte de inspiração aos legisladores que, ao normalizar, podem contemplá-los, caso considerem necessária tal previsão, em atos normativos de forma expressa.

Por fim, ressalte-se que, apesar de esses princípios constarem nas *Privacy Directives* – conjunto de Directivas do Parlamento Europeu e do Conselho da Europa relacionadas ao direito à privacidade[512] – não foram previstos expressamente na legislação nacional de todos os países da UE. Todavia, tal fato não impede a ampla aplicação desses postulados pela jurisprudência, considerando-se que estruturam, em plenitude, o arcabouço axiológico do sistema de proteção de dados pessoais, sendo essencial seu reconhecimento para a efetividade do *direito à privacidade informacional* diante dos avanços da tecnologia da informação.

4.5.2 Princípio da lealdade ou da boa fé

Prevê-se expressamente nas alíneas "a" e "b" do item 1 do art. 6º da Directiva 95/46/CE[513] e na parte final do item 39 do Preâmbulo da Directiva 2002/58/CE o princípio da lealdade[514].

Dispõe que os dados devem ser recolhidos com o conhecimento do respectivo titular, vedando-se a coleta por meio de terceiros, o que implicaria ausência de controle pelo próprio indivíduo. Impõe, ainda, que os dados sejam utilizados para os fins para os quais foram colhidos, ou seja, só podem ser utilizados para a realização dos objetivos propostos e autorizados pelo titular[515].

---

[512] Ver itens 2.4.2.4.2 e 4.3.

[513] *"Artigo 6º 1. Os Estados-membros devem estabelecer que os dados pessoais serão: a) Objecto de um tratamento leal e lícito; b) Recolhidos para finalidades determinadas, explícitas e legítimas, e que não serão posteriormente tratados de forma incompatível com essas finalidades. O tratamento posterior para fins históricos, estatísticos ou científicos não é considerado incompatível desde que os Estados-membros estabeleçam garantias adequadas;"*. In UNIÃO EUROPÉIA. **Directiva 95/46/CE do Parlamento Europeu e do Conselho da Europa**. Op. cit.

[514] "*(39) (...) Qualquer transmissão deve obedecer à condição de que os dados não possam ser utilizados para outros fins diferentes dos que motivaram a sua recolha. Se a parte que recolhe os dados a partir do assinante ou de terceiros a quem os mesmos tenham sido transmitidos pretender utilizá-los para outro fim, quer a parte que recolheu os dados, quer o terceiro a quem foram transmitidos, terá de obter novo consentimento do assinante*". In UNIÃO EUROPÉIA. **Directiva 2002/58/CE do Parlamento Europeu e do Conselho da Europa**. Op. cit.

[515] SAMPAIO, José Adércio. Op. cit., p. 513.

Fere o princípio da lealdade ou da boa fé a coleta de dados pessoais sem o consentimento de seus titulares, seguida da formação de um banco de dados utilizado para se traçar o perfil desses indivíduos, informações depois mercantilizadas com empresas de publicidade e *marketing*. Também se caracteriza ofensa a esse princípio a coleta de dados com tácita anuência do titular para fins de execução de um contrato de prestação de serviço ou produto, seguida da utilização dos mesmos dados para atender a interesses comerciais alheios aos fins para os quais foram coletados e não autorizados por aquele mesmo titular.

Assim, informações coletadas para determinado propósito poderão ser utilizadas para finalidades diversas tão-somente em casos em que haja prévio consentimento de seu titular ou autorização legal. A única hipótese em que os dados poderão ser utilizados para finalidades diversas daquelas para as quais foram colhidos diz respeito à situação em que o próprio Estado promove tal recolhimento, e para fins de preservação de outros interesses públicos, como investigação criminal e exercício da atividade de inteligência. Em tais casos, entende-se que se instala uma situação de colisão entre o direito fundamental à *privacidade* e o valor constitucional *segurança pública*, devendo-se aplicar o *princípio da proporcionalidade* para resolução de tal conflito.

4.5.3 Princípio da publicidade

A obrigatoriedade de os responsáveis por bancos de dados informarem o público sobre sua existência encontra-se norteada pelo princípio da publicidade, impondo-se a divulgação da finalidade da operação e os procedimentos utilizados para tratamento de dados de caráter pessoal. Essas informações devem ser disponibilizadas em meio de ampla divulgação e de fácil acesso, como em *sites* da internet.

O art. 18º da Directiva 95/46/CE[516] determina que a existência e a utilização de qualquer banco de dados com informações pessoais deve ser de conhecimento público, seja pela exigência

[516] "*Artigo 18 Obrigação de notificação à autoridade de controlo 1. Os Estados-membros estabelecerão que o responsável pelo tratamento ou, eventualmente, o seu representante deve notificar a autoridade de controlo referida no artigo 28º antes da realização de um tratamento ou conjunto de tratamentos, total ou parcialmente*

de autorização prévia para funcionar, seja pela necessidade do registro público de sua existência, seja pelo envio de relatórios periódicos ao Estado ou a qualquer entidade interessada. Decorre ainda deste princípio o direito que cabe a qualquer pessoa de solicitar ao órgão de controle – agência ou comissão de proteção de dados pessoais – informações sobre bancos de dados já existentes.

A Lei de Proteção de Dados Pessoais da República Portuguesa (Lei nº 67, de 26 de outubro de 1998, apenas em nível de reforço para o necessário esclarecimento da questão, obriga as entidades que procedem ao tratamento de dados pessoais a notificarem esse tratamento à Comissão Nacional de Proteção de Dados – CNPD, efetuando o registro dessa atividade. Caso o tratamento se refira a dados sensíveis, requer-se, além da notificação, prévia autorização por parte da CNPD[517]. A Lei dispensa a notificação do tratamento apenas nos casos em que os dados não se mostrem suscetíveis de ameaçar direitos e liberdades dos titulares, ou quando houver justificada necessidade de celeridade, economia e eficiência. Tal isenção de notificação, entretanto, não exime o responsável pelo tratamento de prestar esclarecimentos ao titular dos respectivos dados[518].

4.5.4 Princípio da transparência

No art. 10º da Diretiva 95/46/CE[519], na parte inicial do item 39 do Preâmbulo da Directiva 2002/58/CE[520] e no item 1 do art. 12º da Directiva 2002/58/CE[521] prevê-se o princípio da transparência.

---

automatizados, destinados à prossecução de uma ou mais finalidades interligadas". In UNIÃO EUROPÉIA. **Directiva 95/46/CE do Parlamento Europeu e do Conselho da Europa**. Op. cit.

[517] CASTRO, Catarina Sarmento. Op. cit., pp. 70-71.

[518] CASTRO, Catarina Sarmento. Op. cit., p. 109.

[519] "*Artigo 10º Informação em caso de recolha de dados junto da pessoa em causa. Os Estados-membros estabelecerão que o responsável pelo tratamento ou o seu representante deve fornecer à pessoa em causa junto da qual recolha dados que lhe digam respeito, pelo menos as seguintes informações, salvo se a pessoa já delas tiver conhecimento: a) Identidade do responsável pelo tratamento e, eventualmente, do seu representante; b) Finalidades do tratamento a que os dados se destinam; c) Outras informações, tais como: - os destinatários ou categorias de destinatários dos dados, - o carácter obrigatório ou facultativo da resposta, bem como as possíveis consequências se não responder, - a existência do direito de acesso aos dados que lhe digam respeito e do direito de os rectificar, desde que sejam necessárias, tendo em conta as circunstâncias específicas da recolha dos dados, para garantir à*

Impõe tal princípio que, no momento da coleta de dados, o titular seja informado a respeito dos aspectos do tratamento das informações colhidas, como identificação da pessoa responsável pelo banco de dados; finalidade do tratamento; período de conservação dos dados; caráter obrigatório ou facultativo do fornecimento dos dados, e outras informações relevantes para o exercício de seus direitos[522].

Enfim, o princípio da transparência estabelece que o indivíduo seja informado de forma detalhada sobre o tratamento que se oferece aos seus dados. Afronta este princípio o tratamento sub-reptício de dados pessoais, como a coleta não autorizada e às ocultas, feita por meio de *cookies, spywares, keyloggers* e outros dispositivos tecnológicos utilizados para monitoramento eletrônico sem o conhecimento dos internautas – conforme detalhado no item 3.6.

Segundo Pablo Pallazzi, o primeiro componente do princípio da transparência traduz-se na obrigação de se notificar o indivíduo a respeito da coleta de dados pessoais. Dependendo do tipo de dado a ser coletado, requer-se ainda o consentimento expresso do indivíduo. O consentimento expresso pode ser dispensado tão-somente em hipóteses em que os referidos dados são obtidos de fontes de acesso público irrestrito; quando a coleta é exercida pelo próprio Estado; ou quando deriva de uma relação contratual que está sendo firmada[523].

Decorre do princípio da transparência o denominado *direito à informação*. Trata-se da faculdade conferida ao titular de exigir a prestação de informações a respeito do tratamento de seus dados pessoais. Caso os dados sejam utilizados para finalidades diversas daquelas para as quais foram coletados, considera-se que existe um novo tratamento, exigindo-se que o indivíduo seja novamente informado[524].

---

pessoa em causa um tratamento leal dos mesmos". In UNIÃO EUROPÉIA. **Directiva 95/46/CE do Parlamento Europeu e do Conselho da Europa**. Op. cit.

[520] *"(39) A obrigação de informar os assinantes do fim ou fins a que se destinam as listas públicas em que vão ser incluídos os seus dados pessoais deverá caber à parte que recolhe os dados tendo em vista essa inclusão. Nos casos em que os dados possam ser transmitidos a um ou mais terceiros, o assinante deverá ser informado desta possibilidade e do destinatário ou das categorias de possíveis (...)".* In UNIÃO EUROPÉIA. **Directiva 2002/58/CE do Parlamento Europeu e do Conselho da Europa**. Op. cit.

[521] *"Artigo 12. Listas de assinantes 1. Os Estados-Membros assegurarão que os assinantes sejam informados, gratuitamente e antes de serem incluídos nas listas, dos fins a que se destinam as listas de assinantes impressas ou electrónicas publicamente disponíveis ou que podem ser obtidas através de serviços de informações de listas, nas quais os seus dados pessoais podem ser incluídos, bem como de quaisquer outras possibilidades de utilização baseadas em funções de procura incorporadas em versões electrónicas da lista".* In UNIÃO EUROPÉIA. **Directiva 2002/58/CE do Parlamento Europeu e do Conselho da Europa**. Op. cit.

[522] CASTRO, Catarina Sarmento. Op. cit., p. 229.

[523] PALLAZZI, Pablo A. Op. cit. pp. 147-149.

[524] CASTRO, Catarina Sarmento. Op. cit., p. 244.

Nesse sentido, o *direito à informação* obriga que se informe ao titular a respeito de aspectos relacionados ao tratamento de seus dados: identidade do responsável pelo tratamento e, se for o caso, do seu representante; caráter obrigatório ou facultativo das respostas; finalidades do tratamento; destinatários ou pessoas que terão acesso a essas informações; e as condições para o exercício do direito de retificação, atualização ou apagamento. Quando os dados não forem transmitidos pelo próprio titular, essas informações deverão ser fornecidas tanto à pessoa responsável pela comunicação como ao próprio titular[525].

O *direito à informação* pode ser mitigado para preservação de outros valores constitucionais como em casos que envolvem a segurança pública, que exige o tratamento de dados pessoais de forma velada em se tratando de investigação de atividades ilícitas e exercício de atividades de inteligência.

4.5.5 Princípio da proporcionalidade

O disposto na alínea "c" do art. 6º da Directiva 95/46/CE estabelece, em deferência ao princípio da proporcionalidade, que "*os dados pessoais serão adequados, pertinentes e não excessivos relativamente às finalidades para os quais estão sendo recolhidos e para que são tratados posteriormente*"[526]. Também a parte inicial do item 1 do art. 11º da Diretiva 97/66/CE prevê esse mesmo princípio ao declarar que: "*os dados pessoais inseridos em listas impressas ou electrónicas de assinantes acessíveis ao público ou que se possam obter através de serviços de informações telefônicas devem limitar-se ao necessário para identificar um determinado assinante*" [527].

Segundo Pablo Pallazzi, em observância ao princípio da proporcionalidade, não se poderão armazenar informações relativas a obrigações de caráter econômico ou financeiro quando tais informações não se caracterizarem como essenciais aos objetivos propostos ou em caso de dívidas já quitadas. Os organismos públicos, da mesma forma, não poderão comunicar a terceiros – exceto ao Judiciário e desde que resguardado sigilo – informações a respeito de

[525] CASTRO, Catarina Sarmento. Op. cit., pp. 244-245.
[526] UNIÃO EUROPÉIA. **Directiva 95/46/CE do Parlamento Europeu e do Conselho da Europa**. Op. cit.
[527] UNIÃO EUROPÉIA. **Directiva 97/66/CE do Parlamento Europeu e do Conselho da Europa**. Op. cit.

infrações penais ou administrativas prescritas ou quando já houverem sido cumpridas as penas impostas[528].

Assim, o princípio da proporcionalidade impõe a realização de um "juízo de idoneidade" do dado em pauta, para o fim almejado pela coleta, excluindo-se o tratamento de informações não pertinentes à atividade desenvolvida. Caso sejam solicitados ao indivíduo dados inadequados, desnecessários ou desproporcionais aos fins almejados, assegura-se a esse mesmo indivíduo o *direito de opor-se à coleta*, conforme dispõe a alínea "a" do art. 14º da Directiva 95/46/CE[529].

Decorre, portanto, do princípio da proporcionalidade, o chamado *direito de oposição*, isto é, a faculdade de o indivíduo se opor ao tratamento de seus dados pessoais, com base em razões preponderantes e legítimas a serem verificadas no caso concreto. Para isso, deverão ser equacionados tanto os interesses do titular dos dados como também daquele que solicita o fornecimento de informações pessoais alheias, ou seja, deverão ser balanceados os interesses conflitantes, naquela situação particular, em consonância com o *princípio da proporcionalidade*.

Segundo Catarina Sarmento, o *direito de oposição* apresenta-se como uma conseqüência do direito de cada indivíduo de controlar o tratamento de seus dados pessoais. Abarca tanto o direito de negar qualquer pedido de informação, como também o direito de opor-se ao tratamento dos próprios dados pessoais quando essas informações tiverem sido fornecidas por terceiros[530].

O referido direito poderá ser negado tão-somente em situações em que a coleta se impuser por dispositivo legal, como em casos de fornecimento de informações ao poder público para efeitos fiscais; ou quando a medida for essencial à preservação de um interesse público, como combate e prevenção a epidemias, investigação criminal, segurança pública e prevenção a infrações penais.

Assim, diante da obrigação legal ou da necessidade de prestação da informação para preservação de interesse público, o direito de oposição não prevalecerá, sendo obrigatório o fornecimento de dados pessoais. De outro lado, sempre que a solicitação de dados pessoais for

---

[528] PALLAZZI, Pablo A. Op. cit. pp. 176-177.

[529] *"Art. 14º Direito de oposição da pessoa em causa Os Estados-membros reconhecerão à pessoa em causa o direito de: a) Pelo menos nos casos referidos nas alíneas e) e f) do artigo 7º, se opor em qualquer altura, por razões preponderantes e legítimas relacionadas com a sua situação particular, a que os dados que lhe digam respeito sejam objecto de tratamento, salvo disposição em contrário do direito nacional. Em caso de oposição justificada, o tratamento efectuado pelo responsável deixa de poder incidir sobre esses dados;"*. In UNIÃO EUROPÉIA. **Directiva 95/46/CE do Parlamento Europeu e do Conselho da Europa**. Op. cit.

[530] CASTRO, Catarina Sarmento. Op. cit., p. 254

legitimamente considerada inadequada e desnecessária ao cumprimento dos objetivos propostos, o indivíduo poderá negar o pedido de informação, preservando-se a privacidade.

4.5.6 Princípio da veracidade

A alínea "d" do item 1 do art. 6º da Directiva 95/46/CE assegura o referido princípio, nos seguintes termos: "*Artigo 6º 1. Os Estados-membros devem estabelecer que os dados pessoais serão: (...) d) Exactos e, se necessário, actualizados; devem ser tomadas todas as medidas razoáveis para assegurar que os dados inexactos ou incompletos, tendo em conta as finalidades para que foram recolhidos ou para que são tratados posteriormente, sejam apagados ou rectificados;*"[531].

Também é conhecido como *princípio da exatidão e atualização dos dados.* Dispõe que os dados pessoais arquivados sejam verdadeiros; garantindo-se ao seu titular o direito de corrigir as informações incorretas ou obsoletas, bem como apagar dados impertinentes. A falta de correção ou de atualização de informações pessoais pode causar sérios prejuízos ao seu titular, daí a obrigação de os responsáveis por bancos de dados atualizá-los sempre que tais correções se impuserem como necessárias[532].

Para o titular corrigir dados incorretos ou alterar dados desatualizados, deve-se a ele conferir, primeiro, o chamado *direito de acesso*. O referido direito possibilita ao titular o devido acesso aos dados para conhecê-los e, desta forma, modificar ou atualizar as informações armazenadas. É dispensável a apresentação de justificativas, estejam os dados armazenados em entes públicos ou privados. A informação deve ser prestada em um prazo razoável e de forma inteligível.

Segundo Catarina Sarmento, o acesso pode ser direto ou indireto. O *acesso direto* se consuma mediante ação do próprio titular dos dados. Promove-se o *acesso indireto* mediante ação de um terceiro, quando as informações são classificadas como sigilosas ou quando se armazenam em um sistema informático de uso restrito cujo acesso se permite a um estreito

[531] UNIÃO EUROPÉIA. **Directiva 95/46/CE do Parlamento Europeu e do Conselho da Europa**. Op. cit.
[532] CASTRO, Catarina Sarmento. Op. cit., p. 237.

círculo de pessoas. Outra forma de acesso indireto diz respeito aos dados de saúde armazenados por um médico indicado pelo titular, que pode preferir não conhecer os resultados de seus exames[533].

No ordenamento jurídico nacional, o *direito de acesso* a informações de caráter pessoal encontra-se regulamentado pelo parágrafo único do art. 7º da Lei nº 11.111/05 e pela Lei nº 9.507/97 (Lei do *Habeas Data*), conforme visto no item 4.4. Informações classificadas como sigilosas devem ser acessadas indiretamente, a partir da elaboração de um "extrato" do documento sigiloso, revelando-se apenas as informações relacionadas ao indivíduo, subtraindo-se o restante do conteúdo cujo acesso se restringe apenas a quem tenha *necessidade de conhecer* tais dados[534] e seja portador de *credencial de segurança*[535], em conformidade com o descrito no item 1.6, quando se tratou da questão do sigilo para preservação da segurança da sociedade e do Estado.

4.5.7 Princípio da caducidade

Previsto na alínea "e" do art. 6º da Directiva 95/46/CE, o princípio da caducidade estipula que "*os dados pessoais serão conservados de forma a permitir a identificação das pessoas em causa apenas durante o período necessário para a prossecução das finalidades para que foram recolhidos ou para que foram tratados posteriormente*"[536]. E, também, no item 23 do preâmbulo da Directiva 2002/58/CE: "*(23) (...) A comunicação registada deve ser eliminada o mais rapidamente possível e, em todo o caso, o mais tardar até ao termo do período em que a transacção pode ser legalmente impugnada*"[537].

Estabelece que os dados devam ser apagados assim que se atingirem os objetivos para os quais foram colhidos. Assim, dados coletados para celebração de um contrato devem ser

---

[533] CASTRO, Catarina Sarmento. Op. cit., pp. 248-249.
[534] Ver item 3.7.
[535] "*Art. 4º Para os efeitos deste Decreto, são estabelecidos os seguintes conceitos e definições: (...) IV - credencial de segurança: certificado, concedido por autoridade competente, que habilita determinada pessoa a ter acesso a dados ou informações em diferentes graus de sigilo*;". In BRASIL. **Decreto nº 4.553, de 27 de dezembro de 2002**. Op. cit.
[536] UNIÃO EUROPÉIA. **Directiva 95/46/CE do Parlamento Europeu e do Conselho da Europa**. Op. cit.
[537] UNIÃO EUROPÉIA. **Directiva 2002/58/CE do Parlamento Europeu e do Conselho da Europa**. Op. cit.

imediatamente apagados após a prescrição das obrigações estipuladas. Proíbe-se, desta forma, o armazenamento de dados pessoais além do tempo necessário ao cumprimento da finalidade para a qual foram coletados. Excepcionalmente, alguns dados serão armazenados por tempo indeterminado pelo Estado – como ocorre com dados relacionados à identificação civil do cidadão – mas a regra geral é o apagamento após o cumprimento dos objetivos propostos.

Decorre, portanto, do princípio da caducidade o chamado *direito ao apagamento* ou *direito ao esquecimento*. O referido direito faculta ao indivíduo exigir o apagamento de seus dados pessoais, após o período necessário ao cumprimento das finalidades determinantes da coleta, especialmente diante dos novos recursos da tecnologia da informação "que não esquecem" e que não possuem "limites físicos" ao armazenamento de tais informações[538]. O poder que a tecnologia atualmente atingiu eleva-se a patamares tais que se recomenda seja estipulado um limite temporal ao armazenamento de informações pessoais, sob pena de permanecerem registradas indefinidamente; o que afetaria não só a privacidade informacional, mas especialmente o poder de autodeterminação do titular de tais dados.

Um caso interessante na jurisprudência nacional, que espelha o direito ao esquecimento ou direito ao apagamento dos dados, foi julgado pelo STJ, no que se refere ao armazenamento de dados pessoais pelos institutos de identificação criminal, *verbis*:

> EMENTA. RECURSO ORDINÁRIO. PENAL. INQUÉRITO POLICIAL. ARQUIVAMENTO. EXCLUSÃO DE DADOS DOS TERMINAIS DO INSTITUTO DE IDENTIFICAÇÃO. SIGILO DAS INFORMAÇÕES.
> Por analogia ao art. 748 do CPP – que assegura ao reabilitado o sigilo das condenações criminais anteriores na sua folha de antecedentes –, esta Corte Superior tem entendido que devem ser excluídos dos terminais dos Institutos de Identificação Criminal os dados relativos a inquéritos arquivados, de modo a preservar a intimidade do indivíduo".Precedentes. Recurso conhecido e provido[539].

Mais um julgado curioso na jurisprudência do STJ – também relacionado com o direito ao esquecimento ou direito ao pagamento dos dados – refere-se ao arquivamento de dados pessoais pelo Serviço de Proteção ao Crédito – SPC. O relator, ministro Rui Rosado de Aguiar, entendeu que o ordenamento jurídico nacional não permite o armazenamento de dados pessoais de

[538] CASTRO, Catarina Sarmento. Op. cit., pp. 239-240.
[539] BRASIL. Superior Tribunal de Justiça. RHC nº 14376/SP. Recorrente: Fabrício Feres Rosin. Relator: José Arnaldo da Fonseca. Brasília, DF, 02 de março de 2004. **Diário da Justiça da República Federativa do Brasil**, Brasília, DF, 29 mar. 2004, p. 254. Disponível em <http://www.stj.gov.br/SCON/jurisprudencia>. Acesso em: 30 jan. 2007. Grifos nossos.

conteúdo negativo por prazo indefinido, determinando o apagamento de tais informações do sistema informático do SPC. É o que se lê na seguinte passagem de seu voto:

> O Serviço de Proteção ao Crédito (SPC), instituído em diversas cidades pelas entidades de classe de comerciantes e lojistas, tem a finalidade de informar seus associados sobre a existência de débitos pendentes por comprador que pretenda obter novo financiamento. É evidente o benefício que dele decorre em favor da agilidade e segurança das operações comerciais, assim como não se pode negar ao vendedor o direito de informar-se sobre o crédito de seu cliente na praça, e de repartir com os demais os dados que dele dispõe. Essa atividade, porém, em razão de sua própria importância social e dos graves efeitos dela decorrentes – pois para inscrição em concurso público tem sido exigida certidão negativa no SPC – deve ser exercida dentro dos limites que, permitindo a realização de sua atividade, não se transforme em causa de dano social maior do que o bem visado. Em primeiro lugar, é preciso admitir que tal registro só pode ser feito com o conhecimento do interessado, a fim de habilitá-lo a tomar as medidas cabíveis, fundadas na defesa que tiver, inclusive da inexistência do débito. Depois, impende que tal registro não seja perpétuo. O nosso sistema jurídico não autoriza a indefinida permanência dos registros negativos nem para as sentenças criminais condenatórias, cujos efeitos desaparecem pelo simples efeito do tempo (...). No caso dos autos, o cancelamento dos registros feitos há mais de cinco anos, como ficou reconhecido no acórdão, está de acordo com a regra do art. 43, § 1º do CDC.[540]

No ordenamento jurídico nacional, o direito ao apagamento está previsto no art. 748 do Código de Processo Penal – CPP, que determina a exclusão de anotações concernentes a condenações anteriores constantes nos registros dos reabilitados[541]; e no § 1º do art. 43 do CDC, aprovado pela Lei nº 8.078, de 11 de setembro de 1990, que estipula prazo máximo de 5 (cinco) anos para o armazenamento de informações negativas sobre consumidores, nos seguintes termos: *"§ 1° Os cadastros e dados de consumidores devem ser objetivos, claros, verdadeiros e em linguagem de fácil compreensão, não podendo conter informações negativas referentes a período superior a cinco anos*"[542]. Observa-se que o referido dispositivo também expressa o princípio da veracidade – descrito no item anterior – ao exigir que os dados armazenados sejam claros e verdadeiros.

---

[540] BRASIL. Superior Tribunal de Justiça. RESP nº 22337/RS. Recorrente: Clube de Diretores Logistas de Passo Fundo-RS. Relator: Rui Rosado de Aguiar. Brasília, DF, 13 de fevereiro de 1995. **Diário da Justiça da República Federativa do Brasil**, Brasília, DF, 20 mar. 1995, p. 205. Disponível em <http://www.stj.gov.br/SCON/jurisprudencia>. Acesso em: 30 jan. 2007. Grifos nossos.

[541] "*Art. 748. A condenação ou condenações anteriores não serão mencionadas na folha de antecedentes do reabilitado, nem em certidão extraída dos livros do juízo, salvo quando requisitadas por juiz criminal*". In BRASIL. Código de Processo Penal. **Decreto-lei nº 3.689, de 03 de outubro de 1941**. Disponível em: <http://www.planalto.gov.br/ccivil_03/Decreto-Lei/Del3689.htm>. Acesso em: 30 jan. 2007.

[542] BRASIL. **Lei nº 8.078, de 11 de setembro de 1990**. Op. cit.

4.5.8 Princípio da segurança no tratamento

O princípio da segurança encontra-se previsto em diversos dispositivos das Directivas do Parlamento Europeu e do Conselho da Europa, destacando-se os seguintes:

> Artigo 17º Segurança do tratamento
> 1. Os Estados-membros estabelecerão que o responsável pelo tratamento deve pôr em prática medidas técnicas e organizativas adequadas para proteger os dados pessoais contra a destruição acidental ou ilícita, a perda acidental, a alteração, a difusão ou acesso não autorizados, nomeadamente quando o tratamento implicar a sua transmissão por rede, e contra qualquer outra forma de tratamento ilícito. Estas medidas devem assegurar, atendendo aos conhecimentos técnicos disponíveis e aos custos resultantes da sua aplicação, um nível de segurança adequado em relação aos riscos que o tratamento apresenta e à natureza dos dados a proteger.
> 2. Os Estados-membros estabelecerão que o responsável pelo tratamento, em caso de tratamento por sua conta, deverá escolher um subcontratante que ofereça garantias suficientes em relação às medidas de segurança técnica e de organização do tratamento a efectuar e deverá zelar pelo cumprimento dessas medidas.[543]

> Artigo 4º Segurança
> 1. O fornecedor de um serviço de telecomunicações acessível ao público deve adoptar as medidas técnicas e organizacionais adequadas para garantir a segurança dos seus serviços, se necessário conjuntamente com o fornecedor da rede pública de telecomunicações no que respeita à segurança da rede. Tendo em conta o estado da técnica e os custos da sua aplicação, essas medidas devem assegurar um nível de segurança adequado aos riscos existentes.
> 2. Em caso de risco especial de violação da segurança da rede, o fornecedor de um serviço de telecomunicações acessível ao público deve informar os assinantes acerca desse risco e das soluções possíveis, incluindo os respectivos custos.[544]

> Artigo 4º Segurança
> 1. O prestador de um serviço de comunicações electrónicas publicamente disponível adoptará as medidas técnicas e organizativas adequadas para garantir a segurança dos seus serviços, se necessário conjuntamente com o fornecedor da rede pública de comunicações no que respeita à segurança da rede. Tendo em conta o estado da técnica e os custos da sua aplicação, essas medidas asseguram um nível de segurança adequado aos riscos existentes.
> 2. Em caso de risco especial de violação da segurança da rede, o prestador de um serviço de comunicações electrónicas publicamente disponível informará os assinantes desse risco e, sempre que o risco se situe fora do âmbito das medidas

[543] UNIÃO EUROPÉIA. **Directiva 95/46/CE do Parlamento Europeu e do Conselho da Europa**. Op. cit.
[544] UNIÃO EUROPÉIA. **Directiva 97/66/CE do Parlamento Europeu e do Conselho da Europa**. Op. cit. Grifos nossos.

> a tomar pelo prestador do serviço, das soluções possíveis, incluindo uma indicação dos custos prováveis daí decorrentes.[545]
>
> Artigo 7º Protecção de dados e segurança dos dados Sem prejuízo das disposições adoptadas nos termos da Directiva 95/46/CE e da Directiva 2002/58/CE, cada Estado-Membro deve assegurar que os fornecedores de serviços de comunicações electrónicas publicamente disponíveis ou de uma rede pública de comunicações respeitem, no mínimo, os seguintes princípios em matéria de segurança de dados no que se refere aos dados conservados em conformidade com a presente directiva:
> a) Os dados conservados devem ser da mesma qualidade e estar sujeitos à mesma protecção e segurança que os dados na rede;
> b) Os dados devem ser objecto de medidas técnicas e organizativas adequadas que os protejam da destruição acidental ou ilícita, da perda ou alteração acidental, ou do armazenamento, tratamento, acesso ou divulgação não autorizado ou ilícito;
> c) Os dados devem ser objecto de medidas técnicas e organizativas adequadas para garantir que apenas pessoas especialmente autorizadas tenham acesso aos dados;e
> d) Os dados devem ser destruídos no final do período de conservação, excepto os dados que tenham sido facultados e preservados.[546]

O princípio da segurança no tratamento determina que o responsável por bancos de dados nos quais são armazenados dados pessoais adote *medidas técnicas e administrativas* que garantam a segurança de tais informações, protegendo-as do acesso não autorizado (comprometimento do *sigilo*), da alteração (comprometimento da *integridade*) e da destruição (comprometimento da *disponibilidade*), além da exploração de outras *vulnerabilidades*[547]. A exigência de adoção de medidas de segurança no tratamento de dados pessoais impõe-se como requisito essencial, visto tratar-se de uma atividade de risco. Conforme exposto no item 4.2, caso alguém ilicitamente acesse informações pessoais armazenadas em um determinado banco de dados – público ou privado – acarretando dano ao seu titular, aquele que registrou tais dados será responsabilizado pela não adoção dos cuidados devidos para a proteção dessas informações.

[545] UNIÃO EUROPÉIA. **Directiva 2002/58/CE do Parlamento Europeu e do Conselho da Europa**. Op. cit. Grifos nossos.
[546] UNIÃO EUROPÉIA. **Directiva 2006/24/CE do Parlamento Europeu e do Conselho da Europa**. Op. cit. Grifos nossos.
[547] Ver item 3.3.

4.5.9 Princípio da confidencialidade

Relacionado com o princípio da segurança no tratamento, destaca-se o *princípio da confidencialidade* dos dados coletados. Encontra-se previsto expressamente no art. 16º da Directiva 95/46/CE[548] e no art. 5º da Directiva 2002/58/CE[549].

Este princípio impõe o *dever de sigilo* no que se refere ao tratamento de dados pessoais. A divulgação a terceiros, inclusive a outros órgãos governamentais, sem autorização do titular dos dados em questão, implica a violação deste princípio e também do princípio da lealdade ou da boa fé, exceto se tal procedimento for necessário à preservação de outros valores constitucionais considerados preponderantes em relação à privacidade do titular dos dados na análise do caso concreto.

No ordenamento jurídico nacional, destacam-se como informações sigilosas os dados pessoais, independentemente de qualquer classificação de sigilo, por força do disposto no § 4º do art. 23 da Lei nº 8.159/91[550] regulamentado pelo art. 2º do Decreto nº 4.553/02[551]. Assim, toda a

---

548 "*Artigo 16º Confidencialidade do tratamento Qualquer pessoa que, agindo sob a autoridade do responsável pelo tratamento ou do subcontratante, bem como o próprio subcontratante, tenha acesso a dados pessoais, não procederá ao seu tratamento sem instruções do responsável pelo tratamento, salvo por força de obrigações legais*". In UNIÃO EUROPÉIA. **Directiva 95/46/CE do Parlamento Europeu e do Conselho da Europa**. Op. cit.

549 "*Artigo 5.o Confidencialidade das comunicações 1. Os Estados-Membros garantirão, através da sua legislação nacional, a confidencialidade das comunicações e respectivos dados de tráfego realizadas através de redes públicas de comunicações e de serviços de comunicações electrónicas publicamente disponíveis. Proibirão, nomeadamente, a escuta, a instalação de dispositivos de escuta, o armazenamento ou outras formas de intercepção ou vigilância de comunicações e dos respectivos dados de tráfego por pessoas que não os utilizadores, sem o consentimento dos utilizadores em causa, excepto quando legalmente autorizados a fazê-lo, de acordo com o disposto no n.o 1 do artigo 15.o O presente número não impede o armazenamento técnico que é necessário para o envio de uma comunicação, sem prejuízo do princípio da confidencialidade. 2. O n.o 1 não se aplica às gravações legalmente autorizadas de comunicações e dos respectivos dados de tráfego, quando realizadas no âmbito de práticas comerciais lícitas para o efeito de constituir prova de uma transacção comercial ou de outra comunicação de negócios 3. Os Estados-Membros velarão por que a utilização de redes de comunicações electrónicas para a armazenagem de informações ou para obter acesso à informação armazenada no equipamento terminal de um assinante ou utilizador só seja permitida na condição de serem fornecidas ao assinante ou ao utilizador em causa informações claras e completas, nomeadamente sobre os objectivos do processamento, em conformidade com a Directiva 95/46/CE, e de lhe ter sido dado, pelo controlador dos dados, o direito de recusar esse processamento. Tal não impedirá qualquer armazenamento técnico ou acesso que tenham como finalidade exclusiva efectuar ou facilitar a transmissão de uma comunicação através de uma rede de comunicações electrónicas, ou que sejam estritamente necessários para fornecer um serviço no âmbito da sociedade de informação que tenha sido explicitamente solicitado pelo assinante ou pelo utilizador*". In UNIÃO EUROPÉIA. **Directiva 2002/58/CE do Parlamento Europeu e do Conselho da Europa**. Op. cit. Grifos nossos.

550 "*§ 1º Os documentos cuja divulgação ponha em risco a segurança da sociedade e do Estado, bem como aqueles necessários ao resguardo da inviolabilidade da intimidade, da vida privada, da honra e da imagem das pessoas são originariamente sigilosos*". In BRASIL. **Lei nº 8.159, de 08 de janeiro de 1991**. Op. cit.

regulamentação relacionada com a proteção de informações classificadas, no que se refere à garantia da *confidencialidade* dessas mesmas informações é aplicável aos dados pessoais. Destacam-se os seguintes dispositivos, apenas para fins didáticos:

> Art. 2º A Política Nacional de Informática tem por objetivo a capacitação nacional nas atividades de informática, em proveito do desenvolvimento social, cultural, político, tecnológico e econômico da sociedade brasileira, atendidos os seguintes princípios:
> .....
> VIII - estabelecimento de mecanismos e instrumentos legais e técnicos para a proteção do sigilo dos dados armazenados, processados e veiculados, do interesse da privacidade e de segurança das pessoas físicas e jurídicas, privadas e públicas;[552]
>
> Art. 5º As alterações relevantes no patrimônio da autoridade pública deverão ser imediatamente comunicadas à CEP, especialmente quando se tratar de:
> .....
> § 4º A fim de preservar o caráter sigiloso das informações pertinentes à situação patrimonial da autoridade pública, as comunicações e consultas, após serem conferidas e respondidas, serão acondicionadas em envelope lacrado, que somente poderá ser aberto por determinação da Comissão;[553]
>
> Art. 198. Sem prejuízo do disposto na legislação criminal, é vedada a divulgação, por parte da Fazenda Pública ou de seus servidores, de informação obtida em razão do ofício sobre a situação econômica ou financeira do sujeito passivo ou de terceiros e sobre a natureza e o estado de seus negócios ou atividades.[554]

4.5.10 Princípio do não tratamento de dados sensíveis

Este princípio está regulado no art. 8º da Directiva 95/46/CE: *"Artigo 8º Tratamento de certas categorias específicas de dados 1. Os Estados-membros proibirão o tratamento de dados*

---

[551] "*Art. 2º São considerados originariamente sigilosos, e serão como tal classificados, dados ou informações cujo conhecimento irrestrito ou divulgação possa acarretar qualquer risco à segurança da sociedade e do Estado, bem como aqueles necessários ao resguardo da inviolabilidade da intimidade da vida privada, da honra e da imagem das pessoas. Parágrafo único. O acesso a dados ou informações sigilosos é restrito e condicionado à necessidade de conhecer*". In BRASIL. **Decreto nº 4.553, de 27 de dezembro de 2002**. Op. cit.

[552] BRASIL. **Lei nº 7.232, de 29 de outubro de 1984**. Op. cit. Grifos nossos.

[553] BRASIL. **Código de Conduta da Alta Administração, de 21 de agosto de 2000**. Disponível em: <http://www.planalto.gov.br/ccivil_03/Codigos/codi_Conduta/Cod_conduta.htm#codigoconduta>. Acesso em: 30 jan. 2007. Grifos nossos.

[554] BRASIL. **Lei nº 5.172, de 25 de outubro de 1966**. Op. cit.

pessoais que revelem a origem racial ou étnica, as opiniões políticas, as convicções religiosas ou filosóficas, a filiação sindical, bem como o tratamento de dados relativos à saúde ou à vida sexual (...)"[555].

Conforme exposto no item 4.2, dados sensíveis apresentam-se como aqueles que pertencem ao círculo da intimidade ou esfera confidencial do indivíduo, por se referirem a aspectos mais íntimos. Em regra, só podem ser submetidos a tratamento após prévia permissão do titular ou de seu representante. Excepcionalmente, esses dados podem ser recolhidos sem o consentimento do titular, caso haja autorização legal, e também para preservação de outros interesses públicos, como para fins estatísticos ou científicos. Nestes casos, recomenda-se que se evite a identificação de seus titulares[556]. Todavia, em um ou em outro caso deverão ser adotadas medidas especiais de segurança para que se assegure a integridade, a autenticidade e o sigilo de tais informações durante o tratamento.

Segundo Catarina Sarmento, a "sensibilidade" dos dados deve ser avaliada no caso concreto, já que alguns dados, apesar de não parecerem sensíveis, em certas circunstâncias podem macular a intimidade de seus titulares e serem utilizados como fator de discriminação, como nos casos em que o nome revela a origem racial ou étnica. Outros dados já se configuram intrinsecamente sensíveis, como ocorre com aqueles relacionados a origem racial ou ética, a opiniões políticas, a convicções religiosas ou filosóficas, a filiação sindical, a saúde e a vida sexual, incluindo os dados genéticos – daí a expressa previsão de mecanismos especiais de proteção na Directiva 95/46/CE[557].

Ressalte-se que o tratamento de dados sensíveis exige a adoção de medidas e de procedimentos mais rigorosos de segurança, tais como a autenticação de quem acessa o sistema informático; acesso restrito à instalação física, em que o sistema informático se localiza; destruição automática dos dados após o cumprimento das finalidades determinantes da coleta; uso de criptografia para cifragem do conteúdo; dentre outros.

[555] UNIÃO EUROPÉIA. **Directiva 95/46/CE do Parlamento Europeu e do Conselho da Europa**. Op. cit.
[556] PALLAZZI, Pablo A. Op. cit. pp. 156-157.
[557] CASTRO, Catarina Sarmento. Op. cit., pp. 89-90.

4.5.11 Princípio da reciprocidade das vantagens

Determina o princípio da reciprocidade das vantagens que os mesmos meios adotados para a coleta de dados pessoais sejam utilizados também para o exercício dos direitos conferidos aos seus titulares, como o *direito de oposição*, descrito no item 4.5.5; e o *direito de acesso*, exposto no item 4.5.6. Assim, se a coleta se processa por meio da internet, o direito de acesso aos próprios dados e o direito de oposição também deverão ser exercidos por esse canal de comunicação, mediante um simples *click* de um *mouse*, ou seja, devem ser adotados os mesmos meios para o titular dos dados exercer mais facilmente os seus direitos[558]. Evita-se, desta forma, um desequilíbrio na relação jurídica entre os responsáveis pela coleta de dados pessoais – sejam estes representantes de entes públicos ou privados – e os titulares dos referidos dados.

4.5.12 Princípio da responsabilidade objetiva

Dispõe o princípio da responsabilidade objetiva que os indivíduos que controlam as bases de dados devam ser responsabilizados pelos danos decorrentes do descumprimento ou desrespeito de todos os princípios arrolados nos itens anteriores – independentemente de terem agido com dolo ou com culpa. O tratamento de dados pessoais impõe-se como uma atividade de risco, implicando a responsabilização objetiva e o dever de indenizar por qualquer incidente ou quebra de segurança que cause danos morais ou materiais ao titular, como a violação do sigilo ou da integridade das informações.

O referido princípio encontra-se previsto no art. 23 da Directiva 95/46/CE: "*Artigo 23º Responsabilidade 1. Os Estados-membros estabelecerão que qualquer pessoa que tiver sofrido um prejuízo devido ao tratamento ilícito de dados ou a qualquer outro acto incompatível com as disposições nacionais de execução da presente directiva tem o direito de obter do responsável pelo tratamento a reparação pelo prejuízo sofrido. 2. O responsável pelo tratamento poderá ser*

[558] CORREIA, Miguel Pupo. Op. cit., p. 340.

parcial ou totalmente exonerado desta responsabilidade se provar que o facto que causou o dano lhe não é imputável"[559].

4.6 Regulamentação do direito à autodeterminação informativa

Diante de todo o exposto ao longo deste capítulo, observa-se a fragilidade da privacidade diante dos novos recursos tecnológicos que facilitam o monitoramento e a devassa da intimidade dos indivíduos, situação que se materializa também na indiscriminada coleta, armazenamento e interconexão de dados pessoais. Para minimizar os impactos produzidos pela tecnologia, vários países têm editado legislações específicas a respeito da proteção de dados pessoais, especialmente diante dos recursos automatizados. Busca-se, desta forma, preservar a autonomia de cada indivíduo no controle de suas próprias informações. Essa nova faceta da privacidade – conforme visto no item 1.2 – é chamada pela doutrina *privacidade informacional* ou *direito à autodeterminação informativa*.

Consoante apresentado no item 2.4.2.4.2, o referido direito foi reconhecido, pela primeira vez, pela Corte Constitucional Alemã, em decisão datada de 15 de dezembro de 1983, que declarou a inconstitucionalidade parcial da Lei do Censo (*Volkszählungsgesetz*) de 1983, no que dizia respeito à obrigatoriedade, por parte dos cidadãos alemães, de responderem um questionário com informações pessoais. Objetivava-se reunir dados com fins estatísticos; formar um banco de dados para posterior confrontação com informações já existentes nos registros públicos; e transmitir essas informações recolhidas para outras entidades públicas federais, estaduais e municipais.

A opinião pública despertou para o temor de que tais informações fossem utilizadas para controle do comportamento dos cidadãos, ensejando recurso à Corte Constitucional que, na decisão, considerou a necessidade do respeito à personalidade diante dos riscos que a informática desvela[560]. O Tribunal julgou nulo o dispositivo que previa a possibilidade de transmissão de dados para outras entidades, bem como aquele que autorizava a interconexão e a comparação das

[559] UNIÃO EUROPÉIA. **Directiva 95/46/CE do Parlamento Europeu e do Conselho da Europa**. Op. cit.
[560] SAMPAIO, José Adércio. Op. cit., p.476.

informações coletadas com registros já existentes, declarando a inconstitucionalidade parcial da Lei do Censo. A decisão fundamentou-se no reconhecimento do *Recht auf Informationelle Selbstbestimmung* ou *direito à autodeterminação informativa*, ou seja, no direito que se outorga ao indivíduo de controlar e de proteger dados pessoais – opondo-se à coleta, ao armazenamento, à difusão ou a qualquer outra espécie de tratamento irrestrito e não autorizado. Incidentalmente, a Corte ainda conferiu status constitucional à Agência de Proteção de Dados Pessoais, frisando que sua existência se impunha como indispensável à fiscalização e ao controle do tratamento de dados pessoais e à proteção da privacidade dos cidadãos.

Tal decisão representa um grande marco no estudo da conformação do direito à privacidade. Antes visto como uma garantia de *caráter negativo*, ou seja, um manto protetor contra intromissões alheias, o direito à privacidade passou a ser reconhecido também como uma garantia de *caráter positivo*, isto é, revestiu-se da prerrogativa de exigir do Estado o cumprimento de ações positivas para o resguardo da incolumidade da intimidade e da vida privada. Assim, enquanto *direito a prestação* – na modalidade *direito à organização e ao procedimento* – a efetiva proteção da privacidade passou a depender de uma atuação positiva do poder público, no sentido de garantir a não intromissão de terceiros mediante implementação de *medidas administrativas* e *legislativas*; vedando-se a omissão estatal.

Na *via administrativa*, destaca-se a necessidade de criação de uma entidade ou designação de um órgão já existente para a tarefa de fiscalizar e de controlar o tratamento de dados pessoais no setor público e no setor privado. Ressalte-se a importância de se conferir independência funcional a essa agência, comissão ou departamento – conforme seja chamado – em relação aos demais órgãos do governo e às entidades reguladas. De acordo com o exposto no item 4.3, o referido órgão deve exercer funções consultivas, de decisão administrativa, de investigação, de sanção, de representação internacional, de treinamento e de esclarecimento – garantindo-se a imparcialidade de suas deliberações.

Dentre as várias outras *medidas administrativas* cabíveis, salienta-se a necessidade de: (a) sensibilização da população – especialmente das crianças, idosos e adolescentes – para os riscos inerentes à devassa de seus dados pessoais, estimulando o uso mais consciente dos novos aparatos tecnológicos; (b) desenvolvimento de aplicativos e sistemas informáticos que preservem a privacidade dos usuários; (c) fomento de *tecnologias de liberdade* como a criptografia utilizada para garantir o sigilo do conteúdo das comunicações; (d) proteção das bases de dados e dos

sistemas informáticos públicos, evitando-se o acesso por pessoas não autorizadas; (e) treinamento dos servidores públicos que, para o desempenho de funções, cargos ou atividades, dediquem-se ao tratamento de dados pessoais; (f) estruturação interna – dentro de cada órgão público – de um sistema de controle do tratamento de dados pessoais; (g) implementação de mecanismos mais eficientes para o exercício do *direito de acesso*[561] aos próprios dados pessoais constantes nas bases de dados e sistemas informáticos públicos; (h) investimento na área de segurança da informação; (i) definição de procedimentos de segurança para os serviços de *governo eletrônico*[562]; (j) vinculação dos órgãos públicos – no desempenho de suas competências – aos princípios relacionados à proteção de dados pessoais descritos no item anterior; (k) instauração de processos administrativos disciplinares pelo descumprimento das normas de segurança e dos princípios relacionados à proteção de dados pessoais; (l) regulamentação da interconexão de informações armazenadas em diferentes bases de dados públicas.

Enfim, as *medidas administrativas* arroladas representam apenas um referencial a ser seguido pelo poder público. Correspondem a uma obrigação do Estado de implementar os pressupostos fáticos necessários ao exercício efetivo do direito à privacidade diante dos riscos e das ameaças da sociedade da informação. Referem-se, portanto, à implementação das condições materiais para que os cidadãos se libertem da condição de mero "objeto" de informação do poder público e do setor privado – no contexto do tratamento automatizado de dados pessoais com o incremento da tecnologia da informação.

Nesse contexto, as *medidas legislativas* atuam apenas em complementação às medidas de caráter administrativo, impondo certos limites ao tratamento de dados pessoais, bem como conferindo a seus titulares um nível de proteção mais elevado diante dos novos recursos tecnológicos. Destaque-se a necessidade de regulamentação dos procedimentos de segurança a serem adotados por setores responsáveis pelo tratamento de dados pessoais, para que se garanta a integridade, a autenticidade, a disponibilidade e o sigilo dessas informações – os quatro pilares da segurança da informação. Atente-se, ainda, para a necessidade de previsão expressa dos princípios relacionados à proteção dos dados pessoais, bem como dos direitos garantidos aos titulares dos dados como, o direito à informação, o direito de oposição, o direito de acesso e o direito ao apagamento – todos descritos no item anterior.

[561] Direito do titular dos dados de aceder aos mesmos para conhecê-los e, desta forma, poder modificá-los ou atualizá-los. Ver item 4.5.6.
[562] Ver, no item 3.3, a relação das atividades de governo eletrônico.

Seria possível argumentar que essa regulamentação por legislação específica não se faz necessária, tendo em vista o amplo arcabouço normativo já existente em matéria de proteção da intimidade e vida privada das pessoas – conforme visto no item 4.4. Todavia, verifica-se que o direito à autodeterminação informativa – embora se apresente como uma faceta do direito à privacidade – pode se configurar como um direito autônomo. Ressalte-se que esse direito está voltado para era da tecnologia da informação – esta nova fase de desenvolvimento político, social e econômico em que as informações pessoais são até mesmo comercializadas entre os prestadores de serviço da sociedade da informação, para fins de publicidade e *marketing*.

Outros poderiam combater a regulamentação estatal, defendendo a auto-regulamentação por meio das denominadas *soft-laws*, ou seja, códigos de boa-conduta e políticas de privacidade estipuladas pelos próprios prestadores de serviço da sociedade da informação. Esse mecanismo, apesar de muito comum nos EUA, ao longo dos anos tem demonstrado sua ineficiência diante da carência de medidas sancionadoras que coíbam o descumprimento dos princípios relacionados com a proteção de dados pessoais e da dificuldade de exercício dos direitos pelos titulares das informações, em especial do direito de oposição à coleta. Ademais, verifica-se a inaptidão desse sistema para resolução do problema do tratamento de dados pessoais em âmbito público. Em conformidade ao disposto no item 3.3, se a informação se apresenta como o novo "petróleo" da sociedade da informação, as bases de dados públicas configuram-se como o seu principal "jazigo". Isto demonstra que a maior vulnerabilidade em relação ao tratamento de dados pessoais aponta para o setor público propriamente dito, considerando-se que nas bases de dados públicas se armazenam informações criminais, previdenciárias, fiscais, eleitorais, financeiras, dentre tantas outras de caráter sensível.

A respeito da auto-regulamentação, esclarecedoras são as palavras de Hermínia Campuzano Tomé:

> <<autorregulación empresarial>> Este mecanismo supone la adopción, por parte de las empresas, de códigos de conducta a través de los cuales se comprometen a practicar una política de respeto a la vida privada y la confidencialidad de los datos personales. Tales códigos no tienen un carácter obligatoria, sino voluntario, (...) Ello no significa menoscabo del papel importante que puedan desempeñar, si bien no pueden erigirse como único instrumento de protección frente a las intrusiones del sector privado. La autorregulación empresarial debe ir acompañada de normas concretas que permitan a los usuarios hacer efectivas sus reclamaciones. En general, las leyes de protección de datos personales no se ocupan adecuadamente del tema. No obstante, la dimension real que en los últimos anõs el problema ha ido adquiriendo ha llevado a algún país adoptar leyes específicas de protección de la vida privada frente al sector privado.

> Concretamente destaca Canadá, uno de los países que más preocupación demuestra por el tema. (...) En 1996, el Consejo Canadiense declaró el Código de la CSA norma nacional, haciendo de Canadá el primer país del mundo que ha adoptado este tipo de normas[563].

Assim, sustenta-se a necessidade de edição de lei, a fim de que se estabeleça um conjunto específico de normas relacionadas com a proteção de dados pessoais. A referida lei deverá impor ao Estado a obrigação de criar pressupostos fáticos à efetividade do direito à privacidade informacional, ou seja, implementar as *medidas administrativas* necessárias à proteção dos dados pessoais tanto no setor público como no privado, e, ainda, prever os seguintes aspectos: (a) princípios aplicáveis ao tratamento de dados pessoais; (b) deveres dos responsáveis pelo tratamento de dados pessoais por meio de seus empregados, prepostos ou representantes; (c) direitos resguardados aos titulares de dados pessoais, dentre os quais, o *direito a não sujeição a decisão individual automatizada*[564], direito à informação, direito de oposição, direito de acesso e direito ao apagamento; (d) mecanismos procedimentais para o exercício dos direitos conferidos; (e) procedimentos especiais de segurança em caso de tratamento de dados sensíveis; (f) sanções administrativas, civis e penais pelo descumprimento dos dispositivos nela estatuídos; (g) limites à vigilância eletrônica[565] estatal, considerando que a imagem também é um dado pessoal; (h) limites à interconexão de dados pessoais entre diferentes entes públicos; (i) responsabilidades pela divulgação, comercialização ou qualquer outra espécie de tratamento não autorizado pelo titular dos dados.

René Ariel Dotti desde 1980 já chamava a atenção para a utilização abusiva da informática, defendendo que, modernamente, a proteção do direito à privacidade deveria abranger o direito de impedir a compilação de certos dados de natureza íntima, que não poderiam ser registrados, também a possibilidade de se corrigirem informações inexatas, inoportunas ou desatualizadas, prevenindo-se sua utilização abusiva. Segundo o autor, esse controle deveria

[563] CAMPUZANO TOMÉ, Hermínia. Op. cit., p. 64. Grifos nossos.
[564] O *direito a não sujeição a decisão individual automatizada* confere ao titular dos dados a prerrogativa de não ficar sujeito a uma decisão que produza efeitos na sua esfera jurídica como, por exemplo, negação de crédito, tomada exclusivamente com base num tratamento automatizado de dados. A decisão pode ser tomada com base no tratamento de automatizado de dados, desde que seja permitido ao titular se expressar. In CASTRO, Catarina Sarmento. Op. cit., pp. 251-252.
[565] Ver item 3.5.2.

garantir uma adequada proteção das liberdades públicas em geral e da defesa da privacidade em particular[566].

Hoje, esse modelo da regulamentação do direito à autodeterminação informativa por lei específica já foi incorporado por diversos países ao redor do mundo. Joel Reidenberg se refere a esse fenômeno como a "globalização de soluções para a privacidade". Argentina, Paraguai, Nova Zelândia, Chile e Canadá aderiram, por razões comerciais, ou seja, como forma de obter vantagens nas transações com países da UE. Outros, como a Hungria e a Polônia, adotaram o modelo europeu como uma tentativa de futuramente integrar a União Européia; que os leva a adaptar sua legislação interna à legislação comunitária. Por fim, a exportação do modelo europeu ocorreu também em relação aos países do Centro e do Leste europeu, que, com a queda do regime comunista e o temor de retrocesso aos regimes totalitários, passaram a demonstrar certa preocupação em relação à privacidade como a República Checa, a Eslovênia e a Eslováquia[567].

Enfim, observam-se algumas vantagens, como o estímulo ao comércio eletrônico, diante da maior segurança ao consumidor nas relações com os prestadores de serviço da sociedade da informação; clareza na definição dos princípios, direitos e deveres, no que concerne ao tratamento de dados pessoais; maior efetividade dos preceitos, diante da possibilidade de imposição de sanções pelo descumprimento das normas; balanceamento entre a privacidade informacional e as vantagens proporcionadas pelos avanços tecnológicos, segundo critérios preestabelecidos; enfim, a libertação dos indivíduos da condição de mero "objeto" de informação garantindo-lhes o real controle do tratamento de seus dados pessoais.

[566] DOTTI, René Ariel. **Proteção da vida privada e liberdade de informação**. São Paulo: Ed. Revista dos Tribunais, 1980, pp. 256-257.
[567] PALLAZZI, Pablo A. Op. cit. pp. 39-42.

CONCLUSÃO

Pelo exposto, formulam-se conclusões a respeito da conformação do direito à privacidade na sociedade da informação. Trata-se de um esforço no intuito de contribuir para a interpretação e para a aplicação desse direito fundamental de forma mais ampla, levando-se em consideração as múltiplas dimensões desse preceito no contexto do cenário social, político e econômico que se instaura. Ressalte-se a necessidade de implementação de medidas tanto administrativas quanto legislativas para a garantia da maior efetividade desse direito fundamental, diante dos avanços da tecnologia da informação, bem como de conscientização à população quanto aos riscos à privacidade que tais avanços suscitam, especialmente no que concerne ao tratamento de dados pessoais por meio de sistemas automatizados. É o que se faz a seguir.

1. Privacidade e liberdade interligam-se intimamente. Não se assegura privacidade sem liberdade, o que se constata em regimes de exceção; e não se exercita liberdade sem privacidade, sendo esta indispensável à livre manifestação do pensamento, crença e expressão.

2. O direito à privacidade traduz-se na faculdade inerente a cada pessoa de obstar a intromissão de estranhos na sua intimidade e vida privada, assim como na prerrogativa de controlar informações pessoais, evitando-se o acesso e a divulgação de tais dados sem a anuência do referido titular. A intimidade corresponde à esfera mais interior do indivíduo, onde se aninham informações mais sensíveis, pensamentos e crenças; enquanto a vida privada corresponde à esfera que custodia fatos da vida particular, os quais não revelam aspectos extremamente reservados da personalidade da pessoa, mas que se deseja preservar da divulgação ou do conhecimento por terceiros em geral.

3. Classifica-se a privacidade em cinco categorias: física (incolumidade do corpo físico); do domicílio (inviolabilidade do domicílio); das comunicações (inviolabilidade das comunicações); *decisional* (poder do indivíduo de se autodeterminar); e *informacional* (poder do titular de controlar e proteger seus dados pessoais).

4. Na área civil, classifica-se a privacidade como um direito da personalidade juntamente com a proteção do corpo, da honra, da imagem e do nome, o que lhe confere características que a traduzem como personalíssima; geral; necessária; vitalícia; impenhorável; absoluta; irrenunciável

(embora passível de limitação temporária de exercício, a critério do próprio titular); inexpropriável; e extrapatrimonial (embora possa oferecer utilidade financeira).

5. Às pessoas jurídicas de direito privado assegura-se o direito à privacidade, embora não se admita a classificação de referida garantia como um direito da personalidade – uma vez que os direitos da personalidade decorrem diretamente do princípio da dignidade da pessoa humana – preservando-se a privacidade dessas organizações na qualidade de direito fundamental. Em se tratando de pessoa jurídica de direito público, aplica-se o princípio da publicidade, que consagra o dever de todos os órgãos e entidades públicos de manterem plena transparência de seus atos perante os administrados, admitindo-se, todavia, o sigilo para proteção da segurança da sociedade e do Estado ou para preservação da privacidade das pessoas físicas ou das pessoas jurídicas de direito privado.

6. O sistema jurídico brasileiro apresenta-se como um sistema aberto e constitucionalista, comportando tanto normas-regra, que se identificam como mandados definitivos, aplicáveis por subsunção na medida do tudo-ou-nada e subordinados à verificação de validade pelo órgão julgador, mas também normas-princípio, que se expressam como mandados de otimização, aplicáveis por ponderação na medida do possível e não sujeitos à verificação de validade pelo órgão julgador. Nesse contexto, protege-se o direito à privacidade que, dependendo do caso concreto em exame, configura-se ora como norma-regra, ora como norma-princípio. Essa perspectiva revela-se de particular importância e por essa razão deve nortear os operadores técnico-jurídicos na interpretação e na aplicação desse direito fundamental, em especial na resolução dos conflitos com outros direito fundamentais, como o direito à liberdade de expressão e de comunicação, quanto com outros valores protegidos pela Constituição, como o valor segurança pública.

7. Os direitos fundamentais têm uma dimensão subjetiva e uma dimensão objetiva. Em sua dimensão subjetiva, produzem efeitos sobre as relações jurídicas das pessoas físicas e jurídicas com o Estado e com os demais particulares; em sua dimensão objetiva, produzem efeitos sobre toda a ordem jurídica, dirigindo e vinculando o Executivo, o Legislativo e o Judiciário por meio dos valores que protegem. Sob o foco da dimensão subjetiva, o direito fundamental pode assumir tanto um caráter negativo, ao atribuir ao seu titular a faculdade de exigir do Estado uma abstenção de intervenção na sua esfera jurídica (direito de defesa); como também um caráter

positivo, ao conferir ao indivíduo a prerrogativa de exigir do Estado a implementação das condições fáticas e jurídicas necessárias ao pleno exercício desse mesmo direito, bem como a proteção em face das agressões provenientes dos demais concidadãos ou de Estados estrangeiros (direito a prestação).

8. O direito à privacidade, em sua dimensão negativa, outorga ao titular a faculdade de exigir do Estado e dos demais particulares uma abstenção de intervenção na sua esfera jurídica, ou seja, a prerrogativa de impor a terceiros o respeito à sua intimidade e à sua vida privada. Ao proteger a esfera individual do indivíduo contra intromissões do poder público e dos demais concidadãos, o direito à privacidade caracteriza-se como típico direito de defesa – expressão do denominado status negativo. Em que pese a predominância dessa dimensão negativa, verifica-se que a efetividade do direito à privacidade requer não apenas uma abstenção estatal, mas também uma atuação do poder público no sentido de garantir a não intromissão de terceiros na intimidade e na vida privada alheias, ou seja, exige-se uma ação positiva do Estado, expressão do status positivo e dos direitos a prestação.

9. Destaca-se, como um dos pontos relevantes desta dissertação, a constatação de que a efetividade do direito à privacidade – em especial do direito à privacidade *informacional*, também denominado direito à autodeterminação informativa – depende de uma ação positiva por parte do Estado, ou seja, o poder público tem o dever de implementar medidas administrativas e legislativas necessárias à concretização desse direito fundamental, considerando-se a falta de transparência no tratamento de dados pessoais após o advento da tecnologia da informação.

10. Sob essa perspectiva, o direito à privacidade classifica-se como um direito a prestação e impõe ao Estado o dever de implementar procedimentos necessários à salvaguarda das informações pessoais submetidas a qualquer espécie de tratamento, bem como a designação ou a criação de um órgão responsável pela permanente revisão e aperfeiçoamento desses procedimentos aplicáveis tanto no setor público como no privado (direito à organização e ao procedimento). Ainda como direito a prestação, o direito à privacidade exige que o poder público adote medidas que proporcionem o incremento da privacidade, protegendo os cidadãos das intromissões provenientes de outros particulares ou de Estados estrangeiros no contexto da sociedade da informação (direito de proteção).

11. Consagrou-se na doutrina a vinculação das entidades privadas aos direitos fundamentais – denominada eficácia horizontal dos direitos fundamentais –, restando divergência apenas quanto à forma de aplicação de tais preceitos, conforme se adote a teoria da eficácia direta ou imediata ou a teoria da eficácia indireta ou mediata. No ordenamento jurídico nacional, apesar de inexistir expresso dispositivo constitucional determinando a adoção da teoria da eficácia direta ou imediata, tal medida tem prevalecido na jurisprudência nacional, sob o fundamento de configurar-se como uma decorrência lógica do caráter objetivo dos direitos fundamentais, ou seja, resultante da concepção de que os direitos fundamentais representam o estatuto axiológico da sociedade, ao vincular tanto o poder público como os demais particulares de forma direta ou imediata.

12. Nesse contexto, protege-se a intimidade e a vida privada não apenas em face do Estado, mas também em relação aos demais concidadãos, daí falar-se em eficácia horizontal do direito fundamental à privacidade, destacando-se alguns precedentes do STJ a respeito da violação à privacidade por particulares, em casos de interceptação de conversa telefônica sem autorização judicial; divulgação de dados pessoais sem autorização do titular; veiculação de imagem sem permissão do indivíduo filmado; publicação de matéria jornalística com fotos e informações sensíveis a respeito do entrevistado em periódico distinto do previamente autorizado; quebra de sigilo bancário e fiscal; dentre tantos outros.

13. A proteção da intimidade e da vida privada impõe-se como um pressuposto para o exercício da liberdade de consciência, de crença e de expressão, configura-se como uma proteção contra "ingerências alheias" que perturbem o livre desenvolvimento da personalidade, o que não veda a auto-exposição a critério do próprio titular. Sob tal aspecto, a privacidade abrange, em seu âmbito de proteção, a liberdade de divulgação de fatos íntimos, cabendo apenas à própria pessoa o livre-arbítrio de se expor ou de não se expor e, ainda mais importante, até que limite deseja se expor, não se admitindo qualquer interferência estatal, sob pena de violação do direito do indivíduo de se autodeterminar e de tomar suas próprias decisões (privacidade *decisional*). Nesse sentido, a privacidade deve ser analisada sob a concepção do próprio titular do direito e não de acordo com uma visão unidimensional e heterônoma que ignore as antagônicas e incomensuráveis visões de mundo características das sociedades pluralistas.

14. Embora se admita a limitação do direito à privacidade, a critério do próprio titular, tal ato será válido tão-somente quando se respeitarem determinados pressupostos: (i) limitação temporária, afigurando-se como inconstitucional a limitação permanente, o que representaria renúncia à própria titularidade do direito e não apenas ao seu exercício; (ii) preservação do núcleo essencial da garantia, não se tolerando que a pessoa se reduza à condição de mero objeto de informação, o que violaria o princípio da dignidade da pessoa humana; (iii) decisão livre e autodeterminada, vedando-se a imposição da restrição pela parte mais forte da relação jurídica. Sob o fundamento desses critérios, analisa-se a questão da possibilidade de "renúncia" à privacidade nos denominados *reality shows* e nos contratos de trabalho em geral.

15. Em relação aos *reality shows*, constata-se que o comportamento dos participantes preenche os pressupostos de fato, tanto do direito à privacidade como do direito à liberdade de expressão da atividade artística e de profissão (concorrência de direitos fundamentais), concluindo-se pela preponderância do último em relação ao primeiro e pela constitucionalidade da conduta desses indivíduos, no que concerne ao livre-arbítrio para a auto-exposição a que se submetem, inclusive para fins econômicos. Tal comportamento não implica renúncia ao direito à privacidade, mas mera limitação temporária de exercício desse direito fundamental, uma vez que a decisão de auto-restrição é deliberada autonomamente, tem caráter temporário e revogável e não afeta o princípio da dignidade da pessoa humana.

16. Quanto à limitação da privacidade em ambiente laboral, constata-se a inexistência de autonomia real dos empregados ao submeterem-se ao permanente controle por parte das empresas, concluindo-se pela inconstitucionalidade do monitoramento generalizado de todas as comunicações desses indivíduos, ainda que tal previsão exista em normas internas de uma organização e em contratos de trabalho, por violação ao inciso XII do art. 5º da CF, e ao princípio da proporcionalidade – preceito aplicável à resolução dos conflitos entre direitos fundamentais, neste caso, entre o direito à privacidade dos empregados e o direito à propriedade, à livre iniciativa e à imagem da empresa – uma vez que existem outros meios menos invasivos à privacidade dos empregados aptos para resguardar os direitos da empresa.

17. O direito à privacidade abrange, em seu âmbito de proteção, a intimidade, a vida privada, o domicílio, a correspondência, as comunicações e os dados pessoais a respeito de uma determinada pessoa. Uma interpretação mais adequada – segundo os novos parâmetros da sociedade da

informação – inclui no conceito de comunicação, qualquer espécie de comunicação, inclusive mensagens veiculadas por correio eletrônico (*e-mail*), cujo sigilo deve ser preservado.

18. O âmbito de proteção do direito à privacidade possui caráter eminentemente elástico e variável, sofrendo adequações de acordo com o tempo, o espaço e o titular da garantia. A privacidade de políticos, artistas e atletas submete-se a parâmetros de aferição menos rígidos do que a privacidade de pessoas anônimas, em razão da necessidade de auto-exposição e de promoção pessoal daqueles indivíduos. Assim, quanto maior a amplitude da projeção da pessoa pública ou notória, menor a possibilidade de se vetarem intromissões alheias em sua vida privada, pois o interesse público sobreeleva-se à invasão da intimidade desse indivíduo.

19. Os direitos fundamentais – pelo caráter relativo de que se revestem – estão sujeitos a restrições expressas e implícitas. No primeiro caso, a própria Constituição limita o direito fundamental ou prevê a possibilidade de restrição de tal garantia por ato normativo emanado do Legislativo; no segundo, a restrição é imposta mesmo sem expressa previsão constitucional, por ser uma medida essencial à conformação do direito fundamental com outros valores constitucionais. Todavia, tais restrições não podem ser ilimitadas, sob pena de esvaziamento do próprio conteúdo do direito fundamental, daí falar-se em imposição de limites ao poder de restrição.

20. O direito fundamental à privacidade sujeita-se não apenas a restrições expressas – nas modalidades diretamente constitucionais e indiretamente constitucionais – como também a restrições implícitas. Prevê-se restrição diretamente constitucional nos seguintes dispositivos: (i) alíneas "b" e "c" do inciso I do § 1º do art. 136 e inciso III do art. 139 (restrição à privacidade das comunicações); e (ii) inciso XI do art. 5º (restrição à privacidade do domicílio). Adota-se a técnica da restrição indiretamente constitucional, na forma de reserva legal qualificada, no inciso XII do art. 5º. Por fim, impõem-se restrições implícitas quando o direito à privacidade entra em conflito com direito fundamental de outro cidadão, como o direito à liberdade de expressão e de comunicação; ou com outro valor também previsto constitucionalmente, conforme demonstra a jurisprudência no caso de limitação ao sigilo de correspondência de presidiários para preservação do valor segurança pública, embora não exista expressa previsão constitucional.

21. A expressão sociedade da informação define uma nova forma de organização social, política e econômica em que ocorre intensivo uso da tecnologia da informação para coleta, produção, processamento, transmissão e armazenamento de informações; destacando-se a

informação, de *per si*, como a principal matéria-prima desse novo modelo capitalista, daí a nomenclatura atribuída. Além desse traço distintivo, ressaltem-se como principais características da sociedade da informação – também denominada era da informação – o extraordinário avanço no setor de comunicação, especialmente após o advento da internet e o desenvolvimento da microeletrônica; o controle de todas as infra-estruturas críticas por meio de recursos computacionais; o incremento da criminalidade em meio eletrônico (*cybercrimes*); a substituição de recursos humanos por agentes inteligentes em determinadas linhas de produção; a escala global do fluxo de informações, enfraquecendo tradicionais limites territoriais; o surgimento de uma nova especialidade denominada segurança da informação, a fim de incrementar a gestão das informações no setor público e no setor privado, e o forte impacto da tecnologia nas ciências, na cultura, na economia e na política.

22. No cenário da sociedade da informação, cresce o interesse tanto dos governos quanto da iniciativa privada na privacidade das pessoas. O mercado impõe como um dos critérios para avaliação do valor de venda de corporações a quantidade de informações pessoais de que essas entidades dispõem a respeito de seus clientes; o Estado investe em poderosos bancos de dados para interconexão e processamento de informações pessoais, a fim de traçar o perfil dos cidadãos; o comportamento das pessoas torna-se cada vez mais controlado por meio de câmeras de vigilância instaladas por toda parte; as empresas incrementam os procedimentos de monitoramento das comunicações dos empregados; surgem companhias especializadas na coleta e no processamento de dados pessoais para fins de *marketing* e de publicidade; as agências de inteligência firmam acordos, a fim de interceptar comunicações ao redor de todo o mundo; enfim, a sociedade assume contornos de permanente controle e vigilância dos indivíduos por meio dos novos artefatos tecnológicos.

23. A origem de todas essas transformações sociais remonta ao século XIX, quando se incrementou o poder disciplinar, implantado desde a Idade Média nas organizações religiosas. A disciplina foi incorporada pelas instituições de ensino e pelas fábricas, a fim de aumentar a produtividade por meio do controle do comportamento dos indivíduos. O Estado desenvolveu a técnica para controlar não somente os comportamentos passados dos indivíduos, mas também aqueles ainda em fase de desenvolvimento por meio da permanente vigilância que garantisse o funcionamento automático do poder. Para tornar o controle eficiente, utilizava-se uma técnica

batizada por Jeremy Benthan Panóptico – método descrito na década de 70 pelo filósofo francês, Michel Foucault, nas obras *Microfísica do poder* e *Vigiar e punir*.

24. O método panóptico funda-se no princípio da constante vigilância das pessoas, no intuito de construir um saber detalhado sobre esses indivíduos. Mas a grande eficiência da técnica em referência decorre da capacidade de esse procedimento interferir no comportamento do indivíduo ainda em fase de desenvolvimento, uma vez que a pessoa, ao tomar conhecimento de que se encontra exposta a um mecanismo de permanente visibilidade, passa a comportar-se de maneira diversa daquela que agiria, para se adequar aos propósitos do agente de vigilância e se resguardar, assim, de possíveis punições futuras. Essa vigilância "visível", mas "inverificável", assegura o funcionamento automático do poder, daí a sua incorporação pelas sociedades contemporâneas, enquanto mecanismo de fortalecimento dos aparelhos de Estado, estendendo-se por uma rede de controle que permeia todo o corpo social. Em pleno século XXI, na sociedade da informação ainda vigora o modelo panóptico para controle dos indivíduos, diferenciando-se do método vislumbrado por Jeremy Benthan e descrito por Michel Foucault, tão-somente por adotar recursos tecnológicos mais sofisticados.

25. A vigilância sobre o comportamento das pessoas sofreu extraordinário avanço com o advento da tecnologia da informação, que permite o rastreamento, o monitoramento e o controle dos indivíduos a distância mediante dispositivos eletrônicos. Nesse contexto, a videovigilância se materializa como a espécie mais comum de vigilância eletrônica, estruturando-se por meio de circuitos internos de televisão e câmeras de segurança que captam as imagens das pessoas, a fim de influenciar seu comportamento e incrementar a segurança coletiva. Todavia, o uso indiscriminado de dispositivos para vigilância eletrônica tem preocupado juristas e ativistas de organizações não governamentais de defesa das liberdades públicas ao redor de todo o mundo, o que levou a sua regulamentação em diversos países. Destacam-se, ainda, outras formas comuns de vigilância eletrônica como a vigilância mediante o uso de radiofreqüência, o rastreamento via satélite de usuários de celular, o GPS e a utilização de *chips* integrados à internet como o biossensor *Digital Angel*.

26. A internet, ao longo dos anos, também se revelou um meio propício de invasão à privacidade, destacando-se o intercâmbio de informações pessoais entre os diversos prestadores de serviço da sociedade da informação sem a prévia autorização dos titulares dos dados; a

possibilidade de monitoramento eletrônico dos internautas por meio do IP; a disseminação da cultura de auto-exposição em *chats* e em comunidades virtuais; a coleta de informações sobre a navegação dos usuários por meio de *cookies*; e a disseminação de *trojans*, *keyloggers*, *spywares* e outros programas desenvolvidos para execução de ações maliciosas. Objetiva-se, a partir da análise dessas ameaças, tão-somente alertar os usuários da rede para que esses indivíduos passem a desfrutar desse extraordinário meio de comunicação de forma mais consciente no que concerne à preservação da própria intimidade e vida privada no mundo virtual.

27. Existem dois tipos de anonimato: o anonimato completo, em que a pessoa é completamente desconhecida, não havendo como obter a identificação de tal indivíduo; e o pseudoanonimato, em que a pessoa pode ser conhecida, apesar de não ter revelado seu nome ou outra forma de "autenticação direta". Sustenta-se a necessidade de preservação do anonimato na internet, na modalidade do pseudoanonimato, permitindo-se tão-somente a identificação dos usuários responsáveis pela prática de atividades ilícitas por intermédio desse meio de comunicação, o que pode ser feito mediante rastreamento do IP e cruzamento dessa informação com os dados armazenados pelos prestadores de serviços de telefonia e conexão à internet, ou outra forma de identificação do protocolo, e desde que exista prévia autorização judicial para a realização de perícia forense computacional. Ressalte-se a importância do anonimato *on-line*, enquanto medida indispensável ao exercício da liberdade de expressão e de comunicação, à coibição da censura pelo Estado e à consolidação de um autêntico regime democrático.

28. Destaque-se a importância da coleta de informações pessoais como recurso imprescindível ao desempenho das atividades estatais, como investigação de evasão tributária, diminuição e combate à criminalidade, formulação de políticas públicas, dentre tantas outras. Ressalte-se, todavia, a necessidade de se imporem limites ao uso de dados de caráter pessoal, tanto pelos órgãos e entidades públicos como pela iniciativa privada, a fim de se evitarem abusos e excessiva intromissão na intimidade das pessoas. Propõe-se, nesse sentido, a regulamentação a respeito da identificação dos dados os quais podem ser coletados e aqueles que deverão ser proibidos de coleta, além da especificação das medidas e procedimentos de segurança aplicáveis ao tratamento de informações pessoais, tanto no setor público como no setor privado.

29. Além da exagerada coleta de informações pessoais, a intromissão na intimidade e na vida privada dos indivíduos se consuma por meio da espionagem operada pelos sistemas de

inteligência. Hoje, agências de inteligência interceptam comunicações realizadas por meio de telefone, fax, rádio, telex e até internet; o que suscita preocupações em relação ao direito à privacidade. Nesse contexto, destaque-se o Projeto *Echelon* americano e o Projeto *Enfopol* europeu, além dos programas *Carnivore*, *Magic Lantern*, *Matrix*, *TIASystems*, todos implantados pelos EUA. Esses projetos e programas, operados por agentes policiais e agentes de inteligência, escondem seus objetivos sob alegações ancoradas em pretensa necessidade de se combater a corrupção, o terrorismo, o tráfico de entorpecentes e a lavagem de dinheiro, mas o que se observa é a tentativa de se ampliar o já desmesurado poderio econômico dos países que os controlam, e que livremente coletam informações privilegiadas sobre transações comerciais e negociações políticas de todos os povos.

30. Dado pessoal é o dado relacionado a um indivíduo identificado ou identificável, entendendo-se por identificado o indivíduo que já é conhecido; e por identificável a pessoa que pode ser conhecida diretamente pelo próprio possuidor dos respectivos dados, ou indiretamente mediante recursos e meios à disposição de terceiros, sem que seja necessário o dispêndio de tempo, custo ou esforço exagerado. Independentemente do suporte em que se encontrem registrados os dados de um indivíduo, de transmitirem ou não uma mensagem e de estarem ou não diretamente afetos ao sujeito, devem ser protegidos mediante adoção de medidas e procedimentos especiais de segurança, uma vez que, com o incremento da tecnologia da informação, podem ser facilmente cruzados e relacionados por potentes *softwares*, que permitem traçar o perfil dos indivíduos, o que caracteriza uma violação da intimidade e da vida privada do titular em referência.

31. Os dados pessoais podem ser classificados em três espécies: não sensíveis, sensíveis e de tratamento proibido. Os dados não sensíveis correspondem à esfera da vida privada de seu titular; os dados sensíveis, ao âmbito da intimidade; e os de tratamento proibido à esfera do segredo. Os dados não sensíveis podem ser coletados e armazenados sem prévio e expresso consentimento de seu titular ou representante. Os dados sensíveis necessitam de prévia e expressa permissão do titular ou de seu representante para serem tratados; exceto se houver autorização legal, quando será dispensável tal manifestação. Por fim, os dados de tratamento proibido merecem total e absoluta proteção, devendo existir vedação legal de seu tratamento, por se referirem a aspectos relacionados à dignidade humana do titular das informações.

32. Considerando-se que as ocorrências de violação à *privacidade informacional* se agravaram com o advento dos sistemas automatizados, a conformação desse direito foi delineada inicialmente em países que dispunham de um nível de desenvolvimento tecnológico mais avançado. No plano internacional, destaque-se a Convenção nº 108 para a proteção das pessoas relativamente ao tratamento automatizado de dados de caráter pessoal de 1981, a Directiva 95/46/CE, a Directiva 97/66/CE e a Directiva 2002/53/CE, o que demonstra que os maiores avanços ocorreram no continente europeu, onde já se assegura proteção tanto pela via legislativa como pela administrativa. Nos EUA, apesar de ter ocorrido certo desenvolvimento em termos legislativos nas décadas de 70 e 80, atualmente o direito à proteção de dados pessoais não encontra respaldo, especialmente em se tratando de órgãos governamentais, que adotam procedimentos cada vez mais invasivos à privacidade. Na América Latina, a proteção à *privacidade informacional* também se mostra incipiente, existindo legislação específica apenas na Argentina e no Chile.

33. O ordenamento jurídico nacional prevê a proteção de dados pessoais, tão-somente, de forma indireta, a partir da interpretação dos incisos X, XII, XXXIII e LXXII do art. 5º da CF, bem como do previsto nos seguintes dispositivos legais: art. 198 do CTN, § 3º do art. 23 da Lei nº 8.159/91, parágrafo único do art. 7º da Lei nº 11.111/05, Lei nº 9.507/97 (Lei do *Habeas Data*), art. 43 do CDC, art. 313-A do CP, § 1º-A do art. 153 do CP e inciso I do art. 325 do CP.

34. Desde o final da década de 70, as legislações mais avançadas em termos de proteção de dados pessoais arrolam os princípios identificados como necessários à garantia dos direitos e das liberdades dos indivíduos no que respeita a sua *privacidade informacional.* Com o desenvolvimento da tecnologia da informação, ao longo dos últimos anos, reconheceram-se novos princípios aplicáveis ao tratamento de dados pessoais por meio de sistemas automatizados, destacando-se o princípio da lealdade ou da boa fé, o princípio da publicidade, o princípio da transparência, o princípio da proporcionalidade, o princípio da veracidade, o princípio da caducidade, o princípio da segurança no tratamento, o princípio da confidencialidade, o princípio do não tratamento de dados sensíveis, o princípio da reciprocidade das vantagens e o princípio da responsabilidade objetiva. Embora, a maior parte dos postulados de proteção de dados pessoais esteja expressamente prevista nas legislações internacionais e estrangeiras, observa-se que seu

reconhecimento pode efetuar-se tão-somente mediante jurisprudência, o que não lhes retirará a ampla normatividade.

35. A fragilidade do direito à privacidade *informacional* ou direito à autodeterminação informativa diante dos modernos recursos tecnológicos utilizados para coleta, armazenamento e interconexão de dados pessoais, impõe a regulamentação dessa garantia por legislação específica, a fim de que se estabeleça um conjunto de normas que prevejam os princípios aplicáveis ao tratamento de dados pessoais; os direitos garantidos aos titulares das informações; as medidas e os procedimentos de segurança necessários à preservação da integridade, autenticidade e sigilo dos dados; as sanções aplicáveis pelo descumprimento dos preceitos; e outras medidas igualmente importantes à preservação da intimidade e da vida privada dos titulares das informações.

36. Considerando-se a celeridade dos avanços na área da tecnologia da informação, destaque-se, por fim, que a segunda parte deste estudo merece constante atualização, alertando-se para as possíveis transgressões ao direito à privacidade que ainda estão por vir no cenário da sociedade da informação em permanente mudança.

REFERÊNCIAS BIBLIOGRÁFICAS

ALEMANHA**.** *Constituição da Alemanha de 1949*. Disponível em <http://www.alemanha.org.br/embaixadabrasilia/spr_2/willkommen/infos/grundgesetz/constituicao.htm>. Acesso em: 30 jan. 2007.

ALEXY, Robert. Direitos fundamentais no Estado Constitucional Democrático. Tradução de Luís Afonso Heck. *Revista de Direito Administrativo*, Rio de Janeiro: Renovar, nº 217, pp. 55-67, jul./set. 1999.

_____. Direitos fundamentais, ponderação e racionalidade. Tradução de Luís Afonso Heck. *Revista de Direito Privado*, São Paulo: RT, nº 24, pp. 334-343, out./dez. 2005.

_____. *Epílogo a la teoria de los derechos fundamentales*. Tradução de Carlos Bernal Pulido. Madrid: J. San José, 2004.

_____. *Teoria de los derechos fundamentales*. Tradução de Ernesto Garzón Valdés. Madrid: Centro de Estúdios Políticos y Constitucionales, 1997.

ALONSO, Félix Ruiz. Pessoa, intimidade e o direito à privacidade. In: MARTINS, Ives Gandra; PEREIRA JÚNIOR, Antonio Jorge (coordenadores). *Direito à privacidade*. São Paulo: Centro de Extensão Universitária, 2005, pp. 11-35.

ALTHUSSER, Louis. *Aparelhos ideológicos de Estado*: nota sobre os aparelhos ideológicos de Estado (AIE). Tradução de Walter José Evangelista e Maria Laura Viveiros de Castro e introdução crítica de José Augusto Guilhon Albuquerque. Rio de Janeiro: Edições Graal, 1985.

ALVES, Ricardo de Paula. Vida pessoal do empregado, liberdade de expressão e direitos fundamentais do trabalhador: considerações sobre a experiência do direito francês. In: MARTINS, Ives Gandra; PEREIRA JÚNIOR, Antonio Jorge (coordenadores). *Direito à privacidade*. São Paulo: Centro de Extensão Universitária, 2005, pp. 367-390.

ANDRADE, José Carlos Vieira de. *Os direitos fundamentais na Constituição Portuguesa de 1976*. 3ª ed. Coimbra: Almedina, 2006.

ASCENSÃO, José de Oliveira. A sociedade da informação. In: _____(Org.). *Direito da sociedade da informação*. Coimbra: Coimbra Ed., 1999. vol. I.

ASÍS ROIG, Rafael de. *Las paradojas de los derechos fundamentales como límites al poder*. Madrid: Editorial Debate, 1992.

BARROSO, Luís Roberto. *A nova interpretação constitucional*: ponderação, direitos fundamentais e relações privadas. Rio de Janeiro: Renovar, 2003.

_____. Colisão entre liberdade de expressão e direitos da personalidade. Critérios de ponderação. Interpretação constitucionalmente adequada do Código Civil e da Lei de Imprensa. *Revista de Direito Administrativo*, Rio de Janeiro, nº 235, pp. 1-36, jan./mar. 2004.

_____. *Interpretação e aplicação da Constituição*: fundamentos de uma dogmática constitucional transformadora. 5ª ed. rev. atual. ampl. São Paulo: Saraiva, 2003.

BASTOS, Celso Ribeiro; MARTINS, Ives Gandra. *Comentários à Constituição do Brasil*. São Paulo: Saraiva, 1989, vol. 2.

BESSA, Leonardo Roscoe. *O consumidor e os limites dos bancos de dados de proteção ao crédito*. São Paulo: Revista dos Tribunais, 2003.

BITTAR, Carlos Alberto. *Os direitos da personalidade*. 5ª ed. Rio de Janeiro: Forense Universitária, 2001.

BOBBIO, Norberto. *A era dos direitos*. Tradução de Carlos Nelson Coutinho. 19ª Reimpressão. Rio de Janeiro: Elsevier, 1992.

BÖCKENFÖRDE, Ernst-Wolfgang. *Escritos sobre derechos fundamentales*. Tradução de Juan Luis Requejo Pagés e Ignacio Villaverde Menéndez. Baden-Baden: Nomos, 1993.

BONAVIDES, Paulo. *Curso de direito constitucional*. 13ª ed. São Paulo: Malheiros, 2003.

BRANCO, Paulo Gustavo Gonet. Aspectos da teoria geral dos direitos fundamentais. In MENDES, Gilmar Ferreira; COELHO, Inocêncio Mártires; BRANCO, Paulo Gustavo Gonet. *Hermenêutica constitucional e direitos fundamentais*. Brasília: Brasília Jurídica, 2002.

BRASIL, Código de Processo Penal. *Decreto-lei nº 3.689, de 03 de outubro de 1941*. Disponível em: <http://www.planalto.gov.br/ccivil_03/Decreto-Lei/Del3689.htm>. Acesso em: 30 jan. 2007.

_____. *Código de Conduta da Alta Administração, de 21 de agosto de 2000*. Disponível em: <http://www.planalto.gov.br/ccivil_03/Codigos/codi_Conduta/Cod_conduta.htm#codigoconduta>. Acesso em: 30 jan. 2007.

_____. Código de Proteção e Defesa do Consumidor. *Lei nº 8.078, de 11 de setembro de 1990*. Disponível em: <http://www.planalto.gov.br/ccivil_03/LEIS/L8078.htm>. Acesso em: 30 jan. 2007.

_____. Código Penal. *Decreto-lei nº 2.848, de 7 de dezembro de 1940*. Disponível em: <http://www.planalto.gov.br/ccivil_03/Decreto-Lei/Del2848.htm>. Acesso em: 30 jan. 2007.

_____. Código Tributário Nacional. *Lei nº 5.172, de 25 de outubro de 1966*. Disponível em: <http://www.planalto.gov.br/ccivil_03/Leis/L5172.htm>. Acesso em: 30 jan. 2007.

_____. *Constituição da República Federativa do Brasil de 1988*. São Paulo: Revista dos Tribunais, 2004.

_____. *Decreto nº 4.553, de 27 de dezembro de 2002*. Disponível em: <http://www.planalto.gov.br/ccivil_03/decreto/2002/D4553.htm>. Acesso em: 30 jan. 2007.

_____. *Decreto nº 5.584, de 18 de novembro de 2005*. Disponível em <http://www.planalto.gov.br/ccivil_03/_Ato2004-2006/2005/Decreto/D5584.htm>. Acesso em: 30 jan.

_____. Estatuto da Criança e do Adolescente. *Lei nº 8.069, de 13 de julho de 1990*. Disponível em: <http://www.planalto.gov.br/ccivil/LEIS/L8069.htm>. Acesso em 30 jan. 2007.

_____. Lei de Imprensa. *Lei nº 5.250, de 09 de fevereiro de 1967*. Disponível em: <https://www.planalto.gov.br/ccivil_03/Leis/L5250.htm>. Acesso em: 30 jan. 2007.

_____. *Lei nº 10.406, de 10 de janeiro de 2002*. Disponível em: <http://www.planalto.gov.br/ccivil_03/LEIS/2002/L10406.htm>. Acesso em: 30 jan. 2007.

_____. *Lei nº 11.111, de 05 de maio de 2005*. Disponível em <http://www.planalto.gov.br/ccivil_03/_Ato2004-2006/2005/Lei/L11111.htm>. Acesso em: 30 jan. 2007.

_____. *Lei nº 8.159, de 8 de janeiro de 1991*. Disponível em <http://www.planalto.gov.br/ccivil_03/Leis/L8159.htm>. Acesso em: 30 jan. 2007.

_____. *Lei nº 9.507, de 12 de novembro de 1997*. Disponível em: <http://www.planalto.gov.br/ccivil_03/Leis/L9507.htm>. Acesso em: 30 jan. 2007.

CAMPUZANO TOMÉ, Hermínia. *Vida privada y datos personales*: su protección jurídica frente a la Sociedad de la Información. Madrid: Tecnos, 2000.

CANOTILHO, José Joaquim Gomes. Civilização do direito constitucional ou constitucionalização do direito civil? A eficácia dos direitos fundamentais na ordem jurídico-civil no contexto do direito pós-moderno. In: GRAU, Eros Roberto; GUERRA FILHO, Willis

Santiago (Org.). *Direito constitucional*: estudos em homenagem a Paulo Bonavides. São Paulo: Malheiros, 2001, pp. 108-115.

_____. *Direito constitucional e teoria da Constituição*. 7ª ed. Coimbra: Almedina, 2003.

_____. *Estudos sobre direito fundamentais*. Coimbra: Coimbra Editora, 2004.

_____; MACHADO, Jónatas E. M.. *Reality Shows e liberdade de programação*. Coimbra: Coimbra Editora, 2003.

CARLSON, Steven C.; MILLER, Ernest D. Public Data and Personal Privacy. *Santa Clara Computer & High Technology Law Journal*. Santa Clara: HeinOnline, 2000, vol. 16, pp. 83-109.

CARTILHA de Segurança para Internet. Versão 3.1. São Paulo: *Comitê Gestor da Internet no Brasil*, 2006.

CASTELLS, Manuel. *A galáxia da internet*: reflexões sobre a internet, os negócios e a sociedade. Tradução de Maria Luiza X. de A. Borges, Revisão de Paula Vaz. Rio de Janeiro: Jorge Zahar Ed., 2003.

_____. *A sociedade em rede*. Tradução de Roneide Venancio Majer; Colaboração de Klauss Brandini Gerhardt; Prefácio de Fernando Henrique Cardoso. São Paulo: Paz e Terra, 2003.

CASTRO, Catarina Sarmento. *Direito da informática, privacidade e dados pessoais*. Coimbra: Almedina, 2005.

COELHO, Inocêncio Mártires. Elementos da teoria da Constituição e de interpretação constitucional. In MENDES, Gilmar Ferreira; COELHO, Inocêncio Mártires; BRANCO, Paulo Gustavo Gonet. *Hermenêutica constitucional e direitos fundamentais*. 1ª ed. Brasília: Brasília Jurídica, 2002.

CONSELHO DA EUROPA. *Convenção nº 108 para a proteção das pessoas relativamente ao tratamento automatizado de dados de caráter pessoal*. Estrasburgo. 28 de janeiro de 1981. Disponível em <http://www.apdt.org/guia/L/Ldados/108.htm>. Acesso em: 30 jan. 2007.

_____. *Convenção para a Proteção dos Direitos do Homem e das Liberdades Fundamentais*. Roma. 4 de novembro de 1950. Disponível em <http://www.hrea.org/erc/Library/hrdocs/coe/echr_pt.pdf>. Acesso em: 30 jan. 2007.

CORREIA, Miguel Pupo. O caso Echelon: aspectos jurídicos. In: ASCENSÃO, José de Oliveira (Org.). *Direito da sociedade da informação*. Coimbra: Coimbra Ed., 2003, vol. IV.

COSTA JÚNIOR, Paulo José da. *O direito de estar só*: tutela penal da intimidade. 3ª ed. São Paulo: Siciliano Jurídico, 2004.

CRIMES Cibernéticos: manual prático de investigação. São Paulo: *Comitê Gestor da Internet no Brasil e Ministério Público Federal*, 2006.

CUIDADO: sua impressora espiona você. 20 out. 2005. Disponível em <http://tecnologia.terra.com.br/interna/0,,OI717103-EI4801,00.html>. Acesso em: 30 jan. 2007.

DELGADO, Mário Luiz. Big Brother Brasil: *reality shows* e os direitos da personalidade. *Revista Jurídica Consulex*. Ano VIII, nº 169, 31 de janeiro de 2004.

DONEDA, Danilo César Maganhoto. Considerações iniciais sobre os bancos de dados informatizados e o direito à privacidade. In: TEPEDINO, Gustavo (Coordenador). *Problemas de direito constitucional*. Rio de Janeiro: Renovar, 2000. Disponível em: <http://www.doneda.net/pdp/docs/Consideracoes.pdf>. Acesso em: 30 jan. 2007.

_____. Os direitos da personalidade no novo Código Civil. In: TEPEDINO, Gustavo (Org.). *A parte geral do novo Código Civil*: estudos na perspectiva civil-constitucional. Rio de Janeiro: Renovar, 2002. Disponível em: <http://www.buscalegis.ufsc.br/arquivos/130820061.pdf>. Acesso em: 30 jan. 2007.

DOTTI, René Ariel. *Proteção da vida privada e liberdade de informação*. São Paulo: Ed. Revista dos Tribunais, 1980.

DRUMMOND, Victor. *Internet, privacidade e dados pessoais*. Rio de Janeiro: Lumen Juris, 2003.

DWORKIN, Ronald. *Levando os direitos à sério*. Tradução de Nelson Boeira. São Paulo: Martins Fontes, 2002.

ESLOVÊNIA. *Constituição Eslovena de 1991*. Planalto, Brasília, DF. Disponível em <http://www.us-rs.si/en/index.php?sv_path=3583,3519>. Acesso em: 30 jan. 2007.

ESPANHA. *Constituição Espanhola de 1978*. Disponível em <http://www.congreso.es/funciones/constitucion/const_espa_texto.pdf>. Acesso em 30 jan. 2007.

ESTRADA, Manuel Martin Pino. Tele-trabalho suas perspectivas e novidades. In: IBDE, INSTITUTO BRASILEIRO DE DIREITO ELETRÔNICO; UNAMA, UNIVERSIDADE DA AMAZÔNIA. *II Congresso Internacional de Direito Eletrônico*. Belém, 2 a 6 out. 2006.

FARIAS, Edilsom. *Colisão de direitos*: a honra, a intimidade, a vida privada e a imagem versus a liberdade de expressão e informação. Porto Alegre: Fabris, 1996.

_____. *Liberdade de expressão e comunicação*: teoria e proteção constitucional. São Paulo: Editora Revista dos Tribunais, 2004.

FERRANTE, Daniel. O Big Brother é inglês. *Revista Veja*. São Paulo: Ed. Abril, Edição 1848, ano 37, nº 14, 7abr.2004.

FLAHERTY, David H. On the utility of constitutional rights to privacy and data protection. *Case Western Reserve Law Review*, vol. 41, 1990-1991, pp. 831-855.

FORTES, Débora. A morte da privacidade. *Revista Info Exame*. São Paulo: Ed. Abril, ano 15, p. 30-40, jun. 2000.

FOUCAULT, Michel. *A verdade e as formas jurídicas*. Tradução de Roberto Cabral de Melo Machado e Eduardo Jardim. 3ª ed. Rio de Janeiro: NAU Editora, 2003.

_____. *Microfísica do poder*. Organização e tradução de Roberto Machado. Rio de Janeiro: Edições Graal, 1979.

_____. *Vigiar e punir*: nascimento da prisão. Tradução de Raquel Ramalhete. Petrópolis: Vozes, 1987.

FREEDMAN, David H. Why privacy won´t matter. *Newsweek Magazine*. New York: MSNBC. pp. 38-42, 3 abr. 2006.

FRIEDMAN, Thomas. *O mundo é plano*: uma breve história do século XXI. Tradução de Cristina Serra e S. Duart. Rio de Janeiro: Objetiva, 2005.

GAVARA DE CARA, Juan Carlos. *Derechos fundamentales y desarollo legislativo*: la garantia del contenido esencial de los derechos fundamentales em la Ley Fundamental de Bonn. Madrid: Centro de Estudios Constitucionales, 1994.

GERMAN, Christiano. *O caminho do Brasil rumo à era da informação*. São Paulo: Konrad-Adenauer, 2000.

GOMES, Orlando. *Introdução ao direito civil*. 11ª ed. Rio de Janeiro, Forense 1995.

GONÇALVES, Maria Eduarda. *Direito da informação*: novos direitos e modos de regulação na sociedade da informação. Coimbra: Almedina, 2003.

GRAY, Susan H. Eletronic data bases and privacy: policy for the 1990s. In: *Science, Technology, & Human Values*, nº 3, vol. 14, verão 1989, pp. 242-257.

GRINOVER, Ada Pellegrini. Interceptação de dados telemáticos. In: IBDE, INSTITUTO BRASILEIRO DE DIREITO ELETRÔNICO; UNAMA, UNIVERSIDADE DA AMAZÔNIA. *II Congresso Internacional de Direito Eletrônico*. Belém, 2 a 6 out. 2006.

GUERRA, Sidney. *O direito à privacidade na internet*: uma discussão da esfera privada no mundo globalizado. Rio de Janeiro: América Jurídica, 2004.

HÄBERLE, Peter. *Hermenêutica constitucional. A sociedade aberta dos intérpretes da Constituição*: contribuição para a interpretação pluralista e "procedimental" da Constituição. Tradução de Gilmar Ferreira Mendes. Porto Alegre: Sergio Antonio Fabris, 2002.

_____. *La garantía del contenido esencial de los derechos fundamentales en la Ley Fundamental de Bonn*: una contribución a la concepción institucional de los derechos fundamentales y a la teoría de la reserva de la ley. Tradução de Joaquín Brage Camazano. Madrid: Dykinson, 2003.

_____. *Pluralismo y Constitución*: estudios de teoría constitucional de la sociedad abierta. Tradução de Emilio Mikunda. Madrid: Tecnos, 2002.

HESSE, Konrad. *A força normativa da Constituição.* Tradução de Gilmar Ferreira Mendes. Porto Alegre: Sergio Antonio Fabris, 1991.

_____. *Elementos de direito constitucional da República Federal da Alemanha*. Tradução de Luís Afonso Heck. Porto Alegre: Sergio Antonio Fabris, 1998.

HOUAISS, Antônio. *Dicionário eletrônico Houaiss da língua portuguesa*. Editora Objetiva Ltda, 2001. O conteúdo do programa corresponde à edição integral do Dicionário Houaiss da língua portuguesa.

IMPARATO, Nicholas (coordenador) *et al*. *Public policy and the internet*: privacy, taxes and contract. Stanford: Hoover Institution Press, 2000.

INTERNET Governance. Disponível em: <http://ec.europa.eu/information_society /policy/internet_gov/index_en.htm>. Acesso em: 30 jan. 2007.

JABUR, Gilberto Haddad. A dignidade e o rompimento da privacidade. In: MARTINS, Ives Gandra; PEREIRA JÚNIOR, Antonio Jorge (coordenadores). *Direito à privacidade*. São Paulo: Centro de Extensão Universitária, 2005, pp. 85-106.

_____. *Liberdade de pensamento e direito à vida privada*: conflito entre direitos da personalidade. São Paulo: RT, 2000.

KELSEN, Hans. *Jurisdição constitucional*. Introdução e revisão técnica de Sérgio Sérvulo da Cunha. Tradução do alemão de Alexandre Krug, tradução do italiano de Eduardo Brandão e tradução do francês de Maria Ermantina Galvão. São Paulo: Martins Fontes, 2003.

LEONARDI, Marcel. Vigilância tecnológica, bancos de dados, internet e privacidade. *Jus Navigandi*, Teresina, ano 9, nº 499, 18 nov. 2004. Disponível em <http://jus2.uol.com.br /doutrina/texto.asp?id=5899>. Acesso em: 30 jan. 2007.

LÉVY, Pierre. *Cybercultura*. Tradução de Carlos Irineu da Costa. São Paulo: Editora 34, 1999.

LÔBO, Paulo Luiz Netto. Danos morais e direitos da personalidade. *Revista Trimestral de Direito Civil*. Rio de Janeiro: Ed. Patmas, nº 6, pp. 79-97, abr./jun. 2001.

MAIA, Antônio C. Sobre a analítica do poder de Foucault. *Tempo Social – Revista de sociologia da USP*. São Paulo: Universidade de São Paulo, nº 7(1-2), pp. 83-103, out. 1995.

MARQUES, Garcia, MARTINS, Lourenço. *Direito da informática*. Coimbra: Almedina, 2000.

MARTINS, Leonardo (Org.). *Cinqüenta anos de jurisprudência do Tribunal Constitucional Federal Alemão*. Montevidéu: Fundação Konrad Adenauer, 2005.

MASSENO, Manuel Davi. Direito e inteligência artificial In: IBDE, INSTITUTO BRASILEIRO DE DIREITO ELETRÔNICO; UNAMA, UNIVERSIDADE DA AMAZÔNIA. *II Congresso Internacional de Direito Eletrônico*. Belém, 2 a 6 out. 2006.

MCGUIRE, David. House approuves spyware penalties. *Washington Post*. Tuesday, May 24, 2005. Disponível em <http://www.washingtonpost.com/wp-dyn/content/article/ 2005/05/23/AR2005052302000.html>. Acesso em 30 jan. 2007.

MEIRELLES, Hely Lopes. *Direito administrativo brasileiro*. 25ª ed. rev. atual. São Paulo: Malheiros, 2000.

MENDES, Gilmar Ferreira. *Direitos fundamentais e controle de constitucionalidade*: estudos de direito constitucional. 3ª ed. rev. e ampl. São Paulo: Saraiva, 2004.

_____. Os direitos individuais e suas limitações: breves reflexões. In MENDES, Gilmar Ferreira; COELHO, Inocêncio Mártires; BRANCO, Paulo Gustavo Gonet. *Hermenêutica constitucional e direitos fundamentais*. 1ª ed. Brasília: Brasília Jurídica, 2002.

MIRANDA, Jorge. *Manual de direito constitucional*. 2ª ed. Coimbra: Coimbra Editora, 1998, Tomo IV.

_____. *Teoria do Estado e da Constituição*. Rio de Janeiro: Forense, 2003.

MORAIS, Alexandre de. *Direito constitucional*. 12ª ed. São Paulo: Atlas, 2002.

_____. *Direito humanos fundamentais*: teoria geral, comentários aos arts. 1º e 5º da Constituição da República Federativa do Brasil, doutrina e jurisprudência. 6ª ed. São Paulo: Atlas, 2005.

NOVAIS, Jorge Reis. *As restrições aos direitos fundamentais não expressamente autorizadas pela Constituição*. Coimbra: Coimbra Editora, 2003.

OEA. Pacto de San Jose da Costa Rica. *Convenção Americana sobre Direito Humanos*. 22 de novembro de 1969. Disponível em <http://www.mj.gov.br/sedh/ct/legis_intern/conv_americana_dir_humanos.htm>. Acesso em: 30 jan. 2007.

ONU quer internet em todo mundo até 2015. 18 nov. 2005 Disponível em: <http://www.prodatasystems.com.br/noticias/view.asp?id=15>. Acesso em: 30 jan. 2007.

ONU. Declaração Universal dos Direitos do Homem. *Resolução nº 217A (III) da Assembléia Geral das Nações Unidas*. 10 de dezembro de 1948. Disponível em <http://www.mj.gov.br/sedh/ct/legis_intern/ddh_bib_inter_universal.htm>. Acesso em: 30 jan. 2007.

_____. Pacto Internacional de Direitos Civis e Políticos. *Resolução nº 2200-A (XXI)*. 16 de dezembro de 1966. Disponível em <http://www.cidadevirtual.pt/cpr/asilo2/2pidcp.html> Acesso em: 30 jan. 2007.

OPICE BLUM, Renato M. S. *O monitoramento de e-mails e a decisão do TST*. [s.l.]: [s.n.], [200-?]. Publicado no sítio do Instituto Brasileiro de Política e Direito da Informática. Disponível em <http://www.ibdi.org.br /index.php?secao=&id_noticia=452&acao=lendo>. Acesso em 30 jan. 2007.

OXMAN, Stephen A. Exemptions to the European Union Personal Data Privacy Directive: will they swallow the directive? *Boston College International & Comparative Law Review*, vol. 24, 2000-2001, pp.191-203.

PAIVA, Mário Antônio Lobato de; SILVEIRA NETO, Antônio. *A privacidade do trabalhador no meio informático*. [s.l.]: [s.n.], [2003]. Publicado no sítio do Instituto Brasileiro de Política e Direito da Informática. Disponível em <http://www.ibdi.org.br/index.php?secao=&id_noticia=125&acao=lendo>. Acesso em 30 jan. 2007.

PALLAZZI, Pablo A. *La transmissión internacional de datos personales y la protección de la privacidad*: Argentina, América Latina, Estados Unidos e la Unión Europea. Buenos Aires: Editora Ad-Hoc, 2002.

PEIXOTO, Rodney de Castro. Vigilância sem fronteiras: tempos difíceis para as liberdades civis. *Revista Consultor Jurídico***,** [s.l]: [s.n.], 1 set. 2002. Disponível em <http://conjur.estadao.com.br/static/text/10636,1>. Acesso em: 30 jan. 2007.

PEREIRA, Alexandre Dias. Bases de dados de órgãos públicos. In: ASCENSÃO, José de Oliveira (Org.). *Direito da sociedade da informação*. Coimbra: Coimbra Ed., 2002, pp. 243-295, vol. III.

PEREIRA, Jane Reis Gonçalves. Apontamentos sobre a aplicação das normas de direito fundamental nas relações jurídicas entre particulares. In BARROSO, Luís Roberto. *A nova interpretação constitucional*: ponderação, direitos fundamentais e relações privadas. Rio de Janeiro: Renovar, 2003.

PEREIRA, Joel Timóteo Ramos. *Compêndio jurídico da sociedade da informação*: notas práticas, legislação e jurisprudência. Lisboa: Quid Juris, 2004.

PEREIRA, Marcelo Cardoso. *Direito à intimidade na internet.* 2ª ed. Curitiba: Juruá Editora, 2004.

PERLINGIERI, Pietro. *Perfis do direito civil*: introdução ao direito civil constitucional. Tradução de Maria Cristine de Cicco. Rio de Janeiro: Renovar, 1997.

PINHO, Cláudia; MENCONI, Darlene. Tá tudo vigiado. *Revista Isto É.* São Paulo: Editora Três, nº 1848, 16mar.2005.

PIZZOLANTE, Francisco Eduardo Orcioli Pires e Albuquerque. *Habeas data e bancos de dados*: privacidade, personalidade e cidadania no Brasil atual. Rio de Janeiro: Lumen Juris, 2002.

PORTUGAL. Comissão Nacional de Protecção de Dados. *Princípios sobre a privacidade no local de trabalho*: o controlo do correio electrónico, dos acessos à Internet e das chamadas telefónicas dos trabalhadores. Lisboa, 29 out. 2002. Disponível em <http://www.cnpd.pt/bin/orientacoes/principiostrabalho.htm>. Acesso em: 30 jan. 2007.

_____. *Constituição Portuguesa de 1976*. Disponível em <http://www.parlamento.pt/const_leg/crp_port/>. Acesso em: 30 jan. 2007.

QUEIROZ, Cristina M. M. *Direitos fundamentais*: teoria geral. Coimbra: Coimbra Editora, 2002.

RADIO Frequency Identification. 4 abr. 2005. Disponível em: <http://www.eff.org/Privacy/Surveillance/RFID/>. Acesso em: 30 jan. 2007.

REALE, Miguel. *Lições preliminares de direito*. 21ª ed. São Paulo: Saraiva, 1994.

REINALDO FILHO, Demócrito. A imagem de um indivíduo é dado pessoal: a decisão da autoridade francesa de proteção de dados e suas conseqüências. *Revista de Derecho Informático.* [s.l.]: Alfa-Redi, nº 85, ago. 2005. Disponível em <http://www.alfa-redi.org/rdi-articulo.shtml?x=1603>. Acesso: em 30 jan. 2007.

_____. *Uso de cookies pode infringir a privacidade do internauta*: decisão do Comissário para a Proteção de Dados do Canadá. [s.l.]: [s.n.], [200-?]. Publicado no Portal Infojus. Disponível em <http://www.infojus.com.br/webnews/noticia.php?id_noticia=1717&s>. Acesso em: 30 jan. 2007.

REVEL, Judith. *Michel Foucault*: conceitos essenciais. Tradução de Maria do Rosário Gregolin, Nilton Milanez e Carlos Piovesani. São Carlos: Claraluz, 2005.

ROVER, Aires José. *Informática no direito*: inteligência artificial. Curitiba: Juruá, 2001.

RÚSSIA. *Constituição Russa de 1993*. Disponível em <http://www.departments.bucknell.edu/russian/const/ch2.html>. Acesso em: 30 jan. 2007.

SAMPAIO, José Adércio. *Direito à intimidade e à vida privada*: uma visão jurídica da sexualidade, da família, da comunicação e informações pessoais, da vida e da morte. Belo Horizonte: Del Rey, 1998.

SANTOS, Antonio Jeová. *Dano moral na internet*. São Paulo: Método, 2001.

SÃO PAULO (Estado). *Lei nº 12.228, de 11 de janeiro de 2006*. Disponível em: <http://www.legislacao.sp.gov.br/legislacao/index.htm>. Acesso em: 30 jan. 2007.

SARLET, Ingo Wolfgang. *A eficácia dos direitos fundamentais*. 4ª ed. rev. atual. ampl. Porto Alegre: Livraria do Advogado Editora, 2004.

SARMENTO, Daniel. *Direitos fundamentais e relações privadas.* Rio de Janeiro: Lumen Juris, 2004.

SCHNEIER, Bruce. *Segurança.com*: segredos e mentiras sobre a proteção na vida digital. Tradução de Daniel Vieira. Rio de Janeiro: Campus, 2001.

SÊMOLA, Marcos. *Gestão da segurança da informação*: gestão executiva da segurança da informação. Rio de Janeiro: Elsevier, 2003.

SILVA, José Afonso da. *Curso de direito constitucional positivo*. 15ª ed. São Paulo: Malheiros, 1998.

SILVA, Vasco Manuel Pascoal Dias Pereira da. Vinculação das entidades privadas pelos direitos, liberdades e garantias. *Revista de Direito Público*. São Paulo: STJ, nº 82, abr./jun. 1987, pp. 41-51.

SILVA, Virgílio Afonso da. *A constitucionalização do direito*: os direitos fundamentais nas relações entre particulares. São Paulo: Malheiros, 2005.

SOUZA, Carlos Afonso Pereira. O progresso tecnológico e a tutela jurídica da privacidade. In: *Informática e internet:* aspectos legais internacionais. Tarcísio Queiroz Cerqueira, Erick Iriarte, Márcio Morena (organizadores). Rio de Janeiro: Esplanada, 2001.

UNIÃO EUROPÉIA. *Carta de Direitos Fundamentais da União Européia*. 07 de dezembro de 2000. Disponível em <http://europa.eu/scadplus/leg/pt/lvb/l33501.htm> Acesso em: 30 jan. 2007.

_____. Directiva 95/46/CE do Parlamento Europeu e do Conselho da Europa, de 24 de outubro de 1995, relativa à protecção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados. *Jornal Oficial das Comunidades Europeias*. Portugal, 23 nov. 1995. nº L 281, pp. 31-50.

_____. Directiva 97/66/CE do Parlamento Europeu e do Conselho da Europa, de 15 de dezembro de 1997, relativa ao tratamento de dados pessoais e à protecção da privacidade no sector das telecomunicações. *Jornal Oficial das Comunidades Europeias*. Portugal, 30 jan. 1998. nº L 24, pp. 1-8.

_____. Directiva 2000/31/CE do Parlamento Europeu e do Conselho da Europa, de 8 de junho de 2000, relativa a certos aspectos legais dos serviços da sociedade de informação, em especial do comércio electrónico, no mercado interno («Directiva sobre comércio electrónico»). *Jornal Oficial das Comunidades Europeias*. Portugal, 17 jul. 2000. nº L 17, pp. 1-16.

_____. Directiva 2002/58/CE do Parlamento Europeu e do Conselho da Europa, de 12 de julho de 2002, relativa ao tratamento de dados pessoais e à protecção da privacidade no sector das comunicações electrónicas (Directiva relativa à privacidade e às comunicações electrónicas). *Jornal Oficial das Comunidades Europeias*. Portugal, 31 jul. 2002. nº L 201, pp. 37-47.

_____. Directiva 2006/24/CE do Parlamento Europeu e do Conselho da Europa, de 15 de março de 2006, relativa à conservação de dados gerados ou tratados no contexto da oferta de serviços de comunicações electrónicas publicamente disponíveis ou de redes públicas de comunicações, e que altera a Directiva 2002/58/CE. *Jornal Oficial da União Européia*. Portugal, 13 abr. 2006. nº L 105, pp. 54-63.

VASCONCELOS, Pedro Pais de. Proteção de dados pessoais e direito à privacidade. In: ASCENSÃO, José de Oliveira (Org.). *Direito da sociedade da informação*. Coimbra: Coimbra Ed., 1999, pp. 241-253, vol. I.

VENOSA, Sílvio de Salvo. *Direito civil*: parte geral. 6ª ed. São Paulo: Atlas, 2006.

WARREN, Samuel; BRANDEIS, Louis D. The right to privacy. *Harvard Law Review*. Cambridge: Harvard Law Review Association, nº 193, 1890. Disponível em <http://www.louisville.edu/library/law/brandeis/privacy.html>. Acesso em 30 jan. 2007.

WHITAKER, Reg. *El fin de la privacidad*: como la vigilancia total se está convirtiendo en realidad. Tradução de Luis Prat Clarós. Barcelona: Paidós, 1999.