INTEGRAÇÃO DOS ÓRGÃOS DE CONTROLE E COMBATE À CORRUPÇÃO

Ricardo Augusto Panquestor Nogueira

2009

CAMARA DOS DEPUTADOS

CENTRO DE FORMAÇÃO, TREINAMENTO E APERFEIÇOAMENTO

PROGRAMA DE PÓS-GRADUAÇÃO

RICARDO AUGUSTO PANQUESTOR NOGUEIRA

INTEGRAÇÃO DOS ÓRGÃOS DE CONTROLE E COMBATE À CORRUPÇÃO

BRASÍLIA

2009

RICARDO AUGUSTO PANQUESTOR NOGUEIRA

INTEGRAÇÃO DOS ÓRGÃOS DE CONTROLE E COMBATE À CORRUPÇÃO

Artigo apresentado para aprovação no curso de Especialização em Auditoria Interna e Controle Governamental realizado em parceria pelo Instituto Serzedello Corrêa do Tribunal de Contas da União, pelo Centro de Formação, Treinamento e Aperfeiçoamento da Câmara dos Deputados, pela Escola da Advocacia-Geral da União e pela Controladoria-Geral da União – CGU.

Orientadora: Tatiana Malta Vieira

Brasília

2009

Autorização

Autorizo a divulgação do texto completo no sítio da Câmara dos Deputados, do TCU, da AGU e da CGU e a reprodução total ou parcial, exclusivamente para fins acadêmicos e científicos.

Assinatura:_____

Data: ___/___/____.

Nogueira, Ricardo Augusto Panquestor.
Integração dos órgãos de controle e combate à corrupção [manuscrito] / Ricardo Augusto Panquestor Nogueira. -- 2009.
14 f.

Orientador: Tatiana Malta Vieira.
Impresso por computador.
Trabalho de conclusão de curso – Artigo científico (especialização) – Escola da AGU, da Advocacia-Geral da União, Centro de Formação, Treinamento e Aperfeiçoamento (Cefor), da Câmara dos Deputados, Secretaria Federal de Controle Interno (SFC), da Controladoria Geral da União e Instituto Serzedello Corrêa (ISC), do Tribunal de Contas da União, Curso de Especialização em Auditoria Interna e Controle Governamental, 2009.

1.Corrupção, fiscalização, Brasil. 2. Informação sigilosa, proteção, Brasil. 3. Segurança de dados, Brasil. 4. Administração pública, Brasil. I. Título.

CDU 343.352(81)

INTEGRAÇÃO DOS ÓRGÃOS DE CONTROLE E COMBATE À CORRUPÇÃO

Artigo: Curso de Especialização em Auditoria Interna e Controle Governamental do Instituto Serzedello Corrêa do Tribunal de Contas da União – 2º Semestre de 2009.

Aluno: Ricardo Augusto Panquestor Nogueira

Orientadora – Tatiana Malta Vieira.

Examinador – Osiris Vargas Pellanda

Brasília, 16 de dezembro de 2009.

Agradecimentos

Agradeço a todos que contribuíram para a conclusão deste artigo, aos parceiros e amigos, a família, principalmente ao meu filho Vitor, que mesmo não sabendo, é a principal razão de tanto emprenho e confiança no aprimoramento da defesa da coisa pública.

Resumo

Este artigo enfatiza questões referentes ao controle das atividades de combate à corrupção, integração e compartilhamento de dados e informações, assegurando-se durante todo o procedimento o cumprimento das medidas e procedimentos de segurança, destacando-se especialmente os seguintes desafios: (i) ausência de legislação adequada; (ii) receio de compartilhamento de dados e informações por parte dos agentes públicos; (iii) falta de continuidade das operações; (iv) freqüente vazamento de dados e informações sensíveis; e (vi) terceirização no desempenho dessa atividade, o que amplia os riscos relacionados a essa atividade.

Palavras-chaves: Controladoria-Geral da União – CGU; Tribunal de Contas da União – TCU; Advocacia-Geral da União – AGU; Poder Legislativo, Ministério Público Federal; Corrupção, controle, dados, informações, compartilhamento de informações, sigilo, vazamento, segurança.

Sumário:

1. Considerações iniciais

Este artigo enfoca o estudo do tratamento adequado e contínuo de dados e informações necessários aos trabalhos de combate à corrupção. Os órgãos de controle que exercem como atividade finalística o combate à corrupção, independentemente de trabalharem ou não com informações sigilosas, precisam que o ordenamento jurídico que regule os meios e procedimentos de integração e compartilhamento de dados, de forma a tornar suas atividades mais eficazes. Dentro desse contexto, impõe-se uma compreensão adequada da complexidade do tema e da diversidade de situações que podem se contrapor a esse compartilhamento, considerando-se os agentes envolvidos e os padrões dos procedimentos adotados.

Não é de hoje que obstáculos são gerados pela falta de atos normativos e, por vezes, pela inadequada interpretação da legislação existente, bem como pela retenção de dados e informações decorrente do receio de seu compartilhamento, o que dificulta a atuação dos órgãos de combate à corrupção.

Partindo-se dessa premissa, pretende-se demonstrar a necessidade de concepção de um modelo cuidadoso e mais eficaz de troca de dados e informações que permita dar continuidade às operações de combate à corrupção, evitando-se a sobreposição de competências, de forma a se ganhar tempo e agilidade no desempenho dessa atividade.

Nesse contexto, destaque-se a importância do desenvolvimento tecnológico, que possibilita o compartilhamento de dados e informações de maneira segura e eficaz, o que incrementa o trabalho conjunto dos diversos órgãos de controle e combate à corrupção. No cenário da sociedade da informação, ressalte-se a importância da parceria entre os órgãos de controle e a necessidade de se compartilharem informações por meio de dispositivos tecnológicos de ponta, de maneira contínua e segura – tudo isso a fim de salvaguardar o patrimônio público e a sociedade.

Observa-se que esse compartilhamento de dados e informações deve ser regulado por atos normativos que estabeleçam os procedimentos e as medidas de segurança a serem adotados, de forma a preservar seu sigilo, uma vez que o acesso irrestrito por terceiros pode prejudicar a própria investigação ou violar a proteção da

intimidade, vida privada, honra e/ou imagem de pessoas. Assim, não é demais destacar a relevância do princípio norte-americano denominado de *need to know*, segundo o qual só podem ser acessados dados e informações por quem tenha necessidade de conhecê-los para o exercício de cargo, função, emprego ou atividade.

Quanto ao uso de dispositivos tecnológicos, esses devem ser seguros o suficiente para evitar a quebra da autenticidade e integridade dos dados e informações compartilhados. Em relação à atualização dos dados coletados e compartilhados, ressalte-se a importância de adoção de procedimentos eficazes de controle, uma vez que podem remanescer inalterados em determinados bancos de dados e desatualizados nos demais, o que leva à contradição de cadastros em relação a um mesmo fato ou indivíduo, certamente prejudicial no processo de investigação.

Além desse aspecto, deve-se atentar para os tipos de dados pessoais que podem ser compartilhados, proibindo-se a troca 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 e à vida sexual do indivíduo.

Diante desse quadro, faz-se necessário identificar algumas dificuldades no processo de troca de dados e informações, tais como a falta de continuidade em relação aos agentes públicos envolvidos na atividade, o receio de compartilhamento dos dados e informações coletados, o freqüente vazamento desses dados e informações para terceiros, bem como a falta de integração entre os órgãos e entidades dos Poderes Executivo, Legislativo e Judiciário das diversas unidades federativas.

Não se pode ignorar, ainda, o crescimento acentuado da corrupção e de suas ramificações em todas as esferas de Governo e Poder, abrangendo indivíduos dos setores público e privado, que corriqueiramente se associam com o objetivo de praticar condutas ilícitas. Sob essa perspectiva, ressalte-se a importância das pessoas, visto que são elas que movimentam a máquina estatal e possuem as prerrogativas para o exercício regular de suas atribuições dentro de cada órgão ou entidade, sendo, portanto, de suma importância para a eficácia e legalidade dos trabalhos implementados.

Relevante destacar, dentro dessa perspectiva, a significativa existência de agentes públicos sem qualquer vínculo efetivo com a administração envolvidos nas áreas de informação, ou seja, responsáveis pela busca, controle, arquivamento, análise e manuseio de dados sensíveis, o que fragiliza todo o sistema de informações quanto aos aspectos dos recursos humanos e logísticos.

Além da fragilidade do elo humano, a corrupção tem transposto de maneira assombrosa diversos Estados em todas as esferas de poder. Apenas a título exemplificativo, registre-se que de acordo com o representante do *Federal Bureau of Investigation* - FBI, Carlos Alberto Costa, é movimentada uma quantia aproximada de 1,5 (um vírgula cinco) trilhão de dólares por ano em *lavagem de valores*, desconsiderando o narcotráfico e o crime organizado. Isso representa 5% (cinco por cento) da produção mundial e mais de ¼ (um quarto) de todo o comércio internacional de mercadorias. Assim, merece intensa reflexão o substancioso poderio econômico da criminalidade moderna[1].

Assim, o bom senso na execução das diligências e no levantamento dos indícios de criminalidade invoca a utilização de meios mais adequados, sem a participação de intermediários, ou seja, sem a cooperação direta ou indireta de terceiros, exceto quando realmente necessário.

2. Compartilhamento de dados e informações

Conforme já exposto, no processo de combate à corrupção não basta a coleta de dados e informações, sendo ainda mais essencial o seu compartilhamento, fase primordial em todo o complexo sistema de investigação das quadrilhas.

O assunto compartilhamento não remete somente à troca de informações e dados, mas também a uma série de cuidados que contribuem para a boa utilização do conhecimento, pois sem um cuidado razoável no que se refere a risco, proteção do sigilo, segurança e outros temas que serão tratados neste tópico, todo o processo fica prejudicado.

Assim, segundo Jorge Gustavo Serra de Macedo Costa, o crescimento das organizações ilegais demanda a adoção de procedimentos mais eficientes de investigação e de troca de informações entre os agentes do Estado:

> A complexidade das operações realizadas pelos infratores torna indispensável a adoção, pelos órgãos de investigação, de mecanismos eficazes através dos quais se possa conhecer e desvendar a origem da riqueza movimentada.[2]

---

[1] SANCTIS, Fausto Martin de. Juiz Federal da 6ª Vara Criminal de São Paulo. In: JUNIOR, José Paulo Baltazar; MORO, Sergio Fernando. *Lavagem de Dinheiro.*Ed. Livraria do Advogado, 2007. p. 58.

[2] COSTA, Jorge Augusto Cesar de Mancedo. Juiz Federal da 4ª Vara Criminal de Belo Horizonte. . In: JUNIOR, José Paulo Baltazar; MORO, Sergio Fernando. *Lavagem de Dinheiro.*Ed. Livraria do Advogado, 2007. p. 131.

Diante poderio econômico, tecnológico e organizacional dos criminosos, os órgãos de combate à corrupção são forçados a se estruturarem e aprimorarem seus procedimentos para uma adequada prevenção e repressão a essas condutas. Como conseqüência da profissionalização das organizações criminosas, surge a necessidade de se incrementarem os procedimentos de interceptação de dados e informações, inclusive por meio de mecanismos de interceptação ambiental, e de infiltração de agentes de Estado nesses grupos.

No contexto da interceptação de dados e informações, verifica-se que o direito à privacidade e intimidade do investigado, garantido constitucionalmente não é absoluto, pois cede espaço diante do interesse legítimo do Estado e da sociedade, segundo bem assenta o Supremo Tribunal Federal, *verbis*:

> 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 estão sujeitas – e considerando 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[3]

Nesse diapasão, deve-se considerar que em algumas hipóteses o interesse público se sobrepõe ao direito do particular, conforme estabelece a Lei Complementar nº 105, de 10 de janeiro de 2001, que assim registra:

> Artigo 1º As instituições financeiras conservarão sigilo em suas operações ativas e passivas e serviços prestados.
>
> § 4º A quebra de sigilo poderá ser decretada, quando necessária para apuração de ocorrência de qualquer ilícito, em qualquer fase do inquérito ou do processo judicial, e especialmente nos seguintes crimes:
>
> .....
>
> VI – contra a Administração Pública;[4]

---

[3] www.stf.gov.br – MS 23452/RJ (DJ de 12.05.00 p, 00020) – Ministro Celso de Melo. Acesso 20 out. 2009.

[5] In BRASIL. Lei Complementar nº 105, de 10 de janeiro de 2001. Disponível em: < http://www.planalto .gov.br/civil/LEIS/LCP/Lcp105.htm>. Acesso 14 dez. 2009.

Na hipótese de prática de crime contra a Administração Pública, a proteção do sigilo das informações cede frente ao interesse público, permitindo-se a coleta de dados pessoais pelo Estado para fins de investigação criminal mediante autorização judicial. Outra situação em que é legítima a coleta de informações pessoais ocorre quando o próprio titular ou seu preposto autorizam esse procedimento. Assim, existindo concordância por parte do indivíduo ou de seu representante legal, ou autorização legal, passa a ser legítima a obtenção, a interconexão e o compartilhamento de dados e informações pessoais.

Segundo Tatiana Malta Vieira, as 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 recolhidos diz respeito à situação em que o próprio Estado promove tal recolhimento, e para fins de preservação de outros interesses públicos, como a investigação criminal ou o exercício da atividade de inteligência[5].

Além da necessidade de se definirem os procedimentos de interceptação de dados e informações, deve-se levar em consideração a ausência do Estado, a insegurança da sociedade e, o que é pior, o poder de intimidação e de organização dos criminosos, transpassando não só as fronteiras dos muros dos presídios, mas também dos Estados e municípios de maneira assombrosa, fazendo com que o cidadão fique refém dos caprichos e do poder de intimidação dos delinqüentes, conforme relata Carlos Amorim, citado por Cássio M.M. Granzinoli no artigo intitulado “A delação premiada”, quando demonstra a estrutura de logística das quadrilhas:

> No meio da noite, prédios públicos são atacados com rajadas de fuzis automáticos e metralhadoras. Bombas explodem em frente a repartições públicas. Comboios de homens armados percorrem as ruas depois da meia noite. Param o trânsito em grandes avenidas, saqueiam – pessoas são mortas sem nenhuma razão. Magistrados são emboscados e mortos a tiros. Funcionários de alto escalão são ameaçados. Pelo mar chegam armas e drogas. É o cenário de uma guerra que não se quer admitir. Escolas, comércio e bancos fecham a mando de meninos descalços, que se dizem porta-vozes de grandes traficantes e bandidos. Todos obedecem. Inimigos dos bandos armados são apanhados, julgados e executados sumariamente. Os policiais escondem suas identidades e se

[5] VIEIRA, Tatiana Malta. *O direito à privacidade na sociedade de informação*: efetividade desse direito fundamental diante dos avanços da tecnologia da informação. Porto Alegre: Sergio Antonio Fabris Ed., 2007, p. 253..

> protegem atrás de barricadas. Trinta mil presos chegam a se rebelar de uma só vez, atendendo ao comando de uma liderança de cinco homens. Agora não é mais ameaça. A sombra ganhou contornos próprios. Porque o crime organizado no Brasil é uma realidade terrível. Atinge todas as estruturas da sociedade, da comunidade mais simples, onde se instala o traficante, aos poderes da República. Passa pela polícia, a justiça e a política. A atividade ilegal está globalizada e o país é um mercado privilegiado no tabuleiro do crime organizado.[6]

As medidas tomadas pela administração são tímidas em comparação ao quadro que se apresenta, o que faz com que a corrupção avance de maneira exponencial, prejudicando o interesse público. Na medida em que o Estado não consegue executar o seu papel ou é ausente, os criminosos controlam atividades estratégicas como o comércio e a própria segurança dos moradores das favelas.

Diante ineficiência estatal, destaca-se a necessidade de regulamentação das medidas e procedimentos de compartilhamento de dados e informações para fins de combate à corrupção, uma vez que nenhum órgão detém todo o conhecimento necessário a uma eficaz investigação.

Nesse contexto, fortalece-se a área do conhecimento denominada de *segurança da informação*, responsável por resguardar os pilares da informação enquanto ativo, quais sejam: disponibilidade, integridade, confidencialidade e autenticidade, além da legalidade, conforme destacam alguns autores[7].

Vale lembrar que a proteção da informação deve ocorrer em todos os seus ciclos, pois a violação de alguma de suas propriedades em qualquer fase de seu tratamento (produção, reprodução, utilização, acesso, transporte, transmissão, recepção, distribuição, armazenamento, eliminação e controle) poderá prejudicar todo o sistema, o que recomenda o mapeamento das ameaças, vulnerabilidades, riscos e impactos, bem como dos interessados em sua obtenção, a fim de diminuir os danos acarretados por uma eventual quebra de segurança.

Dentre as vulnerabilidades, destaca-se o grande número de profissionais terceirizados desempenhando funções que deveriam ser exclusivas de servidores públicos, tendo em vista seu caráter estratégico. Entre as ameaças, as mais preocupantes são os ataques cibernéticos aos sistemas informatizados públicos e a disseminação de vírus e outros códigos maliciosos. Os riscos são fatores inerentes a esse tipo de

---

[6] GRANZINOLI, Cássio M.M.. Juiz Federal. In: JUNIOR, José Paulo Baltazar; MORO, Sergio Fernando. *Lavagem de Dinheiro.* Ed. Livraria do Advogado, 2007. p. 145.
[7] SÊMOLA, Marcos. *Gestão da Segurança da Informação.* Ed. Módulo Security, 12ª tiragem, 2003. p. 9.

atividade e sua previsibilidade constitui o critério de diferenciação, conforme leciona Marcos Sêmola:

> Com a aceitação do axioma de que "é necessário medir para administrar", consolidou-se a idéia de que, para ter utilidade nos negócios, um determinado evento de risco deve ser previsível em termos de probabilidade de ocorrência (incidência), e deve ser passível de estimativa quantitativa (impacto). A administração do risco tem por diretiva que "risco é uma opção, não é destino", portanto devem ser assumidos, mitigados (alocados, controlados, compartilhados ou financiados) ou, simplesmente, evitados. A assunção de um risco inerente pressupõe a tomada de medidas negociais ou de controle por parte da empresa visando reduzi-lo, restando o chamado risco residual, o qual é muito comum na administração o risco operacional. O risco operacional decorre da realização das operações, estando associado às deficiências nos controles internos (...) o risco operacional é definido como o risco de perda resultante de pessoas, sistemas e processos internos inadequados ou deficientes, ou de eventos externos. O risco operacional se materializa em fraudes praticadas por empregados e falhas nos processos e nos sistemas informatizados, e ocorrem em função de desenho organizacional inadequado, da falha de planejamento e de monitoração na delegação de poderes, da utilização de procedimentos sem uniformidade e da observância de produtos e processos. Com esse amplo leque de origens, o risco operacional interpenetra os demais tipos de risco e mantém interseção causal com esses mesmos riscos.[8]

Dentre os riscos que devem ser evitados, destaca-se o compartilhamento de informações em partes, vez que ter ciência de dados incompletos pode gerar resultados diversos do desejado, fazendo com que o Estado imprima resultados ilegais e irreais, o que pode prejudicar todo o processo de investigação, daí a necessidade de cuidado durante todo o tratamento das informações, especialmente nas fases de transmissão e recepção.

3. Panorama atual

O panorama atual, apesar de melhor se comparado há alguns anos, continua perturbador. Os corruptos agem sob suporte jurídico, político e estatal, o que força a reestruturação e reorganização dos órgãos de controle por meio de estratégias de caráter nacional, a exemplo da ENCCLA (Estratégia Nacional de Combate à Corrupção e à Lavagem de Dinheiro).

[8] SÊMOLA, Marcos. Op. cit., p.158.

Contudo, somente este trabalho não basta, eis que, em algumas operações o tempo e a segurança limitam a atuação do Estado, pois a demora e o retardamento da ação dos agentes de controle facilitam à corrupção, o que remete à necessidade de modernização dos entes estatais, conforme leciona Ada Pellegrini: "*o sistema italiano não se limitou à reforma das leis penais e processuais (estas, por vezes, criticáveis), mas se preocupou em adotar os órgãos de investigação e de persecução dos instrumentos necessários a enfrentar a criminalidade organizada, reequipando-os, modernizando-os e coordenando as atividades conjuntas do Ministério Público e da polícia*"[9].

Rodolfo Tigre Maia destaca o fortalecimento das organizações criminosas, o que poderia ser evitado através de uma completa reordenação das instituições públicas:

> Não se pode olvidar hoje que a ameaça do crime organizado à segurança nacional e internacional, em especial aos regimes democráticos, "é uma conseqüência inevitável das atividades de organizações que negam ao Estado seu legítimo monopólio da violência, que corrompem as instituições estatais, que ameaçam a integridade dos setores financeiros e comerciais da sociedade, e que, rotineiramente, desconsideram ou violam normas e convenções legais e sociais, quer no nível nacional, quer no internacional. O que faz essas formas de comportamento cada vez mais perturbadoras é o fato delas possibilitarem às organizações criminosas acumular um grau de poder e riqueza que rivaliza e, em alguns casos, ultrapassa o possuído pelos governos. Na medida em que estas organizações aprofundam suas raízes nas suas respectivas sociedades, elas caracterizam uma ameaça para ambas, democracia e aplicação da lei[10].

Nesse contexto, é imperioso dar tranqüilidade e meios aos agentes responsáveis pelo combate à corrupção, pugnando por melhores condições de trabalho com o fito de facilitar o compartilhamento e a troca de informações, única forma de coletar as provas necessárias à persecução criminal. No clássico caso de Al Capone, apesar desse indivíduo ter cometido inúmeros crimes, acabou sendo condenado apenas pela conduta de lavagem de dinheiro, a única em relação a qual existiam provas válidas, uma vez que diversas provas foram afastadas pelo Judiciário por serem consideradas nulas, o que também ocorreria no ordenamento jurídico nacional.

Destarte, as provas encontradas pelos meios de informações são inúmeras, e, nem sempre todas podem ser utilizadas, sendo prudente verificar o momento em que a prova pode ser utilizada de forma a não prejudicar a investigação e quais agentes

---

[9] JUNIOR, José Paulo Baltazar; MORO, Sergio Fernando. *Lavagem de Dinheiro*. Texto de Cássio M. M. Granzinoli, p. 160.

[10] MAIA, Rodolfo Tigre. . *Lavagem de Dinheiro*. 2ª edição. 2007. Malheiros Editores. p. 14. (Williams e Savona, 1996:vii).

públicos podem legitimamente acessá-la no desempenho de suas funções, o que corrobora o entendimento de que os diversos órgãos e agentes devem estar muito bem interligados, vez que, uma única prova pode contribuir para uma eficiente persecução criminal.

Outro ponto que não se pode deixar de considerar, é a auto-existência e o senso de preservação das quadrilhas e dos corruptos que as compõem. Elas não se exaurem por si só, pois sempre buscam meios alternativos de perpetuação em âmbito nacional e internacional.

Portanto, o panorama atual demonstra a necessidade de um intenso trabalho de parceria entre os órgãos de controle, de forma a melhor compartilhar as informações coletadas necessárias à comprovação das infrações relacionadas à corrupção.

4. Integração entre órgãos e agentes de controle

A eficiência da atividade de controle e combate à corrupção depende intrinsecamente da integração entre os órgãos de controle interno e externo. Nesse contexto, destaque-se a importante função da Controladoria-Geral da União, que de acordo com a Lei n. 10.683, de 28 de maio de 2003, funciona como órgão responsável pelo assessoramento direto ao Presidente da República no que se refere à defesa do patrimônio público, controle interno, auditoria pública, correição, prevenção e combate à corrupção, incrementando a transparência da gestão no âmbito da administração pública. Indiscutível também a importância de integração com os órgãos de controle externo, tais como o Tribunal de Contas da União – TCU, Ministério Público Federal - MPF e tribunais do Poder Judiciário, de forma a garantir um fluxo saudável de comunicação entre os diferentes setores.

A integração entre órgãos e agentes de controle e combate à corrupção consiste em um fator extremamente importante no contexto do fortalecimento das instituições do Estado Democrático de Direito, sendo de suma importância para a maior eficiência da máquina estatal no desempenho dessa atividade.

Nesse contexto, propõe-se a criação de um comitê federal formado por representantes da Controladoria-Geral da União – CGU, do Tribunal de Contas da União – TCU, do Ministério Público Federal – MPF, do Conselho Nacional de Justiça – CNJ e da Agência Brasileira de Inteligência – ABIN. Poderiam ser instituídos ainda,

comitês estaduais, distritais e municipais, de forma a garantir a participação de todos os entes federados.

Observa-se que nesse processo de abrangência nacional, deve-se evitar a pulverização dos agentes envolvidos, o que tornaria a articulação morosa e o ambiente competitivo, prejudicando inclusive o cumprimento dos trabalhos.

Portanto, recomenda-se a existência de uma ou mais estruturas, que possam se articular com facilidade, a partir da adoção de procedimentos e medidas de segurança sólidos, buscando informações nos setores diretamente envolvidos.

Segundo essa concepção de gestão, o comitê central, formado pelos representantes mencionados, deverá ter a atribuição específica de controle dos comitês setoriais, bem como dos processos de maior envergadura e relevância. Os comitês setoriais, formados à semelhança do comitê central, deverão ter a atribuição de realizar a fiscalização em nível estadual, distrital ou municipal, podendo contar com a participação de representantes de outros órgãos ou entidades, conforme suas necessidades específicas.

Para uma eficácia operacional plena, o comitê central deverá ter privilégio de acesso aos trabalhos desenvolvidos pelos setores envolvidos, garantindo-se o sigilo dessas informações em relação a terceiros.

As normas de constituição e controle desse sistema, antes de serem publicadas, devem ser discutidas entre pessoas com experiência e conhecimento específico sobre a atividade de controle, preferencialmente servidores públicos de carreira.

Conforme já destacado, o fortalecimento do crime organizado tem formado verdadeiros conglomerados de quadrilhas, o que, sem sombra de dúvida, torna ainda mais importante a atividade de informação. Devido à estrutura criminosa que não deixa qualquer dúvida acerca do seu dinamismo e poder, não há como se falar em trabalho de informação individualizado, até porque várias condutas delituosas abrangem muitas áreas, além de exigir expertise em ramos bem diferenciados, e que, um só órgão não possui pleno domínio. Determinadas capacidades de trabalho são diretamente ligadas a setores específicos, obrigando órgãos e estruturas de informação a reunirem elementos e dados de diversos setores.

Destarte, a interação entre as comunidades de informação caracteriza-se como de extrema importância, devendo ter uma estrutura que possa abranger a maior quantidade de dados e informações a serem disseminados de maneira segura aos setores responsáveis e competentes em cada esfera e comitê.

No contexto da busca da segurança pública, o setor de informação deve atuar em cooperação, carecendo de avaliação periódica para verificar a efetividade e o cumprimento das suas atribuições. Fatores como diversidade de autores e estruturas e redes ilimitadas de atuação, não podem permitir desempenhos isolados dos entes públicos, senão o Estado estará fadado ao fracasso.

5. Proposta de solução

Deve ser implementado um contato mais estreito entre os setores que trabalham com informação, no sentido de aprimorarem o manuseio dos dados e garantirem o seu adequado tratamento.

No que tange ao compartilhamento de dados, deve-se buscar o uso de tecnologias que possam garantir a confidencialidade das informações por meio de procedimentos de cifragem ou codificação de seu conteúdo, que somente pode ser acessado após a decifração ou decodificação.

Outro procedimento a ser adotado consiste na exigência de assinatura de Termos de Responsabilidade e Confidencialidade pelos agentes credenciados ao tratamento de dados e informações sigilosos. Os referidos documentos são utilizados para coibir os eventuais vazamentos, tanto intencionais como decorrentes da desídia de profissionais mal treinados para o desempenho dessa atividade.

Deve ser realizada, ainda, a sensibilização e o fortalecimento da cultura de segurança da informação, pois ela tem o propósito de formalizar o compromisso e o entendimento do servidor, diante de suas novas responsabilidades relacionadas à proteção das informações que manipula.

Os servidores devem ser informados de que seus desvios podem ser punidos, tanto por ação quanto por omissão, vez que, inúmeros agentes públicos não possuem noção da dimensão de suas responsabilidades e nem da importância das informações que manuseiam.

Nesse contexto, deve-se lembrar que o elemento mais fraco no processo de tratamento de dados e informações sigilosos são os recursos humanos, pois é inegável a sua presença em todas as fases, desde a coleta até o descarte ou destruição. Assim, os riscos podem ser minimizados por meio de um treinamento contínuo das pessoas,

especialmente quanto aos processos de controle de senhas e utilização de certificados digitais.

6. Considerações finais

Importante registrar que os agentes públicos não devem temer a execução de certas tarefas, mesmo aquelas que vão de encontro às questões políticas e de repercussão social, pois a administração pública deve trabalhar para o cidadão e para a sociedade e não para governos.

O ambiente de combate à corrupção e de informação deve ser limpo e seguro, de forma a diminuir as oportunidades de corrupção e os riscos de vazamento de dados e informações sigilosos, considerando as facilidades e a generalizada falta de ética.

O compartilhamento de dados e informações é legítimo caso seja baseado na preservação do interesse público, resguardando-se em todas as hipóteses os direitos individuais como a proteção da privacidade dos envolvidos, o que exige dos agentes públicos reserva, agilidade e comprometimento com o Estado e com a informação.

A existência de reciprocidade no processo de compartilhamento da informação entre os órgãos e setores é ponto determinante e essencial para o fiel cumprimento do dever de combate à corrupção, dando credibilidade aos agentes e organismos envolvidos.

No que tange ao combate à corrupção, são importantes as medidas já desenvolvidas pela administração, mas são incontestáveis as possibilidades de riscos e a necessidade de cuidados permanentes, sempre buscando o equilíbrio ideal entre a segurança e o dever do Estado de combater a corrupção nos diferentes setores.

REFERÊNCIAS BIBLIOGRÁFICAS

ALMEIDA, Marcelo Cavalcanti. *Auditoria: um curso moderno e completo*. 6. ed. São Paulo: Ed. Atlas, 1998.

ATTIE, William. *Auditoria: conceitos e aplicações*. 3ª ed. São Paulo: Ed. Atlas, 1998.

BARBOSA, Lívia. *Igualdade e meritocracia*: *a ética do desempenho nas sociedades modernas*. Rio de Janeiro: Fundação Getulio Vargas, 1999.

BALTAZAR JUNIOR, José Paulo. *Lavagem de Dinheiro*. 1. ed. Livraria do Advogado. 2007.

BERNSTEIN, Peter L. *Desafio aos deuses: a fascinante história do risco*. Rio de Janeiro: Ed. Campus, 1997.

BOYNTON, William C; JOHNSON, Raymond N; KELL, Walter G. Auditoria, capítulos 9,10 e 12. Tradução José Evaristo dos Santos. São Paulo. Atlas, 2002.

CASTRO, Domingos Poubel. *Auditoria e Controle Interno na Administração Pública*. São Paulo: Ed. Atlas, 2008.

CRUZ, Flávio da. *Auditoria Governamental*. 3. ed. São Paulo: Ed. Atlas, 2007.

GIL, Antonio de Loureiro. Auditoria Operacional e de Gestão. 3. ed. São Paulo: Atlas, 1998.

GOMES, Jonas; BRAGA, Gilberto. "*Governança e Governabilidade*". Valor Econômico, 24 de agosto de 2005.

GONÇALVES, Joanisval Brito. *Atividade de Inteligência e Legislação Correlata*. 1. ed. Ed. Impejus.

Instituto Brasileiro de Governança Corporativa (IBGC). Disponível em: <www.ibge.org.br>.

JUNIOR, José Paulo Baltazar; MORO, Sergio Fernando. *Lavagem de Dinheiro*. Ed. Livraria do Advogado. Porto Alegre.2007.

KAPLAN, Robert S.; NORTON, David P. A Estratégia em Ação – Balanced Scorecard. 16. ed. Rio de Janeiro: Ed. Campus.1997.

MAIA, Rodolfo Tigre. . *Lavagem de Dinheiro*. 2. ed. São Paulo. 2007. Ed. Malheiros.

REVISTA BRASILEIRA DE CONTABILIDADE. Brasília: 2000. n. 121, jan-fev. ARAÚJO, Francisco J. *Influência dos controles internos no trabalho do auditor independente*.

REVISTA DO BNDES. Rio de Janeiro. v. 12. n. 24. Dez. 2005. p. 149-188. In: JUNIOR, Sebastião Bergamini. Controles Internos como um Instrumento de Governança Corporativa.

REVISTA VALOR ECONÔMICO. Business Week. *Executivos perdem poder de decisão*. Valor Econômico, 3 de maio de 2005.

REVISTA DE CONTABILIDADE E FINANÇAS DA USP. São Paulo. Ano XIII, n. 28, jan-abril. 2002. Nilton Martins Cano. Da Contabilidade à Controladoria: a Evolução Necessária.

REVISTA PENSAR CONTÁBIL. Rio de Janeiro. n. 2. Nov. 1998. Francisco Aristides Neves Garcia. Controle Interno: Inibidor de Erros.

SÁ, Antonio Lopes de. *Curso de Auditoria*. 10ª ed. São Paulo: Ed. Atlas, 2002.

SÊMOLA, Marcos. *Gestão da Segurança da Informação*. 12ª ed. Ed. Módulo Security. São Paulo. 2003.

VIEIRA, Tatiana, Malta. *O direito à privacidade na sociedade de informação*: efetividade desse direito fundamental diante dos avanços da tecnologia da informação. Porto Alegre: Sergio Antonio Fabris Ed., 2007.

VIDIGAL, Antonio C. *Gestão de Risco e Governança Corporativa*. Disponível no site www.ibcbrasil.com.br/riskupdate.