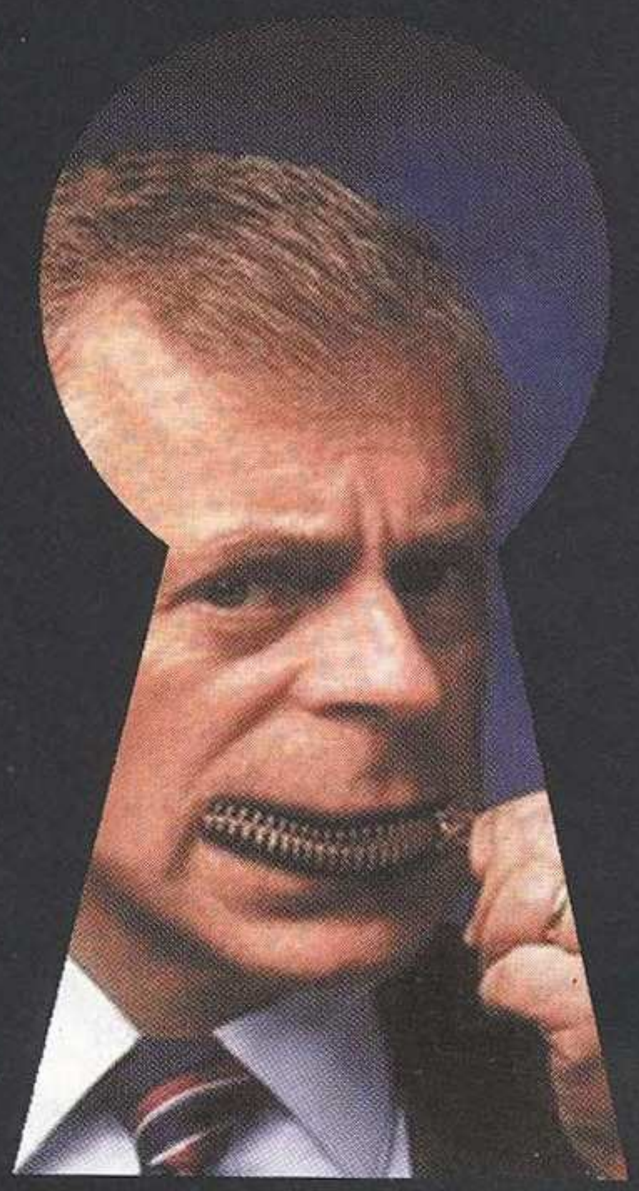

SEGREDOS PÚBLICOS

MARCO CEPIK
CIENTISTA POLÍTICO

UM DILEMA DEMOCRÁTICO

Se é verdade que o acesso público às informações sobre o que os governantes fazem e sobre o que eles sabem é uma condição necessária para manter os governos contemporâneos minimamente representativos, um dos principais dilemas enfrentados pela teoria democrática é o problema da compatibilização entre a autonomia que os governantes precisam ter para defender os governados contra ameaças à sua segurança e seus interesse e a existência de mecanismos capazes de assegurar que as ações dos governantes serão conduzidas respeitando-se a vontade manifestada pelos governados (responsividade) e, ainda, que essas mesmas ações serão avaliadas posteriormente (*accountability*) através de mecanismos de controle verticais (eleições) e horizontais (*checks-and-balances*).[1] No âmago desse dilema está o chamado segredo governamental, uma forma de regulação de fluxos de informação aparentemente incompatível com a democracia.[2]

Nesse artigo, discuto o cerne do dilema democrático contemporâneo examinando os limites impostos pelo segredo e as possibilidades de sua compatibilização com o princípio da publicidade.[3] Além de apresentar as possíveis justificações públicas para o segredo governamental na democracia, discuto os mecanismos que o tornam efetivo e, ao mesmo tempo, dificultam o controle dos cidadãos sobre essa instituição. Há muitas referências no texto sobre o papel dos serviços de inteligência e de segurança estatal na formação e gestão de um sistema de segredo governamental, mas isso se justifica pela centralidade que essas agências governamentais têm na aplicação desse tipo de regulação a importantes fluxos informacionais contemporâneos.

JUSTIFICATIVAS PÚBLICAS PARA O SEGREDO

De acordo com a conhecida definição do sociólogo Edward Shils (1996:26), um segredo é uma retenção compulsória de conhecimento, reforçada pela perspectiva de punição em caso de revelação. Essa definição apenas em parte é equivalente a outras definições correntes na literatura especializada, tais como a de Sissela Bok (1982:05), que afirma ser um segredo qualquer coisa mantida intencionalmente escondida.

Enfatizando esse aspecto intencional do segredo como sendo uma propriedade da informação que é escondida do conhecimento de outrem, Kim Lane Scheppele utiliza uma formulação bastante concisa e abrangente: "*A secret is a piece of information that is intentionally withheld by one or more social actor(s) from one or more other social actor(s)*".[4] O problema dessa definição é que ela é abrangente demais para os propósitos da discussão a ser feita sobre segredo e democracia. Scheppele reconhece que a retenção intencional de informações na relação entre dois ou mais atores sociais varia segundo os contextos da interação, mas sua definição não nos permite diferenciar segredos privados de segredos públicos.

A abordagem de Shils é preferível, pois ela mantém a idéia de intencionalidade e acrescenta um elemento regulador externo para a retenção da informação: a punição legalmente estatuída no caso de revelação. O segredo público é assim distinto de uma informação qualquer que é mantida privadamente em segredo, a qual não passa de uma retenção voluntária de conhecimento reforçada pela indiferença alheia.[5]

Nesse sentido um tanto paradoxal, segredos são uma forma de regulação pública de fluxos de informação. Há pelo menos cinco categorias de informações reguladas pelo sigilo de tipo público: 1) defesa nacional; 2) política externa; 3) processos judiciais; 4) propriedade intelectual e patentes; 5) privacidade dos cidadãos. A justificação pública para a necessidade de sigilo varia muito em cada categoria.[6] Das cinco categorias, as duas primeiras contêm a maioria das informações mantidas em segredo com base em considerações de segurança nacional. Esse é o tipo de segredo público de que se ocupará esse artigo. Vale notar que a justificação do segredo baseada no risco potencial para a segurança nacional não é facultada aos atores privados, mas apenas ao Estado e seus representantes e mesmo assim em situações especiais.

Os segredos governamentais são compatíveis com o princípio de transparência dos atos governamentais somente quando a justificação de sua necessidade pode ser feita, ela própria, em público. Isso é o que David Luban (1996:154-198) chama de máximas de primeira ordem e de máximas de segunda ordem relativas ao princípio da transparência. Uma defesa não apriorística desse princípio envolve admitir o segredo governamental a respeito de normas, procedimentos e políticas (máximas de primeira ordem) desde que as razões para a regulação secreta dessas informações (máximas de segunda ordem) possam ser expostas e justificadas publicamente.[7]

Nada impede, entretanto, que máximas de terceira ou quarta ordem sejam adotadas por governos para justificar (freqüentemente de forma apodítica) uma decisão de manter em segredo as próprias razões pelas quais eles mantêm em segredo certas políticas.[8] Ou seja: não há antídotos definitivos contra o abuso do recurso ao segredo governamental. No limite, é preciso admitir que esse é um tipo de regulação poderosa que se baseia em confiança (*trust*). Entretanto, justamente porque o uso excessivo de máximas de terceira ordem conduz à deslegitimação e ao cinismo em relação às próprias instituições que se pretende proteger através do segredo, um regime democrático precisa tentar traduzir o princípio moral da transparência em proposições de desenho institucional.

Ao cabo, o segredo governamental pode ser compatível com o princípio de transparência somente quando decisões sobre a aplicação desse tipo de regulação a determinados fluxos informacionais são tomadas através de mecanismos institucionais publicamente estabelecidos no contexto de regras do jogo democráticas.

Nas áreas de atuação governamental relacionadas com a defesa nacional e a política externa, a principal justificativa para a restrição da circulação de informações produzidas ou mantidas pelo governo é o dano potencial que sua apropriação por uma terceira parte (um governo estrangeiro ou organização adversária) poderia causar para a segurança estatal e, por decorrência, para a segurança individual dos membros da coletividade. Por exemplo: sistemas de armas, planos de contingência e mobilização, pesquisa científica e tecnológica de aplicação militar, intenções em negociações de acordos internacionais, desempenho de capacidades defensivas e outras coisas semelhantes, uma vez conhecidas por um adversário ou inimigo, potencializam nossas vulnerabilidades e fornecem uma vantagem comparativa crucial para os adversários nas interações conflitivas.

Além de ser necessário por razões puramente defensivas, o segredo muitas vezes também é decisivo para que os governos possam planejar, implementar e concluir missões militares e diplomáticas. Um exemplo óbvio do papel crucial do segredo é a tentativa de obtenção de surpresa em ataques militares, mas também se pode argumentar na mesma direção em relação ao sucesso de negociações diplomáticas sensíveis (ver, por exemplo, as negociações secretas entre China e Estados Unidos que precederam a visita de Nixon a Pequim em 1972, ou as negociações secretas entre representantes palestinos e israelenses que precederam os chamados Acordos de Oslo em 1993). Nesses casos, a justificação do segredo baseia-se mais na necessidade de impedir que os objetivos governamentais sejam frustrados pela publicização precoce da informação do que nos danos potenciais à segurança nacional.

A necessidade de sigilo também é reivindicada em processos de deliberação intragovernamental sobre os temas domésticos considerados relevantes para a segurança nacional (energia, transportes, policiamento etc.), processos decisórios durante os quais a revelação prematura das divergências de opinião dentro do governo poderia ser danosa para a segurança das operações e para a possibilidade de sucesso de qualquer das metas e planos eventualmente escolhidos. Nesses casos, a aplicação de restrições de sigilo são muito mais problemáticas em termos legais e, principalmente, políticos. O risco envolvido, do ponto de vista da democracia, é que o recurso ao sigilo impeça a necessária transparência dos atos governamentais, tanto pela impossibilidade de verificação de responsabilidades individuais na história administrativa das decisões, quanto pela restrição pura e simples dos direitos políticos dos cidadãos.[9]

Uma última justificativa genérica para o segredo estatal é a necessidade de proteger as identidades e relacionamentos confidenciais de agências governamentais com certos indivíduos, grupos e governos. A necessidade de sigilo nesses relacionamentos emerge de uma variedade de contextos e toma formas diversas, embora o caso mais evidente seja justamente o da proteção de fontes e métodos na área de inteligência. Além do risco de vida para os próprios indivíduos e suas famílias, a exposição (*blow*) desse tipo de relacionamento através do fracasso de uma das partes em manter segredo tem efeitos em cadeia sobre a disposição de cooperação futura, o que é considerado prejudicial para a segurança nacional e para a perspectiva de viabilização dos interesses e políticas governamentais na arena internacional.

A justificativa para o segredo estatal é a necessidade de proteger as identidades e relacionamentos confidenciais de agências governamentais com certos indivíduos, grupos e governos

Para além da justificação pública sobre sua necessidade prática e validade moral, os segredos de Estado não se manteriam secretos se contassem apenas com a discrição dos indivíduos que partilham a informação sigilosa ou com a indiferença alheia. Na próxima seção discutem-se os mecanismos de proteção aos segredos governamentais.

PROCEDIMENTOS OPERACIONAIS

A proteção dos segredos de Estado depende de três processos complementares: 1) procedimentos de classificação, 2) controles de acesso e 3) punições em caso de revelação não autorizada.

No primeiro caso, autoridades legalmente competentes identificam conjuntos informacionais sensíveis para a segurança nacional e aplicam regras de classificação que definem o grau de sigilo necessário e a intensidade das medidas de restrição física de acesso para cada informação.

As classificações de segurança são feitas através da atribuição de marcadores externos que definem a importância de cada informação para a segurança nacional (tipicamente, são utilizadas as categorias de confidencial, secreto e ultra-secreto).[10] A atribuição de um marcador específico para um documento ou conjunto informacional é feita — em tese — por um funcionário ou órgão legalmente autorizado. No caso de informações consideradas extremamente vitais para a segurança nacional, por exemplo, a atribuição da categoria de ultra-secreto só pode ser feita pela autoridade mais alta do país ou por sua expressa delegação.[11] As categorias de sigilo também prevêem tempos de duração para a restrição de acesso correspondentes ao grau de sigilo atribuído, ou seja, quanto mais secreta uma informação maior o tempo que transcorrerá até sua completa publicização.

No segundo bloco de medidas (controles de acesso), as medidas de restrição física de acesso a essas informações implicam sistemas de vigilância, manejo, armazenamento e transmissão, não importa em que mídia específica as informações estejam. A disciplina de segurança de sistemas de informações (*infosec*) preocupa-se não apenas com a criptografia das mensagens e acervos informacionais, mas cada vez mais com a redução das vulnerabilidades sistêmicas das redes de produção, armazenamento e comunicação de informações. No caso, trata-se de evitar que as informações sigilosas de categorias diversas sejam interceptadas por usuários não-autorizados, sejam alteradas ou destruídas.[12]

As classificações de segurança são feitas através da atribuição de marcadores externos que definem a importância de cada informação para a segurança nacional

Garantias adicionais de preservação dos segredos governamentais são obtidas através de sistemas de veto de acesso para pessoas não-autorizadas, bem como através de restrições adicionais de circulação das informações sigilosas através da aplicação do princípio conhecido como "necessidade de conhecer" (*need-to-know*).

Sistemas de veto envolvem a aplicação de procedimentos de checagem de segurança para todas as pessoas que se candidatam a um emprego em agências governamentais na área de defesa, inteligência e segurança. Nas áreas consideradas críticas para a segurança nacional, controles de segurança são aplicados tanto para funcionários civis e militares quanto para empregados de empresas privadas que mantenham contratos com agências governamentais. No caso das agências de inteligência, além das checagens padronizadas sobre antecedentes criminais e fichas de crédito e saúde, são realizadas entrevistas mais detalhadas com parentes, vizinhos e conhecidos sobre o passado individual, além da aplicação de testes especiais (*background investigations*). Depois de passar satisfatoriamente pelos sistemas de veto e investigação, para ter acesso a informações classificadas (sigilosas) os ocupantes de cargos públicos precisam obter credenciais correspondentes ao nível de classificação da informação (reservada, confidencial, secreta e ultra-secreta). Em geral, o nível de acesso depende do grau de senioridade do funcionário e/ou da importância do cargo ocupado. Vale observar que, uma vez concedida a credencial de acesso, a mesma não acompanha o funcionário ou a autoridade eleita independentemente dos cargos que ele ocupar ou do período transcorrido. Checagens de segurança periódicas são, ao menos em tese, necessárias para a renovação das credenciais de acesso.[13]

Porém, por mais drásticos que sejam os procedimentos de segurança para a concessão de credenciais, o acesso aos segredos governamentais depende ainda da aplicação do princípio *need-to-know*. Basicamente, a necessidade de conhecer diz que cada documento ou conjunto informacional pode ser acessado apenas pelos funcionários que efetivamente precisam ficar sabendo do seu conteúdo, e não por qualquer um que possua uma credencial de acesso com nível de classificação compatível. Isso gera novos marcadores externos e restrições adicionais para o acesso aos segredos governamentais. No caso do sistema de classificação dos Estados Unidos, por exemplo, além das três categorias ascendentes de segurança (*confidential*, *secret* e *top secret*), são utilizados cerca de cinqüenta marcadores adicionais que, embora não tenham o mesmo estatuto legal, muitas vezes estabelecem regulação mais intensa do que o sistema formal. Programas, informações e documentos com acesso especial (SCI – *special compartimented information*) podem ser estabelecidos com base no princípio da "necessidade de conhecer".[14]

No terceiro bloco de medidas, se falham os procedimentos

de segurança entram em cena os elementos dissuasórios que diferenciam a definição de segredo de Edward Shils: sanções administrativas e penalidades legais. Nesse caso, é importante diferenciar a obtenção de segredos através da espionagem do mero vazamento de informações sigilosas para o público.

Segundo Lustgarten e Leigh (1994: 221-248), por se tratar de uma ação discreta e/ou furtiva a espionagem bem-sucedida abre uma cunha na segurança de informações que o governo demora a perceber ou sequer toma consciência. Um espião operando em favor de um governo estrangeiro, independentemente de suas motivações (ideologia, dinheiro, chantagem, vingança etc.), não pode alegar o bem comum da nação que ele está espionando e tampouco da humanidade como um todo para justificar sua ação. Quer se trate de um agente recrutado (cidadão ou residente permanente), ou de seu controlador estrangeiro (que pode ter cobertura diplomática ou não), o ato de espionar é uma ação que altera a distribuição de poder internacional e trai a confiança na qual se baseia a própria cidadania. Em um mundo de Estados que precisam defender-se a si próprios, a espionagem é uma conduta criminalizada na maioria dos ordenamentos legais. Nos Estados Unidos, como se sabe, dependendo da gravidade do caso a espionagem pode ser punida pelo júri com a prisão perpétua ou mesmo com a pena de morte.[15] Mesmo que muitos espiões não cheguem sequer a ser processados, o que ocorre inclusive por razões intrínsecas à própria lógica das operações de contra-inteligência, o ponto a ser destacado é que a gravidade com que a espionagem é encarada contrasta com a relativa banalização dos vazamentos de informações sigilosas nas democracias.

A causa desse fenômeno reside no entendimento da jurisprudência de que a divulgação não-autorizada de informações sigilosas causa relativamente menos dano do que a espionagem porque a própria publicização da informação imediatamente alerta o governo e desencadeia contramedidas e tentativas de controle de danos. Também pode ser que a divulgação não autorizada de informações sigilosas tenha sido acidental, ou que tenha sido intencionalmente motivada pela decisão de expor alguma corrupção, arbítrio ou incompetência governamental que vinha sendo ocultada através do manto do segredo público. Nesses casos, mesmo que a motivação do agente que torna pública a informação faça diferença para a avaliação de sua credibilidade, os danos para a segurança nacional devem ser contrastados com o eventual benefício público resultante da transgressão. Obviamente, isso é sempre controverso.[16]

Na maioria dos casos que aparecem corriqueiramente na mídia, na verdade o vazamento de informações sigilosas (*leakage*) é um recurso de poder utilizado por membros do próprio governo para lançar balões-de-ensaio sobre políticas e projetos, para torpedear uma política da qual discordam ou meramente para avançar seus próprios interesses na disputa interburocrática. Nos Estados Unidos, o vazamento de informações sigilosas é penalizado com medidas administrativas (desde a censura até a perda do cargo ou emprego), multas em dinheiro e até dez anos de prisão.[17] Porém, nos Estados Unidos, assim como na maioria dos países, a relativa impunidade dos vazamentos de informações sigilosas por membros do alto escalão do governo central tende a gerar, por um lado, descrédito público para a necessidade de operar sistemas de classificação e, por outro lado, uma reação defensiva da parte dos órgãos de segurança que pode ser descrita como hiperclassificação.

Aliás, pode-se dizer que falhas em qualquer um dos três processos descritos nessa seção tendem a gerar uma expansão excessiva nos outros dois, como uma espécie de "compensação" perversa. Daí advém os riscos mais salientes para a compatibilização dos segredos governamentais com a democracia.

CONCLUSÃO: RISCOS E DEMANDAS POR CONTROLE

Seja como for, o segredo governamental é uma forma de regulação de fluxos de informação bastante utilizada no Estado contemporâneo. Os dados mais imediatamente disponíveis referem-se ao caso dos Estados Unidos, sabidamente de difícil comparação em função da escala. No relatório final da comissão criada pelo Congresso para analisar a "Proteção e Redução do Segredo Governamental" (1997), consta que apenas os documentos classificados com mais de vinte e cinco anos somavam naquele ano mais de 1,5 bilhão de páginas. O montante total de documentos classificados não é conhecido. Estima-se que num único ano (1992), o governo dos Estados Unidos tenha gerado 6,2 milhões de páginas de documentos classificados (sigilosos).[18] Cerca de 99% das classificações originais são feitas em quatro órgãos do governo federal: 53% no Departamento de Defesa, 30% na CIA, 10% no Departamento de Justiça, 3% no Departamento de Estado e 3% no

Departamento de Energia. É muito claro o peso dos órgãos de inteligência na formação do sistema de segredo governamental dos Estados contemporâneos.

Como lembra Michael Herman (1996:88-93), a relação entre segredo e atividades de inteligência começa pelo fato das operações de coleta de informações em inteligência visarem justamente a obtenção de informações que não podem ser obtidas (ou são mais dificilmente obteníveis) através de meios corriqueiros de pesquisa. Nesse sentido, como já disse Kenneth Robertson (1987), inteligência trataria, antes de tudo, da descoberta dos segredos de outros através da utilização de meios secretos. Na verdade, seria mais adequado afirmar que a *rationale* do segredo na área de inteligência assenta-se em três diferentes tipos de consideração a respeito de fontes, informações, operações, métodos e tecnologias empregadas.

Em primeiro lugar, utiliza-se o segredo como forma de regulação quando o valor da inteligência obtida depende do alvo não ficar sabendo o que efetivamente se sabe sobre ele. Por exemplo: o conhecimento prévio de um plano inimigo para um ataque surpresa abre a possibilidade de se preparar uma emboscada. Mas isso só é possível se o inimigo não souber que a vítima do ataque sabe que será atacada.

Em segundo lugar, o segredo deriva também da precária situação legal dos métodos empregados para coletar inteligência. Principalmente em tempo de paz, espionagem, vigilância eletrônica e invasão de redes de computadores (*computer hacking*) contrariam as leis dos países/alvos e mesmo as leis internacionais que garantem a inviolabilidade do território, do espaço aéreo e das águas territoriais. Os custos políticos dessas violações podem ser minimizados através do segredo, que também permite um manejo diplomático mais eficaz das crises eventuais.

Em terceiro lugar, a razão mais forte para o segredo é a vulnerabilidade das fontes às contramedidas de segurança que o alvo tomaria, caso soubesse do esforço adversário em obter inteligência. De qualquer modo, o que se pretende proteger através do segredo não é qualquer informação em particular que uma fonte já tenha fornecido, mas sim a continuidade dos fluxos de inteligência. [19]

Na guerra e na paz, segredos marcam profundamente o *modus operandi* e a cultura organizacional dos serviços de inteligência, mesmo quando o trabalho de análise baseia-se principalmente em fontes ostensivas, não secretas. Note-se que não existe relação direta e unívoca entre a natureza secreta das fontes ou meios de coleta e a qualidade das análises produzidas em inteligência. Há sim, no entanto, associações negativas entre a intensidade/quantidade de segredos governamentais e a possibilidade de controle dos cidadãos sobre o governo.

Portanto, do ponto de vista dos arranjos institucionais democráticos a aplicação desse tipo de regulação a um fluxo informacional qualquer teria um duplo ônus da prova: o da necessidade do segredo para a eficácia da missão governamental e o da garantia de controle público, ainda que indireto. A aplicação desse duplo teste deveria ser feito regularmente pelo Congresso e por mecanismos de inspetoria dentro do próprio poder executivo. Essa seria uma forma — a mais simples e até onde me ocorre a única possível — de se realizarem testes cruciais para o dilema da compatibilização entre autonomia governamental e representatividade democrática nessa área extrema do segredo governamental.

e-mail: mcepik@fafich.ufmg.br

NOTAS

1 A formulação geral do dilema da representatividade, assim como a distinção entre responsividade (ex ante) e accountability (ex post) e a reflexão sobre a centralidade do acesso à informação para a efetividade dos mecanismos de controle público e para a representatividade são formulados de maneira mais extensa em: PRZEWORSKI, Adam & STOKES, Susan & MANIN, Bernard [editors]. Democracy, Accountability, and Representation. Cambridge-UK, Cambridge University Press, 1999. Páginas 01-27 e 329-344.

2 Para um aprofundamento da discussão realizada aqui sobre segredo governamental, ver principalmente: U.S. GOVERNMENT. (1997). Report of the Commission on Protecting and Reducing Government Secrecy. Pursuant to Public Law 103-236. Chairman of the Commission: Daniel P. Moynihan. Washington-DC, GPO, 1997. 114 pp [plus 110 pp with appendices]. SHILS, Edward A. (1956). The Torment of Secrecy. Chicago, Ivan R. Dee Inc., 1996. [reprint]. SCHEPPELE, Kim Lane. (1988). Legal Secrets: Equality and Efficiency in the Common Law. Chicago-MI, Chicago University Press, 1988. Juntamente como o livro de Sissela Bok - Secrets: On the Ethics of Concealment and Revelation, 1982 - estes foram os trabalhos teóricos sobre segredo que me pareceram mais relevantes.

3 Sobre a gênese da esfera pública burguesa e a posterior transformação da função política da esfera pública e do princípio da publicidade, ver: HABERMAS, Jürgen (1962). The Structural Transformation of the Public Sphere: An Inquiry into a Category of Burgeois Society. Cambridge-MA, MIT Press, 1994. Páginas 17-26 e 181-211. Sobre a distinção público/secreto, um comentário adicional pode ser encontrado em: BOBBIO, Norberto (1989). "Público/Privado". In: Enciclopédia Einaudi, volume 14 [Estado-Guerra]. Lisboa, Imprensa Nacional-Casa da Moeda, 1989. Páginas 176-190.

4 SCHEPPELE (1988:12).

5 A edição original do livro de Edward Shils, The Torment of Secrecy, é de 1956, mas utilizei a reimpressão de 1996, na qual há um texto introdutório de Daniel Patrick Moynihan também bastante útil.

6 Para uma teoria da interpretação legal do sigilo de informações econômicas privadas (propriedade intelectual e direito de patentes), bem como do sigilo para a garantia de privacidade individual e dos limites à revelação de informações sigilosas em processos judiciais, cf. SCHEPPELE (1989:109-320). A juridificação dos segredos privados não me interessa diretamente nesse trabalho sobre segredos públicos na área de segurança nacional, embora considerações

sobre os limites do segredo governamental venham a ser feitas incidentalmente, principalmente com base no direito do público à informação governamental e no direito dos indivíduos à privacidade.

7 A conhecida proposição kantiana ("todas as ações relativas aos direitos de outros homens, cuja máxima não é compatível com a publicidade, são injustas") é um imperativo categórico que redunda, para sermos consistentes com ele, na inaceitabilidade de quaisquer formas de segredo, bem como na inaceitabilidade da existência de serviços de inteligência. A proposição de Kant não se sustenta por razões teóricas e práticas. A partir de uma série de contra-exemplos de políticas moralmente corretas e formalmente justas, mas que não poderiam ser tornadas públicas por implicarem em riscos de auto-destruição ou incentivos perversos ao comportamento de transgressores (wicked), Luban propõe uma reformulação do princípio de publicidade/transparência nos seguintes termos: "All actions relating to the right of other human beings are wrong if publicizing their maxim would lead to self-frustration by undercuting the legitimacy of the public institutions authorizing those actions". LUBAN (1996:192). Além de implicar uma defesa do princípio de publicidade quase que pela sua negação, essa proposição é muito pouco clara, como reconhece seu próprio autor. Como um todo, porém, o ensaio de Luban é bastante provocativo e procura escapar consistentemente do beco sem saída de uma defesa transcendental do princípio de publicidade. Ver: LUBAN, David. (1996). "The Publicity Principle". In: GOODIN, Robert E. [editor]. (1996). The Theory of Institutional Design. Cambridge-UK, Cambridge University Press, 1996. Pages 154-198. A versão kantiana do princípio da publicidade é enunciada no segundo apêndice ao ensaio sobre a Paz Perpétua, chamado de "Sobre o Acordo entre Política e Moral segundo uma Concepção Transcendental do Direito Público". Cf. KANT, Immanuel (1795). "To Perpetual Peace: A Philosophical Sketch". In: KANT, Immanuel. (1983). Perpetual Peace and Other Essays. Indianapolis-IN, Hacket, 1988. Pages 135-139. Translated by Ted Humphrey. Ver também: KANT, Immanuel. (1984). Textos Seletos. Petrópolis, Vozes, 1985. Segunda edição.

8 David Luban cita o exemplo do escândalo Irã-Contras nos Estados Unidos, mas também discute criticamente a tradição que, de Platão até Hegel, justificou o uso de "nobres mentiras" devido à incapacidade do público de compreender e julgar adequadamente as razões dos governantes. Contra o argumento das "nobres mentiras", Luban defende o princípio de publicidade com base no que ele chama de "rational skepticism" a respeito da própria capacidade dos governantes e de uma expectativa razoável, não ingênua, a respeito da possibilidade de uma opinião pública educada formar juízos sobre as máximas de primeira e segunda ordem apresentadas pelos governantes. Cf. LUBAN (1996: 188-195).

9 Cf. BOBBIO, Norberto (1999). "Democracia e Segredo". In: BOVERO, Michelangelo [org.] e BOBBIO, Norberto. (1999). Teoria Geral da Política: A Filosofia Política e as Lições dos Clássicos. Rio de Janeiro, Campus, 2000. Páginas 399-415.

10 Na letra dos decretos, a atual regulamentação brasileira sobre segredo governamental é mais frouxa e genérica do que a norte-americana em relação ao que pode ou não ser classificado como sigiloso. O exato significado e os usos do texto legal dependeria de comparações sistemáticas sobre o manejo do segredo governamental nos dois países, o que não é possível fazer aqui. No Brasil, o capítulo III do decreto 2.134/97 prevê ainda uma categoria de classificação de sigilo inferior a essas três, chamada de "reservada". Essa categoria não é utilizada nos Estados Unidos, mas aparece na legislação britânica, canadense e australiana como "restricted". Para o caso brasileiro, cf. o decreto 2.134/97. In: BRASIL. (1999). Legislação Pertinente à Salvaguarda de Assuntos Sigilosos. Brasília, ABIN, 1999. 49 páginas. Para o caso norte-americano, cf. a executive order 12.958/95. In: U.S. CONGRESS. (1998). Compilation of Intelligence Laws and Related Laws and Executive Orders of Interest to the National Intelligence Community. Washington-D.C., GPO, 1998.797 páginas. Para informações sobre classificações de segurança na Grã-Bretanha, Canadá e Austrália, ver LUSTGARTEN e LEIGH (1994: 104-126).

11 Com base nesse princípio, em 1995 havia nos Estados Unidos 29 agências governamentais com delegações de autoridade para aplicar classificações de sigilo em primeira instância. Segundo o relatório da Comissão sobre Segredo Governamental citado anteriormente, o número de indivíduos com poder de atribuir sigilo caiu de cerca de 60.000 em 1970, para 5.400 em 1995. No caso brasileiro, o decreto 2.137/97 prevê que a classificação de ultra-secreto só poderá ser feita pelos chefes dos três poderes da República. Entretanto, as delegações de autoridade previstas para as categoriais secreto, confidencial e reservado são feitas em cascata, começando com governadores e ministros de Estado e indo até coordenadores de projetos em secretarias de governos municipais. Por exemplo, a classificação de segurança de um documento como sendo "reservado" introduz restrições de acesso público por até cinco anos. As autoridades que podem atribuir esse marcador são os chefes dos poderes Executivo, Legislativo e Judiciário federais, governadores, ministros de Estado, titulares de órgãos da administração pública federal, do distrito federal, estados e municípios, bem como por agentes públicos formalmente encarregados da execução de projetos, planos e programas. Até onde sei, não existem estudos sistemáticos sobre a eficiência e os problemas do atual sistema de classificação de segredos governamentais no Brasil.

12 Para uma introdução aos problemas de infosec, cf. o capítulo IX ("Defensive Measures for Intelligence") do trabalho já citado de KRIZAN (1999: 61-70). Para uma abordagem mais técnica e alentada, ver a parte dois ("Nuts and Bolts") do livro de MARTIN, Frederick T. (1999). Top Secret Intranet: How U.S. Intelligence Built Intelink. Upper Saddle River-NJ, Prentice Hall, 1999. Para o caso do Brasil, cf. o decreto 2.910/98, que estabelece normas para a salvaguarda de documentos, materiais, áreas, comunicações e sistemas de informações de natureza sigilosa. Para o caso do Brasil, cf. ABIN (s.d.). Algumas Dicas para Salvaguardar o Conhecimento na sua Organização. [texto redigido provavelmente em 1999 no âmbito do Programa Nacional de Proteção ao Conhecimento - PNPC].

13 Além das referências já mencionadas, no caso dos sistemas de veto de segurança para candidatos a empregos e das investigações de background de funcionários para a concessão de credenciais de acesso, ver: LUSTGARTEN e LEIGH (1994:127-163). Nos Estados Unidos, em 1993, mais de 3,2 milhões de funcionários federais e trabalhadores de firmas contratadas possuíam credenciais de acesso a informações classificadas (2,29 milhões possuíam nível de acesso secret, 768 mil top secret e 154 mil confidential). Cf. o capítulo IV ("Personnel Security: Protection Through Detection") in: U.S. GOVERNMENT. (1997). Report of the Commission on Protecting and Reducing Government Secrecy. Washington-DC, GPO, 1997. Páginas 75-94.

14 No caso brasileiro, embora o decreto 2.134/97 preveja medidas adicionais de controle com base no princípio da "necessidade de conhecer", o único marcador adicional previsto é o DSC - "documento sigiloso controlado". Nos Estados Unidos, além de uma categoria similar (ORCON - "Dissemination and Extraction of Information Controlled by Originator"), camadas extras de classificação de segurança envolvem o uso, por exemplo, de marcadores não sigilosos como FOUO (para uso oficial apenas), NOFORN (vetado para estrangeiros) e NOCONTRACT (vetado a empreiteiros ou contratados), até marcadores que aprofundam o sistema de sigilo, tais como WNINTEL (nota de alerta: fontes ou métodos de inteligência foram utilizados) NATO secret e NATO high secret, além das chamadas listas BIGOT (listas que necessitam de códigos especiais de acesso), para citar apenas alguns exemplos. Cf. U.S. GOVERNMENT. (1997). Report of the Commission on Protecting and Reducing Government Secrecy. Washington-DC, GPO, 1997. Páginas 19-48.

15 Chapter 37 (Espionage and Censorship) of Title 18, United States Code. In: U.S. CONGRESS. (1998). Compilation of Intelligence Laws and Related Laws and Executive Orders of Interest to the National Intelligence Community. Washington-D.C., GPO, 1998. Páginas 359-366.

16 No caso do ex-membro da CIA Philip Agee, que publicou em 1975 um livro-denúncia sobre as operações da agência na América do Sul com uma lista de 2.500 nomes reais de operadores e agentes, a justificativa do autor era que sua campanha serivia aos interesses das vítimas de atividades ilegais da CIA e que os nomes revelados estavam envolvidos em assassinatos e desestabilização de regimes democráticos. A Suprema Corte dos Estados Unidos não aceitou essa justificativa e cassou a cidadania de Agee em 1981. O Congresso americano aprovou uma lei em 1982 (Intelligence Identities Protection Act) criminalizando a revelação da identidade de funcionários norte-americanos de agências de segurança nacional operando sob cobertura. A controvérsia sobre o caso Agee nos Estados Unidos arrasta-se até hoje. Embora tenham surgido denúncias sobre a ligação de Philip Agee com o serviço de inteligência de Cuba, o ex-funcionário da CIA nunca foi processado por espionagem nos Estados unidos. Cf. POLMAR & ALLEN (1997:06). O caso Agee interessa aqui apenas para ilustrar os mecanismos de sanção à publicização de informações secretas e suas ambigüidades. A literatura de denúncia sobre a CIA na década de setenta é bastante vasta. Sugiro começar pelo próprio: AGEE, Philip (1975). Dentro da Companhia: Diário da CIA. São Paulo, Civilização Brasileira, 1976. Ver também: MARCHETTI, Victor, & MARKS, John. (1979). The CIA and the Cult of Intelligence. New York: Times Books, 1979.

17 Cf. parágrafo 798 (disclosure of classified information) do capítulo 37 (Espionage and Censorship) do Title 18 do United States Code [U.S.C.] In: U.S. CONGRESS. (1998). Compilation of Intelligence Laws and Related Laws and Executive Orders of Interest to the National Intelligence Community. Washington-D.C., GPO, 1998. Páginas 359-366.

18 A informação sobre quantas páginas de documentos classificados existem hoje nos Estados Unidos, caso o próprio governo saiba, é classificada. Documentos classificados com mais de 25 anos são elegíveis para revisão e desclassificação automática com base na executive order 12.958/95. Documentos mais recentes são revisados para desclassificação sob requerimento amparado no Freedom of Information Act (FOIA). Cf. U.S. GOVERNMENT. (1997). Report of the Commission on Protecting and Reducing Government Secrecy. Washington-DC, GPO, 1997. Páginas 49-74.

19 Cf. Michael HERMAN (1996: 90-92) sobre por que a imprensa deveria se abster de publicar informações sigilosas obtidas de um adversário e que aparentemente o inimigo/adversário/competidor já sabe que foram obtidas. O argumento diz basicamente que isso contribuiria apenas para alertar as autoridades superiores do país adversário de que houve uma brecha de segurança, levando-as a investigar e rever os procedimentos, o que interromperia o fluxo de informações potencialmente oriundo daqueles canais.