Centro Universitário de Brasília – UNICEUB

Faculdade de Ciências Jurídicas e Sociais

Adelson Silva Moita

INTERCEPTAÇÕES TELEFÔNICAS: VIABILIDADE JURÍDICA DA AUTOMAÇÃO DO PROCEDIMENTO

Trabalho de Conclusão de Curso apresentado como requisito para obtenção do título de Bacharel em Direito pelo Centro de Ensino Universitário de Brasília – UNICEUB.
Orientador: Msc. Lásaro Moreira da Silva

Brasília
2009

Este trabalho é dedicado à minha esposa Vanessa e meus filhos Nadyne, Artur e Gabriel, que com paciência, compreensão e esforço, aceitaram e concordaram em abdicar de importantes momentos em família para que este trabalho pudesse ser concluído.

Agradeço primeiramente a Deus, por mais uma conquista; ao meu Orientador Dr. Lásaro Moreira, pela dedicação e correções, ao Dr. Marcus Vinícius Bastos pelo apoio e estímulo, ao Amigo e Ex-chefe, Delegado PCDF Dr. Celso Ferro, pelas discussões e dicas em torno do tema, e a todos os meus amigos da DIPO/PCDF pelas informações prestadas sobre a prática operacional das atividades de interceptação de telecomunicações telefônicas e telemáticas

RESUMO

As sociedades modernas se mostram cada vez mais exigentes com relação às respostas dos governos na garantia do usufruto dos direitos e garantias constitucionais onde quer que se manifestem. Em um contexto mundial onde tudo se mostra mais veloz, mais objetivo, informatizado e conectado, torna-se difícil conviver com sistemas que não estejam sintonizados com os novos paradigmas e novas tendências tecnológicas. O crime, igualmente, se torna tecnológico e demanda maior versatilidade do Estado para fazer face ao potencial ofensivo que traz como consequência. As leis, processos e procedimentos, necessitam, também, ser adequados aos novos problemas e situações que deve regular. Como um recorte de um tema bastante controverso por tocar na questão das garantias dos direitos de inviolabilidade da intimidade, nesta pesquisa procura-se discutir os conceitos doutrinariamente aceitos sobre as interceptações e os principais problemas observados na atividade em questão, os efeitos das vulnerabilidades detectadas no procedimento e discutem-se alternativas para solucionar as questões de vazamento das informações, da morosidade e da inserção efetiva dos órgãos judiciais no controle e fiscalização de tais operações, quais sejam o Tribunal de Justiça, Ministério Público e Polícias Judiciárias.

Palavras chave: Automação de processos. Gestão de interceptações. Interceptação Legal. Telecomunicações telefônicas e Telemáticas. Viabilidade jurídica.

LISTA DE FIGURAS

SUMÁRIO

INTRODUÇÃO

O objetivo do presente trabalho é discutir se a automação do procedimento das atividades técnicas de interceptação de comunicações telefônicas e telemáticas é juridicamente viável para fins de investigação criminal.

Embora a matéria não esteja pacificada nos meios jurídicos, deve ser encarada como passível de evoluir e se ajustar a novos métodos, práticas e tecnologias computacionais que lhe garantam maior segurança, compartimentação, sigilo e celeridade.

Os casos de irregularidades no processo de interceptação telefônica como o vazamento de informações, a percepção técnica de setores envolvidos nas operações de inteligência e a observação empírica do processo operacional, desde a representação formal pela interceptação legal até a liberação de sinais de áudio pelas operadoras de telefonia, e os dados relacionados à quebra de sigilo, administrados por empresas terceirizadas, servem de base para revelar um quadro de gravidade e comprometimento do processo.

Na primeira parte do trabalho apresenta-se uma síntese dos conceitos sobre interceptação telefônica à luz da doutrina vigente e, na mesma sintonia, apresenta-se, na sequência, uma síntese das tendências mundiais de automação de processos dos mais simples aos mais complexos, por meio do emprego de tecnologia da informação.

Discutem-se os principais problemas observados na atividade em questão, sob a óptica da Polícia Judiciária bem como os efeitos das vulnerabilidades detectadas em todos os ambientes por onde trafegam os documentos físicos decorrentes das representações, despachos e autorizações judiciais, desde as polícias, passando pelos tribunais de justiça, promotorias até chegar nas operadoras de telefonia fixa ou móvel.

No que pertine à análise da viabilidade jurídica da automação do processo, dentro da sistemática prevista na Lei 9.296 de 24 de julho de 1996, discutem-se alternativas para solucionar as questões vazamento das informações, da morosidade e da inserção efetiva dos órgãos judiciais no controle e fiscalização de tais operações.

O marco conceitual apoiou-se na doutrina jurídica específica sobre a temática da Lei em apreço, bem como nos trabalhos sobre informatização de processos nos âmbitos Federal, Estadual e municipal atualmente em efervescência no país e no mundo.

A metodologia utilizada no trabalho foi baseada em pesquisa bibliográfica documental e parte em trabalho de campo, junto à Polícia Civil do Distrito Federal – PCDF.

1 DOS ASPECTOS GERAIS DA INTERCEPTAÇÃO TELEFÔNICA E TELEMÁTICA

1.1 As interceptações Telefônicas e a Sociedade Moderna

A tecnologia disseminada nas sociedades modernas, sobretudo nos grandes centros urbanos, favorece a agilidade nas relações e amplia as possibilidades de maior número de negócios e trocas de informações. O que se percebe, também, e que vem a reboque dessa onda tecnológica, é o seu emprego, cada vez maior, no cometimento de crimes.

Na "Sociedade da informação" e no contexto de complexidade do ambiente social moderno, tanto para as pessoas quanto as organizações, sofrem as ações da rápida difusão tecnológica e massificação dos meios de comunicações (FERRO JÚNIOR, 2004; BRAGA, 2004).

Nessa sociedade identificam-se fatores tipicamente associados á evolução tecnológica e que se relacionam à velocidade, conectividade, intangibilidade e à complexidade ambiental, fazendo com que o crime também se aperfeiçoe e se desenvolva com características de organização, planejamento, diversificação de atividades, atuação sem limites territoriais, facilidade de comunicação e acesso à informação. (FERRO JUNIOR, 2009).

Nesse contexto as ações criminosas têm se globalizado e se apresentado predominantes à capacidade de combate do Estado, que ao que parece, tem dificuldades de fazer face ao movimento crescente de aperfeiçoamento e organização do crime, talvez, mais por temor aos impactos políticos do que sociais, fazendo com que as organizações policiais tenham que se confrontar diretamente com esses cenários desafiadores e complexos. (FERRO JUNIOR, 2009).

O grau de massificação dos crimes nessa sociedade tecnológica, e sua complexidade, revelada pelo volume de relações ilícitas amplamente divulgadas na mídia, permite estabelecer que dificilmente ocorram ações delitivas sem comunicação e sem o emprego de dispositivos de alta tecnologia, como é o caso dos telefones celulares, comunicações VoIP (voz sobre protocolos de internet) skype, messenger, telefones satelitais, correspondências eletrônicas etc. (FERRO JÚNIOR, 2005)

Os casos de irregularidades no processo de interceptação telefônica como o vazamento de informações, a percepção técnica de setores envolvidos nas operações de inteligência e a observação empírica do processo operacional, desde a representação formal pela interceptação legal até a liberação de sinais de áudio pelas operadoras de telefonia, e os dados relacionados à quebra de sigilo, administrados por empresas terceirizadas, servem de base para revelar um quadro de gravidade e comprometimento do processo. (FERRO JÚNIOR, 2005; GRECO FILHO, 1996).

É nesse contexto que as atividades de interceptações se inserem demandando maior profissionalismo e maior seriedade de todos os atores, inclusive na proposição de novas metodologias que tenham por escopo equilibrar os direitos e garantias constitucionais das pessoas e a necessidade do Estado em levar a efeito as investigações que possam solucionar de forma segura, célere e sigilosa crimes perpetrados contra a sociedade, sobretudo os que se relacionam com o crime organizado e crimes hediondos. (MOITA, 2009)

1.2 Contexto Jurídico e aplicabilidade da Interceptação Telefônica

Neste tópico buscar-se-á analisar como a doutrina tem interpretado a problemática da interceptação telefônica e telemática, buscando-se entender algumas diferenças existentes sobre o termo interceptação e seu emprego jurídico no Brasil.

O sentido que se deve dar à medida denominada de interceptação telefônica para efeitos jurídicos, sobretudo no contexto da Lei 9296/1996, não é o da etimologia da palavra e sim o da abrangência resultante do entendimento do legislador sobre a mesma (GOMES e CERVINI, 1997).

No sentido etimológico o termo interceptar pode significar interrupção do curso, deter, impedir na passagem, cortar, reter etc.[1]. Já na exegese jurídica aplicada, o termo possui, de acordo com a melhor doutrina, o sentido de captar, tomar conhecimento, ter contato com o teor de uma comunicação (GOMES e CERVINI, 1997).

Na interceptação haverá sempre a ingerência externa de um terceiro (GOMES e CERVINI, 1997; GRECO FILHO, 1996).

Do entendimento acima decorre a conclusão sucinta de que interceptação telefônica é a captação do conteúdo de uma comunicação estabelecida entre dois ou mais interlocutores, sempre levada a efeito de forma velada e sem a percepção ou conhecimento dos demais agentes da comunicação (GOMES e CERVINI, 1997; GRECO FILHO, 1996).

Destaca-se que não se pode confundir escuta telefônica com interceptação. A escuta telefônica é espécie do gênero interceptação, que consiste na captação de conversa telefônica entre dois ou mais interlocutores, porém um deles sabe ou tem conhecimento de que sua conversa está sendo monitorada ou mesmo gravada (GOMES e CERVINI, 1997).

A lei 9296/1996 abarca tanto a interceptação bem como a escuta telefônica.

---

1 Fonte:Novo Dicionário Aurélio, Ed. Nova fronteira 1ª ed.1997

O conceito utilizado por Gomes e Cervini, (1997), relativamente ao termo comunicação telefônica, empresta o sentido dado pela lei geral de telecomunicações que o define como sendo "o modo específico de transmitir informação, decorrente das características particulares de transdução, de transmissão, de apresentação da informação ou de combinação destas, considerando-se formas de telecomunicações, dentre outras, a telefonia, a telegrafia, a comunicação de dados e a transmissão de imagens" (GOMES e CERVINI, 1997).

Depreende-se do conceito que a locução comunicação telefônica é ampla, abarcando a transmissão ou recepção de símbolos, sinalizações, caracteres, imagens, sons ou informações de qualquer natureza, seja ela originária da telefonia fixa (STFC)[2] ou móvel (SMP[3]; SME[4] etc.)

Os dados relacionados ás chamadas telefônicas, que se perfazem nos registros técnicos de eventos havidos durante uma comunicação não se encontram explicitados na Lei 9296-96, e não gozam, segundo entendimento doutrinário, de sigilo absoluto, podendo, sim, ser objeto de quebra de sigilo pela via legal (GOMES e CERVINI, 1997).

O regime jurídico, pois, da interceptação e da escuta, em sentido estrito, prevê que se devidamente autorizada, nos termos da Lei 9296-96, constitui prova lícita e admissível; se não autorizada constituirá crime nos termos do art. 10 do diploma legal, sendo considerada prova ilícita, portanto, não admissível. (GOMES e CERVINI, 1997; GRECO FILHO, 1996).

---

2 STFC: Sistema de Telefonia Fixa Comutada ou simplesmente Sistema de Telefonia Fixa.

3 SMP: Sistema Móvel Privado ou Sistema de Telefonia Celular

4 SME- O Serviço Móvel Especializado também conhecido como Trunking ou sistema troncalizado, é um serviço muito semelhante ao serviço celular destinado a pessoas jurídicas ou grupos de pessoas caracterizados pela realização de atividade específica, não podendo, em regra, ser oferecido a pessoas físicas individualmente. Oferece a possibilidade comunicação tipo despacho (push to talk) para um grupo

1.3 O processo de Interceptação

Inobstante esteja disposto no regramento jurídico sobre as interceptações a forma como se deve proceder para levá-la a efeito, pretende-se apresentar neste tópico, como o tema procedimental é entendido pela doutrina, inclusive os pontos controversos entre autores que entendem, com base na experiência empírica, que há necessidade de se rever a forma que se tem solidificado como mais recomendável, mas que, na prática, acaba por inserir mais vulnerabilidade nessa sensível operação.

O procedimento de interceptação telefônica serve tanto para a instrução criminal, que se dá depois da instauração da ação penal, como para a investigação criminal, tendo como finalidade a produção de prova processual penal (GOMES e CERVINI, 1997; GRECO FILHO, 1996).

Para que seja autorizada a quebra do sigilo telefônico, há que se observarem os requisitos específicos conforme descritos no artigo 2º da Lei 9266/1996.

> Art. 2° Não será admitida a interceptação de comunicações telefônicas quando ocorrer qualquer das seguintes hipóteses:
> I - não houver indícios razoáveis da autoria ou participação em infração penal;
> II - a prova puder ser feita por outros meios disponíveis;
> III - o fato investigado constituir infração penal punida, no máximo, com pena de detenção.
> Parágrafo único. Em qualquer hipótese deve ser descrita com clareza a situação objeto da investigação, inclusive com a indicação e qualificação dos investigados, salvo impossibilidade manifesta, devidamente justificada.

A competência para a autorização da medida é absoluta, isto é, o juiz que determinar a quebra do sigilo estará automaticamente prevento para a ação principal (GOMES e CERVINI, 1997; GRECO FILHO, 1996).

De acordo com os termos da Lei 9296/1996, a interceptação poderá ser determinada pelo juiz de oficio ou a requerimento da autoridade policial, na investigação criminal, ou por membro do Ministério Público, tanto na investigação criminal como na instrução processual penal.

Das hipóteses acima, por conta do sigilo processual requerido, o contraditório só se dará a *posteriori* (GRECO FILHO, 1996).

Para a concessão da medida haverá necessidade de restar comprovado, por parte das autoridades requerentes (polícia ou Ministério Público), a imprescindibilidade da medida, a presença dos requisitos legais bem como a indicação dos meios a serem empregados (GOMES e CERVINI, 1997; GRECO FILHO, 1996).

Prevê-se na Lei que regulamenta a matéria que a autoridade policial poderá requisitar serviços e técnicos especializados às concessionárias, podendo, inclusive, realizar a diligência pessoalmente ou por intermédio de outra pessoa (GRECO FILHO, 1996).

Pela doutrina de GRECO FILHO (1996), sugere-se que, para contornar eventual problema de se ter a intimidade das pessoas e a segurança do sigilo da operação comprometido, deve o magistrado determinar que seja a medida executada exclusivamente pela concessionária de serviço telefônico, ou caso não se possa fazê-lo, que se proceda à identificação precisa de toas a pessoas que participarem da medida, e outros cuidados que entender apropriado para a manutenção do sigilo e responsabilidade na hipótese de sua quebra.

A respeito do posicionamento acima, existem pontos discordantes de outros autores (FERRO JUNIOR, 2006) já que seria temerário incumbir a um terceiro, sobretudo se for de natureza jurídica privada, o papel do Estado representado por um de seus representantes, isto é Tribunal de Justiça, Ministério Público ou Polícias Judiciárias.

O pedido de quebra de sigilo é, em regra, feito por escrito, admitido também o pedido verbal, devendo neste ultimo caso, ser reduzido a termo.

Para fins de cumprimento das formalidades legais (GOMES e CERVINI, 1997; GRECO FILHO, 1996), será imprescindível que o juiz fundamente a autorização, utilizando jurisprudência, doutrina, lei e, ainda, argumentos fáticos específicos do caso.

A deliberação, a partir do pedido, não deverá exceder ao prazo de 24 horas, devendo ser lembrado que o período máximo autorizado para a diligência não poderá ser superior a 15 dias.

A lei não se manifesta acerca de eventuais prorrogações, subtendendo-se, daí, que de acordo com o caso, poderá o magistrado conceder prorrogações em iguais períodos, se julgados necessários (GRECO FILHO, 1996).

Não há necessidade, para o deferimento da medida, da manifestação do Ministério Público em face do atendimento dos princípios da oportunidade e celeridade devendo-se observar, porém, que se não houver demanda de urgência será conveniente ao juiz submeter à sua apreciação inclusive para a garantia de utilização da prova posteriormente (GOMES e CERVINI, 1997; GRECO FILHO, 1996).

Caberá, em regra, à autoridade de polícia judiciária, federal ou estadual, a condução das diligências, sendo que o produto deverá ser encaminhado ao juiz na forma de auto circunstanciado apresentando o resumo das operações, as gravações e sua transcrição etc.

Depreende-se do exposto que para se levar a efeito medidas de quebra de sigilo para fins de instrução penal ou no curso das investigações pela Polícia, será facultado à autoridade policial ou representante do Ministério Público, representar pela quebra do sigilo telefônico dos suspeitos, desde que preenchidos os requisitos previstos na retrocitada lei.

Uma vez representado pela quebra do sigilo das ligações telefônicas, de determinado alvo, o processo se dá resumidamente conforme abaixo (GRECO FILHO, 1996; GOMES e CERVINI, 1997; PARIZZATO, 1997):

- Autoridade policial representa junto ao Tribunal de Justiça com base no Inciso I do art. 3° da lei 9296/96.

- De acordo com o Art. 3° da lei 9296/96, a interceptação das comunicações telefônicas poderá ser determinada pelo juiz, de ofício ou a requerimento da Autoridade policial (art. 3°, I) ou do Ministério Público (art. 3°, II)

- O juiz, depois de conhecer a opinião do MPDFT, na hipótese de deferimento do pleito da autoridade policial, gera e encaminha o Mandado Judicial de Quebra de Sigilo de Comunicação, em papel impresso à operadora para proceder à interceptação.

- Uma vez encaminhado, a operadora, em regra, recepciona o documento ou no setor de protocolo ou em uma central de "fax", o qual será registrado e encaminhado ao destinatário, que normalmente é o presidente da empresa, o qual, por sua vez, despacha para o setor jurídico e posteriormente para departamento técnico para que se iniciem os procedimentos para disponibilização dos sinais e dados requeridos (FERRO JÚNIOR, 2006).

- No atual processo de Interceptação Telefônica a operadora, além de realizar tecnicamente a operação, detém relativo controle sobre qualquer interceptação levadas a efeito em suas instalações, cabendo somente à polícia o recebimento do áudio para a análise e gravação dos conteúdos (FERRO JÚNIOR, 2006).

Esquema adaptado do fluxo do processo de interceptação telefônica tradicional.

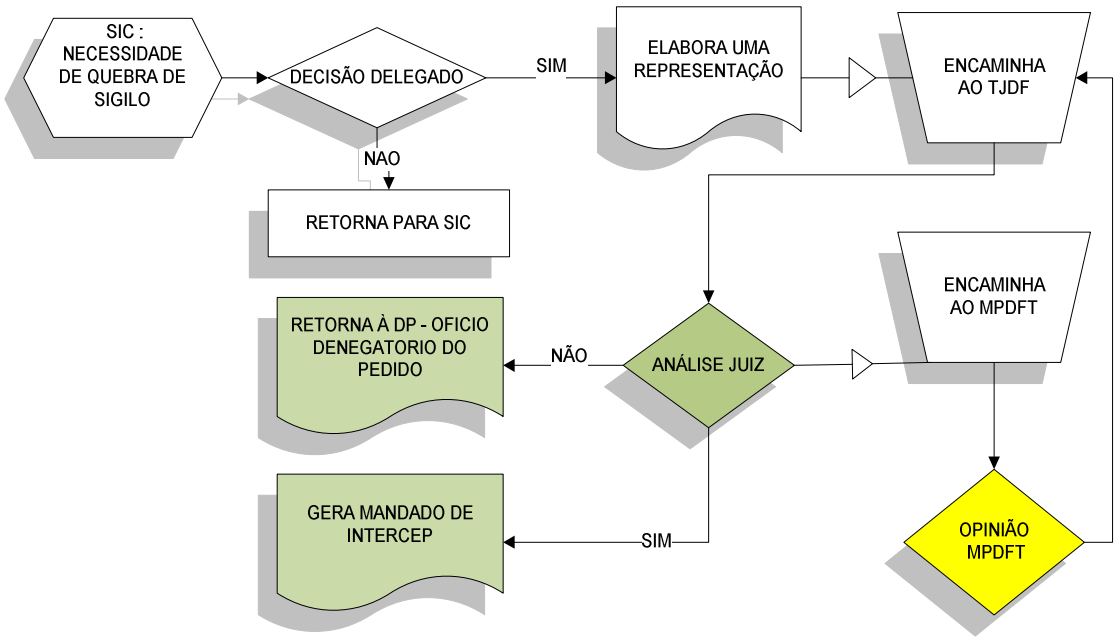

Figura 1 Fluxograma simplificado do processo de interceptação segundo a Lei 9296-96 (fonte: Projeto Ion-PCDF)

O fluxograma em destaque reflete de forma simplificada o processo a ser iniciado na unidade policial, passando pelo Tribunal de Justiça e Ministério Público, terminando nas operadoras que se encarregam, por costume, de realizar a interceptação telefônica, entregando o produto, de áudio e dados relacionados às chamadas, aos órgãos destinatários – polícias judiciárias ou Ministério Público.

1.4 O Problema nas Interceptações Legais

A constante e inequívoca evolução tecnológica das telecomunicações (CHAIN et al, 2004) tem proporcionado indubitável conforto, agilidade e praticidade aos homens da Era moderna.

A realidade da telefonia móvel celular, inimaginável há algum tempo, ganha rápido e largo espaço na atual conjuntura sócio-econômica, traduzindo-se como indispensável na vida diária de seus usuários (FERRO JÚNIOR, 2005).

O efeito colateral resultante da massificação do uso da tecnologia móvel, trouxe substancial aumento de delitos que gravitam em sua órbita, ora como objeto da cobiça dos criminosos, ora como valioso instrumento na elaboração, planejamento e execução de crimes (FERRO JÚNIOR, 2004).

No Brasil os recursos de telecomunicações estão sob domínio de empresas privadas. Das dificuldades enfrentadas diuturnamente pelas Polícias, merece destaque as de insustentável conflito com as operadoras de telefonia que, valendo-se de equivocada interpretação, assumem condição de fiscalizadores da atividade, estabelecem procedimentos de controle e administração totalmente vulneráveis, com manipulação de dados e informações por empresas terceirizadas (FERRO JÚNIOR, 2006).

O controle ineficiente patrocinado pelas empresas no que concerne à interceptação telefônica e o envolvimento destas, direta ou indiretamente, dificultando a ação policial em casos de interceptação ilegal é evidente em diversas investigações. Isso pode ser confirmado como exemplo na Operação Zodíaco, pela Polícia Civil do DF, na qual operadoras se recusavam a fornecer dados para a investigação criminal, descumprindo ordens judiciais, quando houve necessidade de cumprimento de mandados de busca e apreensão de dados nos computadores de empresas telefônicas da Capital Federal. (FERRO JÚNIOR, 2006).

Registre-se ainda, que o processo atual as interceptações telefônicas são realizadas exclusivamente por operadoras de telefonia (a polícia somente grava os sinais de áudio enviados), que comandam todo procedimento de interferência na comunicação de pessoas, têm o domínio e conhecimento de todas as informações e ações da justiça criminal, sem nenhuma fiscalização dessa atividade por órgãos do governo, Justiça ou Ministério Público (FERRO JÚNIOR, 2006).

1.4.1 As fragilidades no atual processo de interceptação legal

Na apresentação deste tópico, pretende-se demonstrar, segundo relato dos profissionais de inteligência policial, os principais nós de vulnerabilidades do procedimento de interceptações, desde as policias judiciárias até as operadoras de telefonia fixa e móvel. Diante do fato, chama-se atenção para a necessidade de encetar-se esforços no sentido de combater e eliminar, ao máximo, essas vulnerabilidades que oneram a atividade autorizada e causam frustrações e descrédito dos sistemas de segurança.

De fato Juízes e Promotores relacionados ao processo não fazem parte do sistema e, em regra, desconhecem o produto que está sendo gerado (FERRO JÚNIOR, 2006).

Os encaminhamentos de mandados judiciais, tradicionalmente são feitos aos presidentes de operadoras, não por estar estabelecido em lei, mas por uma questão de cultura, já que antes da eclosão tecnológica, órgãos policiais não possuíam condições e conhecimentos técnicos sobre os sistemas telefônicos (FERRO JÚNIOR, 2006).

Atualmente a capacitação dos profissionais de polícia e a alta tecnologia disponível proporcionam uma mudança no procedimento no sentido de se restabelecer a sua correta ordem, qual seja, somente o Judiciário, o Ministério Público e as Polícias Judiciária são os atores fundamentais nas operações de interceptação telefônica e telemática (FERRO JÚNIOR, 2006).

Nas operadoras, por suas características e dinâmicas de empresas privadas, considerando-se as particularidades administrativas e políticas adotadas, percebe-se que a documentação jurídica para fins de quebra de sigilo, recepcionada, sofre, invariavelmente, manipulações por diversas pessoas de seu quadro, possibilitando os problemas de vazamento e comprometimento de operações dessa natureza (FERRO JÚNIOR, 2006).

A título de exemplo sabe-se que no roteiro do mandado judicial, no âmbito das operadoras, (FERRO JÚNIOR, 2006) destacam-se pelo menos duas formas de encaminhamento já dadas como aceitáveis pelas empresas, mas de grande vulnerabilidade para os trabalhos policiais: a) o uso dos *fac-símiles* para envio de cópia de Mandados de Justiça, com o fim de agilização da operação, mas que na verdade, segundo os profissionais da área de inteligência das policiais, acabam por gerar mais problemas e atrasos, fazendo ruir por terra os princípios da oportunidade e imediatividade que deveriam caracterizar essas operações e b) o encaminhamento pessoal do documento por agentes da autoridade.

Nestes casos, desde a recepção do mandado judicial até o recebimento no departamento jurídico das empresas, existe a possibilidade de manipulação por pessoas que podem ter extensa rede de comunicação/conhecimento com familiares, parentes, amigos, colegas etc., dos envolvidos sob suspeita (FERRO JÚNIOR, 2006).

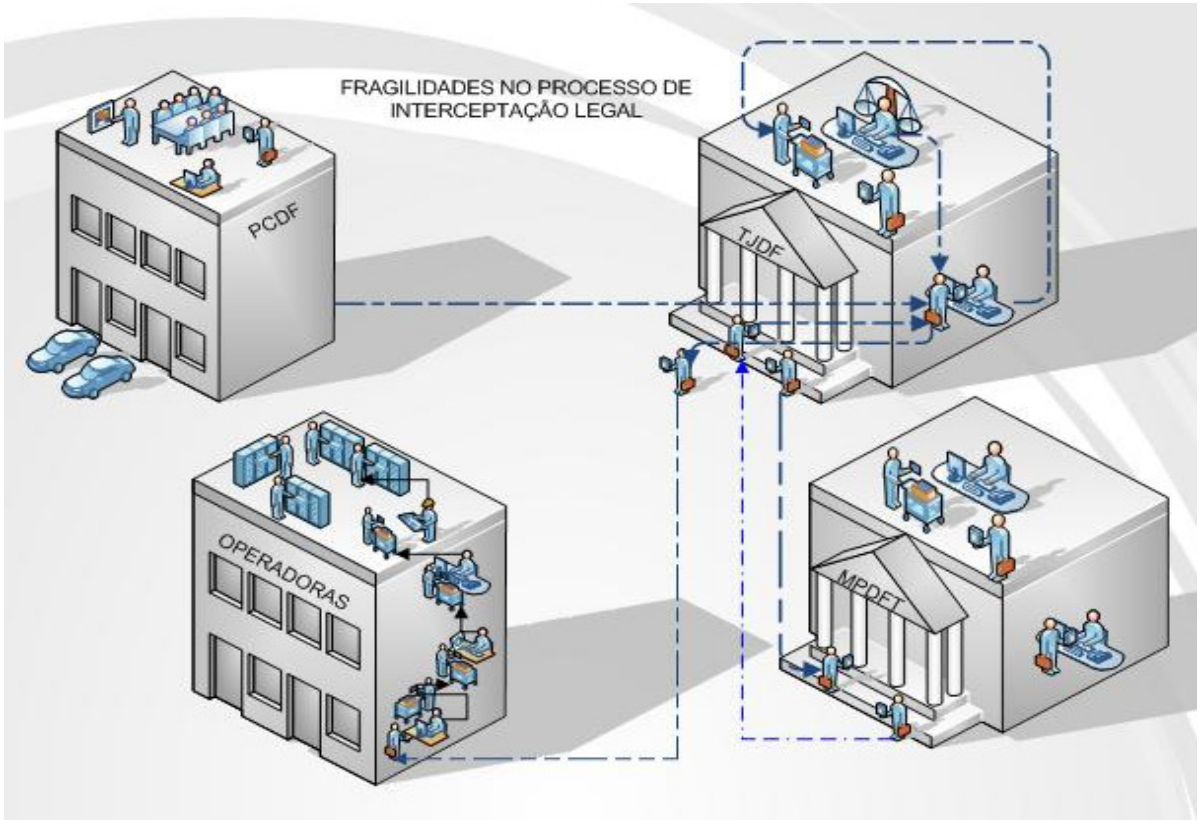

Figura 2 *adaptação de gráfico representativo das vulnerabilidades no processo de interceptação legal*.

O processo acima esquematizado chama atenção para o quanto os papeis "caminham", desde que partem na forma de uma representação por quebra de sigilo, até culminar na execução técnica, que hoje se dá necessariamente nas operadoras de telefonia.

O gráfico demonstra que existem inúmeras fragilidades no processo da interceptação legal iniciando-se na própria Polícia, já que muitas pessoas poderiam, ali, ter acesso a documentos com informações que deveriam ser sigilosas, porém, como têm que tramitar internamente, acaba-se tendo vistas aos dados de alvos destinados a quebra de sigilo.

Do mesmo modo nos demais órgãos há inúmeras pessoas que acabam tendo vistas à representação (estagiários, funcionários de secretarias, protocolo, etc.) ainda que fortuitamente, podendo, eventualmente, conhecer o alvo da quebra do sigilo, vindo a prejudicar a operação a partir do vazamento de informações.

Observa-se, porém, pelo relato de profissionais de Polícia Civil do Distrito Federal, que é no ambiente das operadoras que a suscetibilidade de vazamentos é mais acentuada, em face do grande número de pessoas que podem ter vistas aos mandados.

Elencam-se desde porteiros, assistentes de secretaria, advogados, funcionários de limpeza, estagiários, técnicos etc., que normalmente têm que dar andamento ao processo técnico, e, se eventualmente, tiverem qualquer conhecimento do alvo, já será suficiente para colocar em risco qualquer operação[5].

Outro ponto de observação que se destaca no procedimento da interceptação no âmbito das operadoras, diz respeito aos executores. Em certos casos (e.g. telefonia fixa) um técnico recebe a ordem para execução da operação, quando, neste caso, terá acesso a diversas informações sobre os "alvos" da investigação criminal (FERRO JÚNIOR, 2006).

---

5 Relato técnico de representante do setor de gestão de interceptações da Polícia Civil do DF.

Aspecto importante, ainda, a se considerar, diz respeito à forma de disponibilização do áudio e dados relacionados às chamadas telefônicas (GOMES e CERVINI, 1997), vez que dependendo da técnica empregada, o que deveria ser altamente sigiloso no processo, passa a ser altamente vulnerável e passível de ser "controlado ou acompanhado" (FERRO JÚNIOR, 2006) em tempo real por empresas terceirizadas, contratadas por operadoras para gerenciar o fluxo de todas as informações relacionadas à interceptação, tarefa essa que deveria ser desenvolvida por auditorias do Ministério Público.

Dessarte, no sentido de buscar a eliminação dos problemas comentados parece ser urgente a mudança do atual paradigma por meio de uma proposta consistente de automação de todo o processo legal das interceptações telefônicas e telemáticas, por meio do emprego de alta tecnologia que permitirá, em tese, a eliminação drástica das vulnerabilidades detectadas no atual processo (FERRO JÚNIOR, 2006).

Por efeito de diversas reclamações das polícias judiciárias e diversos eventos confirmadores das fragilidades citadas no âmbito das operadoras de telefonia, foi realizado em agosto de 2009 um reunião em São Paulo convocada pelas empresas de telefonia, onde estavam presentes representantes das Polícias Civis e Polícia Federal, membros do Ministério Público e operadoras para discutirem as questões operacionais e novas metodologias visando a redução das vulnerabilidades.

Algumas operadoras já implementaram e outras estão em fase de estudos para a apresentação de soluções mais eficientes e automatizadas de operações com recursos de rastreabilidade das informações prestadas às polícias, em atendimento a autorizações para quebra de sigilo telefônico.

Nota-se a preocupação com a segurança e a busca conjunta de soluções tendentes a automação de procedimentos operacionais, como seria inevitável em um contexto de informatização pelo qual passam todos os órgãos e instituições públicas e privadas.

1.4.2 Os crimes previstos na norma e sua abrangência

Nesta abordagem busca-se elencar os crimes previstos na lei 9296/1996 bem como traça-se a linha média do entendimento doutrinário sobre o tema, sempre visando a proteção da intimidade contra a violação do direito ao sigilo das comunicações.

A vigência da norma incriminadora da interceptação que antes era prevista no art. 151, § 1º, II, parte final, do CPB passou a ser aplicada com o entendimento do art. 10 da Lei n. 9.296/96, acima descrita.

Antes do advento da Lei 9296/96, quando ainda vigorava a disposição do art. 151, §1º, II parte final do CPB, relativamente à violação das Comunicações de um modo geral, o crime, de acordo com a maioria da doutrina, somente se aperfeiçoava com a divulgação, transmissão ou utilização abusiva da conversação, consumando-se nesse momento (JESUS DAMÁSIO, 1996, P.460.)

Dessa leitura percebe-se que se ocorresse a interceptação e não houvesse a difusão do conteúdo não se constituiria o crime, conforme se depreende de jurisprudência da época, (TACrimSP, HC 171.586, RJDTACrimSP, 2:212).

Já com a disposição do artigo 10 da Lei n. 9.296/96, a incriminação ocorrerá independentemente da divulgação, bastando que seja levada a efeito sem a devida autorização judicial ou com objetivos não autorizados em lei.

Nota-se que o legislador buscou a tutela da privacidade do cidadão, consubstanciado no direito de qualquer indivíduo poder comunicar-se privativamente e por qualquer meio com outro, sem interferência de terceiro.

De acordo, pois, com a norma incriminadora (art. 10 Lei 9296/96), configurar-se-á delito o fato de quem, sem autorização judicial ou com objetivos não autorizados em lei, realizar interceptação de comunicação telefônica, de informática ou telemática, ou quebra segredo de justiça referente à diligência (arts. 1º, caput e 8º, caput, da mesma Lei).

Firmado o entendimento de que o crime da interceptação se verifica com o simples fato de sua realização sem consentimento judicial, resta verificar a ocorrência da quebra do segredo de justiça que na visão dos profissionais de segurança pública é o que mais onera as operações autorizadas (FERRO JUNIOR, 2006), que pode ocorrer em qualquer momento ou lugar do procedimento, já que é de difícil controle na forma em que se processam as atuais medidas judiciais.

O que se afirma acima se observa na casuística policial em que se verificam, mormente no ambiente das operadoras (FERRO JUNIOR, 2006), a agressão às regras tanto do art. 1º e 8º quanto da parte final do art. 10º, nos casos de vazamentos de informações sobre quebra autorizada de sigilo telefônico ou telemático, inviabilizando a investigação policial , pelo fato de muitos investigados serem, mediante cooptação de pessoas a elas ligadas, previamente comunicado sobre a medida em curso.

Nestes casos o investigado simplesmente deixa de fazer uso do meio de comunicação por ter recebido informação privilegiada de alguém que tomou conhecimento da medida no curso do procedimento.

Atualmente muitas operadoras de telefonia, cientes de tais vazamentos em seus próprios ambientes, criaram setores específicos para tratamento de tais operações intencionando maior controle e minimizar os efeitos danosos à investigação, porém, inobstante a iniciativa positiva, verifica-se na prática, que a medida é ineficaz em face do numero de pessoas envolvidas desde o momento da representação judicial até a consecução do procedimento que ora é totalmente manual (FERRO JUNIOR, 2006).

A lei 9296/1996 disciplina os casos em que se permitem lançar mãos da medida de interceptação de telecomunicações telefônicas e telemáticas, mas, também, buscou, conforme se depreende das disposições do seu Art. 10º, descrever o tipo legal e os elementos normativos que restringem a incriminação bem como os casos que serão objeto do alcance da norma penal.

De acordo, pois, com o dispositivo legal se prevê que

> "Constitui crime realizar interceptação de comunicações telefônicas, de informática ou telemática, ou quebrar segredo da Justiça, sem autorização judicial ou com objetivos não autorizados em lei" [6].

Na perspectiva penal da regra do artigo 10 encontram-se presentes tanto os elementos normativos do tipo quanto os subjetivos, quais sejam a falta do consentimento judicial para a realização da interceptação, assim como a violação do segredo de justiça e do sigilo das diligencias (arts. 1 e 8). Os tipos descritos exigem outro elemento subjetivo, contido na exigência de que o sujeito realize o fato para fins diversos dos estabelecidos pela lei de investigação criminal ou prova em processo penal (JESUS, DAMÁSIO, 1999).

Na análise dos elementos subjetivos, observa-se que no caso do art. 10º está presente o dolo, observável na vontade de interceptar a comunicação telefônica, e nos artigos 1º e 8º no ato que der causa à quebra do segredo de justiça ou o sigilo das diligencias.

---

6 BRASIL. PRESIDENCIA DA REPÚBLICA Lei 9296/1996. Art. 10. Disponível em http://www.planalto.gov.br/ccivil_03/LEIS/L9296.htm acesso em 15/05/2009

Há ainda considerar o fato de que o artigo 10º em comento, os tipos descritos exigem outro elemento subjetivo, contido na exigência de que o sujeito realize o fato para fins diversos dos estabelecidos pela lei de investigação criminal ou prova em processo penal.

Por tratar-se de crime de mera conduta, conforme leciona Damásio E. Jesus(1999) perfaz-se, independentemente dos resultados, com o simples comportamento do sujeito, sendo que o momento consumativo se dá no ato em que se inicia a gravação do conteúdo trafegado no meio utilizado para a comunicação seja ele telefônico fixo, móvel, satelital, internet etc.,

Destaca ainda o doutrinador que nos casos em que ocorra a divulgação do conteúdo da comunicação não se configurará novo delito, tratando-se de simples exaurimento, salvo eventual crime de calúnia, difamação etc (JESUS, 1999)

Em torno, pois, do tema em questão considerando-se as suscetibilidades de crimes que o atual procedimento comporta na sua forma convencional de operacionalização, urge seja proposto ou feito algo que de um lado garanta a legalidade de toda e qualquer operação de interceptação telefônica e telemática bem como, e principalmente, seja capaz de conter a ocorrência dos vazamentos de informações que alem de fragilizarem o processo geram vários ônus ao Estado nas ordens econômica, jurídica, social e política.

1.4.3 Projetos de leis substitutivos à Lei 9296/96

A lei 9296/96, segundo vários autores, encontra-se defasada e aquém das necessidades normativas e do alcance tecnológica decorrente da evolução tanto dos meios de comunicação como das variantes dos crimes cometidos com seu emprego. Nesse contexto busca-se, neste ponto da discussão sobre o tema, apresentar os esforços feitos no sentido de atualizar o dispositivo legal regulamentador.

Tramitam atualmente na câmara federal dois projetos de lei que se propõem modernizar o regramento jurídico que disciplina as atividades de quebra de sigilo telefônico e telemático.

Tratam-se dos projetos de Lei PL 5285 e PL 5286, ambos apresentados pela Comissão Parlamentar de Inquérito (CPI) das Escutas Telefônicas Clandestinas que encerrou suas atividades em abril de 2009.

A razão de dois projetos, ao que se depreende do contexto, deve-se a pontos divergentes relativos à competência para demandar a medida de exceção, se das polícias judiciárias ou do Ministério Público**,** projeto PL 5286/09, onde tanto a polícia como o Ministério Público poderiam pedir ao juiz a quebra do sigilo telefônico, e no PL 5285/09, a medida para prova em investigação criminal e em instrução processual penal, dependeria de ordem expressa do juiz competente, não estendendo ao Ministério Público essa prerrogativa.

No Projeto de Lei 5285/2009 a proposta inova prevendo o controle e a fiscalização na produção, comercialização e uso de equipamentos destinados a quebra de sigilo telefônico de forma não prevista.

Segundo se noticia em sites e artigos sobre o tema, o propositor do Projeto de Lei 5285/2009, defende que as atuações das Polícias judiciárias e do Ministério Público não se confundem eis que entende os autores, que quem tem legitimidade constitucional para proceder a investigações, segundo consta do Art. 144 da Constituição Federal brasileira, será a Polícia Judiciária, seja ela estadual, federal ou do Distrito Federal.

Nesta perspectiva se manifesta contrário à participação do Ministério Público em investigações, defendendo tão somente que o órgão deverá se limitar ao requerimento de diligencias.

O posicionamento do autor, encontra-se manifesto nos seguintes termos:

> "Pela Constituição, não cabe ao Ministério Público promover investigação. Quem investiga, segundo o artigo 144, é a polícia judiciária. Quem compõe a polícia judiciária são as polícias civis dos estados e a Polícia Federal, no âmbito nacional. Portanto, o Ministério Público tem todos os poderes de fiscalizar a atuação da polícia e também de requerer diligências à polícia, que é obrigada a cumprir essas diligências e requisições." [7]

O que se nota ainda em comum nos dois textos é a menção, ainda que tímida, da aplicação de procedimentos eletrônicos nas medidas em comento, parece uma tendência firme no sentido da automação e, ao que se percebe, recomendável pelos efeitos produzidos sob a óptica da segurança, celeridade, sigilo e possibilidade de auditabilidade em todos os entes participativos da medida.

Inobstante o aspecto inovador que prevê a automação do procedimento, percebe-se que ambos os projetos de Lei são genéricos em definir os papeis dos atores que efetivamente deveriam participar ativamente nas medidas de exceção.

No mesmo sentido nota-se que em ambos se busca legitimar, agora de direito, o papel da operadora como um ente ativo e sobre o qual recai a responsabilidade de efetivamente proceder, controlar e informar sobre todas as operações em curso.

Sobre o que e a quem informar os projetos igualmente parecem se omitirem, mas como há nítida participação do Conselho Nacional de Justiça nesse processo legislativo, depreende-se por dedução que seria a esse órgão que as operadoras deveriam se reportar.

---

7 Disponível em: **http://www2.camara.gov.br/internet/homeagencia/materias.html?pk=135878.** Artigo CPI das Escutas defende projetos para regulamentar interceptações. Fonte Agência Câmara. Data de Publicação: 5 de junho de 2009. Reportagem - Idhelene Macedo/ Rádio Câmara Edição - Regina Céli Assumpção. Obtido em 19/08/2009.

Naturalmente é discutível e suscetíveis de críticas as previsões legais lançadas como base jurídica que se propõe, com modernidade e segurança, substituir a lei 9296/1996, eis que os contextos de mais de uma década atrás, já não se aplicam na atualidade e observa-se que os projetos em comento não lançaram vistas a um contexto tecnológico futuro onde novos desafios se imporão e demandarão uma lei mais elástica em termos de persecução penal.

1.5 As Interceptações no Contexto da Polícia Judiciária

As polícias judiciárias têm aprimorado suas técnicas investigativas na tentativa de opor resistência ao crescimento dos crimes em seus diversos matizes. Neste tópico se apresenta o cenário onde atuam as forças policiais e seus esforços para, com uso dos instrumentos legais facultados pela legislação pátria, solucionar os casos mais complexos com o emprego de alta tecnologia.

Com a evolução das tecnologias e sua massificação, recrudescem, no mundo, os crimes com emprego de sofisticados aparatos eletrônicos para burlar a capacidade das agencias de segurança, sobremaneira das Polícias judiciárias, no combate ou mesmo controle da criminalidade (FERRO JUNIOR, 2008).

A diversidade de crimes cometidos com o emprego maciço de equipamentos de telecomunicações chama atenção das polícias judiciárias eis que não há limites para os criminosos.

Uma das explicações pode ser o fato de que o dinheiro que é utilizado para tais aquisições é fruto do mesmos crimes que a cada dia recrudescem e dificultam o controle por parte das autoridades.

Dentro do acervo tecnológico disponível destaca-se que o emprego de sistemas telefônicos de ultima geração tais como GSM[8], VOIP[9], IDEN[10] etc., têm se apresentado como os meios mais utilizados para a comunicação de massa (FERRO JUNIOR, FRAGA PRETO, e OLIVEIRA FILHO), e de maiores complexidades para as atividades de investigação de crimes que tem por base sua utilização nas comunicações, pois tanto vítimas quanto os criminosos os utilizam habitualmente (FERRO JUNIOR, 2008).

As atividades de inteligência policial se apóiam em todas as áreas da ciência para deslindar, prever, controlar e anular ameaças e crimes (FERRO JUNIOR, 2008) por meio do emprego dos recursos de alta tecnologia voltadas especificamente ou mesmo adaptadas para as atividades de segurança pública.

Como, de regra, todo crime prescinde da comunicação entre seus agentes. Parte-se do pressuposto que para se levar a efeito atos criminosos, seus consecutores necessitam se comunicar e é exatamente neste ponto que se insere as atividades de inteligência policial por meio das técnicas de análise de sinais, análise de vinculos etc. (FERRO JUNIOR, 2008).

Para se levar a efeito as atividades próprias da investigação policial, se faz necessário empregar vastamente a tecnologia eletrônica e computacional, pois há grande necessidade de se relacionar os eventos partindo-se de pontos referenciais para o início das operações, sendo estes tomados justamente dos recursos de telecomunicações e informática.

---

8 GSM: **Global System for Mobile Communications**, ou Sistema Global para Comunicações Móveis (**GSM**: originalmente, *Groupe Special Mobile*) é uma tecnologia móvel e o padrão mais popular para telefones celulares do mundo. Telefones GSM são usados por mais de um bilhão de pessoas em mais de 200 países Global System Mobile – Sistema Global Móvel- fonte: http://pt.wikipedia.org/wiki/GSM, obtido em 5/11/2008 17:13h

9 VoIP: **Voz sobre IP**, também chamado **VoIP**, **telefonia IP**, **telefonia Internet**, **telefonia em banda larga** e **voz sobre banda larga** é o roteamento de conversação humana usando a Internet ou qualquer outra rede de computadores baseada no Protocolo de Internet; conceito disponível em: http://pt.wikipedia.org/wiki/VoIP, obtido em 5/11/2008 17h15minh

10 IDEN: **Integrated Digital Enhanced Network** (**iDEN**) é uma tecnologia de comunicação móvel, desenvolvida pela Motorola, que fornece aos usuários de celular rádio e celulares. No Brasil, a tecnologia iDEN é utilizada pela operadora de telefonia celular NEXTEL. Conceito disponível em: http://pt.wikipedia.org/wiki/iden, obtido em 5/11/2008 17:21h

Nesse diapasão havendo um crime qualquer e chegando a informação ao conhecimento da autoridade policial e seus agentes, a possibilidade de localização aproximada da região onde se encontram a vítima ou o autor dependendo do caso, será muito grande (FERRO JUNIOR, FRAGA PRETO, e OLIVEIRA FILHO, 2008).

A justificativa técnica encontra-se no fato de que todos os eventos ocorridos numa seção de conversação, deslocamento, envio ou recebimento de mensagens curtas em celulares etc., ou mesmo o simples fato de mudanças de locais do aparelho, operações de ligar ou desligar um celular, etc., já são registrados como eventos ou sinalizações ao sistema, extraindo-se, daí, importantes elementos para a análise criminal, permitindo-se o mapeamento das atividades criminosas de traficantes, sequestradores e criminosos comuns.

No atual contexto de controle das operadoras de telefonia, dado apenas pelo costume e ausência do Estado nos processos de Interceptações legais, (FERRO JUNIOR, FRAGA PRETO, e OLIVEIRA FILHO, 2008) essas empresas, alheias ao sofrimento das vitimas e das necessidades de informações pelas polícias para se chegar mais rapidamente aos criminosos, negam-se a colaborar com os órgãos policiais alegando responsabilidade sobre o sigilo das informações de seus usuários.

Incorrem em equivoco de interpretação eis que o ordenamento jurídico e a jurisprudência (FERRO JUNIOR, FRAGA PRETO, e OLIVEIRA FILHO, 2008) não elegem a sinalização dos eventos técnicos havidos numa seção de comunicação como quebra de sigilo das comunicações já que não são revelados conteúdos de áudio ou dados cadastrais que venham a expor os assinantes, pois não há, de fato e de direito, a interferência da polícia nas comunicações.

Os trabalhos policiais que se valem da utilização das sinalizações próprias dos sistemas de telefonia móvel e fixa, são potencializados em nível de eficácia, tempo e recursos logísticos, porém são obstados paulatinamente pelas operadoras de telefonia que detêm o controle sobre tais informações (FERRO JUNIOR, FRAGA PRETO e OLIVEIRA FILHO, 2008).

Os recursos de alta tecnologia utilizados pelos criminosos devem ser combatidos com outros recursos igualmente de alta tecnologia, de modo a estabelecer o necessário equilíbrio da criminalidade nos grandes centros urbanos onde se verificam os problemas da criminalidade em todo o planeta.

Os sistemas de gestão de interceptações baseados em sistemas computacionais de ultima geração permitem dentre outras funcionalidades, que se tenha o mapeamento muito aproximado das localizações dos criminosos, permitindo traçar rotas, horários, desvios etc., (FERRO JUNIOR, FRAGA PRETO, e OLIVEIRA FILHO, 2008) eventualmente tomados com o fim de ludibriar o aparato policial , e permite ainda que se façam as correlações entre facções, grupos e criminosos entre si em determinado espaço geográfico e temporal e entre correlatos em outros municípios, estados e até países.

Dentre outras perspectivas, pode-se conceber que se as polícias judiciárias em nível estadual e federal fazem uso de tais sistemas, poder-se-á integrá-los, resguardadas as limitações legais relativas ao sigilo e compartimentação de informação, construindo-se uma malha de inteligência (FERRO JUNIOR, FRAGA PRETO, e OLIVEIRA FILHO, 2008) capaz de não só ampliar a capacidade do Estado no combate ao crime em todas as suas formas de cometimento, bem como, de propiciar maior controle e gerenciabilidade das ações legais no tocante aos trabalhos baseados em interceptações (FERRO JUNIOR, FRAGA PRETO e OLIVEIRA FILHO, 2008).

Necessário, pois, que se encetem ações em tal sentido e o quanto antes, eis que os criminosos não perdem tempo em se equiparem para a prática criminosa, e o Estado, em face da burocracia e publicidade de seus atos, tem grande dificuldade em acompanhar a evolução tecnológica na velocidade em que se disponibiliza no mercado.

Neste sentido assinala-se a necessidade não só de investimentos em tecnologia, bem como na criação de órgãos especializados, no âmbito das polícias, dos tribunais de Justiça e Ministério Público, com equipes especializadas no combate conjunto ao delito que se vale das tecnologias de massa ou outras especificas, de forma isenta e norteada pela busca da máxima eficiência na resolução e principalmente na prevenção e controle da criminalidade (FERRO JUNIOR, FRAGA PRETO e OLIVEIRA FILHO, 2008).

2 O PROCESSO JUDICIAL ELETRÔNICO

2.1 A automação de processos e as tendências mundiais

Para oferecer consistência ao discurso de automação ou informatização de processos, destaca-se que o cenário mundial indica a prevalência dessa sistemática em todos os campos de atuação do homem. Nesse contexto apresenta-se neste tópico, as tendências mundiais e nacionais em relação à modernização das comunicações tendentes à automação ou informatização de processos e procedimentos.

A internet encurtou distâncias e disponibilizou uma massa de informações que culminou na democratização do conhecimento tornando o mundo mais ágil e ao mesmo tempo mais suscetível a mudanças também muito rápidas (BRAGA, 2004).

O Brasil figura entre os países que possuem um histórico bem sucedido de automação de seus processos, sobretudo nas áreas financeiras, controle fazendário (BRAGA, 2004).

"A telemática – a união das tecnologias de informação e de comunicação eletrônicas digitais e convergentes – oferece meios poderosos e cada vez mais baratos de aperfeiçoar nossa democracia, pagar nossa divida social e estimular nossa economia" (CHAIN, et al, 2004).

O investimento em telemática deve ser uma prioridade governamental e deve ter como pano de fundo a inovação focada no preenchimento de lacunas gerenciais e processuais que hoje impedem que o país seja melhor administrado (FERNANDES, 2004).

As experiências do setor privado em muito contribuem para o avanço do Estado, que deverá buscar sintonia com as melhores práticas no campo da telemática.

Assim as relações entre as agencias ou órgãos governamentais, também conhecidas no mundo digital como "G2G"[11] podem ser classificadas como ralações horizontais (dentro de órgãos de um nível da federação e entre eles) e verticais, que são as relações entre órgãos das diferentes instancias da federação, a saber, a União, as grandes regiões, os estados, as regiões metropolitanas, os municípios etc. (BRAGA, 2004)

A questão da segurança da informação deve receber tratamento destacado e permanente.

No Brasil foi publicado o Decreto 3505/2000 que estabelece a política de Gestão da Segurança da Informação do Poder Executivo Federal, (PGSI), que criou o Comitê Gestor de Segurança da Informação (GSI), constituído por representantes de doze ministérios (CHAIN et al, 2004). Esta informação é muito importante, pois demonstra a intenção do governo brasileiro em priorizar a automação e integração de seus sistemas de modo a garantir maior celeridade, publicidade e transparência administrativa.

Na mesma linha foi definido como metas de automação dos processos de gestão, dentre outras a seguintes e prioritárias ações

Coordenar e articular a implantação de programas e projetos para a racionalização da aquisição e da utilização da infra-estrutura, dos serviços e das aplicações de tecnologia da informação e comunicações no âmbito da administração pública federal; (BRAGA, 2004)

- Estabelecer diretrizes e estratégias para:
- Planejamento da oferta de serviços e de informações por meio eletrônico
- Definir padrões de qualidade para as formas eletrônicas de interação.

---

11 G2G (ou Gov to Gov) termo que significa relação horizontal de comunicação de Governo para Governo (tradução livre)

- Coordenar a implantação de mecanismos de racionalização de processos, no âmbito da administração pública federal etc.

Varias foram as conquistas já atingidas pelo Estado no tocante às ações de informatização de seus processos dentre as quais se destacam os sistemas de licitações eletrônicas, imposto de renda, acompanhamento de processos judiciais, penhora eletrônica, rede multi serviço Br@sil.gov. Etc.

Como parte da política de automação de processos visando o governo eletrônico federal, priorizará a articulação entre União e Estados da federação buscando unidade processual e padronização, e como na proposta desta pesquisa, visa-se a integração de órgãos dos poderes executivo e judiciário (Polícias Judiciárias, Ministério Público e Tribunal de Justiça), entende-se que as ações de informatização em implementação por todo o país, justificam os esforços, para que, no tocante ao processo das interceptações legais, se priorize ações e investimentos.

A Governança[12] Eletrônica (BRAGA, 2004), que vem a reboque de todo processo de informatização, contempla um conjunto de atividades destinadas a fomentar a elaboração de políticas publicas, tomada de decisões, melhoria de arrecadação, segurança da informação, integração e padronização de processos e sistemas dentre outras.

Vários Estados da federação iniciaram seus processos nos setores mais sensíveis como o da arrecadação fiscal, fiscalização, padronização de bancos dados de contribuintes, etc., e evoluíram para a disponibilização de serviços a comunidade de sorte a terem respostas mais exatas em termos de senso e atualização cadastral de suas bases (FERNANDES, 2004).

---

12 Segundo o Banco Mundial, em seu documento Governance and development, de 1992, a definição geral de governança é "o exercício da autoridade, controle, administração, poder de governo". Precisando melhor, "é a maneira pela qual o poder é exercido na administração dos recursos sociais e econômicos de um país visando o desenvolvimento", implicando ainda "a capacidade dos governos de planejar, formular e implementar políticas e cumprir funções". Obtido em http://conpedi.org/manaus/arquivos/Anais/Alcindo%20Goncalves.pdf. O Conceito de Governança. 13/11/2008

Na administração destaca-se a governança dos processos de compras dos estados e União onde se verifica grande avanço e inclusão social, por meio da desburocratização de processos antes considerados densos e ineficientes, transparência, auditorias mais ágeis, maior possibilidade de participação de empresas, sobretudo as de pequeno porte (BRAGA, 2004).

A expectativa de ampliação dos processos de automação visando à governança é de crescimento e maior abrangência territorial e orgânica, visto que propicia maior eficiência administrativa, maior segurança, maior publicidade e, portanto maior transparência e maiores condições de realização de auditorias (FERNANDES, 2004).

2.2 Processo Eletrônico e legislação

A via eletrônica como forma de garantia de celeridade, otimização do fluxo de trabalho, controle e rastreabilidade processual, publicidade e segurança, neste ultimo caso se baseado em tecnologia robusta e proprietária, alem de ser uma tendência sem retorno no mundo atual, passa a cada dia a fazer parte da rotina do cidadão, e não poderia ser diferente com relação aos procedimentos ligados à justiça (CLEMENTINO 2008)

Conforme disciplina o art. 22 da Constituição Federal (CFB) compete privativamente a União legislar sobre direito processual, mas estabelece, entretanto, como competência legislativa concorrente entre a União, Estados e o Distrito Federal a legislação sobre custas de serviços forenses, procedimentos processuais e assistência jurídica etc., (CLEMENTINO, 2008)

Neste contexto é útil elencar várias iniciativas legislativas tendentes a adoção da automação processual e sua harmonização com os princípios constitucionais insculpidos na Carta Magna brasileira.

Observa a edição de varias Leis, desde 1999 (Lei 9800/99) que permitiriam a adoção de medidas eletrônicas para a prática de atos processuais, que, inobstante tímidas e limitadas, inauguram um novo momento do sistema judiciário como um todo, viabilizando novas discussões e inovações tendentes ao desenvolvimento do Processo Virtual e à regulamentação da utilização da internet como meio de viabilização de uma prestação mais eficaz do Estado em beneficio da sociedade, e, no tocante aos processos judiciais, como forma de combate à morosidade na entrega da prestação jurisdicional (CLEMENTINO, 2008).

A Lei 9800/99 sofreu diversas propostas de alterações, indicando que o tema merecia maiores reflexões por parte da sociedade representada na Câmara Federal e outras leis igualmente tendentes à inserção desses processos eletrônicos na pratica jurídica nacional, porém com maior abrangência e vinculação a princípios constitucionais, o que culminaria, após longo processo de maturação jurídica, na criação da Lei 11.419/2006, que regulamenta a utilização do processo eletrônico no âmbito do sistema judiciário. (CLEMENTINO, 2008)

O advento da supracitada lei inaugura uma nova fase do sistema judiciário brasileiro no tocante aos procedimentos e tramites documentais que caracterizam as atividades processuais do Poder Judiciário.

Nesta perspectiva, na visão dos defensores do novo paradigma, vislumbra-se possivel que todos os atos processuais possam viabilizados pelo meio eletrônico.

Um dos aspectos que realçam o valor da automação nos processos e procedimentos judiciais é o consequente aumento de disponibilidade de informações ao magistrado encarregado da entrega da prestação, já que se prevê, e isso é mesmo inevitável no atual contexto tecnológico, a integração das bases de dados do judiciario a outras de significativa relevância para o órgão, tais como tribunais de justiça das esferas federal e estadual, polícias judiciarias e militares, sistemas hospitalares, receita federal, organismos e governos internacionais, secretarias de segurança pública de todo o pais, etc.

Tão logo se passou a trabalhar em favor da automação do judiciário, vários órgãos e representantes de entidades de classe como a OAB, passaram a questionar e inclusive propor ações de inconstitucionalidade sobre as iniciativas, eis que faltava o competente arcabouço legal ensejador da automação.

Com a aprovação da Leis 11419/2006, que trata justamente dessa regulamentação em nível legislativo, e que dispõe sobre os poderes do Magistrado para determinar a exibição e o envio de dados e documentos necessários à instrução do processo por meio eletrônico, restou superada essa discussão e todos os demais processos e projetos que dependiam de um diploma regulador, passaram do papel para a prática.

Como exemplo mais significativo e de há muito utilizado pelos magistrados, destaca-se o sistema de penhora eletrônica denominado de “Bacen Jud”, que já está em sua segunda versão, e já plenamente utilizado, mesmo por juizes mais conservadores.

2.3 Supremacia do Interesse Público no Processo Eletrônico

Embora não esteja previsto em nenhum dispositivo da constituição Federal do Brasil o princípio da supremacia do interesse público sobre o privado, parece ser pacífico em todas as sociedades mundiais, e não poderia ser diferente no Brasil.

Inobstante não seja, a bem da verdade, absoluto o predomínio desse princípio, eis que conforme ensinamentos de renomados doutrinadores não se pode menosprezar a necessária dignidade que merecem as pessoas que formam a nação. (CLEMENTINO, 2008), a supremacia do Interesse Público alcança o sistema jurídico brasileiro como um todo, sobretudo no processo penal onde se verificam situações de conflitos entre o direito a intimidade do acusado e o do Estado que tem por dever investigar para fazer cumprir a lei que disciplinam e punem condutas.

O princípio da supremacia do interesse público sobre o interesse privado se consubstancia na condição própria da existência da sociedade sendo este princípio um pressuposto lógico do convívio social. (MELLO, 2001)

Nesse diapasão, em se tratando de conflitos de interesses particulares o raciocínio caminha no mesmo sentido, isto é, o direito à intimidade é relativo, devendo-se, como ensina CLEMENTINO (2008),"efetivar o sopesamento entre os interesses em discussão e verificar-se no caso concreto qual interesse deverá prevalecer", inobstante o empenho do Estado em garantir a proteção contra o indevido uso de informações que possam ferir as garantias constitucionais dos indivíduos.

É no âmbito do direito administrativo que mais se verifica a validade da prevalencia do interesse público sobre o interesse privado, mas isso não se configura num limite de aplicação dessa possibilidade eis que se deve conceber que as bases racionais garantidoras dessa faculdade estatal, se irradiam por todo o sistema juridico nacional, inclusive sobre o Direito Processual e especialmente o Processual Penal, onde se verificam, com constância o conflito entre o direito à intimidade do acusado e o direito do Estado em investigar, para, uma vez comprovada sua culpa, promover o *jus puniendes*.

Em todo caso deve-se agir com ponderação, razoabilidade e moderação eis que a aplicação dessa faculdade do Estado, deve ser utilizado somente quando inexistentes outras forma não invasiva de alcançarem os objetivos de interesse coletivo sobre o particular.(CLEMENTINO, 2008)

No procedimento eletrônico pela via da automação e padronização de processos, o que se espera, segundo seus defensores, é o maior controle sobre os atos, eis que todos as entradas em um sistema com o mínimo de recursos de rastreabilidade, permite se, em tese, verificar diversos parâmetros de acesso, obtenção de dados e informações, data, hora, conteudo acessado, matricula, orgão etc.

Nessa perspectiva percebe-se que os cuidados para não se ferir interesses privados ficam muito mais resguardados no procedimento eletrônico pelas possibilidades de cruzamento de informações entre bancos de dados e todas as ferramentas de rastreabilidade que se verificam nos sistemas destinados a automação, eis que afiguram-se como essenciais à gerencia e auditoria.

Em outra vertente o que se pretende tambem verificar nessa discussão é se seria viável que o Estado, necessitando de acessar dados sobre acusados em sede de processo Penal, poderia fazê-lo utilizando-se de recursos de alta tecnologia.

Pelo exposto e considerando-se a total rastreabilidade e controle do judiciário sobre a persecução penal levada a efeito por meio eletrônico, se afasta a possibilidade de abuso em face do que a tecnologia pode disponibilizar em termos de gerenciabilidade, com todos os efeitos do poder do magistrado sobre esses procedimentos. (CLEMENTINO, 2008).

2.4 Princípios Aplicados ao processo Eletrônico

Na presente obra buscou-se avaliar quais os princípios que são observados no processo legal normal e sua aplicabilidade no mesmo processo porém com procedimento automatizado.

As observações e conclusões corroboram com os da maioria absoluta que defende a inovação como forma de garantia de maior celeridade, publicidade e abrangência do procedimento eis que não são afastados pela tecnologia, mas, antes, consolidados requerendo-se pouco ou nenhum investimento, mas, sem dúvida, preparo, capacitação e readequação ao novo paradigma procedimental.

Abaixo analisam-se os principais princípios presentes no processo e suas eventuais repercussões no procedimento.

2.4.1 Princípios Processuais Constitucionais

O Processo Eletrônico se caracteriza por viabilizar a transferência dos registros ou logs dos atos processuais e demais dados do processo para o ambiente digital e por esse motivo, estaria intimamente vinculado aos atos processuais. (STUDER, 2008)

Na fase da transferência poderá ocorrer ou não desrespeito aos princípios que o compõe, sendo que os princípios, como fundamento ou base técnica de amparo que formam o Devido Processo Legal, são referentes ao ato processual, e se relacionam com a nulidade, a produção de provas, a sentença e com o recurso. (STUDER, 2008)

O processo eletrônico inova e pode ter grande influência na produção das provas, posto que esta (prova) poderá ser apresentada digitalmente, ou produzida virtualmente, de modo que se enriquece e detalha o conjunto probatório com os recursos da informática, pode também sofrer edições e colocar essa prova em descrédito, gerando graves consequências para as partes. (STUDER, 2008)

Relativamente à nulidade, sentença e recurso, entende-se que o Processo Eletrônico não teria influência direta sobre os atos do magistrado, por se referirem à motivação das decisões, que nenhuma interferência sofre pela informatização do processo. (STUDER, 2008)

2.4.2 Princípios vinculados aos atos processuais

De acordo com STUDER (2008) os atos processuais, são amparados pelos seguintes princípios:

2.4.2.1 Princípios do debate

Este princípio, no Processo Eletrônico está, segundo STUDER (2008), preservado e manifesto pelo amplo acesso às partes, para que acompanhem e avaliem todos os atos do processo, e no mesmo sentido, o próprio magistrado teria, cada vez mais, acesso a bancos de dados e maior facilidade para a produção de provas (STUDER, 2008)

2.4.2.2 Princípio do impulso oficial

No Processo Eletrônico serão feitos, por meio de programação ou configuração, pelo próprio sistema, que sinalizará, de forma personalizável, sempre que houver a necessidade de um impulso oficial, garantindo-se, destarte, um controle muito mais eficiente e prático sobre o andamento processual, que dentre outros efeitos positivos, eliminaria erros humanos como o esquecimento ou engavetamento desses nos cartórios das varas. .

2.4.2.3 Princípio da boa-fé

Este princípio, dita, conforme se manifesta STUDER (2008) que as "partes devem buscar os seus direitos com moralidade, respeito e de acordo com a verdade; devem ter lealdade processual".

Em um sistema virtual, com ferramentas de controle de acesso e registros de operações dos usuários, entende-se que deixarão de existir manobras prejudiciais tal como a retenção de autos, já que estes não serão físicos, e, segundo STUDER (2008) os que ainda o forem, o sistema controlará os prazos de todos os processos, mesmo os mandados, independente do número existente na unidade jurisdicional já que um sistema de controle de processos poderá emitir listas daqueles que estejam em poder dos oficiais de justiça por mais de 30 dias, por exemplo,

2.4.2.4 **Princípio do contraditório**

Que segundo STUDER (2008) trata-se da bilateralidade dos atos praticados no processo, ou seja, do direito às partes, de forma ampla e efetiva, serem informadas, de participarem e se contraporem a tudo que for produzido no processo., a fim de poderem influir no convencimento do julgador.

No contexto do Processo Eletrônico, pode-se dizer conforme observações de STUDER (2008) que há amplo respeito ao contraditório, pois restam garantidos o acesso a qualquer tempo e a disponibilização de informações e de dados ou documentos do processo às partes, praticamente no momento de sua entrada no sistema, facilitando, assim, a assistência técnica jurídica, já que o Advogado poderá acompanhar por completo e remotamente o andamento processual e, ainda, com varais facilidades que o processo manual não se possui.

2.4.2.5 **Princípio da representação por advogado**

Apoiados ainda em STUDER (2008) ressalta-se o fato de que o processo eletrônico requer adaptações para fins de utilização por parte dos usuários, como é sói ocorrer em todo processo inovador, porém antes de causar dificuldades o sistema eletrônico viabilizará os meios de acesso e uso das ferramentas quando se tratar de ação em que a parte não necessite de advogado.

Nesse caso o cartório certamente terá funcionários aptos a transcreverem os fatos e pedidos da parte, sendo que esta ao fazer o pedido já será intimada da data da audiência, como já ocorre, isto se o processo não for todo oral com a simples gravação da audiência. Portanto, não haverá grandes mudanças quanto aos excluídos digitais ou outra forma de exclusão de conhecimento ou meio, sendo que o Poder Judiciário tem meios para se adequar a estes tipos de situações, sem prejuízo da instalação do Processo Eletrônico, conforme bem se expressa STUDER (2008).

2.4.2.6 Princípio da publicidade

Que deve ser, a bem da verdade, do processo e não apenas no processo, como afirma STUDER (2008), sendo que o sistema permite o acesso aos autos virtuais, para leitura a qualquer pessoa, e não apenas aos advogados, com exceção dos casos defesos em Lei.

Uma vez como parte ou terceiro interessado, como já ocorre hodiernamente, os sistemas eletrônicos facultam pleno acesso às informações que podem naturalmente ser publicadas nos ambientes de visualização e acompanhamento processual. Está é já uma situação vivida em todos os tribunais de justiça do país.

2.4.2.7 Princípio da celeridade

Princípio que se destaca no Processo Eletrônico, por agilizar os atos via próprio sistema e de forma automatizada e padronizada, dispensando ou reduzindo-se em muito a intervenção humana. Como no processo eletrônico o que se muda é apenas a dinâmica ou a sistemática, não há falar-se em perda de qualidade da prestação, pois a participação do magistrado não ficará comprometida, cabendo a ele sempre a decisão.

2.4.2.8 Princípio da preclusão

Este princípio, como mencionado por STUDER (2008), prevê que a preclusão poderá ser lógica, temporal ou consumativa.

Nas preclusões lógicas e consumativas o processo eletrônico nada interfere por ser o instituto ato das partes. Já na preclusão temporal antes de prejudicar, o processo eletrônico acaba ajudando ao advogado que poderá, por meio de configurações de email, receber os andamentos processuais e se ajustar com maior facilidade aos atos que precisa provocar.

2.4.2.9 Princípio da indisponibilidade procedimental e da preferibilidade do rito ordinário

No processo eletrônico prevê-se que o próprio sistema conterá as opções de seleção de ritos, de acordo com a tecnologia e desenvolvimentos utilizados nos softwares, de tal sorte que poderá haver mecanismos de correção de ritos, nos casos de ingressos equivocados de entradas pelo autor, salvo se a confirmação deste se der no sentido de preferir rito ordinário a outro que também seja cabível.

2.4.3 Princípios relativos à produção da prova

Conforme orienta a doutrina a produção e obtenção da prova deve se dar de forma lícita e ser norteada pelo princípio da busca da verdade real (STUDER, 2008). O Processo Eletrônico, além de viabilizar a produção de provas de forma mais célere, segura e mais rica em detalhes, dependendo da natureza dessa prova, permitirá ao magistrado tanto consultar outras bases de dados que poderão agregar maior valor à sua decisão, tornando-a cada vez mais próxima da justiça pretendida pelas partes. (STUDER, 2008)

2.4.3.1 Inferência

As formalidades legais do tradicional método manual, com exceção das arraigadas na burocracia manual tradicional, todos os serviços são perfeitamente implementáveis no processo eletrônico.

O processo eletrônico diferencia-se do tradicional ou manual, apenas na forma da tecnologia empregada. Nessa perspectiva é metodologicamente mais moderno e prático, o que é inevitável em tempos de plena informatização mundial, que ademais, no contexto hodierno se busca priorizar o alcance da tutela, por meio de um processo mais ágil, seguro, econômico e moderno

2.5 Processo Judicial Eletrônico - em Conformidade com a Lei 11.419, de 19.12.2006"

A título de contextualização temática do presente capítulo, importa dizer que o Brasil ainda é um país onde prevalecem os desequilíbrios na distribuição de riquezas, fazendo com que cheguem cada vez mais expressivos numero de demandas ao judiciário com vistas à solução de conflitos de interesse (CLEMENTINO, 2008).

As consequências, via de regra inevitáveis, é a morosidade na entrega da prestação judiciária e o acumulo de processos em todas as instancias judiciais, se considerado o número insuficiente de juízes em face da crescente demanda, decorrentes de dois principais fatores, segundo se depreende da doutrina, quais sejam da falta de legislação compatível com esse aumento vertiginoso da demanda judicial ou da falta de implantação de sistemas informatizados capazes de agilizar a entrega da prestação judicial (CLEMENTINO, 2008)

Neste ultimo enfoque que ressalta a tecnologia como meio de agilização do processo judicial há que se equilibrarem os valores que lhes são inerentes e que estão estabelecidas como regras ou normas que inspiram todo o arcabouço legislativo vigente e que se consubstanciam nos Princípios Processuais (CLEMENTINO, 2008).

Como o próprio nome inspira a interpretação e o sentido do termo, Princípio é o começo, a origem a fonte de algo, porém como ensina Clementino, (2008.p.59) em Direito, possuem uma conotação mais ampla e transcendente, eis que lançam luz sobre o objeto ou às regras, fornecendo elementos ao hermeneuta para extrair do conjunto de normas os melhores efeitos.

Havendo colisão entre princípios, ainda que se considere não haver, sob a óptica jurídica, hierarquia entre princípios constitucionais, como defendem alguns autores, há considerar-se que deverá prevalecer o de maior relevância no caso concreto, e isso é de fundamental importância quando se busca harmonizar a aplicação de princípios jurídicos solidificados em bases tradicionais de manuseabilidade em face de um novo paradigma procedimental que tem por elemento viabilizador a tecnologia da informação. (CLEMENTINO 2008)

2.6 O documento eletrônico

A palavra documento deriva do Latim Clássico,"documentum", subtendendo-se por prova, lição, ensino, instrução; docere que quer dizer mostrar, ensinar.(CLEMENTINO, 2008).

No Código de Processo Penal Brasileiro[13] em seu art. 232 define, para fins legais que se considerará documento: "quaisquer escritos, instrumentos ou papéis, públicos ou particulares" e complementa em seu Parágrafo único que "À fotografia do documento, devidamente autenticada, se dará o mesmo valor do original".

Percebe-se que o legislador não elenca apenas um tipo de documento e sim outros que sejam validados e dotados de meios de reconhecimento de sua autenticidade, como é o caso da fotografia do documento desde que autenticada.

Ampliando o conceito e em sintonia com a melhor doutrina pode-se se dizer que documento é todo objeto do qual se extraem fatos em virtude da existência de símbolos, ou sinais gráficos, mecânicos, eletromagnéticos etc.(GRECO FILHO 1996), não restando dúvidas sobre a abrangência terminológica da palavra e do significado do termo documento.

Analisando-se na terminologia própria da área da informática, pode-se dizer que os documentos eletrônicos, cujo conceito em sentido *lato*, segundo sugere Marcacini (2008), seria os registros inseridos em um programa de computador, que para a máquina nada mais é "uma sequência de bits", tendo na saída (tela ou impressora) um texto representativo de um fato, como o mesmo conteúdo de um documento que tivesse sido datilografado ou manuscrito.

---

13 Fonte: BRASIL. **Decreto-Lei Nº 3.689, de 3 de Outubro de 1941.** Código de Processo Penal. Disponível em: HTTP//WWW.planalto.gov.br/declei3689_compilado.htm. Acesso em 06/05/2009

Em outras palavras se extrai que o documento eletrônico comporta, por suas características virtuais, total independência do meio físico tangível, mas se subsume à existência de um aparato tecnológico dotado de um programa que possa materializá-lo em forma de imagem estática ou dinâmica em um monitor de vídeo ou texto impresso por meio de uma impressora, que permitem extrair os textos tal como se faz com máquinas de escrever.

O documento eletrônico por sua virtualidade se apresenta, portanto, de forma autônoma em relação ao meio físico e pode apresentar-se de forma estática como os escritos, desenhos, fotos digitalizadas etc., bem como dinâmicos como vídeos, filmes, áudios etc., podendo apresentar características que permitem sua edição de forma mais versátil, ou, contrariamente, impedem a edição nos casos de segurança.

Conforme CLEMENTINO (2008) assim como nos documentos produzidos em substratos físicos como o papel, por exemplo, os elementos de qualquer documento são: seu autor, o meio de formação e o conteúdo.

Nessa perspectiva pode se considerar como autor qualquer indivíduo que tenha intelectual ou fisicamente produzido o documento.

No prisma da origem intelectual se poderá classificá-los, de acordo com CLEMENTINO (2008), como público ou privado, e sub-classificados como autótrofos – caso em que há identidade entre o autor do documento e o autor do fato documentado; e heterógrafos – quando o autor do documento é terceiro em relação ao autor do fato documentado, como é o caso dos documentos públicos.

Na mesma idéia de classificação os documentos podem ser escritos, gráficos, diretos, (quando o fato representado se transmite diretamente para a coisa representativa) e indiretos, quando o fato representado se transmite através do sujeito do fato representado (CLEMENTINO, 2008).

Em relação ao conteúdo os documentos podem ainda segundo o mesmo autor, se subdividir em formais, que são aqueles que podem se apresentar como provas de determinado ato; e não formais, cuja forma é livre, eis que o ato que encerram pode ser provado pelos meios admissíveis em direito, sem restrições (CLEMENTINO, 2008).

O Princípio da Segurança Jurídica exige naturalmente que os procedimentos em tramitação pela via eletrônica devem trazer elementos que confiram o mesmo grau de certeza quanto à autenticidade e à integridade dos documentos eletronicamente produzidos bem como garantir sua proteção contra acesso indiscriminado, como ocorre no Processo tradicional (CLEMENTINO, 2008).

Neste sentido para que a automação se mostre segura e se desenvolva satisfatoriamente é necessário que os procedimentos e trâmites que lhes caracterizam, sejam consubstanciados por documentos eletrônicos que preencham certos requisitos de validade, a saber, a autenticidade, a integridade e a proteção contra acesso não autorizado.

2.7 Requisitos de Validade do Documento Eletrônico

2.7.1 Garantia de Autenticidade e Integridade

Com a finalidade de se garantir a validade dos procedimentos eletrônicos que caracterizam os processos de automação, sobretudo nos processos judiciais, deve-se perseguir a integridade e autenticidade dos documentos que o compõe.

A respeito da integridade dos documentos pode-se dizer que está diretamente relacionada com a proteção contra alteração posterior, pois "impõe que seja possível confiar-se na Integridade do Documento eletronicamente produzido, devendo-se garantir sua inalterabilidade por quem o recebe ou por qualquer outro indivíduo que a ele tenha acesso" (CLEMENTINO, 2008).

No mesmo sentido, porém tratando-se da autenticidade dos documentos concebe-se, que esteja relacionada com a indicação verdadeira do autor e da subscrição do documento, ou seja, que realmente haja a correspondência entre o autor aparente e o autor real do documento.

Na mesma linha raciocínio concebe-se então que a autenticidade do documento deve representar a exata correlação de certeza entre o documento e seu autor, ou seja, que o documento tenha sido assinado pelo seu autor, sendo essa assinatura passível de verificação quando a firma for reconhecida por um tabelião.

A autenticidade é tratada de maneira distinta em virtude de o documento apresentado ser público ou particular. O documento público tem fé pública, ou seja, sua autenticidade é presumida, ainda que relativa e sujeita à contestação como ocorre no incidente de falsidade. Por sua vez o documento particular é considerado autêntico quando a firma de quem o assinou tiver sido reconhecida por um tabelião (CLEMENTINO, 2008).

Então a autenticidade é a certeza quanto à autoria, que pode ser constatada através da subscrição.

Conforme SANTOS (2009) em razão das características de virtualidade dos documentos no Processo Eletrônico, “a assinatura se reveste de caráter especial”, devendo também ser igualmente digital.

Por essa razão a Assinatura Digital torna-se elemento fundamental no processo eletrônico, pois será o meio de identificar e se garantir tanto a autenticidade quanto a integridade do documento que se manipulará no processo.

2.7.2 A Assinatura Digital a Autenticidade e a Integridade do Documento Eletrônico

Assinar, em sua raiz etimológica, provém do latim *assignare*, que significa firmar com seu nome ou sinal, por sua vez, o verbo firmar, em latim *firmare*, corresponde a tornar seguro, estável, definitivo, confirmado, ratificado.

Conforme se depreende dos ensinos de Carnelutti[14] a assinatura digital possui em si três propriedades que podem assim ser definidas:

"a) indicativa, de quem é o autor do documento;

b) Declaratória quanto à manifestação da vontade expressa;

c) probatória da existência da indicação e declaração apostas no documento".

Assim, trazendo para o universo das terminologias da tecnologia da informação, a assinatura digital é uma espécie do gênero de assinatura eletrônica, resultante da aplicação de algoritmos matemáticos para lhe conferir as garantias relativas de segurança e, assim, possibilitar sejam aferidas a origem e a integridade do documento.

---

14 CARNELUTTI, Francesco. A prova civil. Apud STUDER.2007.p.48. .

O processo decorrente da aplicação do algoritmo[15] que confere segurança na aferição da origem e sua integridade propicia uma forte vinculação entre a assinatura e o documento eletrônico estabelecendo, destarte, uma "imutabilidade lógica" de seu conteúdo, significando que qualquer sinal de edição tornará a assinatura invalida para efeitos legais. (BRASIL, 2008).

Para Menke apud Studer (2007) "a assinatura digital é a espécie do gênero Assinatura Eletrônica, e representa um dos meios de associação de uma pessoa, a uma declaração de vontade que será veiculada eletronicamente, 'refere-se exclusivamente ao procedimento de autenticação baseado na criptografia assimétrica[16]', enquanto que a Assinatura Digital é uma sequência lógica de dígitos que somente é reconhecida através de algoritmos, sendo escrita e lida em linguagem de baixo nível (linguagem de máquina), por isso diz-se que é baseada em criptografia assimétrica de bytes.

---

[15] Algoritmo: segundo dicionário virtual da Língua Portuguesa <http://www.priberam.pt>, significa: a) s. m., Mat., forma da geração dos números; processo de cálculo em que um certo número de regras formais resolvem, na generalidade e sem exceções, problemas da mesma natureza; qualquer procedimento que permita mecanizar a obtenção de resultados de tipo determinado, podendo um resultado ser obtido por mais do que um algoritmo; b) Inform., conjunto de etapas bem definidas necessárias para chegar à resolução de um problema. Para BURNETT (apud STUDER, 2007, p.40) "na criptografia computadorizada, os algoritmos são às vezes operações matemáticas complexas ou apenas manipulações de bits. Existem vários algoritmos de criptografia e cada um tem sua própria lista particular de comandos ou passos. Assim, você pode ter um programa que jogue paciência ou um que compute a trajetória de satélites". BURNETT, Steve; PAINE, Stephen. Criptografia e Segurança: o guia oficial RSA. Rio de Janeiro: Campos, 2002. p. 14.

[16] Na criptografia assimétrica, cada parte da comunicação possui um par de chaves. Uma chave é utilizada para encriptar e a outra para decriptar uma mensagem. A chave utilizada para encriptar a mensagem é publica, isto é, ela é divulgada para o transmissor; enquanto a chave para decriptar a mensagem é privada, isto é, ela é um segredo pertencente ao receptor. Disponível em http://www.gta.ufrj.br/grad/06_2/renan/CriptografiaAssimtrica.html. Acesso em 30/05/2009.

Nesse raciocínio pode-se concluir, a titulo de diferenciação que a Assinatura Eletrônica refere-se a qualquer mecanismo, não necessariamente criptográfico, para identificar o remetente de uma mensagem eletrônica e a Assinatura Digital refere-se a um método de autenticação de informação digital tipicamente tratada como análoga à assinatura física em papel que prova de forma inegável que determinada mensagem veio do emissor e que é espécie que se obtém a partir de implementação de criptografia assimétrica de chaves públicas.

Com base nas características garantidoras de autenticidade e integridade ao Documento Eletrônico apresentados por Carnelutti, surgem inevitavelmente questões sobre a forma de como se garantir a identificação da origem ou de quem haja criptografado ou assinado o documento eletrônico seja mesmo seu titular ou um terceiro mal intencionado e fazendo-se passar por aquela pessoa. Como saber quem foi o emissor da chave pública e qual o programa a ser utilizado para a decodificação do algoritmo e qual o órgão normatizador ou gerador das chaves?

A resposta a estas questões poderão ser obtidas pelo conhecimento de como se tem tratado o tema no Brasil, relativamente à questão da certificação digital.

2.8 Certificação Digital

O sistema nacional de certificação digital brasileiro, conhecido como Infra-estrutura de Chaves Públicas Brasileiras - ICP-Brasil, está disciplinado pela Medida Provisória 2.200-2 de 24 de agosto de 2001, atestando a tendência de plena utilização de documentos eletrônicos em todo o país, criando, por isso, uma infra-estrutura pública, mantida e auditada por um órgão público, que segue regras de funcionamento estabelecidas pelo Comitê Gestor da ICP-Brasil, no caso, o Instituto Nacional de Tecnologia da Informação, como forma de dar estabilidade, transparência e confiabilidade ao sistema.

Segundo normas da ICP-BRASIL, a autoridade Certificadora ou AC, é o ente que está associado à emissão dos atributos das chaves utilizadas, e que atesta, por meio de Certificados Digitais, a veracidade dos conteúdos das mensagens e documentos emitidos e recebidos através do sistema de Chaves Públicas e Privadas. (STUDER. 2007.p.42).

De acordo com as definições do ICP-BRASIL[17] o certificado digital é um documento eletrônico, assinado digitalmente por uma terceira parte confiável, que associa uma entidade (pessoa, processo, servidor) a uma chave pública.

Neste contexto o certificado digital deverá conter os dados de identificação de seu titular, tais como: nome, e-mail, CPF, chave pública, nome e assinatura da Autoridade Certificadora que o emitiu.

Ainda de acordo com o ICP-BRASIL, o certificado digital, na prática "funciona como uma 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 para assegurar confidencialidade, integridade das informações e confirmação de autoria." (BRASIL, ICP, 2009) 18.

Conforme normas do ICP Brasil, os certificados digitais emitidos pela AC com base nos padrões ITU X.509 (Institute of Communication *Union) ou ISO 9594-8 (International Organization for Standardization), tem* validade variável segundo os seguintes padrões detemporalidade e tipos:

Tipo A1 e S1, validade de um anos,

Tipo A2 e S2, validade de 2 anos

Tipo A3, S3, A4 e S4 validade de três anos

---

17 Disponível em https://www.icpbrasil.gov.br/apresentacao. Acesso em 01/06/2009.

18 Ib Idem

Segundo STUDER (2007), “findo o prazo, ou a pedido do usuário detentor da Chave privada (como por exemplo, ocorre na perda ou extravio de cartões de crédito), o certificado passa para Lista de Certificados Revogados LCR” e anota que os esses dados dos certificados digitais contidos na LCR permanecem armazenados por 30 anos por força da legislação brasileira.

A Autoridade Certificadora na condição de terceiro imparcial e aceito como confiável por aqueles que utilizam o sistema, faria às vezes do tabelião público para subscrever um documento de próprio punho.

O sistema de certificação digital implantado no Brasil, a ICP-Brasil, como vimos, é um conjunto de técnicas, métodos e entidades organizadas hierarquicamente e regidas por uma legislação específica com o intuito de emitir e controlar os certificados digitais expedidos, garantindo a autenticidade, a integridade e o acesso autorizado aos documentos eletrônicos com mesmo valor jurídico dos documentos em papel.

Esse sistema por sua vez tem lastro na técnica criptográfica, a qual abordará com mais detalhes a seguir.

2.9 Criptografia

A criptografia está intimamente ligada à história da escrita, tendo surgido em decorrência da necessidade de sigilo das mensagens escritas, havendo relatos de seu emprego na Grécia e Roma antigas quando generais de guerra valiam-se de mensagens codificadas para transmitirem ordens aos campos de batalha.

Sobre o tema posiciona-se Clementino (2008), que “Criptografia é um conjunto de técnicas que permite tornar incompreensível uma mensagem ou informação, com observância de normas especiais consignadas numa cifra ou num código”.

Em resumo seria um método matemático destinado a alterar código de arquivos eletrônicos ou não, com uso de sequências de cálculos ou rotinas de programação que tornam o conteúdo dos dados alterados incompreensível à quem os vêem ou tentem lê-los, sendo, portanto, uma técnica considerada segura contra interferências não autorizadas."

Seja como for a Criptografia será, então a aplicação de técnicas capazes de conferir os três aspectos indispensáveis á validade jurídica dos documentos eletronicamente produzidos (autenticidade, integridade e proteção contra acesso não autorizado), de modo a assegurar a integridade dos dados, na medida em que garante que a informação não sofreu alterações em seu conteúdo e formatação original, permitindo, por exemplo, que o destinatário de uma mensagem enviada em um meio eletrônico como a internet, por exemplo, não foi alterada no processo de envio.

No procedimento eletrônico informatizado é normal e recomendável que os conteúdos de documentos e outros conjuntos de dados, seja criptografados para que possam circular com segurança, ao menos relativa, nos meios virtuais.

2.10 Contrastes de opiniões sobre o processo eletrônico.

No contexto de modernização da Administração Publica, seja para seguir a tendência mundial ou para realmente se buscar prestar um serviço mais célere, seguro e acessível à sociedade, o processo eletrônico é um passo, a nosso ver, inevitável em um mundo onde predominam a tecnologia da eletrônica digital e da informática, já que a cada dia o que se vê são procedimentos tradicionalmente manuais se converterem em eletrônicos, não só mantendo-se resguardados os aspectos autenticidade e integridade como adicionando novos elementos de rastreabilidade e de auditoria.

Tanto é assim que milhões de processos eletrônicos tramitam no Judiciário com as mesmas expressões ritualísticas dos processos baseados em substratos tradicionais como os papeis. (CURADO, 2008)

O processo eletrônico inobstante vantagens já largamente expostas anteriormente, não deixa de enfrentar críticas em que se questionam desde a segurança no trato e armazenamento de dados, sobretudo os considerados sigilosos, até eventuais riscos à saúde dos operadores e, o que mais impressiona a nosso ver, pela suposta "exclusão" do mercado de trabalho dos usuários não familiarizados com a nova tecnologia (CURADO, 2008).

Pelo que se observa da publicação de artigos na internet, as resistências que preponderam são, em geral, de vieses culturais e motivados, quase sempre, pelo desconhecimento e pelas concepções de procedimento inovadores em relação às rotinas já assimiladas e costumeiras desde há muito.

Como expoente contrário à inovação pretendido pela informatização do processo, tem-se que a própria OAB tenha contestado o artigo 1º, III, "b", da Lei 11.419/2006, no qual se prevê que as assinaturas eletrônicas serão obtidas perante o Judiciário, "mediante cadastro prévio de usuário, conforme disciplinado pelos órgãos respectivos", justamente pelo fato de figurarem, entre os usuários, os advogados.

Neste contexto de contrariedade a entidade chegou a pedir uma audiência pública motivada pela solicitação de várias entidades que em tese desejariam atuar como interessados na causa de uma ADI ajuizada pela OAB para debater as consequências da Lei 11.419/2006[19].

---

19 Fonte: CONJUR. Briga da informatização. Anamatra critica ação da OAB contra informatização de processo Disponível em: http://www.conjur.com.br/2007-set-20/anamatra_critica_acao_processo_eletrônico. Acesso em 04/06/2009.

No sentido contrario à corrente opositora, se verifica um numero maior de entidades jurídicas que se posicionam favoráveis ao processo eletrônico.

Como exemplo de postura favorável manifesta-se o vice presidente da Associação Nacional dos Magistrados da Justiça do Trabalho que “a informatização da Justiça brasileira é aspecto fundamental para superar algumas mazelas contemporâneas relacionadas com a morosidade processual, em especial no cenário de uma sociedade que cada vez mais estabelece relações através dos meios eletrônicos", no mesmo sentido .

No mesmo sentido favorável, conforme se depreende do vasto apoio observado pelos setores de informática e de inteligência das polícias judiciárias, ressalta-se que a opinião técnica de todos quantos operam com seriedade as tecnologias surgidas para padronizar procedimentos e garantir recursos de segurança, celeridade, auditabilidade e outros requisitos inerentes à informatização, apóiam as medidas de automação, e dentre estes nos posicionamos no mesmo sentido, por restar cristalino que em futuro muito próximo não mais se falara em procedimentos manuais quando todo o planeta se torna uma grande rede interligada e integrada.

3 AUTOMAÇÃO DO PROCESSO DE INTERCEPTAÇÃO TELEFÔNICA E TELEMÁTICA

3.1 Uma proposta Tecnológica de Automação

Neste ponto da discussão, depois de trazer à baila discursos favoráveis e desfavoráveis sobre a informatização de procedimentos das interceptações telefônicas e telemáticas, depois de elencar princípios e confrontá-los com os seus efeitos em um ambiente operacional virtualizado, depois de apresentar a tendência de informatização pretendida e já levada a efeito nos tribunais de justiça do Brasil, capitaneados pelo Conselho Nacional de Justiça, pretende-se apresentar um esforço que vem sendo feito pela Polícia Civil do Distrito Federal (PCDF) no sentido de se adequar e também de desencadear junto às demais instituições de segurança pública, um movimento tendente à padronização e informatização de processos, apresenta-se, de forma resumida, a descrição do trabalho e os conceitos tomados como premissas para o desencadeamento de uma nova cultura operacional que pretende se tornar um paradigma e constante construção e aperfeiçoamento.

Trata-se de projeto conceitual denominado de “Projeto Ion”.

O mnemônico Ion deriva da forma reduzida e adaptada do termo Interceptação On line, que quer dizer, no jargão técnico, em tempo real.

O projeto em comento, idealizado e apresentado pela primeira vez à ANATEL em abril de 2007, tem como um dos autores, o, também, autor deste trabalho monográfico, e já repercutiu em termos de apresentações junto a órgão normatizador do setor de telecomunicações brasileiro, (ANATEL), onde foi muito bem recebido, operadoras de telefonia fixa e móvel de todo o Brasil, fabricantes nacionais e estrangeiros de equipamentos voltados para atividades de interceptação, polícias judiciárias Federal e Estaduais, Conselho Nacional de Justiça, Ministério Público do Distrito Federal e Territórios, Conselho Nacional de Chefes de Polícias Civis dentre outros.

A idéia da divulgação seria a de difundir o conceito e apresentar um desafio a todos os envolvidos no processo, de forma direta ou indireta, para que, baseado em melhores práticas, se construísse um projeto viável que tornasse essa atividade mais célere, segura, sigilosa, gerenciável e, por conseguinte, totalmente auditável.

Nesse contexto apresenta-se a seguir as idéias e tópicos julgados importantes e em sintonia com o presente trabalho que tem por propósito avaliar a viabilidade jurídica da automação do procedimento de interceptação telefônica e telemática no Brasil, tomando-se por base as ações dos principais órgãos da justiça brasileira e as legislações vigentes.

3.1.1 O Projeto Ion da Polícia Civil do Distrito Federal.

Com a estruturação da Divisão de Inteligência na Polícia Civil do Distrito Federal em 1999, recursos eletrônicos e sistemas de tecnologia voltados para as atividades de interceptação legal foram adquiridos, abrindo-se perspectivas de inovação na investigação policial , resultando de imediato a demanda destes dispositivos em quase todos os trabalhos investigativos realizados pelas delegacias policiais do Distrito Federal.

A partir da edição das leis 9.296/96 e 10.217/01, as quais permitem na investigação criminal a utilização da interceptação telefônica e ambiental, mediante autorização judicial, a Divisão de Inteligência da Polícia Civil passou a gerenciar os recursos visando proporcionar uma padronização, metodologia, normatização e disseminação das operações técnicas.

Nesse contexto, recursos de investimento foram disponibilizados para a implementação de soluções tecnológicas que permitissem o exercício responsável, fiscalizado e gerenciado de todas as ações desta natureza, no âmbito da Polícia Civil do Distrito Federal - PCDF.

Estes sistemas de apoio a atividades de inteligência permitem que haja plena interação tanto com as operadoras locais e nacionais, quanto com os Tribunais de Justiça do DF e Ministério Público, para a implementação da solução de interceptação judicial on-line com segurança, comunicação encriptada e controle de senhas.

Com a entrada em vigor da Lei 11.419-2006, o projeto passa, naturalmente, a ser viabilizado em seu aspecto legal, observado que a tendência em todo o sistema judiciário é o da automação dos processos com vistas às garantias de celeridade, economia processual, segurança, sigilo aplicado, dentre outros princípios que devem nortear as ações do Estado nos contextos jurídicos nos quais participa.

Ademais importa mencionar que o projeto é e será sempre totalmente aderente à legislação vigente à época de sua implantação e mesmo a eventuais alterações legislativas que venham a reger a matéria, bem como a novos diplomas infraconstitucionais que possam se materializar em razão de novas tendências sociais ou jurídicas.

As vulnerabilidades constatadas e já comentadas estão presentes em todos os nós de comunicação envolvidos no processo legal atual, sobretudo nas Operadoras de Telefonia e Provedores de Internet, em face da variedade procedimental e dos trâmites internos particulares de cada empresa, isso pelo fato de não haver legislação especifica sobre o procedimento que verse sobre padronização no âmbito geral dessas atividades.

Tais constatações se verificam pela observação empírica da falta de controle sobre os processos de comunicações internas, favorecendo que documentos sigilosos tramitem entre várias pessoas, sem qualquer filtragem ou segurança, para somente depois de algum tempo chegarem ao destinatário, que após recepcionar, despacha para outras pessoas executarem (FERRO JUNIOR, 2006).

Adiciona-se a tais constatações o fato de que o quadro de funcionários dessas empresas é formado por profissionais de diversas categorias, com graus de comprometimento bastante variado em relação a questões de ordem jurídico institucionais, sendo sabido que a grande parte de sabotagens e espionagem empresarial ocorre no próprio meio funcional das empresas (FERRO JUNIOR, 2006).

No projeto conceitual foram mapeadas as dificuldades internas observadas como pontos que necessitam ser vencidos dos quais se destacam

a) Necessidade de atualização tecnológica dos sistemas de interceptação/gravação, instalados na Divisão de Inteligência Polícia (DIPO) da PCDF.

b) Previsão de ampliação de investimentos em capacitação e formação técnica no uso das novas ferramentas tecnológicas para a investigação criminal;

c) Disseminação do conhecimento e conceito do Projeto ION para Autoridades Policiais, Juízes e Promotores de Justiça com descentralização de recursos tecnológicos e integração de base de dados;

d) Desenvolvimento de sistemas de mediação multi plataformas que deverão interfacear tecnicamente os sistemas judiciários e as centrais telefônicas e provedores de sistemas telemáticos.

e) Desenvolvimento de projetos e aplicação de recursos em processo de Gestão de Conhecimento.

f) Adoção de medidas internas para garantia de sigilo em todo o processo de investigação e compartilhamento de dados;

g) Envolvimento das entidades co-participantes do processo, quais sejam os Tribunais de Justiça Federal e Estaduais, Conselho Nacional de Justiça, Ministério Público e Polícias Judiciárias Federal, Estaduais e do Distrito Federal.

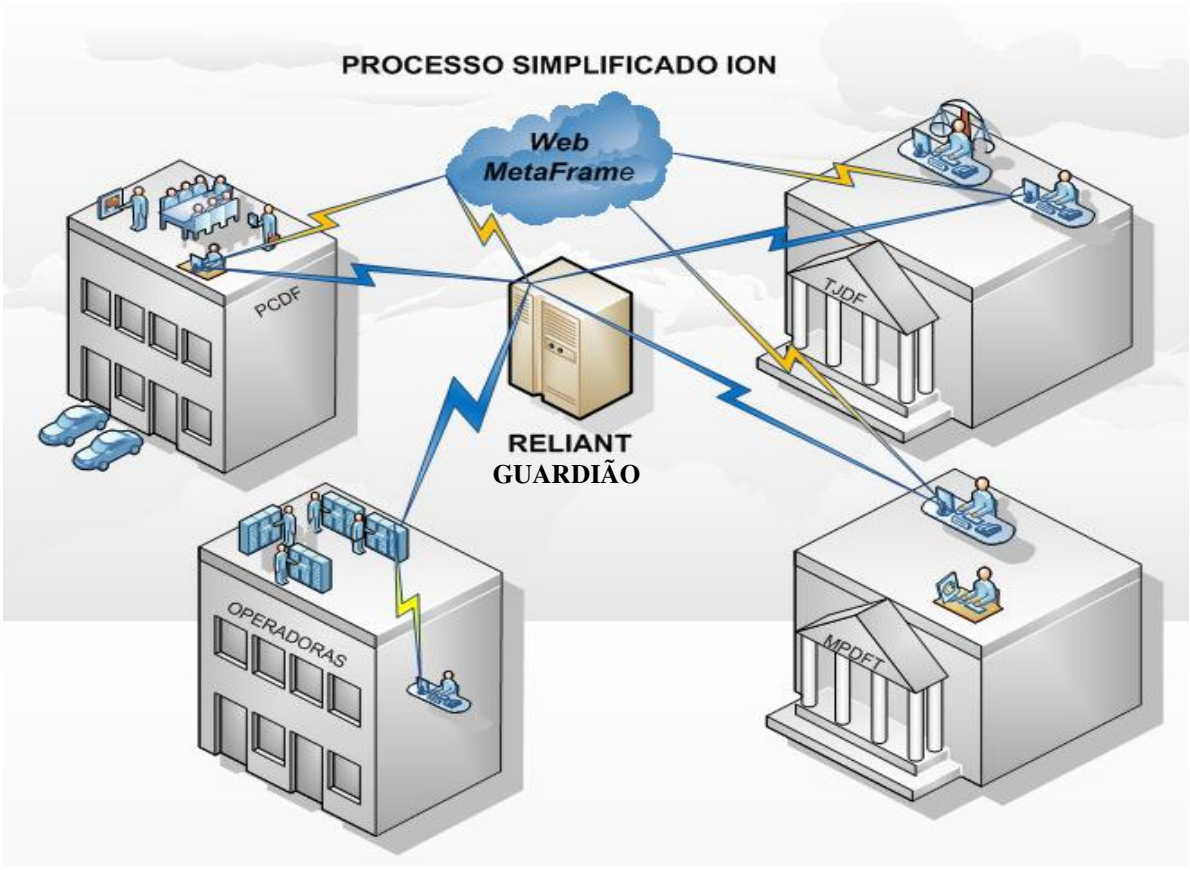

Figura 3 - Projeto Ion e a integração dos Órgãos envolvidos no processo.

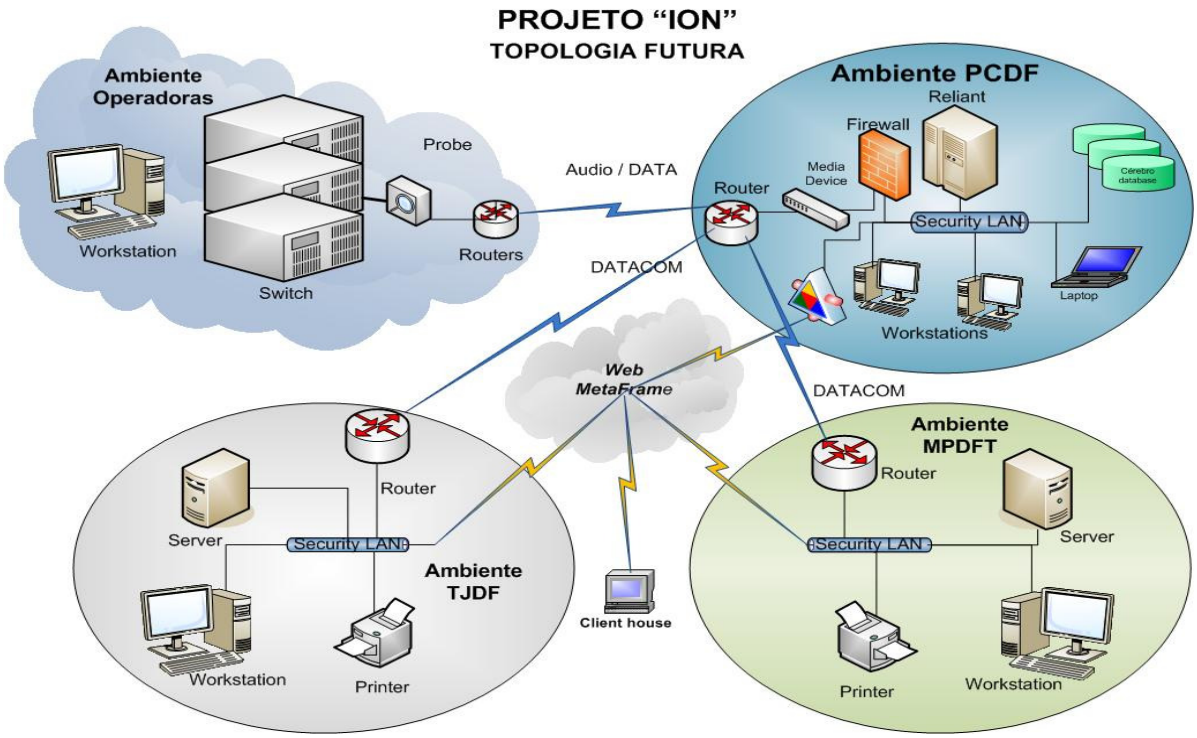

Figura 4 - Projeto ION - Topologia geral da Rede de áudio e dados.

Outros aspectos que merecem destaque no projeto em comento é que foram pensados aspectos técnicos, processuais e jurídicos que repercutem naturalmente em uma solução com os propósitos já apresentados.

Nesta perspectiva foram feitas sugestões sobre os seguintes aspectos:

Desenvolvimentos de TI no âmbito dos Tribunais de Justiça, Ministérios Público Federal e Estaduais, Polícias judiciárias nos níveis Federal, Estadual e Distrito Federal.

Destaca-se a importância e necessidade de criação de um subsistema de protocolo eletrônico para as atividades em comento sub módulos para documento eletrônico de quebra de sigilo junto ao judiciário, acompanhamento e fiscalização de operações pelas respectivas promotorias vinculadas a casos em andamento nas polícias dentre outros que sejam necessários ao processo.

Concebe-se que uma vez interligadas e integradas todas as promotorias com as varas criminais dos tribunais de justiça e estes com acesso aos módulos das plataformas de interceptação, o promotor vinculado ao determinado caso, mediante simples “login” ao sistema, selecionará a opção disponível seja para acompanhamento, fiscalização ou opinião sobre pedidos originários do TJ.

Ao acessar os módulos disponíveis do sistema, este retornará uma série de telas que vinculará o(s) promotor(es), ao caso e disponibilizará varias opções de interação junto ao sistema, permitindo a análise dos fundamentos jurídicos do pedido, o despacho dos Magistrados, os argumentos da autoridade policial etc., e por fim, disponibilizará telas com informações sobre o caso para que possa emitir seu parecer com segurança, celeridade e sigilo próprio do sistema em apreço.

Depois de preenchidos os questionários oferecidos pelo sistema, a promotoria vinculada ao caso e à vara criminal do Tribunal de Justiça, poderá visualizar um resumo do documento eletrônico gerado pelo sistema, de forma padronizada e previamente aprovada pelo Tribunal de Justiça, com todos os elementos legais necessários para o processamento do parecer.

Estando o documento completo e em condições de ser enviado ao TJ, poderá o promotor, mediante simples acionamento de tecla provocar várias ações próprias do órgão tais como:

- Despachos eletrônicos com vistas ao judiciário;
- Geração de assinatura digital válida e certificada;
- Impressão de via com marca d'água de segurança do próprio Ministério Público e também do sistema;
- Protocolo de saída para envio à vara criminal a que esteja vinculado o procedimento;
- Outras diretivas a serem implementadas de acordo com disposição legal ou requerimento de segurança aplicáveis.

Uma vez aceito e opinado pela quebra do sigilo de determinado objetivo, e no caso de acolhimento pelo magistrado, o promotor passa a receber em sua estação de trabalho virtual, todas as informações que forem autorizadas pelo magistrado.

Lembra-se que o intervalo de tempo na tramitação eletrônica de todos os documentos é mínimo, na casa de milissegundos e com total segurança.

Da mesma forma prevêem-se módulos de interação do Sistema de Interceptação Ativa Ion com os Sistemas de protocolo e tramitação documental eletrônico dos Tribunais. .

Estes subsistemas lógicos integrarão as seguintes plataformas eletrônicas

- Subsistema de Protocolo integrado entre TJDF, MPDFT e PCDF.
- Tramitação de documentação eletrônica interna
- Mediação com operadoras para ativação de alvos/objetivos de forma ativa.
- Outros.

Todos os módulos de interação entre os sistemas eletrônicos do TJDF e os das plataformas de interceptação ativa deverão ser desenvolvidos pelas equipes de desenvolvimento de softwares do próprio TJDF, e a razão encontra-se na sensibilidade e nas políticas internas de cada órgão participante no tocante à segurança e métodos de trabalho já consolidados nos respectivos órgãos da justiça.

Estes módulos deverão permitir a interação entre TJs e os congêneres da PCDF e do MPDFT, de tal sorte que ao receber um documento eletrônico possa:

- Permitir seja identificado a origem do documento, data e hora do envio, hora do recebimento, assunto, juízo destinatário;
- Sincronização de horário pelo sistema de interceptação legal, que por sua vez estará vinculado ao horário do relógio atômico do Observatório Nacional Brasileiro;
- Emita recibo automático ao órgão de origem do documento com os dados da recepção do documento eletrônico, matrícula do servidor do protocolo, dados da distribuição etc.
- Permita o envio de registros do trâmite eletrônico do documento em tempo real
- Não permita a abertura do documento digital recebido a não ser pelo magistrado da vara pertinente ao caso.
- Permita a distribuição aleatória em ordem das políticas próprias dos Tribunais de Justiça e de acordo com legislação vigente.

- Nos casos de juízos preventos deverá operar a distribuição automaticamente ao respectivo juízo.
- Outras funções de segurança que poderão ser identificadas quando da implementação do sistema.

Um subsistema de Tramitação de documentação eletrônica deverá também, ser criado e permitir operações de forma integrada entre os órgãos apenas no que concerne ao envio de mensagens às autoridades policiais, promotores e agentes cadastrados em determinado Caso de investigação, sobre o status do documento ou processo eletrônico em tramitação.

Deverá dentre outras funcionalidades, possibilitar no mínimo as seguintes:

- Envio de mensagens curtas sobre o status da tramitação a emails cadastrados das autoridades policiais, agentes e promotores públicos cadastrados nas respectivas operações e casos em andamento;

Há previsão de instalação de uma interface de mediação que, na perspectiva técnica, será o mais complexo e requererá a instalação de um equipamento denominado Mediador, o qual tem a função precípua de viabilizar a integração das diversas tecnologias de diferentes fornecedores numa planta de telefonia.

O equipamento tem a função de integração de ambientes tecnológicos heterogêneos, onde diversos equipamentos de fabricantes diferentes têm que se relacionar de forma transparente ao usuário normatizando todas as entradas e saídas, interpretando e convertendo comandos manuais dados pelos magistrados diretamente nas plataformas de telefonia móvel e fixa.

Mediante comandos previamente padronizados o magistrado uma vez logado ao sistema, aporá suas razões no documento eletrônico gerado e quando decidir que a interceptação deverá ser iniciada, depois de conclusas as formalidades legais dentro do sistema, este abrirá uma tela onde o juiz poderá em tempo real:

- Enviar para a operadora o documento eletrônico de autorização da medida, devidamente autenticado,
- Poderá comandar o início da operação de interceptação com todos os requisitos de segurança, de fixação de prazos de início e fim de operação;
- Enviar automaticamente à autoridade policial, agentes e promotoria encarregados de acompanharem o caso, mensagem instantânea de início de operação ou do status em que se encontre, caso opte, por deixar para a autoridade policial o início da operação.
- Permitirá ao magistrado encerrar a qualquer momento qualquer operação já iniciada, mediante decisão lançada no sistema. Nestes casos prevê-se que quando o juiz abra uma tela de acompanhamento de caso que haja autorizado ou esteja presidindo, ao lançar em campo próprio, argumentos para o encerramento extemporâneo da operação em curso, o sistema habilitará uma tecla virtual de bloqueio instantâneo ou programado da operação.
- Permitirá ampliar o prazo de operações em curso dentro da forma da lei. O sistema oferecerá teclas virtuais com opções, que ao serem selecionadas abrirão telas com campos próprios para lançamento de justificativas e decisões.
- Enviará aos sistemas das operadoras a requisição da liberação e a confirmação de uma chave de segurança “token” com vida útil de poucos minutos, dentro do qual a operação deverá ser confirmada pelo magistrado para que ocorra a liberação da operação.

- Outras ações de segurança serão acrescidas com a evolução do sistema de modo a garantir plena confiabilidade e disponibilidade das operações.

Embora não se tenha adentrado na totalidade dos aspectos discutidos no projeto, ressalta-se que um dos mais importantes a ser observado é o novo paradigma operacional que se fundamenta no emprego maciço de tecnologia da informação, com todos os requisitos de segurança e adaptabilidade aos diplomas legais vigentes e regentes da matéria.

Além do exposto, ressalta-se que o projeto apresentado insere definitivamente o sistema judiciário como ator ativo do processo e o Ministério Público como fiscal em tempo real do que se levam a efeito nessas operações, resguardados os limites legais.

No mesmo sentido disciplina o papel das operadoras, limitando-as a colaborarem integralmente com as medidas, sem que isso implique em que tenham que gerir, controlar e até decidir sobre a possibilidade ou não de atender à ordem, como atualmente já se verificou na casuística policial .

CONCLUSÃO

Sem desejar abandonar o foco da discussão sobre a questão da viabilidade jurídica da automação do procedimento das interceptações telefônicas e telemáticas, convém apresentar importante questão que paira como pano de fundo de todo o processo relacionado a essa atividade e que se relaciona com os atores que em qualquer instancia deveriam figurar como participes desse procedimento.

Doutrinariamente parece prevalecer entendimento que as operadoras de telefonia compõem o roll de atores envolvidos no processo regulado atualmente pela lei 9296/1996. (GRECO FILHO, 1996; GOMES & CERVINI, 1997)

Raciocinando nesses termos, há quem lance oposição a essa tese, com base em posicionamentos de renomados gestores da segurança pública, que entendem ser equivocado o pensamento, doutrinariamente prevalente, de que as operadoras devem realizar as operações de interceptações e informar à justiça, na melhor interpretação possível. (FERRO JUNIOR, 2006)

Justifica-se o entendimento sobre o equívoco assinalado, no fato de que essas empresas parecem verdadeiras e poderosas "caixas pretas", que, em tese, possuiriam o poder de "ouvir" aqueles clientes que eventualmente pudessem ser interessantes a algum propósito, e este cliente ou o Estado, nada poderia, também em tese, fazer no momento atual para romper com eventuais práticas dessa natureza, no sentido de reivindicar informações sobre sua forma ou método de operarem ou tratarem o volume de dados diariamente trafegados em suas redes. (FERRO JUNIOR, 2006)

A razão parece simples e intuitiva. Para os órgãos policiais, por meio dos gestores de inteligência policial, essa situação decorre do fato dessas empresas serem privadas e estrangeiras.

Pelo processo da privatização a elas foram assegurados os direitos para gerenciar e rotear, todos os fluxos e conteúdos de dados, voz, textos etc. sinais e registros, enfim as telecomunicações de todo o país, sem que até o momento as autoridades se alertassem para esta realidade.

Questão de direito internacional e também de direito internacional privado, torna-se complexa na medida em que se permeia de aspectos criminais e de soberania, segundo relato dos gestores de inteligência policial .

Com o advento da privatização, inobstante as melhores intenções dos Governantes do país, comenta-se, em tímida análise, que pode ter havido equívocos estratégicos ao não se prever os mecanismos de defesa contra possível evasão dos "tesouros informacionais" que trafegam nas redes dessas operadoras.

Tecnicamente qualquer potencial objetivo ou alvo (cidadãos comuns, políticos, empresários, juízes, promotores, advogados, financistas, banqueiros etc.) que se comuniquem, trafeguem dados, realizem operações quaisquer, que possam ser do interesse desses grupos, ou de alguém dentro desses grupos que detenham poder decisor, estaria mercê de quebra de sigilo de suas comunicações sem que ninguém pudesse fazer nada, guardadas as restrições meramente de natureza circunstanciais, eis que o Estado brasileiro não conseguiria, em regra e nos moldes da atual legislação, exercer qualquer controle sobre os sistemas dessas operadoras.

Essa reflexão retrata uma preocupação, que, se passou pela mente de alguém na esfera dos poderes legislativo ou judiciário, ainda não repercutiu em forma de projeto de lei, eis que os se encontram em tramitação na Câmara Federal, tentam, sim, legitimar como ator de direito as operadoras de telefonia, como se depreende do projetos de lei que tramitam na Câmara Federal.

Nos dois instrumentos legislativos que tramitam na Câmara dos Deputados (Projetos de Lei 5285/2009 e 5286/2009), e que visam substituir a atual lei 9296/96, observa-se essa tendência preocupante, eis que não só legitima, como dá poderes às operadoras para gerenciar e informar ao judiciário o que se passa, em termos de interceptações em seus "intransponíveis" muros tecnológicos.

Tão grave como o que acima se mencionou é fato dos legisladores, imbuídos que estão e fazer o melhor pelo país, parecerem agir ingenuamente no sentido de cogitar que o que se lhes pedirem (às operadoras de telefonia) se lhes responderão, e quando pouco se lhes responderão com a verdade.

Fazendo um paralelo com o que acima se relatou, fruto de reflexões, deduções e conhecimento empírico sobre o que se afirmou, muito mais como provocação de novos raciocínios que levem a buscar elementos probatórios para, ainda que tardiamente, se confirmar o que se mencionou, (nesse sentido observe-se os relatórios da CPI dos grampos telefônicos que trouxe a lume vastos casos de descontrole e de atividades levadas a efeito dentro de operadoras, algumas delas veiculadas na mídia como espionagens internacionais, envolvendo empresas, pessoas etc.), entende-se que diante da problemática apresentada e considerando as tendências nacionais e mundiais no sentido da informatização de processos, a automação dos procedimentos das interceptações telefônicas e telemáticas, poderiam inclusive, dependendo do nível de profundidade e de interatividade como os sistemas telefônicos das operadoras, lançar luz e controle sobre a forma que as empresas estariam trabalhando com informações, que em última análise pertencem ao povo brasileiro.

Não se fala aqui de quebrar sigilos em nível de massa, mas de registrar e rastrear eventuais evasões de informação que eventualmente não estivessem respaldadas por ordem judicial.

Nesse contexto, um órgão gestor, mediante sistema de controle de fluxo e com base em comandos específicos, extrairia, para fins de auditoria, os registros de operações e todos os registros técnicos de desvios (interceptações) levados a efeito por todas as operadoras.

Do confronto entre os procedimentos autorizados ao longo do país, e os dados obtidos de forma transparente dos sistemas das operadoras, seria possível saber ou identificar eventuais operações ilegais que naqueles muros poderiam ser levadas a efeito.

O Brasil ao privatizar sua base ou plataforma de telecomunicações parece ter o dever, por meio dos legisladores e cidadãos, de ficar em alerta e se precaverem de não facilitar a ofensa a sua soberania ou aos tesouros mais valiosos da nação, que se consubstanciam no seu poder e na sua liberdade de se comunicar.

Mais do que previsão legal e mudanças no ordenamento jurídico especial e constitucional, é necessário que os legisladores e cidadãos percebam a sensibilidade estratégica presente nessa discussão.

Nesse diapasão, como os procedimentos de automação de processos têm, por natureza, capacidade intrínseca de fomentar a padronização, o controle e auditoria, e como já há legislação nacional permissiva de que se processem, em atividades também sensíveis como a penhora eletrônica, levada a efeito pelo sistema BacenJud, resta ao legislador, em caráter mais pontual se posicionar em relação ao tema.

Impossível em um contexto de evolução tecnológica deixar de ser favorável a uma proposta que tenha por escopo disciplinar, padronizar, tornar célere, segura, sigilosa e auditável as operações de quebra de sigilo telefônico e telemáticos.

Nesse sentido, considerando serem viáveis e necessárias ao bom e correto andamento dessas atividades, tomando-se por premissa os conceitos já apresentados no projeto Ion da PCDF, bem como outros que dêem suporte legal e técnico a tal medida, como a lei 11.419/2006, parece inegável que a automação do procedimento das interceptações telefônicas de telemáticas são viáveis, factíveis e necessárias ao país, seja qual for o ordenamento jurídico vigente sobre o assunto.

REFERÊNCIAS

BRAGA, Carlos Alberto Pinto. “Governo Eletrônico.” In: *@-Gov.br. A próxima revolução brasileira*, por Ali CHAIN, Maria Alexandra CUNHA, Peter T. KNIGHT e Solon Lemos PINTO, 15-53. São Paulo: Prentice Hall, 2004.

BRASIL, República Federativa. *Planalto.gov.br.* 19 de dezembro de 2006. http://www.planalto.gov.br/ccivil_03/_Ato2004-2006/2006/Lei11419.htm. (acesso em 02 de maio de 2009).

CARNELUTTI, Francesco. “A prova civil.” 54. São Paulo: Bookseller, 2005.

CLEMENTINO, Edilberto Barbosa. *Processo Judicial Eletrônico.* Curitiba: Juruá Editora, 2008.

CURADO, Rubens. *Processo Administrativo e Processo Judicial Eletrônico.* 2009. http://www.carreirasjuridicas.com.br/resumo_oficinas/processo_administrativo_e_processo_judicial_eletrônicos (acesso em 04 de 06 de 2009).

DIAS, Cláudia. *Segurança e Auditoria da Tecnologia da Informação.* Rio de Janeiro: Axcel Books, 2000.

FANAIA, Saulo Castrilon. *Interrogatorio por video conferencia, um breve comentário sobre a Lei 11.900/2009.* janeiro de 2009.

FERNANDES, Ciro Campos Christo. “Governo eletrônico e transformação da administração pública.” In: *@-Gov.br. A próxima revolução brasileira*, por Ali CHAIN, Maria Alexandra CUNHA, Peter T. KNIGHT e Solon Lemos PINTO, 102-108. São Paulo: Prentice Hall, 2004.

FERRO JUNIOR, Celso Moreira. *Inteligência policial* . Brasilia: UCB, 2005.

FERRO JUNIOR, Celso Moreira. “Interceptações Telefônicas e Ambientais.” *Revista Jurídica Consulex* (Consulex) 191 (2004): 26-30.

—. “Investigação policial e Empresas de Telefonia.” *Revista Juridica Consulex*, 15 de janeiro de 2006: 7 - 9.

FERRO JUNIOR, Celso Moreira, Hugo César FRAGA PRETO, e Edmundo Dias OLIVEIRA FILHO. *Segurança Pública Inteligente (Sistematização da Doutrina e das Técnicas da Atividade).* Goiânia: Kelps, 2008.

GOMES, Luiz Flávio, e Raúl CERVINI. “O que se entente por "Interceptação telefônica".” In: *Interceptação Telefônica: Lei 9296, de 24.07.96*, por Luiz Flávio GOMES e Raúl CERVINI, 95-110. São Paulo: Revista dos Tribunais, 1997.

GRECO FILHO, Vicente. *PROCEDIMENTO DA INTERCEPTAÇÃO* . Vol. 1, em *Interceptações Telefônicas*, por Vicente GRECO FILHO, 27-39. São Paulo: Saraiva, 1996.

JESUS, Damásio Evangelista. *Código Penal Anotado.* 6ª ed. São Paulo, SP: Saraiva, 1996.

—. *Curso Professor Damásio.* 1999. http://www.angelfire.com/ut/jurisnet/art69.html (acesso em 16 de maio de 2009).

LEVY, Pierre. *As tecnologias da Inteligência: o futuro do pensamento na era da informática.* São Paulo: 34, 2000.

MELLO, Celso Antonio Bandeira. *Curso de Direito Administrativo.* 13ª ed. Sâo Paulo: Malheiros, 2001.

MENKE, Fabiano. " Assinatura Eletrônica, as pectos jurídicos no direito brasileiro." 42. São Paulo: Revista dos Tribuanis, 2005.

MOITA, Adelson Silva. *Interceptação Telefônica: Integração e Automação do Procedimento Legal com Base no Projeto Ion da Polícia Civil do Distrito Federal.* Brasília: UniDF/ICAT, 2009.

PARIZZATO, João Roberto. *Comentários à Lei 9296, de 24-07-96 - Interceptação de Comunicações Telefônicas.* São Paulo: LED Editora de Direito, 1997.

SANTOS, Valfredo J. "O documento eletrônico no processo judicial eletrônico." *Revista Jus Vigilantibus.* janeiro de 2009. http://jusvi.com/artigos/37784/2 (acesso em 16 de 05 de 2009).

STUDER, Andréa Cristina Rodrigues. Processo Judicial Eletrônico e o Devido Processo Legal. 2007. 116 f. Dissertação (Mestrado) - Curso de Pós Graduação Stricto Sensu Em Ciência Jurídica, Universidade Do Vale Do Itajaí - Univali, Itajaí, 2007.

TAKAHASHI, Tadao. "A sociedade da Informação e a democracia eletrônica." In: *@-GOV-BR - A Proxima Revolução Brasileira*, por Ali CHAIN, Maria Alexandra CUNHA, Peter T. KNIGHT e Solon Lemos PINTO, 85-95. São Paulo: Prentice Hall, 2004.