DEPARTAMENTO DE TAQUIGRAFIA, REVISÃO E REDAÇÃO

NÚCLEO DE REDAÇÃO FINAL EM COMISSÕES

TEXTO COM REDAÇÃO FINAL

TRANSCRIÇÃO *IPSIS VERBIS*

CPI - ESCUTAS TELEFÔNICAS CLANDESTINAS		
EVENTO: Audiência Pública	Nº: 0090/08	DATA: 04/03/2008
INÍCIO: 18h23min	TÉRMINO: 21h30min	DURAÇÃO: 3h07min
TEMPO DE GRAVAÇÃO: 3h06min	PÁGINAS: 70	QUARTOS: 38

DEPOENTE/CONVIDADO - QUALIFICAÇÃO
RENATO LIRA DA COSTA - Gerente do Núcleo de Difusão do Conhecimento da Tempo Real Tecnologias de Informação. MARCELO BANDEIRA RODRIGUES - Coordenador de Tecnologias de Informação da Tempo Real Tecnologias de Informação. RAIMUNDO PINHEIRO DE CASTRO VIEIRA JÚNIOR - Diretor de Relações Institucionais da RONAN Internacional Ltda.

SUMÁRIO: Tomada de depoimentos.

OBSERVAÇÕES
Houve intervenções fora do microfone. Inaudíveis. Houve exibição de imagens. Há falhas na gravação.

O SR. PRESIDENTE (Deputado Marcelo Itagiba) - Convido o Sr. Marcelo Bandeira Rodrigues a tomar assento à mesa.

Com a palavra o Sr. Marcelo Bandeira Rodrigues, por até 20 minutos, para fazer a sua explanação.

(Intervenção fora do microfone. Inaudível.)

O SR. PRESIDENTE (Deputado Marcelo Itagiba) - Sr. Renato, o senhor está também identificado aqui junto à CPI, já fez o termo de compromisso? (*Pausa*.)

(Intervenção fora do microfone. Inaudível.)

O SR. PRESIDENTE (Deputado Marcelo Itagiba) - Então: e o Sr. Renato Lira da Costa, também para tomar assento à mesa. O Sr. Renato, que fará a exposição inicial, com a palavra.

O SR. RENATO LIRA DA COSTA - Sr. Presidente, Srs. Parlamentares, senhores que estão assistindo a esta audiência, eu, Renato Lira, e Marcelo Bandeira estamos representando a empresa Tempo Real, uma empresa de capital 100% nacional. Tem sede no Rio de Janeiro e trabalha com produtos voltados à área de investigação e inteligência para as forças de segurança pública no Brasil. Nós vamos falar aqui, eu e o Marcelo, sobre um conjunto de ferramentas, umas novas, que estão chegando a partir de ontem no Brasil, que eu tive a oportunidade de buscar no exterior, e o Marcelo sobre alguma coisa que já tem bastante tempo e bastante utilização pelas nossas forças de segurança pública. Eu vou falar sobre biometria de voz, e o Marcelo Bandeira sobre as ferramentas da i2, particularmente Analyst's Notebook, iBase, Text Chart e outras tantas, que já foram utilizadas, inclusive, nesta Casa, em outras apurações que ocorreram no passado. *(Segue-se exibição de imagens.)* Bom, senhores, como o tema aqui é a parte de interceptação, a ferramenta que nós estamos trazendo agora para o Brasil trabalha com a parte de biometria de voz — está sem sinal aqui na... *(Pausa.)* Bom, a biometria de voz é uma coisa recente, mesmo na área internacional. No passado, existiam as pessoas que tinham formação e qualificação técnica para dizer se uma voz correspondia a uma pessoa, baseadas em determinados fonemas ou sobreposição de palavras que essas pessoas diziam. A biometria de voz, que começou com um estudo no MIT, ela analisa os sons emitidos por uma pessoa, baseados em toda a compleição física dela, toda a passagem do som por esôfago, céu da boca, nariz, os dentes que ela

tem na boca, e vão produzir uma chave de identificação única, tal qual o sistema de impressão digital, que é o AFIS, os sistemas, e de DNA. Isso já foi utilizado no Brasil, não com o nosso *software*, que representamos com exclusividade, mas por enviar um trecho de áudio daquele traficante, o Abadia, que foi preso no ano passado, em São Paulo, para a polícia dos Estados Unidos. E foi possível fazer a identificação do Abadia, para a sua prisão, puramente pela voz que se tinha dele, um trecho de voz. Quer dizer, é uma coisa que já rendeu frutos para a polícia brasileira no ano passado — um passado recente. Bom, a nossa parceira é a Agnitio, na Espanha. E a Tempo Real — está a logo ali em cima — é a nossa empresa no Brasil. Algumas referências, para mostrar que não é um produto de laboratório, é um produto que já está em utilização. Aqui temos três da Espanha: a Guarda Civil, que foi a parceira dessa empresa, da Agnitio, no desenvolvimento do produto, o primeiro produto foi chamado de Saivox; o Ministério da Defesa da Espanha; o Corpo Nacional de Polícia, também da Espanha. Eles utilizam esses produtos. Também, o Centro Nacional de Inteligência; a Polícia da Comunidade Basca; a Polícia Nacional do Chile; a Polícia Chinesa; o Departamento de Justiça da Colômbia; o Instituto Forense da Holanda — que é uma das mais importantes referências que nós temos, porque existe uma certificação européia dizendo que as ferramentas, o motor de identificação de voz funciona mesmo. O Instituto Forense da Holanda, por utilizar muito essas ferramentas, tem contribuído para essa certificação. Eu vou mostrar o instituto mais à frente. Ainda: a Procuradoria-Geral da Coréia do Sul; a Polícia Criminal Alemã — que também, tal qual aquele centro de perícia da Holanda, contribuiu muito no desenvolvimento; e a Polícia Nacional Francesa. Existem, na gama de produtos, produtos distintos para necessidades distintas. Então, eu vou falar de 4 produtos. O primeiro é o Batvox, um produto destinado exclusivamente a peritos. Ele pressupõe, e exige, em certos casos, um conhecimento técnico para que seja utilizado. Mas ele vai dizer, com absoluta fidelidade, que uma voz que eu tenha que fazer o batimento contra uma outra voz que eu achei em algum lugar corresponde à daquela pessoa, inclusive gerando o mesmo método de avaliação utilizado para os sistemas de impressão digital ou DNA, que é o Likelihood Ratio, um método reconhecido mundialmente e que é empregado aqui com o mesmo sucesso. Então, o Batvox é uma coisa que é destinada a um homem ou a um grupo de

homens numa sala, que precisam de mais tempo para produzir um resultado que vai ser levado a um tribunal. A outra é a mais nova de todas as que eu vou mostrar. O Batvox é o mais antigo. A partir dele é que as outras ferramentas foram desenvolvidas. Ele é que tem a inteligência, o que chamamos de o motor de reconhecimento da biometria de voz. A mais nova, mas não menos importante, é o APT, que é uma ferramenta que vai fazer o que as duas próximas que eu vou mostrar fazem, só que num computador portátil. Num *notebook* igual ao meu, eu vou poder fazer, em menor escala, coisas que eu vou mostrar a seguir, nas próximas duas, que são o ASIS, que é um banco de dados... Tal como eu posso ter, à medida que eu freqüente locais de crime, ou delegacias policiais, ou institutos de identificação, um conjunto de impressões digitais para que eu armazene para posterior consulta, eu posso ter vozes, que sejam criados modelos dessas vozes, para que eu armazene em bancos de dados para posterior consulta. Vamos dizer que uma ligação está chegando em um telefone celular, comunicando um seqüestro relâmpago de uma autoridade, e eu vá ao banco e diga que a voz que eu tenho daquela autoridade não corresponde àquela ameaça de seqüestro, ou confirme. Então, o ASIS é isso, é uma grande base de dados, como eu tenho a base de dados do AFIS, que é de impressão digital. E o BS3, que talvez seja o que tenha maior correlação com a audiência de que estamos participando agora, que é um produto que permite monitorar, em tempo real ou quase real, dentro de um fluxo de ligações entrantes, de interceptações, a voz de um alvo que eu queira buscar. Então, se eu estou, por exemplo, ao lado de um presídio, interceptando uma, duas ou três ERBs do presídio, eu sei que o preso pode usar um celular ou o celular de inúmeros presos ali dentro. E se eu tenho 7 mil ligações por dia sendo interceptadas naquela ERB, para saber se um determinado preso que eu quero buscar falou, eu vou ter de ouvir as 7 mil ligações para saber se fulano de tal utilizou um telefone. Com esse produto, eu pego um modelo da voz dessa pessoa que é o meu suspeito, coloco junto ao sistema de interceptação — nós não fazemos a interceptação —, coloco junto, e estabelecemos regras. Então, se chegar uma voz que corresponda à voz desse modelo, dentro do fluxo de interceptação, por favor, me salve este arquivo de voz em determinada pasta, passe um *e-mail* para determinada pessoa, emita um alerta na tela para o operador. Podem-se criar uma série de regras para um ou mais

suspeitos. Isso traz um ganho na privacidade do cidadão, porque aqueles que não são alvos não precisam estar sendo ouvidos nas conversas que têm. Essa tecnologia é robusta, ela já está desde 2005 no mercado. Ela não é antiga, mas ela é robusta, tem demonstrado o seu valor naquelas instituições que eu apresentei anteriormente. E anualmente esse motor de busca é submetido à homologação em dois importantes institutos de tecnologia: um americano, que é o NIST, e outro europeu, que é o NFI, que eu falei que fazia parte do Instituto Forense holandês. Só tem uma ferramenta ou uma tecnologia que conseguiu suplantar nos últimos testes a tecnologia da Agnitio e Tempo Real, que é justamente a do MIT, e que não é colocada para venda no mercado internacional porque ela é utilizada pelo Governo americano. E o Governo americano só libera esse tipo de ferramenta, julgada por eles estratégica, depois de 10 anos de uso, quando ela começa a se tornar obsoleta, e eles estão desenvolvendo outras coisas que eles consideram mais de ponta.

O SR. PRESIDENTE (Deputado Marcelo Itagiba) - Só aproveitando para esclarecer. Então, por exemplo, vamos partir de um princípio de que o americano está interceptando um canal de comunicação satelital, por onde circulam milhões de vozes, e o americano deseja estabelecer se por aquele canal passou a voz do Bin Laden, por exemplo. Então, com esse *software* estabelecido, ele conseguirá pescar naquele canal, se o Bin Laden, por exemplo, falar naquele canal, a voz do Bin Laden, e identifica. E, aí, tranca aquilo para a gravação, é isso?

O SR. RENATO LIRA DA COSTA - Em teoria, sim, mas o tamanho que o senhor apresentou extrapola a capacidade. Alguém estava me perguntando durante a apresentação da Dígitro, quando estávamos ali aguardando, justamente sobre isso, se, por exemplo, uma cidade como Brasília poderia ser interceptada, e eu disse que não. Eu vou mostrar um diagrama um pouco mais à frente...

O SR. PRESIDENTE (Deputado Marcelo Itagiba) - Nem com o sistema do MIT?

O SR. RENATO LIRA DA COSTA - Com o do MIT, eu não sei. Eu não tenho informação sobre isso. Até foi uma outra pergunta que me fizeram sobre a locução de determinadas palavras. É dito por muitos e provado por ninguém que algumas palavras ditas em telefonia ou escritas em *e-mail* — por exemplo, bomba, Bush e outras —, elas são interceptadas e são levadas para um grande centro de defesa

que tem ali na região perto da Virgínia, nos Estados Unidos. Isso todo mundo fala, mas ninguém prova. Eu também só escuto as pessoas falarem. No nosso caso aqui, o tamanho não é desse porte que o senhor está falando. Mas uma exposição que esteja havendo, por exemplo, ao Parque do Anhembi, ou a um presídio, ou a uma empresa, talvez, não sei o tamanho daqui do Senado Federal, mas em que eu tenha um grande PABX, com muitos troncos de saída, e a pessoa possa utilizar qualquer um telefone interno para falar, eu posso colocá-la como alvo e buscar, através de 7 segundos da voz dela ao telefone. Eu não preciso ouvir durante muito tempo para poder fazer essa busca. Bom, a biometria de voz, ela tem por si só algumas vantagens. Ela á objetiva, não depende de conhecimentos perceptuais do perito analista. Nós temos aqui pessoas mais novas, eu tenho 50 anos de idade, e, quando eu era adolescente, com 12 anos, tinha um filme, *My Fair Lady*, com Audrey Hepburn, em que ela vendia flores em Londres, e tinha um professor de inglês que a levou para casa para ensinar que ela falasse. E esse professor sabia dizer, ao ouvir uma pessoa falando no filme, de que bairro ou de que cidade próxima a Londres essa pessoa era. Ele era considerado por nós, naquela época, um perito de voz. Só que hoje isso muda. Porque se eu sou um perito de voz, estou analisando alguém, com esse tipo de conhecimento, e me chega uma gravação de uma pessoa falando em inglês ou espanhol, eu perco todo o meu arsenal intelectual para poder fazer aquela avaliação. A biometria de voz derruba isso, porque independe de palavras, independe da língua que a pessoa esteja falando. Então, no caso da Agnitio, independe do texto. Eu posso ter a gravação de uma pessoa em português e depois pegar um outro trecho para fazer a comparação em inglês, chinês, francês ou alemão, e se consegue fazer esse batimento. Porque não tem nada a ver com fonema, não tem nada a ver com sobreposição de vocábulos. Então, ele independe do idioma, trabalha em qualquer idioma. A da Agnitio, que já foi, já foi feita com inglês, árabe, espanhol, russo, romeno, alemão, chinês e português. Eu estava, na semana passada, na matriz da empresa me submetendo a um treinamento e recebendo os *softwares* para trazer, para realizar provas de conceito. E no primeiro dia que eu recebi o APT, eu tinha um caso de estudo que era de narcotraficantes colombianos. Então, eu tinha algumas conversas telefônicas, que eram poucas, 5 ou 10, para fazer estudo, e coloquei um exemplo meu. Eu li um texto em português de 2

minutos, depois gravei um texto em inglês de 20 segundos. Na hora que eu mandei fazer toda a comparação, ele identificou a mim mesmo. A biometria de voz, ela é mais rápida, permite cálculo de LR, como eu falei — que é uma coisa que já é reconhecida —, baseado num grande volume de dados. Então, existe um processamento árduo para se chegar àquele cálculo do LR. E no caso da Agnitio, nós sabemos que existem diferenças no canal que é utilizado para transmitir a voz. Se a pessoa fala ao microfone, a voz se expressa de um jeito; se ela utiliza um rádio de comunicação, outro; se ela utiliza a voz sob IP, que é a telefonia da Internet, um outro; se ela utiliza a voz GSM, também um outro. Existem distorções. O *software* da Agnitio é todo preparado para, informado a ele qual é a origem da gravação, ele estabelecer filtros de normalização daquela voz, para poder trabalhar e chegar ao resultado que esperam. Então, esta aqui é uma tela da primeira ferramenta que eu falei, que é o Batvox — é a única que eu vou mostrar na tela —, que é destinada aos peritos, em que ele vai incluindo as vozes todas que ele quer trabalhar. A partir desses áudios, são gerados modelos matemáticos. Tudo na realidade aqui são modelos matemáticos. Depois eu coloco o áudio da pessoa que eu tenho suspeita que pertença a um daqueles modelos, e ele vai executar então a tarefa dele — esse aqui eu já falei. Ele vai executar, vai mostrando passo a passo. Isso tudo fica registrado em *log* — todos os passos que o perito executou; se quiser haver uma comprovação posterior em juízo —, e ao final ele me traz o resultado dos verdes, que estão acima da linha de convergência. Podem ser 3 áudios da mesma pessoa ou áudios muito parecidos. A taxa mais alta vai apontar para a pessoa que é a que eu estou procurando. E também ele mostra gráficos, histogramas que podem ser apresentados ao juiz. Aqui, nesse caso, essa curva vermelha — a curva de Gauss, vermelha — faz uma análise da voz que nós colocamos como suspeita sobre uma população de referência. Então, ele não faz essas contas à toa. Se eu quero fazer... E por isso eu não vou mostrá-lo aqui. Porque como eu cheguei domingo de viagem e eu recebi a informação desta apresentação — eu estava na Espanha —, não tive tempo hábil de preparar uma população de referência. Eu preciso de pelo menos 25 vozes em português, falando ou ao microfone, ou ao telefone, para estabelecer uma população de referência que vá ser usada na verificação daquela voz que eu estou colocando do suspeito. Então, para cada voz que eu venha a trabalhar, eu tenho que

ter uma população de referência associada, que é justamente para tentar causar um erro em cima do *software*. Então, nesse caso aqui, por exemplo, a voz do nosso suspeito, que é o verde, está mais próxima da população de referência. Isso significa que aquela voz não é reconhecida como a voz da pessoa. Nesse caso aqui, a nossa voz do suspeito está mais próxima das vozes que estavam lá colocadas como modelo. Então, isso mostra a percepção de paridade com aquilo que a gente esperava. É o que se mostra aqui no caso, o LR baixo, Likelihood Ratio baixo, porque ele está longe dos nossos áudios e próximo da população de referência; e aqui o Likelihood Ratio alto, porque ele está próximo das nossas vozes de análise. Bom, o Batvox evoluiu por necessidade das próprias forças de segurança e foi criado o ASIS*,* que eu falei que é um banco de dados de vozes, que é a semelhança do AFIS e do Codes, que trabalham com impressão digital e DNA. Ele se presta a fazer uma busca dentro de uma base bem grande. Hoje tem uma base na Colômbia já com 600 mil vozes. Hoje se espera que até o final do ano contenham 600 mil modelos de áudio nessa base da Colômbia. Depois, nasceu também o BS3, que é o sistema de detecção de locutores. Todos em cima daquele mesmo núcleo do Batvox. Então, o ASIS, são as vozes de detidos. Por exemplo, na Espanha, em alguns lugares, eles já estão fazendo isso. Quando da detenção de uma pessoa, ao chegar na delegacia, para colher a foto, a digital, eles estão colhendo também trecho de locução para alimentar essa base que venha a ser de investigação posterior. Então, o conceito do ASIS é esse. Eu submeto uma voz desconhecida contra um conjunto de vozes que eu tenho armazenadas, e ele vai me trazer ou uma ou algumas. Ele pode me trazer uma voz só ou assim: *"Essas 10 aqui estão muito próximas dessa voz que você me apresentou."* Aí o perito, o investigador pode utilizar o Batvox, ou vai separar do universo dele de investigação — porque a investigação não se resume em um processo, eu não faço investigação só por impressão digital ou por uma análise do local de crime. Cada elemento influi no seguimento e no resultado final de uma investigação. Então, só por ele separar, por exemplo, 10 pessoas de uma lista de 30 suspeitos que eu tenha, isso já vai facilitar o prosseguimento da investigação. Vai acelerar o passo. Essa é a arquitetura. Eu tenho um servidor central. O banco de dados são os mais difundidos no mercado, e tenho motores de busca. Os motores de busca vão permitir controlar até 30 mil

buscas por minuto em cima daquela base. Porque toda vez que estou inserindo a voz, ele vai gerar um modelo para fazer o batimento matemático contra tudo. Além disso, ele pode se integrar com bases de dados externas. Então, achado, por exemplo, um delinqüente, ele pode ir na base exterior que já exista no sistema de segurança pública e trazer os dados daquele delinqüente que tem lá. Os áudios podem ser submetidos ao ASIS, através de uma rede local, ou por investigadores que estejam na Internet. Não há nenhum empecilho nisso. Não há obrigatoriedade de que esteja sentado do lado da máquina. A voz pode vir, como eu falei, de detenções. Vozes capturadas do rádio em arquivos na rede, CDs ou DVDs, fitas de vídeo, telefonia celular. Aqui eu posso passar por um *software* que acompanha a ferramenta quando da aquisição, que é o Edivox, que faz o seguinte: quando existe uma interceptação e uma gravação, eu tenho, às vezes, num canal mono — não é estéreo —, as 2 pessoas falando. E, para separar aquelas vozes, é uma coisa muito trabalhosa. O Edivox é uma ferramenta que eu separo 30 segundos da voz de um dos locutores, 30 segundos da voz do outro locutor — e eu posso ter vários locutores numa conversação telefônica, numa mesma conversação —, depois, eu mando o Batvox trabalhar. Ele vai separar em vários arquivos de áudio diferentes só os trechos que cada uma das pessoas estava falando. Então, se eu estou ligando para o Marcelo, que está falando com uma pessoa, e chama uma outra na conversa, eu tenho 4, 5 pessoas na mesma conversa, eu dou 30 segundos de voz de cada um, e o Edivox vai separar em 5 arquivos de áudio daquela conversação. E eu posso continuar a ouvir o áudio todo com as 5 pessoas ou só as locuções de cada uma das pessoas. Só o que elas falaram. Então, depois de passado no Edivox, se eu precisar — eu posso não precisar disso —, isso vai passar pelo núcleo e vai gerar um modelo e vai para a base de dados. Depois, as pessoas vão submeter ao servidor de buscas para obter resultado da identificação. O BS3 é um sistema que não é de interceptação. Aqui ele está bem falado. É um sistema que se integra com sistemas de interceptação de comunicações e aumenta as possibilidades de mineração do áudio ali dentro. Que sistemas de interceptação? Qualquer um, desde que a empresa... No caso, aqui, é bom fazer uma ressalva. Todos esses produtos que estão sendo trazidos para o Brasil pela Tempo Real só poderão ser comercializados para instituições de segurança pública e inteligência. Não são destinados à iniciativa

privada em hipótese alguma. Isso está no acordo comercial firmado com a matriz. Então, como eu falei, ele faz a detecção de locutores específicos.

O SR. PRESIDENTE (Deputado Marcelo Itagiba) - Permite, só um questionamento?

O SR. RENATO LIRA DA COSTA - Sim.

O SR. PRESIDENTE (Deputado Marcelo Itagiba) - Quer dizer, é em função de um contrato estabelecido com o detentor dos direitos de *software*, é isso?

O SR. RENATO LIRA DA COSTA - Sim.

O SR. PRESIDENTE (Deputado Marcelo Itagiba) - Por exemplo, não teria mal nenhum em se vender isso como um instrumento de... Um banco, por exemplo, onde se faz transações através de voz, não haveria... Lá também existe esse impedimento, ou só o pode vender para a instituição também?

O SR. RENATO LIRA DA COSTA - Não. Perfeita a sua colocação. Está sendo trabalhado. Espera-se que isso esteja concluído até o final do ano ou meados do ano que vem um produto destinado a instituições principalmente financeiras — o que o senhor falou —, ao mercado de *call center*. Ao ligar para um banco, já seria identificado pelo atendedor do *call center*, ou para fazer a validação numa caixa de ATM, de atendimento automático. Mas vai ser um produto isolado, usando o mesmo motor de busca, mas que não vai fazer essas coisas que estão aqui. Quando isso acontecer é claro que a Tempo Real o trará para o Brasil. Aí, sim, esse estará destinado a mercado empresarial como um todo.

O SR. PRESIDENTE (Deputado Marcelo Itagiba) - Aproveitando, não existe no Brasil nenhuma restrição legal a que se fizesse. A sua restrição é apenas contratual, não é isso?

O SR. RENATO LIRA DA COSTA - Sim, sim, sim. Há uma preocupação que da mesma forma que isso pode ser utilizado... Aliás, qualquer tecnologia ou arma, ela pode ser utilizada para o bem ou para o mal. Então, foi uma preocupação que aconteceu desde o início das conversações entre a Agnitio e a Tempo Real. Isso vinha transcorrendo desde abril do ano passado e só agora foi tudo fechado, porque houve critério de ambas as partes para que não fosse dado nenhum passo muito longo que não pudesse ser sustentado, que não tivesse base para isso. Então, ao contrário do ASIS, onde eu tinha um suspeito e o submetia a uma base de vozes,

houvesse 3, submete-se um suspeito a vários fluxos que eu não tenha identificados. Aí, ele vai identificar o fluxo que eu desejo, que compõe aquela voz.

(Intervenção fora do microfone. Inaudível.)

O SR. RENATO LIRA DA COSTA - É o contrário do ASIS, exatamente o contrário.

O SR. DEPUTADO JORGINHO MALULY - É o contrário?

O SR. RENATO LIRA DA COSTA - Desculpe. Então, é o contrário. Exatamente o contrário.

(Intervenção fora do microfone. Inaudível.)

O SR. RENATO LIRA DA COSTA - Isso. Com uma que eu conheço. É o contrário. Exatamente.

O SR. PRESIDENTE (Deputado Marcelo Itagiba) - Desculpem-me, só para registrar a presença do ex-Deputado Júlio Lopes e atual Secretário de Transporte do Rio de Janeiro que honrou sempre esta Casa.

O SR. RENATO LIRA DA COSTA - Então, essa é a arquitetura do BS3. Eu tenho também o meu servidor, onde eu tenho os meus suspeitos, que eu falei que eu podia ter uma voz, ou vários suspeitos sendo submetidos aos fluxos entrantes, que eu chamo aqui de *buffer* de entrada, onde eu tenho: aqui pode ser antenas de ERBs, ou as empresas de telefonia convencional, que vão chegar numa máquina, que é onde está o sistema, por exemplo da Dígitro, que falou antes de nós, que tem o Guardião, mas poderia ser o Sombra, poderia ser Digivox, poderia ser o que tem em Israel, cujo nome não me lembro agora, poderia ser qualquer um deles. Desde que fosse falado como ele grava esta informação no *buffer*, desde que seja dito como é o *buffer* de entrada dele. O BS3 vai capturar a informação do *buffer* de entrada, vai aplicar as regras e ver os suspeitos, com os motores de busca — aí eu posso ter aqui até 128 motores de busca, eu tenho crescimento aqui, mas eu não tenho a convicção para afirmar ao senhor daquela sua pergunta, se 128 motores de (*falha na gravação*) eu não posso informar isso.

O SR. PRESIDENTE (Deputado Marcelo Itagiba) - Já encerramos os 30 minutos da exposição inicial.

O SR. RENATO LIRA DA COSTA - (*Falha na gravação.*) Ele coloca as mesmas informações que ele recebeu no *buffer*, como *buffer* de saída, acrescida da

identificação daquele locutor. Então, é esse o desenho, um pouco mais técnico: tem as interceptações, as bases de dados, e ele gera os arquivos de áudio. Da mesma forma, os nossos clientes podem estar em rede local ou *web*. E o APT, que faz a mesma coisa que o ASIS e que o BS3 fazem. Eu posso ter uma base de dados para submeter um suspeito, saber se existe naquela base de dados. Ou posso pegar um fluxo de áudio desconhecido para bater contra um modelo que eu tenha. Só que em menor porte, em menor quantidade. Esse é um produto para rodar, em vez de naqueles servidores, num *notebook* para um delegado, um investigador poderem fazer determinadas tarefas que eles precisem para um caso específico. Eles podem até se socorrer de sistemas maiores, mas eles podem utilizar o APT para executar as tarefas do dia-a-dia. Essa é minha parte.

O SR. PRESIDENTE (Deputado Marcelo Itagiba) - Nós temos outro grupo para ser ouvido, e na verdade, eu acho o esclarecimento principal o seguinte. Os senhores não detêm nenhum equipamento de invasão em interceptação, nem realizam interceptações. Na verdade o equipamento que V.Sas. detêm é um equipamento de reconhecimento de voz dentro de um sistema de interceptação que venha a ser estabelecido ou instituído. É isso?

O SR. RENATO LIRA DA COSTA - Sim. E a outra ferramenta, que é o que o Marcelo Bandeira ia demonstrar, não é nem apresentação em *powerpoint*, porque eu fiz, é sistema de cruzamento de informações

O SR. PRESIDENTE (Deputado Marcelo Itagiba) - De dados?

O SR. RENATO LIRA DA COSTA - De dados, inclusive de movimentações financeiras, ou chamadas telefônicas, ou uma conjunção dos dois: chamadas telefônicas com movimentações financeiras. Ele já foi utilizado nesta Casa em 3 CPIs, no Congresso, e já foi apresentado numa audiência pública, no ano passado, de ciência e tecnologia.

O SR. PRESIDENTE (Deputado Marcelo Itagiba) - Vou aproveitar a oportunidade e passar logo às perguntas por parte dos Deputados, porque daremos celeridade e vamos mais objetivamente às questões. A única pergunta que me caberia aqui seria: o senhor não acredita que, para que se tenha hoje um equipamento executando escuta telefônica, seria condição *sine qua non* para a certificação de que a pessoa grampeada é aquela mesma, ou aquela pessoa

interceptada é aquela mesma — inclusive para posterior encaminhamento à Justiça — a necessidade de que esse *software,* ou esse tipo de *software* fizesse parte do sistema?

O SR. RENATO LIRA DA COSTA - V.Exa. poderia explicar um pouco melhor? Não entendi qual o encaminhamento.

O SR. PRESIDENTE (Deputado Marcelo Itagiba) - Vou explicar. O meu questionamento é o seguinte: o senhor acredita... Hoje existe um sistema de interceptação, seja ele um gravador, seja ele um conjunto...

O SR. RENATO LIRA DA COSTA - Mas que só perde por um número.

O SR. PRESIDENTE (Deputado Marcelo Itagiba) - ...de *hardware* ou *software.*

O SR. RENATO LIRA DA COSTA - Então, mas só perde um número, a fim de ser interceptado.

O SR. PRESIDENTE (Deputado Marcelo Itagiba - Ele está sendo interceptado. O senhor acha que seria necessária, para configuração de que o interlocutor é aquele mesmo, a utilização do seu *software* ou de *software*s similares, sob pena de muitas vezes está interceptando a pessoa errada, ou acreditar que é a mesma pessoa, mas não é, como já houve caso no passado?

O SR. RENATO LIRA DA COSTA - Sim. Por 2 circunstâncias: a primeira é essa que o senhor citou, de a pessoa que está ouvindo os áudios de interceptação, imaginar, por exemplo, que aquela voz me pertence, e pertencer ao meu irmão, que tem uma voz muito parecida com a minha, que a minha própria mãe confundia achando que às vezes estava falando comigo, e estava falando com meu irmão. Então esse é o primeiro caso. O segundo é o ganho de tempo na investigação. É o caso de um local em que eu estive, que é uma prova de conceito que vamos realizar dentro de pouco tempo: existiam 8 mil ligações interceptadas por dia. Aquelas 8 mil ligações, de alguma forma, tinham que ser ouvidas, para saber se os interceptados estavam naqueles áudios, para poder separá-los e encaminhar para os investigadores. Com a nossa tecnologia, não há necessidade de ouvir as 8 mil ligações interceptadas, porque se eu coloco os modelos de voz dos suspeitos que eu tenho, eu mando que grave, sim, se eu quiser, as 8 mil interceptações numa pasta e aquelas que ele selecionou como os suspeitos que eu tinha, em outra pasta,

que podem ser 100. Então eu me abstive de ouvir 7.900 ligações. O primeiro aspecto aí é economia de tempo, a economicidade. E o segundo é a inviolabilidade daqueles que não tinham nada a ver com nenhum delito. Porque se eu estou querendo ouvir o Renato, e ele utilizou o mesmo telefone que eu deveria utilizar, porque está grampeado, para fazer uma ligação, a ligação dele não será ouvida. A princípio, é lógico, porque se o investigador quiser ouvir ele vai ouvir. Mas a princípio não será ouvida, porque o arquivo que foi separado foi o arquivo do momento em que eu efetivamente utilizei o telefone, e aquele áudio foi gravado numa outra pasta. Então esses 2 aspectos são importantes.

O SR. PRESIDENTE (Deputado Marcelo Itagiba) - Esse esclarecimentos de V.Sa. foi importantíssimo até para que não se cometa muitas vezes a ilegalidade de, por ter um número interceptado, na verdade, acabar se interceptando uma terceira pessoa que nada tem a ver com a ocorrência sob a investigação. Então eu achei o esclarecimento perfeito, muito bem colocado por V.Sa.

Vou passar a palavra ao Relator para seus questionamentos.

O SR. DEPUTADO NELSON PELLEGRINO - Primeiro queria agradecer a presença ao Sr. Renato Costa. E a primeira pergunta que eu teria a fazer é a seguinte: esses *software* que foram aqui apresentados foram adquiridos por algum órgão de segurança pública do País?

O SR. RENATO LIRA DA COSTA - Ainda não. Vou fazer 2 provas de conceito ainda. Eu mostrei... Isso que eu mostrei para os senhores, para algumas pessoas... Eu tenho também origem em segurança pública, então eu tenho alguns interlocutores, eu sou policial militar inativo, do Rio de Janeiro, trabalho na área de tecnologia desde 1988. Então, é óbvio que eu conheço alguns delegados, alguns oficiais da Polícia, tanto do Rio quanto de outros Estados. E levei esta notícia para eles. Mas não poderia passa nada além de notícia, porque não havia ainda um acordo comercial firmado entre a Tempo Real e a Agnitio. Então, seria até uma leviandade minha fazer uma coisa que não poderia acontecer depois. E somente na semana passada é que eu estive na Espanha, na sede da empresa, para passar por todo treinamento das ferramentas e receber a documentação, porque todo *software* que venha a ser vendido para o Poder Público brasileiro tem que estar em língua portuguesa. Esses não estão. Então é uma das tarefas que eu tenho. Fui lá também

buscar todas as páginas de tradução para botar o *software* em português. Então ainda temos algumas etapas a vencer antes de poder dizer assim: temos um primeiro cliente no Brasil.

O SR. DEPUTADO NELSON PELLEGRINO - Mas teria sido contactado por que tipo de autoridade? Secretarias Estaduais, Polícia Federal?

O SR. RENATO LIRA DA COSTA - Não. Não, informalmente eu levei as pessoas que eu conhecia, alguns delegados, oficiais da Polícia. Eu tenho... Meu irmão é oficial da Polícia, meu primo é oficial da Polícia, meu pai era oficial da Polícia, eu tenho um primo que é promotor de justiça, tenho um primo que é detetive. Então, essas pessoas... E os conhecidos meus. Se eu tivesse encontrado o Dr. Marcelo no Rio eu teria falado com ele também: *"Olha tem uma coisa boa para o senhor conhecer depois*". Mas só como notícia mesmo, não teve nenhuma vinculação comercial.

O SR. DEPUTADO NELSON PELLEGRINO - É política... Essa Agnitio é uma empresa espanhola?

O SR. RENATO LIRA DA COSTA - Espanhola.

O SR. DEPUTADO NELSON PELLEGRINO - Ela trabalha também desenvolvendo soluções só para a área de segurança pública ou para outras?

O SR. RENATO LIRA DA COSTA - Não, ela só trabalha com esse produto BATVOX. Os engenheiros de *software* estudavam na Escola Politécnica de Madri, quando estavam buscando esse motor de biometria de voz, e foram contactados, ou alguém da guarda civil espanhola esteve com eles e achou interessante, e buscaram o desenvolvimento daquela primeira ferramenta, que foi o SAIVOX. A partir daí, eles se consolidaram como empresa. Hoje eles têm aquele mercado que lhe mostrei ali.

O SR. DEPUTADO NELSON PELLEGRINO - Este é um *software* que só é comercializado para órgãos de segurança pública.

O SR. RENATO LIRA DA COSTA - Sim.

O SR. DEPUTADO NELSON PELLEGRINO - Não é comercializado para...

O SR. RENATO LIRA DA COSTA - Não, não.

O SR. DEPUTADO NELSON PELLEGRINO - Nem lá na Espanha também?

O SR. RENATO LIRA DA COSTA - Nem lá na Espanha. É o que eu lhe falei: para o mercado empresarial, de uma forma geral, eles estão fazendo um outro

produto. Lógico que usa o mesmo motor de busca e o mesmo processo de inteligência. Não há por que se reescrever isso daí. Mas o produto será específico para a área comercial.

O SR. DEPUTADO NELSON PELLEGRINO - Mas esse *software*, digamos, que seria similar, desenvolvido para a área empresarial, poderia ser utilizado para esse trabalho de...

O SR. RENATO LIRA DA COSTA - Eu não sei. Eu não tive acesso. Como eles pretendem ter esse *software* talvez no final deste ano, ou meados do ano que vem...

O SR. DEPUTADO NELSON PELLEGRINO - Mas não estão comercializando esse *software* ainda.

O SR. RENATO LIRA DA COSTA - Não. Não.

O SR. DEPUTADO NELSON PELLEGRINO - O único *software* que eles comercializam são esses *softwares* que foram apresentados.

O SR. RENATO LIRA DA COSTA - Só esses.

O SR. DEPUTADO NELSON PELLEGRINO - Bom, então eu posso presumir que no caso da Agnitio eles também não teriam, digamos assim, um processo de comercialização dessa solução. Porque pelo que entendi do depoimento de V.Sa., outros *softwares*, tipo guardião, tipo outros que V.Sa. citou, poderiam incorporar essa tecnologia a eles como elemento de...

O SR. RENATO LIRA DA COSTA - Não, não é questão de incorporar. É questão de integrar.

O SR. DEPUTADO NELSON PELLEGRINO - É integração, isso!

O SR. RENATO LIRA DA COSTA - A saída de um se torna a entrada do outro. Então, eu começo a trabalhar com o resultado gerado por um *software,* ou por um *software* e *hardware*, um conjunto de *software* e *hardware* de interceptação. Qualquer que seja, desde que me diga, como é a saída que ele produz. Então, entendida a saída, aquilo para mim passa a ser entrada, eu gero um processamento e coloco numa saída. Esta saída que eu coloco, que é a mesma interceptação com a identificação, pode vir a ser utilizada até por um sistema próprio de uma Secretaria de Segurança, de mineração de dados que tenha, por exemplo, como entrada para eles, para que eles façam um outro processamento e gerem um outro conjunto de

informações, para Secretários de Segurança, ou Comandante Geral da Polícia, ou chefe da Polícia Civil. É isso que a gente chama de integração. É o encadeamento de dados, saindo de um sistema, entrando em outro, saindo, entrando em outro.

O SR. DEPUTADO NELSON PELLEGRINO - Mas pelo que entendi também pela exposição de V.Sa., ele não é um sistema de interceptação telefônica.

O SR. RENATO LIRA DA COSTA - Não, não. Em hipótese alguma.

O SR. DEPUTADO NELSON PELLEGRINO - Mas ele poderia ser utilizado nesse sentido?

O SR. RENATO LIRA DA COSTA - Não. Ele não...

O SR. DEPUTADO NELSON PELLEGRINO - Por que? Porque é um sistema que não se comunica diretamente com a central telefônica?

O SR. RENATO LIRA DA COSTA - Não, nunca. Ele não tem isso. Ele só...

O SR. DEPUTADO NELSON PELLEGRINO - Ele só se propõe a fazer o processo da identificação.

O SR. RENATO LIRA DA COSTA - Ele só pega um áudio que, dependendo do que eu for trabalhar, eu preciso de 40 segundo de áudio sem silêncio — ou seja, posso ter um áudio de 1 minuto, mas me dá 40 segundos, ou 7 segundo, dependendo do que eu vou fazer.

O SR. DEPUTADO NELSON PELLEGRINO - Então, é um sistema de autenticação que pode ser utilizado como um sistema integrado, por exemplo. É um guardião como um sistema seletivo?

O SR. RENATO LIRA DA COSTA - Ele é um modelo matemático que é aplicado sobre arquivos de áudio para estabelecer uma identificação unívoca de uma pessoa.

O SR. DEPUTADO NELSON PELLEGRINO - Com a mesma segurança que se utiliza hoje, por exemplo, na identificação digital.

O SR. RENATO LIRA DA COSTA - Com a mesma segurança que o senhor tem para ...

O SR. DEPUTADO NELSON PELLEGRINO - Mesmo que o senhor tenha um irmão com voz parecida?

O SR. RENATO LIRA DA COSTA - Sim. sim.

O SR. DEPUTADO NELSON PELLEGRINO - Seu irmão tem identidade.

O SR. RENATO LIRA DA COSTA - Sim. Inclusive, como eu tinha 20 minutos e não poderia me alongar, um caso clássico de exemplificação é com irmãos gêmeos, e ele identifica a voz de um e a voz do outro.

O SR. DEPUTADO NELSON PELLEGRINO - Mas ele pode ser integrado?

O SR. RENATO LIRA DA COSTA - Ele é integrado, ele não trabalha sem essa integração, porque eu não vou ter de onde...

O SR. DEPUTADO NELSON PELLEGRINO - Mas ele poderia ser integrado tipo um sistema, tipo guardião, ele poderia ser integrado.

O SR. RENATO LIRA DA COSTA - Sim, com certeza.

O SR. DEPUTADO NELSON PELLEGRINO - Como elemento de filtro, de crítica, para dizer o que intercepta, o que não intercepta, como já foi aqui ...

O SR. RENATO LIRA DA COSTA - Sim. Para aqueles 2 itens que o Presidente perguntou e eu falei: para ter economicidade do pessoal envolvido e para ter a inviolabilidade do interlocutor que não tem nada de suspeito.

O SR. DEPUTADO NELSON PELLEGRINO - Posso concluir que a função primordial desse sistema é que ele é um sistema identificador de voz.

O SR. RENATO LIRA DA COSTA - Sim, ele é um sistema de biometria de voz.

O SR. DEPUTADO NELSON PELLEGRINO - Essa é a função fundamental dele.

O SR. RENATO LIRA DA COSTA - O que o Marcelo tem aqui para mostrar é sistema de tratamento de informações, que podem ser chamadas telefônicas. Ele não vai falar em áudio; para ele não interessa áudio; para ele interessa data, hora, número que ligou, duração da chamada, isso tudo. Todas as informações que venham... Ele vai falar isso. Ele é talvez... Não vou falar nem talvez, que estou desmerecendo uma pessoa que respeito como profissional e é um amigo de trabalho e de carona. Ele é o maior profissional hoje qualificado no Brasil para falar sobre esse tipo de ferramenta, quer seja no setor público, quer seja no setor privado. Ninguém entende mais no Brasil dessas ferramentas do que o Marcelo Bandeira, que vai falar agora.

O SR. DEPUTADO NELSON PELLEGRINO - Sr. Presidente, no caso da exposição do Sr. Renato, estou satisfeito. Não sei se seria o caso dos Deputados

ainda poderem fazer inquirições complementares, para depois ouvirmos o Sr. Marcelo. Porque penso que a exposição do Sr. Renato foi quase que completa em relação aos objetivos da Comissão Parlamentar de Inquérito.

O SR. PRESIDENTE (Deputado Marcelo Itagiba) - Passo a palavra então ao Sr. Marcelo, para que ele mostre o seu sistema de cruzamento de informações, e em seguida, passarei a palavra aos Deputados, para que façam seus questionamentos, se tiverem algum.

O SR. MARCELO BANDEIRA RODRIGUES - Muito boa noite a todos. Serei mais breve do que o Renato Lira. Vim aqui mostrar um outro segmento da empresa que são os *softwares* da i2 Tecnologia, uma empresa americana que detém 94% do mercado de análise e investigação visual. Então, eu vou mostrar casos reais com 3 *softwares* comercializados para o tempo real, dos 9 que temos como arsenal. O primeiro é o *analyst's notebook,* que é um *software* criado desde 1990, utilizado por diversas instituições em mais de 140 países. Mais de 4 mil organizações utilizam esse produto. Esse *software* é utilizado pelo FBI, Cia, Interpool, diversos polícias no Brasil, Ministérios Públicos, Procuradorias e também por instituições privadas no combate a fraude. Então, tem bancos, telecons que já fazem uso desses aplicativos i2. Então, eu tenho um primeiro caso, que é um caso de fraude em cartões de crédito. *(Segue-se exibição de imagens.)* Eu tenho um extrato bancário, que vou abrir aqui para os senhores: esse extrato tem quase 7 mil chamadas telefônicas, que eu tenha a data, a hora da chamada, a duração da chamada, telefone de origem e telefone de destino. Obviamente que esse conjunto de aplicativos só trabalha com dados oriundos de autorizações judiciais. Então, eu vou fazer importação desse extrato, cujo objetivo era pegar uma quadrilha que estava fraudando esses cartões de crédito. Então, tinha o principal elemento fraudador, o principal indivíduo que fraudava, o telefone dele. A partir desse telefone foram pedido várias quebras de sigilo. Entretanto, os analistas passaram 3 meses nesses extratos, nessas quase 7 mil chamadas telefônicas, e não conseguiam detectar os outros envolvidos, além do mentor da fraude. Vou fazer, neste momento, a importação para um diagrama, ou seja, eu paro de ver uma planilha e começo a olhar gráficos, que é a forma mais fácil de fazer as investigações. Aplicando aqui um zum, eu consigo identificar os telefones. E tem aqui na ligação a quantidade de chamadas realizadas entre 2

telefones: 8 chamadas, por exemplo, dou um duplo clique, e eu tenho todos os históricos dessas 8 chamadas. Eu posso ter a ERB da chamada *(falha na gravação)*. Todas as informações que foram *(falha na gravação)* pela operadora vão ficar aqui nesse cartão para compor a prova da informação. Essa ferramenta tem diversos recursos, diversos formatos de apresentação da mesma informação. Então, eu posso examinar essas quase 7 mil chamadas telefônicas em núcleos. Então, eu tenho aqui vários núcleos. Vou aplicar o zum em um deles. Este telefone central foi o telefone que foi pedido a quebra de sigilo. E aqui eu já consigo identificar que eu tenho vários núcleos e as ligações entre eles. Então, por exemplo, eu tenho um telefone aqui que fala com 3 núcleos. Vou aplicar lá um realce, ele fala com 3 elementos investigáveis, 3 telefones alvos da minha investigação. Eu tenho um outro telefone que fala com 5 núcleos. Outro telefone, com 4 núcleos. Então, esses telefones, uma vez identificados, já que eles falam com vários alvos da investigação, eu posso estar pedindo também a quebra de sigilo desses telefones. Eles aparecem aqui porque eles eram comuns a vários alvos da investigação. Apareciam na conta reversa de vários alvos. Bom, o principal formato, que é esse formato que eu vou aplicar, o agrupado, ele já monta automaticamente para mim um grupo, que é esse grupo central, dos telefones que se conectam, ou seja, os telefones que falam entre si. Eu tenho aqui um desses telefones que fala com vários outros telefones, que estão aqui na parte superior do diagrama, que a princípio não me interessa analisar. Então, eu vou copiar com um *Ctrl* C aquele núcleo, detectado automaticamente pela ferramenta, para um novo diagrama. Bom, neste momento, obviamente, eu tenho um ponto de partida, que é o telefone do mentor do assalto que já tinha sido identificado. É o início da investigação, que é o telefone final 3344. Eu vou mandar localizar esse número, 3344 — pode estar no início, no final, pode estar em qualquer chamada telefônica —, e a ferramenta encontrou para mim 8 objetos. Vou aplicar um zum só para nós identificarmos. Está aqui o telefone e as ligações que ele realizou. Com o botão direito eu vou selecionar para quem ele ligou desse núcleo e vou copiar novamente para o novo diagrama. Ou seja, neste momento, desse grupo de telefones, naquelas quase 7 mil chamadas telefônicas, eu tenho todos os elementos que fizeram alguma conexão com o telefone 3344, que é justamente do mentor da fraude em cartão de crédito. Vou levar esse grupo para um novo diagrama. Vou só

organizar aqui para facilitar a visualização. Todo esse trabalho levou cerca de meia hora, entre a importação dos extratos e a identificação desse grupo. Isso é muito rápido. Então, eu tenho aqui um telefone. Esse telefone aqui é do mentor do assalto. Obviamente que a ferramenta me permite continuar a minha investigação a partir desse momento, estabelecendo novos vínculos, colocando novos elementos nessa investigação. Então, está aqui o mentor do assalto. Ele fazia 245 chamadas para esse outro telefone. Essas 245 chamadas já haviam sido detectadas, porque é um número muito elevado naquele extrato inicial. Porém, 8 chamadas telefônicas, 12 chamadas, 53, 26. Este telefone aqui recebeu 4 chamadas do alvo e realizou 4 chamadas. Fica muito difícil de detectar e também é muito oneroso o tempo despendido para... Esse trabalho é muito grande e muitas vezes o que acontece é que os investigadores não conseguem detectar todo o grupo envolvido. É uma análise parcial devido ao volume de dados. Então, esse trabalho... Houve também um trabalho de apoio de escuta e realmente tinham prestadores de serviços envolvidos, tinham pessoas de facções criminosas envolvidas nessa fraude. Bom, eu vou pegar aqui, para mostrar uma outra ferramenta, o mesmo extrato e vou fazer uma importação. Só que agora eu vou mostrar todas aquelas chamadas telefônicas associadas ao tempo. Então, tem aqui uma barra temporal e as chamadas telefônicas estão todas aqui na vertical. Então, eu consigo, por exemplo, identificar que esta chamada aqui aconteceu antes desta, e assim conseqüentemente. Eu tenho, na horizontal, os telefones; na vertical, eu tenho as chamadas telefônicas entre esses telefones. Bom, se eu colocar numa barra temporal quase 7 mil chamadas telefônicas *(falha na gravação)* difícil detectar padrões nessas chamadas. O que os analistas tinham necessidade? Bom, sabe-se que os atos ilícitos acontecem ao longo do tempo. Pode ser uma freqüência semanal, uma freqüência mensal ou qualquer ordem. É necessário analisar diversos estágios telefônicos e detectar padrões nessas chamadas telefônicas. Então, por exemplo, eu tenho 5 grupos de telefones e eles se falam toda semana. E toda vez que eles se falam eles praticam algum ato ilícito. Bom, pedir para um analista ou vários analistas de uma unidade de inteligência analisar esse extrato, ele levaria meses e não conseguiria detectar esses padrões. Então, a i2 criou, desenvolveu uma nova ferramenta, que trabalha alinhada ao *analyst's notebook*, que eu vou demonstrar neste momento.

Então, eu vou abrir aqui uma base de dados com as mesmas chamadas telefônicas. Simplesmente aqui, com o botão direito, eu consigo exibir, por exemplo, os telefones que estão nesta base. Eu consigo também exibir as chamadas telefônicas. Bom, o analista aqui tem uma opção de buscar padrões, ou seja, essa ferramenta vai buscar padrões nessas chamadas telefônicas, não importa quais sejam os alvos, por uma coincidência temporal. Então, por exemplo, eu sempre falo com o Renato Lira. Ligo para ele neste momento. Após 15 minutos ele faz uma ligação para outra pessoa. Essa outra pessoa, passada meia hora, ela liga para outra pessoa. Isso acontece 10 vezes ao longo de 1 ano. Essa ferramenta, na hora em que eu clicar aqui em buscar padrões, ela vai varrer todas as chamadas telefônicas e detectar esses padrões para mim, automaticamente, por uma coincidência temporal. Eu vou pegar um desses padrões e vou exibir no nosso gráfico. Ele está envolvendo 6 telefones. São 5 chamadas e 34 vezes ele aconteceu. Então, está aqui. Este é um dos padrões encontrados. Então, rapidamente, eu sei que entre esses telefones existe alguma relação, eles se falam de alguma forma. Eu não precisei analisar 7 mil chamadas telefônicas. Bom, para ficar mais claro ainda o que é esse padrão, eu vou pedir para a ferramenta exibir na barra temporal essas chamadas telefônicas. Então, aqui está. Cada linha dessas, na vertical, esse conjunto de chamadas. Eu tenho aqui um primeiro conjunto. Isso aqui é um padrão, uma instância do padrão, 2, 3, 4, 5... Aconteceu 34 vezes. Eu vou organizar melhor a informação. Vou pedir para exibir também a data e hora dessas chamadas telefônicas, para facilitar o entendimento desse padrão. Então, tem aqui: um primeiro padrão aconteceu entre esses telefones na data de 5/06/2001. Houve uma chamada, tem um intervalo de poucos minutos, e acontece uma outra chamada entre esses telefones, outra chamada e outra chamada. Passado o dia 5 de junho, eu tenho novamente aqui o padrão acontecendo, só que agora esse padrão aconteceu no dia 6, no dia seguinte. Depois aconteceu novamente esse padrão no dia 12, e assim sucessivamente. Esses telefones se falam sempre em seqüência. É o que geralmente acontece nos assaltos, nos seqüestros. Há uma quadrilha atuando, e eles se falam em seqüência, e, por isso, essa ferramenta consegue detectar isso muito rapidamente, o que tem um ganho muito grande nas investigações, inclusive podendo tomar ações preventivas. Se eu detectei um padrão em que eles se falam toda semana, ou de 15

em 15 dias, ou mensalmente, eu sei que em breve alguma ação eles muito provavelmente vão realizar, algum ato ilícito eles vão realizar. (*Pausa*.) Para finalizar, eu vou mostrar um terceiro *software* que é o *iBase.* O *iBase,* na verdade, é uma base investigativa. Esse *software*, por exemplo, foi utilizado na CPMI dos Correios. Isso é público. Essa informação é pública. E o que foi utilizado? Chamadas telefônicas e transações financeiras. Porém, nessa base de dados, como estou demonstrando, posso fazer o cruzamento de qualquer informação. Por exemplo, a ERB que foi utilizada, a antena que foi utilizada nas chamadas telefônicas. Posso utilizar também eventos que aconteceram, organizações, facções criminosas, enfim, todas as informações que forem relevantes para as investigações são colocadas nessa base investigativa para uma posterior análise ou cruzamento de dados. Essa ferramenta dispõe de um importador muito poderoso que permite importar dados de diferentes fontes, arquivos em *Excel*, e *Access*, base de dados corporativos. Vou ser breve e vou demonstrar aqui uma pesquisa, envolvendo chamadas telefônicas. Bom, essa ferramenta não exige grandes conhecimentos técnicos. Eu tenho aqui ícones e eu arrasto esses ícones para essa tela e faço as ligações. Então, por exemplo, aqui. Eu coloquei uma pessoa, um proprietário de um telefone, que fez uma chamada telefônica, e, na chamada telefônica, eu coloquei um filtro num período de data, e também pela duração. Então, eu estou procurando nessa base de dados — porque eu posso ter aqui milhões de informações — chamadas telefônicas ocorridas entre setembro de 2001 e setembro de 2003. E também essas chamadas têm que ter duração superior a 9 minutos. Os parâmetros que eu coloco aqui são de acordo com o analista. Ele pode colocar aqui filtros, por exemplo, para pessoas. Se o CPF da pessoa não está regularizado, se essa pessoa está incluída numa RAES. Qualquer informação que ele quiser cruzar a ferramenta permite. Pode o dado estar em pessoa, pode o dado estar em conta, em evento, em ERB, em qualquer um desses elementos da investigação. Bom, executando essa pesquisa, a ferramenta vai me retornar algumas chamadas telefônicas. Tenho aqui 1.444 chamadas telefônicas e vou colocar num *software* de análise, num *software* visual, essas chamadas telefônicas. Vou adicionar essas chamadas para o *anayist's notebook* para poder fazer essa análise. Então, a ferramenta vai adicionar num gráfico temporal para mim todas aquelas 1.444 chamadas telefônicas, realizadas naquele período e com

duração superior a 5 minutos. Muito bem, aqui estão os telefones e as chamadas telefônicas. Bom, continuo tendo um volume grande de informações. Eu posso utilizar aqui um dos recursos disponíveis que é identificar os principais telefones. Eu tenho aqui 6 telefones que têm grande número de conexões. Ou seja, eu tenho um telefone aqui, o primeiro, que se conecta a... fez 21 chamadas telefônicas. Então, eu vou dar um O.K., vou aplicar aqui um filtro e vou levar esses telefones para um novo diagrama, para uma análise mais resumida. Organizando aqui a informação, eu tenho a informação aqui na tela. Bom, estão aí os telefones que eu desejo analisar. Esses 3 telefones. Bom, esses telefones fazem parte de uma base investigativa. No caso de uma CPI, posso ter meses de investigação. Eu quero saber o que que tem associado nesses telefones na base de dados. Bom, por exemplo, esses telefones usaram alguma...Qual a antena que eles utilizaram para fazer essas chamadas telefônicas? Vou selecioná-los e vou fazer a expansão. Significa que a ferramenta trouxe para mim as antenas dessas chamadas. Essa chamada aqui, por exemplo, foi feita utilizando qual antena? Organizando melhor a informação, está aqui... Vou só organizar para uma melhor visualização. Então, está aqui. Essa chamada telefônica aqui foi feita utilizando uma antena no núcleo bandeirante. Depois, eu tive uma outra chamada que utilizou uma antena no setor Sudoeste e, por fim, no SIA. Isso permite até que eu faça o trajeto que uma pessoa fez usando o celular. Isso elucida muitos crimes. Bom, esse telefone aqui, por exemplo. Eu quero saber se tem algum proprietário associado a ele na base de dados, ou se ele foi utilizado em algum caso no passado. O que eu faço? Eu vou simplesmente fazer a expansão desse telefone. Então eu vou pegar aqui o telefone, vou escolher o que eu quero descobrir dele na base de dados. Quero descobrir se tem alguma pessoa, algum proprietário associado a ele, ou algum usuário desse telefone. Ele está selecionado, eu faço a expansão. Só antes aqui escolher um dado, e pronto. Faço a expansão desse telefone, e está aqui: descobri o proprietário desse telefone. Bom, esse proprietário também está numa base investigativa. Eu quero saber dessa pessoa o que tem nessa base de dados da CPI, por exemplo. Eu clico aqui, nessa pessoa, escolho o que eu quero descobrir — vou deixar tudo — e vou expandir essa pessoa. Estão aqui as informações sobre ela, e assim sucessivamente. Vou fazendo esse trabalho de explorar os dados que estão no diagrama que me interessam. A ferramenta vai

nessa base investigativa e faz a expansão. Eu posso ter aqui, por exemplo — só para finalizar a apresentação —, eu posso também partir aqui, pegar uma pessoa. Vou pegar o Gene, que é uma pessoa que está sendo investigada. Vou adicionar ele ao a*nalyst's notebook.* Quero saber o que já foi levantado, o que já foi coletado de informações dessa pessoa e que faz parte dessa base, de uma CPI, de uma instituição policial ou qualquer entidade que esteja investigando. Vou fazer aqui a expansão. A ferramenta vai lá na base de dados e traz tudo associada a essa pessoa. Bom, essa conta... se eu quero saber a movimentação do Gene nessa conta, eu pego aqui, clico na conta e faço a expansão. A ferramenta vai lá e traz para mim todas as transações realizadas pelo Gene. Se eu quiser, obviamente, fazer uma totalização dessas transações, eu posso simplesmente configurar minha ferramenta, para finalizar, e fazer novamente a expansão. Eu tenho aqui: essa conta do Gene, fez 25 transações para essa conta, 9 para essa, 2 para essa. Eu posso totalizar pelo montante. E assim são feitas, atualmente, por diversas instituições no Brasil, as investigações. Passo a palavra para o Presidente da Mesa.

O SR. PRESIDENTE (Deputado Marcelo Itagiba) - Obrigado pelas explanações, ambas bastante elucidativas e que demonstram que a teia está armada e que hoje a tecnologia está a serviço da inteligência policial. Sem inteligência não se faz polícia. E se nós utilizássemos todos esses instrumentos que hoje está à disposição, talvez a violência nas grandes cidades estaria muito mais reduzida.

Eu passo a palavra ao Relator para seus questionamentos e, em seguida, para demais inscritos.

O SR. DEPUTADO NELSON PELLEGRINO - Eu serei até muito breve, Sr. Presidente, porque acho que...concordo que a...eu não quero secundar a declaração de V.Exa. Eu tenho defendido isso há algum tempo. Se tivéssemos mais inteligência policial e mais tecnologia, teríamos muito mais eficiência. Eu constatei isso de forma simples na CPI do Narcotráfico. Com os parcos recursos que nós tínhamos na época, pudemos identificar e ajudar a desarticular diversos esquemas criminosos no País. E, olhe, que não tínhamos naquela época a tecnologia que temos hoje. Então, eu penso que esse aparato, se ele estiver nas mãos do Estado e for convenientemente utilizado será um grande serviço à sociedade. Mas eu penso que

a explicação do Marcelo foi também muito auto-explicativa. Só teria breves questionamentos a fazer. Primeiro, essa solução é livremente comercializada? Qualquer empresa, qualquer órgão, pode adquiri-la?

O MARCELO BANDEIRA RODRIGUES - Todas as solicitações... Há uma prévia análise da idoneidade das instituições. Já houve o caso de empresas pequenas, nós não realizamos as vendas, justamente com essa preocupação. Então, hoje o usuário das ferramentas são grandes empresas, grandes corporações.

O SR. DEPUTADO NELSON PELLEGRINO - Mas ela não é uma ferramenta que só está à disposição do poder público. Empresas particulares, grandes corporações têm acesso a essa ferramenta?

O SR. MARCELO BANDEIRA RODRIGUES - Tem, sim, exatamente por essa flexibilidade de detecção de fraude.

O SR. DEPUTADO NELSON PELLEGRINO - Porque o sigilo telefônico está assegurado na Constituição, e não é só o sigilo telefônico, mas é o sigilo das informações em relação aos telefones também. Eu entendi que, um pouco, essa base de dado se alimenta de dados que estão protegidos legalmente, não só dados em termos de sigilo telefônico, mas como sigilo financeiro também. Ela se alimenta de dados que são... A minha movimentação bancária só interessa a mim, ela não pode ser publicamente revelada, a não ser para a Receita Federal, que tem acesso a essa coisa toda. Então, eu sei que vocês comercializam a solução. A base de dados é alimentada à parte.

O SR. RENATO LIRA DA COSTA - Não só alimentada, como definida. Ou seja, os nossos usuários são empresas de telefonia. Para o uso em prevenção de fraude. Então, eles não têm movimentação financeira, não têm conta corrente. Eles vão ter a pessoa que é o proprietário do telefone, o endereço de remessa da conta (*falha na gravação*), o número do CPF são os dados da operadora. Se uma Secretaria de Segurança Pública adquire a ferramenta e vai fazer investigação sobre crimes contra o patrimônio, ela pode criar uma base com alguns objetos, que nós chamamos de entidades, voltados para aquele tipo de investigação. Então, o caso disso tudo que o Marcelo falou... E eu entendo sua preocupação, mas a ferramenta é comercializada para empresas da iniciativa privada, pela flexibilidade que ela tem na manipulação de grandes volumes de dados e de trabalhar com

padrões que existam. Não significa, pelos exemplos que o senhor viu aqui, que as empresas venham a utilizar esse tipo, da forma...

O SR. DEPUTADO NELSON PELLEGRINO - Ou que tenham capacidade de fazer a manipulação desses dados todos como...

O SR. RENATO LIRA DA COSTA - Até porque eles não dispõem desses dados. Esses dados são dados protegidos...

O SR. DEPUTADO NELSON PELLEGRINO - Porque alguns são protegidos legalmente.

O SR. RENATO LIRA DA COSTA - Sim. No caso ali...

O SR. DEPUTADO NELSON PELLEGRINO - Na época da CPI tinha algumas informações, alguma investigação.

O SR. RENATO LIRA DA COSTA - Justamente.

O SR. DEPUTADO NELSON PELLEGRINO - É um *software*, é uma ferramenta que cria atalhos, é uma ferramenta que permite atalhos, que permite, de forma inteligente, classificar dados que seriam impossíveis de serem classificados humanamente, por verificação. Ou então levaria anos, meses ou dias, e uma ferramenta que pode em horas dar os dados ou fazer cruzamentos ou dar informações que, numa verificação manual, ela levaria um tempo muito maior.

O SR. MARCELO BANDEIRA RODRIGUES - Não só levaria tempo maior como a eficiência não seria a mesma. Isso é um ponto pacífico entre os analistas de inteligência. Com as ferramentas, com a tecnologia consegue-se não só detectar parte das fraudes, mas todo o esquema dos atos ilícitos. Bem ressaltado... Os dados que são trabalhados pela ferramenta são os que questão disponíveis pela instituição que adquiriu. Então, no caso de um banco, ele vai utilizar os dados que ele tem disponível já no sistema de informação dele.

O SR. DEPUTADO NELSON PELLEGRINO - Teria a informação de que órgãos na área pública teriam adquirido essa ferramenta?

O SR. MARCELO BANDEIRA RODRIGUES - Sim. Nós temos alguns clientes mencionados no nosso *site*. Então, tem a Secretaria de Segurança Pública da Bahia, Banco do Brasil, a Vivo, como operadora, tem também o Departamento de Polícia Federal, o Ministério Público do Distrito Federal e Territórios. Esses são alguns que posso comentar porque tenho autorização para publicação no nosso *site.*

O SR. DEPUTADO NELSON PELLEGRINO - Mas outros órgãos de segurança pública de outros Estados podem ter adquirido também?

O SR. MARCELO BANDEIRA RODRIGUES - Sim.

O SR. DEPUTADO NELSON PELLEGRINO - Isso é o que o Estado autorizou que fosse divulgado? No caso da Secretaria de Segurança Pública da Bahia, ela adquiriu que tipo de base de dados?

O SR. RENATO LIRA DA COSTA - Não, não. Nenhum...

O SR. DEPUTADO NELSON PELLEGRINO - Base de dados não, que tipo de ferramenta?

O SR. RENATO LIRA DA COSTA - O Analyst's Notebook e o iBase. É que, diferentemente do que as instituições fazem, nós não divulgamos, nós não perguntamos se podemos divulgar a instituição que adquiriu. Nós deixamos que a instituição nos diga que pode ser divulgado. Então, até que uma instituição diga para a Tempo Real *"Olha, vocês podem dizer que nós somos clientes"*, até aquele momento ela é cliente e não é dito que ela é cliente. Tá? É o contrário.

O SR. DEPUTADO NELSON PELLEGRINO - E a Secretaria de Segurança Pública da Bahia adquiriu que tipo de solução?

O SR. MARCELO BANDEIRA RODRIGUES - O Analyst's Notebook e o iBase, que foi o primeiro *software*, que é o que faz o gráfico, e essa base investigativa.

O SR. DEPUTADO NELSON PELLEGRINO - Mas para efeito de quê, na área de inteligência de segurança pública?

O SR. MARCELO BANDEIRA RODRIGUES - Na área de inteligência. Aí, a aplicabilidade...

O SR. DEPUTADO NELSON PELLEGRINO - Possível de manipular que tipo de dados?

O SR. MARCELO BANDEIRA RODRIGUES - Justamente...

O SR. DEPUTADO NELSON PELLEGRINO - Telefônicos...

O SR. MARCELO BANDEIRA RODRIGUES - Justamente esse tipo de perguntas que a gente fica muito preso, porque nós temos as questões contratuais. Por exemplo, o Senado Federal, ao adquirir a ferramenta, há um impeditivo de contrato até de comentar. Só é possível comentar hoje devido a uma audiência

pública, também na Câmara, em que tiveram integrantes do Senado que fizeram esses comentários de utilização da ferramenta.

O SR. DEPUTADO NELSON PELLEGRINO - Mas a Comissão Parlamentar de Inquérito pode requerer essa informação, evidentemente que com a devida cautela no manuseio, porque esse é um dado que a CPI pode requisitar. Evidentemente, essas informações estarão sob responsabilidade da Comissão Parlamentar de Inquérito, e o vazamento dela também seria responsabilidade da CPI.

O SR. RENATO LIRA DA COSTA - Correto. Mas não é... Talvez o Marcelo tenha se expressado um pouco diferente. Quando nós fazemos uma venda, pode ser para a Secretaria de Segurança Pública do Rio de Janeiro ou do Espírito Santo ou da Bahia, eles dizem mais ou menos o que eles precisam: *"Olha, nós queremos fazer investigação."* Então, se uma pessoa chegar para nós, *"Olha, para fazer investigação, você vai precisar fazer os diagramas"*, que é onde há todo o entendimento, e esse diagrama, ele é aceito como prova em juízo hoje também. *"Bom, mas eu quero ir acumulando conhecimento ao longo do tempo."* Então, para acumular conhecimento, você vai precisar do iBase, que tem um banco de dados associado. Agora, como a Secretaria de Segurança vai criar as entidades no iBase, em quase a totalidade das vezes, nós não sabemos, porque eles têm os analistas de sistema....

O SR. DEPUTADO NELSON PELLEGRINO - Ela que vai determinar qual é a base de dados que ela vai trabalhar.

O SR. RENATO LIRA DA COSTA - Que às vezes podem ser bases de dados que ela tenha dentro do Governo do Estado, e outras vezes coisas que os investigadores venham a alimentar na medida dos seus levantamentos em campo nessa base de dados. Então, por exemplo, eu tenho lá uma entidade que é uma pessoa chamada Renato Lira, que está lá, e na base existe lá, por exemplo, "local de controle", se ele tem uma soberania sobre algum local, "carros que possui", "igreja que freqüenta". Eu não vou trazer essas informações de base de dados, mas o investigador, ao ir para campo e acumular esse conhecimento, ele volta e insere naquela base de dados. Então nem sempre o senhor vai achar... ou o senhor pode ter a conjunção das duas coisas: o senhor trazer dados de uma base e esses dados

serem refinados ou acrescidos de informações dos investigadores. Então, na maior parte dos casos, a Tempo Real comercializa a ferramenta e dá os treinamentos, para que as pessoas da instituição possam caminhar com as suas próprias pernas.

O SR. DEPUTADO NELSON PELLEGRINO - Não, porque... Hein? O COAF tem uma solução dessas?

O SR. RENATO LIRA DA COSTA - Não tem. Não sei dizer se tem. Pode ter, porque, por exemplo, eu sou o Gerente do Núcleo de Difusão do Conhecimento e ele é o de Tecnologia, mas ele não é o de Vendas.

O SR. DEPUTADO NELSON PELLEGRINO - Os senhores não se recordam em que ano a Secretaria de Segurança Pública da Bahia adquiriu essa solução?

O SR. RENATO LIRA DA COSTA - Foi final de 2004 para início de 2005. O último foi em 2005.

O SR. DEPUTADO NELSON PELLEGRINO - É só, Sr. Presidente. Obrigado.

O SR. PRESIDENTE (Deputado Marcelo Itagiba) - Deputado Maluly, autor do requerimento.

O SR. DEPUTADO JORGINHO MALULY - Sr. Presidente, vou ser bastante breve, por causa do horário. Em primeiro lugar, eu queria agradecer a presença dos senhores aqui, principalmente do Marcelo, que já esteve conosco também na Comissão de Ciência e Tecnologia, onde nós tratamos desse assunto.

Presidente, a primeira conclusão que eu tiro aqui é lamentar o baixo *quorum*. Acho que hoje nós tivemos um dia extremamente proveitoso na nossa CPI, e é uma pena que não temos 5 Deputados aqui, fora o Presidente e o Relator, para ouvir essa gama de informações que foram passadas até agora para cada um de nós. Eu estava conversando com o Deputado Abi-Ackel aqui, ao longo da apresentação, e ele, que é jurista, especialista na área do Direito, está impressionado com o nível de ferramentas existentes hoje à disposição, vamos dizer assim, da segurança, de uma maneira geral. Esta é a primeira colocação que eu faço: um apelo para que cada um de nós e o próprio Presidente intercedam junto aos colegas, pelo menos para que cada partido ou cada bancada insista pelo menos num revezamento aqui, para que a gente tenha *quorum* numas audiências desta magnitude.

Outra coisa importante. Dentro do mundo do Direito, só vale o que está no processo. Então, quando se vai montar o conjunto de provas para se preparar um

processo, é fundamental a consistência dessas provas. E eu entendo que esses mecanismos, essas ferramentas, são essenciais nesse processo. Eles não... Hã? Exatamente. Não são as únicas, mas são importantes. Por exemplo, você tem a suspeita de que alguém está recebendo propina de um determinado órgão, em cima de uma obra. Vamos falar da Gautama aí, por exemplo. Teve um Ministro que caiu porque dizem que a pessoa entrou com um envelope de dinheiro, supostamente entrou com um envelope de dinheiro no gabinete do então Ministro. Só estou dando um exemplo do que saiu na mídia nacional, não estou dizendo que aconteceu isso. Mas se pode pegar um instrumento desses e pegar... Ao longo do padrão que o senhor disse, os pagamentos são feitos todo dia 15, todo dia 20. Em torno desse dia, você vai ver que tem mais ligações, talvez daquele diretor financeiro daquela empresa para o Prefeito ou para o Secretário de Fazenda.

O SR. MARCELO BANDEIRA RODRIGUES - Só um comentário. O padrão pode ser também no setor financeiro.

O SR. RENATO LIRA DA COSTA - Eu tinha perguntado ao Marcelo, porque aquela...

O SR. DEPUTADO JORGINHO MALULY - Saques, depósitos, transferências...

O SR. RENATO LIRA DA COSTA - Pode ser feita a conjugação na linha de tempo das ligações telefônicas e das movimentações financeiras. Então dá para identificar muito bem quando uma pessoa liga para outra, o dinheiro sai de uma conta e vai para outra, aí uma terceira pessoa liga para alguém dizendo que aquele dinheiro caiu... Todo esse encadeamento era o que eu tinha perguntado ao Marcelo se ele ia mostrar, que é um caso muito bonito de ver.

O SR. DEPUTADO JORGINHO MALULY - Então, eu queria deixar clara a importância dessas ferramentas complementares, com outras, no processo de formação, de consistência de provas.

E aí vou nas 2 outras vertentes, que estão claras aqui, Sr. Presidente, e eu faço um apelo desde já para V.Exa., porque nós temos a obrigação de criar um marco regulatório nesse sentido. Nós estamos vendo aqui que as coisas correm soltas: não temos ninguém fiscalizando quem compra, quem vende, quem faz, quem usa, como usa, de que maneira usa, não temos nada. Nós temos uma lei que o

nosso nobre Relator comentou, mas eu acho que ela está defasada com o grau da modernidade em que as coisas estão acontecendo. Então eu faço este apelo aqui à CPI: que nós tenhamos no foco de V.Exa., além de tantas outras nossas... A criação, no final deste processo de investigação, de depoimentos, que nós criemos uma sugestão de criação do marco regulatório jurídico nesses assuntos que nós estamos tratando aqui.

Outra coisa também. É claro que nós temos que apoiar o investimento financeiro nos órgãos de segurança deste País. Não dá para conceber que, com esse nível de mecanismos que nós temos à disposição, ainda aconteçam telefonemas de dentro de penitenciárias, aconteçam seqüestros relâmpagos e outros crimes, como o tráfico de drogas, enfim. Com isso tudo aí, se a Polícia tiver condições de se utilizar — chantagem... — desse... eu chamaria de arsenal, vamos chamar assim, de combate ao crime organizado, a eficiência da Polícia com certeza seria muito melhor do que a que a gente vê hoje.

Então eu acho que nós temos que apoiar V.Exa., Sr. Presidente, que é um ilustre e honrado representante da Polícia Federal do nosso País. Temos que dar apoio financeiro e orçamentário nas verbas, na aquisição desses equipamentos pelos órgãos competentes.

Agora, objetivamente, em termos de perguntas, está claro aqui, eu acho, que a biometria, ela é fundamental na investigação policial. Eu acho que não preciso dizer isso, porque vocês deixaram isso claro. Vocês entendem também, como eu disse agora que... Eu coloquei errado, vou corrigir. A nossa legislação que está aí hoje respalda a biometria de... a voz? Nós temos mecanismos jurídicos que permitem esse uso, toda essa parte como prova? Isso faz parte do Código de Processo Penal ou outras legislações? Pode se utilizar disso, ou não, isso pode ser rebatido num processo?

O SR. RENATO LIRA DA COSTA - Não entendo que possa haver uma idéia contrária dos juristas, porque a metodologia utilizada para aferir a autenticidade ou não da voz é a mesma adotada cientificamente para aferir o DNA e as impressões digitais. É um método estudado e aceito no mundo inteiro, inclusive no Brasil. Apenas é mais uma nova tecnologia, que está sendo apresentada com a mesma forma de validação.

O SR. DEPUTADO JORGINHO MALULY - Para concluir, 2 colocações objetivas. O senhor disse que acabou de chegar da Espanha agora, onde o senhor foi, vamos dizer, aprimorar, ou buscar novos conhecimentos para trazer aqui para a Tempo Real no Brasil. Esse intercâmbio internacional, isso é respaldado por tratados? Quem pode? Eu posso ir, por exemplo, a uma empresa lá na Espanha, ou nos Estados Unidos, ou em Israel, por exemplo, que deve ter muito isso, e eu posso comprar um equipamento desses e trazer e montar uma empresa aqui? Como é regulamentada essa relação internacional dos países nessa área?

O SR. RENATO LIRA DA COSTA - Pode. O senhor pode inclusive... A empresa pode abrir uma sucursal no Brasil. Também pode. É óbvio que é mais prático para uma empresa procurar parceiros, né? E, graças ao trabalho que vem sendo executado com seriedade ao longo dos anos pela Tempo Real, a Ignite observou e a qualificou como uma empresa séria para representar a sua linha de produtos no Brasil. Isso nos deixou extremamente satisfeitos, porque, cada dia que nós vamos num cliente — e nós temos muitos clientes envolvidos com a parte de segurança e inteligência —, nós passamos a ser mais e mais reconhecidos como pessoas sérias, e pessoas novas, porque eu sou um dos mais velhos lá, a maior parte está na faixa dos 30, 35 anos, e eu tenho 50. São pessoas novas que têm seriedade naquilo que se propõem a fazer, têm competência e têm a dignidade de respeitar as leis do País, as leis da instituição, as normas que regem aquele critério de confidencialidade que as empresas possuem. Lógico, a Ignite poderia ter vindo aqui, como nós poderíamos ter ido procurar qualquer outra empresa. Graças ao bom Pai, foi um casamento. Nós conseguimos uma empresa que tem o mesmo padrão de seriedade e de envolvimento com o serviço de inteligência e de investigação lá fora para poder representar os produtos aqui no Brasil.

O SR. DEPUTADO JORGINHO MALULY - O senhor comentou aí sobre essas ferramentas em cima de arquivos que são passados para quem está operando aí o sistema. Isso pode ser mantido, por exemplo, paralelamente, quando a Polícia está fazendo um processo de investigação com autorização judicial para grampo de determinada pessoa? Isso pode ficar ligado automaticamente ao longo dessa investigação, parafraseando o nome da empresa, e em tempo real essas informações já serem... Ou tem que esperar armazenar, para depois alguém avaliar?

O SR. RENATO LIRA DA COSTA - Pode. Pode. Depois de um tempo que a gravação está ocorrendo, tão logo o sistema de interceptação... Eu lembro que eu falei que integração pressupunha uma entrada que vinha do sistema de interceptação, um processamento nosso e uma saída que era colocada para um outro sistema que viesse depois, ou só a presença do investigador. Tão logo o sistema de interceptação grave, no que se chama de *buffer* de entrada, os dados daquela ligação e o áudio, o nosso sistema pode começar a trabalhar com áudio. Se o sistema de interceptação vai fazer isso logo que a ligação começa a ocorrer, nós vamos trabalhar em tempo real. Se ele faz esse procedimento ao final da chamada, quando é desligada, nós vamos fazer quase em tempo real. Nós só vamos poder começar a trabalhar quando o sistema de interceptação colocar aquela informação lá.

O SR. DEPUTADO JORGINHO MALULY - A última, para concluir, Presidente. Pode ser? Até que o Presidente pode achar que esteja um pouco fora do âmbito da CPI, mas eu queria uma opinião pessoal dos senhores que são especialistas no assunto de um fato que mudou a história do mundo e interferiu no Brasil também. Com esse grau de tecnologia, e já foi dito aqui por outros até que os Estados Unidos não liberam algumas que eles têm, que são mais avançadas ainda, eu chego à conclusão... Tem um documentário aí na mídia mundial de que supõe-se que os Estados Unidos tinham conhecimento claro do ataque de 11 de setembro. E eu entendo que uma operação daquele tamanho, com envolvimento de aviões, de pilotos, de tudo isso, não pode ser feita da noite para o dia, deve ter tido uma evolução ao longo do tempo. Os senhores entendem que, com tudo isso, não seria possível evitar uma tragédia como aquela? E agradeço mais uma vez.

O SR. RENATO LIRA DA COSTA - Aí eu vou passar até do mundo da suposição. Houve a veiculação de notícias, já em 2002, de que a CIA havia informado à Casa Branca dos riscos que estavam sendo passados pelo Governo americano e por aqueles prédios em particular. O que foi falado na época, em 2002, pela Casa Branca é que o Presidente Bush tinha entendido que não era alguma coisa séria. De fato — isso o senhor não está supondo, nem eu — isso aconteceu. A CIA tinha um conjunto de informações, não se sabe de qual fonte, mas que diziam

que havia todo aquele risco. E eles achavam que o risco não era tão grande e pagaram para ver.

O SR. DEPUTADO JORGINHO MALULY - Sr. Presidente, obrigado. O Deputado Abi-Ackel está me pedindo um aparte. O senhor permite que eu conceda, por causa do tempo, ou não?

O SR. PRESIDENTE (Deputado Marcelo Itagiba) - Não vou permitir o aparte ao Deputado Abi-Ackel porque vou conceder a ele a palavra tão logo V.Exa. termine.

O SR. DEPUTADO JORGINHO MALULY - Então encerro e agradeço, Presidente. Muito obrigado. Eu agradeço e concluo.

O SR. PRESIDENTE (Deputado Marcelo Itagiba) - Quero parabenizá-lo mais uma vez pela qualidade do requerimento, que foi bastante esclarecedor por parte daqueles que hoje aqui compareceram.

O SR. DEPUTADO JORGINHO MALULY - Obrigado, Presidente. A intenção foi colaborar.

O SR. PRESIDENTE (Deputado Marcelo Itagiba) - Com a palavra o Deputado Paulo Abi-Ackel.

O SR. DEPUTADO PAULO ABI-ACKEL - Sr. Presidente, Sr. Relator, Drs. Marcelo e Renato, eu vi apenas, infelizmente, parte do depoimento, porque, infelizmente, estava no exercício da Liderança da Minoria no plenário, de forma que a minha pergunta corre o risco até mesmo de já ter sido objeto de esclarecimento.

Então, com essa ressalva e com a desculpa de ter chegado atrasado, eu gostaria de saber de V.Sa., Dr. Renato, se há alguma dedicação — tempo, enfim, investimento — dentro da empresa no sentido de fazer com que esse *software*, tanto quanto ele é visivelmente... — não sou especialista, mas posso concluir e verificar que ele é, sem dúvida nenhuma, extremamente eficiente no combate à criminalidade —, se há a hipótese e a preocupação sobretudo no sentido de, na medida em que ele é extremamente capaz de perseguir uma informação, se ele é também capaz de parar a investigação no momento em que o *software* consegue detectar, ou aquele que está usando o *software*, melhor dizendo, consegue detectar que ele começa a chegar num ambiente, num universo... pessoas que são completamente estranhas ao processo investigatório. Então eu pergunto o seguinte. Eu sei que o *software* é vendido e outras pessoas o utilizam. Aí fica o critério dessa pessoa de fazer parar o

processo naquele momento. A minha pergunta é se, tanto quanto a empresa investe em fazer com que ele seja capaz de ser o mais agressivo possível no combate de hipóteses de situações criminosas, se também a empresa desenvolve algum mecanismo, algum sistema, alguma modalidade, enfim, alguma forma de fazer com que ele também, de maneira independente daquele que utiliza — se ele tem algum tipo de alerta para a preservação daquelas pessoas que estão ali vitimadas pela eficiência do *software*, vamos dizer assim, na medida em que, pelo que eu pude depreender, e se estiver errado, o senhor tem todo o direito de dizer que estou errado, lhe dou esse direito...

Eu fico me indagando o seguinte: ele é extrema... Vi muitas vezes o senhor falar: *"Não, ele é capaz de ir buscando, ir buscando, ir buscando e até dar o caráter mais amplo possível à investigação"*. Mas eu fico me perguntando o seguinte: o *software* é capaz de sinalizar ou de pelo menos fazer com que aquele que o está utilizando perceba que ele começou a sair completamente fora do objeto dele? Digamos aqui no sentido prático com a linguagem do leigo. Vamos dizer que ele começou numa... o senhor usou aí uma expressão, no SIA, numa área aqui de Brasília de que agora eu não me recordo — citou 3 áreas aqui de Brasília —, e de repente isso passou, foi parar lá no Rio Grande do Sul. Então, há algum dispositivo no programa, no *software*, no sistema, que faz com que a pessoa perceba que ele está se distanciando completamente, ou isso é apenas do convencimento daquele que o está utilizando?

O SR. PRESIDENTE (Deputado Marcelo Itagiba) - Deputado Paulo Abi-Ackel, só para ver se eu peguei o sentido, também para que eu possa compreender melhor, vamos trabalhar na questão da interceptação telefônica e naquele sistema que faz o reconhecimento de voz. Então, V.Exa. estaria indagando do depoente que, no caso de aparecer uma voz estranha que não é aquela interpretada, se ele teria condições de bloquear o sistema de interceptação de forma automática para que não houvesse invasão na privacidade de terceiro não envolvido com a investigação. Seria isso?

O SR. DEPUTADO PAULO ABI-ACKEL - Seria exatamente. Eu até parabenizo V.Exa. que soube formular melhor a pergunta, até porque V.Exa. é treinado para fazer esse tipo de leitura, de interpretação. É exatamente isso. E —

aqui o leigo falando de novo — eu poderia dizer o seguinte: caímos numa conversa que não tem nada a ver com a investigação, uma conversa íntima, ou caímos ali numa conversa de pai para filho. É possível, então, que isso seja percebido exatamente como o Deputado Marcelo Itagiba fala?

O SR. RENATO LIRA DA COSTA - Talvez este tenha sido o grande apelo que me fez ir trabalhar com esse tipo de tecnologia: a preservação dos direitos das pessoas. Eu tinha falado aqui — eu entendi que o senhor estava numa outra atividade que compete ao seu mandato — que este era um dos grandes ganhos, o ganho da economicidade, porque o investigador não precisaria mais despender um montante grande de tempo para ouvir todas aquelas ligações a fim de me identificar. E o segundo é que, me colocando como alvo de 8 mil chamadas, ele selecionaria as 100 onde eu efetivamente participasse para colocar numa determinada pasta e desprezaria as outras 7.900. Então, seria o que o senhor falou. Se na minha conversa tivesse uma conversa de pai para filho, onde não tinha nada com a investigação? Não, não tenho como filtrar isso, porque eu coloquei foi um alvo do Renato. Eu não tenho nenhuma maneira de avaliar a locução ou as palavras, porque o *software* tem a característica de biometria, ele não interpreta se eu falei “amor” ou “fedor”, “bonito” ou “feio”. Ele não interpreta isso. Ele vai ver o ar que vai ser expelido pelo meu corpo, vai passar por uma série de órgãos até mexer aqui o ar que está externo e gerar um som. Isso, através de modelos matemáticos, vai gerar o meu padrão biométrico. Isso independe de se eu estou gripado ou não estou, a não ser que esteja extremamente gripado, ou se eu fiz uma operação de câncer na boca, tive que mexer no céu da boca, mas tirando os casos de extrema exceção, o *software* vai me identificar a pessoa ou vai me apontar como um provável muito grande para eu realizar uma investigação sobre ela. Mas como a facilidade do *software* é a biometria, eu não vou poder identificar, no meio de uma conversa, se ela tem um foco direto com a investigação ou não para interromper. Isso vai ficar a cargo do investigador. Mas eu posso lhe dizer também com toda a propriedade, toda a tranqüilidade: as pessoas envolvidas na área de inteligência no Brasil e fora do Brasil são pessoas que passam por treinamentos muitos rígidos e por freqüentes avaliações de comportamento e de personalidade para poder pertencer ou não àquele serviço. Então, se, no caso que o senhor citou, é uma conversa particular, e

ele vai continuar ouvindo, eu lhe garanto que é um desvio, e que esse desvio vai ser uma exceção, ele não vai ser o caso corrente dentro da área de inteligência.

O SR. DEPUTADO JORGINHO MALULY - Antes de o Deputado Paulo Abi-Ackel chegar, parece que o senhor comentou que aquele traficante foi identificado em cima desse...

O SR. RENATO LIRA DA COSTA - Ele foi identificado, o Abadia... O Abadia foi identificado única e exclusivamente por sua voz, não com a nossa tecnologia. Os arquivos de áudio foram mandados para os Estados Unidos, e o governo americano, com as tecnologias secretas deles, é que identificaram.

O SR. MARCELO BANDEIRA RODRIGUES - Posso complementar só a parte do *software* 2? Esse conjunto de *software* tem um controle total de auditoria. Então é capaz de o *software* me mostrar que hoje um determinado investigador, acessando de um determinado computador, fez uma consulta na pessoa do Renato. Eu sei exatamente o que ele está pesquisando nessa base investigativa. Eu sei tudo que ele acessou nessa base investigativa. E esse *software* permite também a compartimentação da informação. Ou seja, eu tenho a minha equipe trabalhando em chamadas telefônicas, essa equipe só consegue enxergar as chamadas telefônicas. Apesar de ele estar lançando uma base completa, ele só acessa dados de chamadas telefônicas: os telefones e as chamadas, e mais nada. Ele não enxerga, por exemplo, aqui na tela, que eu tenho uma conta corrente, o endereço daquela pessoa. E mais, se eu tenho uma pessoa que está sendo investigada e é uma autoridade, uma pessoa da sociedade, muito conhecida, eu posso deixar restrita só ao meu grupo de investigadores, ou seja, se eu tenho mil pessoas acessando essa base de investigação, só o meu grupo, que tem meia dúzia de investigadores, sabe que aquela informação está na base de dados. Então isso permite um controle total de todas as transações que são feitas, e permitindo justamente ao responsável pela investigação detectar esse possível tipo de arbitrariedade.

O SR. DEPUTADO PAULO ABI-ACKEL - Eu compreendi que, em meio a um processo investigatório, o investigado pode então vir a ser considerado, vamos dizer assim, a prova pode surgir, digamos assim, de uma conversa de terceiros, entre 2 pessoas usando o telefone dele. É verdadeira essa hipótese?

O SR. RENATO LIRA DA COSTA - Hoje isso acontece. Hoje isso acontece. Mas isso é o acaso. Com a biometria de voz, também será o acaso, porque quando o investigador tem um suspeito, por exemplo, sobre o Renato Lira, é porque ele tem certas convicções formadas ou informações de relevância anterior já obtidas que fazem com que o Renato Lira seja o suspeito. Então para que o senhor, que é o investigador, ao invés de ouvir as ligações feitas pelo Renato Lira, vai ouvir as do Marcelo Bandeira? Não é? É óbvio que num determinado momento o Marcelo Bandeira pode falar com o Sr. João, e o Sr. João falar com o Renato Lira. Isso não vai ser pego na biometria de voz. O registro das ligações que aconteceram entre o Renato e o Sr. João, entre o Sr. João e o Marcelo Bandeira é que vai permitir o cruzamento, daquela forma que o senhor está vendo ali, e o investigador vai concluir que embora não houvesse um vínculo imediato entre o Renato e o Marcelo Bandeira, ele passa a haver por intermédio de uma terceira pessoa envolvida, por exemplo, o padrão de chamadas, ou quando encontrar caminhos. Nesse *software* — é que o nosso tempo não é tão longo, o Marcelo poderia passar aqui o dia inteiro mostrando cada uma das ferramentas —, eu posso ter uma parte da investigação que começa em mim e vai terminar na pessoa que está no último banco desta sala, que aparentemente não tem uma ligação. Mas o senhor fala assim: *"Vê se existe um caminho entre o Renato e aquela última pessoa"*. Se existir, mesmo que passe por uma firma em que eles trabalharam juntos, um carro que foi vendido de um para o outro... É lógico que essas informações têm que existir na base de dados de investigação, porque não somos nós que criamos, são os investigadores que obtêm ou inserem essas informações.

O SR. MARCELO BANDEIRA RODRIGUES - Alimentam.

O SR. RENATO LIRA DA COSTA - Alimentam essa base.

O SR. DEPUTADO PAULO ABI-ACKEL - Mas aí me ocorre o seguinte: essa pessoa que está lá no fundo, ela não teve o seu sigilo quebrado, ela...

O SR. RENATO LIRA DA COSTA - Ela só vai aparecer se, em algum arquivo que veio de alguma fonte de informação dos investigadores, consta alguma informação sobre ela.

O SR. DEPUTADO PAULO ABI-ACKEL - Pois é, então...

O SR. RENATO LIRA DA COSTA - Uma sociedade de empresa: aquela senhora que está na última fileira pode ser sócia cotista numa empresa em que eu também sou sócio cotista.

O SR. DEPUTADO PAULO ABI-ACKEL - Pois é, mas aí eu pergunto a V.Sa.: aí não há — e eu aqui não estou falando que é de vocês —, mas aí não há exatamente a ocorrência de um procedimento irregular por quem está fazendo, na medida em que essa senhora do fundo não teve o seu sigilo quebrado? Quer dizer, então o *software* está programado para fazer um trabalho num universo, como vi ali, de 12, 20 telefones que estão, portanto, com o seu sigilo quebrado mediante ordem judicial.

O SR. RENATO LIRA DA COSTA - Sim.

O SR. DEPUTADO PAULO ABI-ACKEL - Mas dali surge uma conversa com a vigésima primeira pessoa, cuja ligação se deu, e até a informação foi pertinente para o processo investigatório, porém...

O SR. RENATO LIRA DA COSTA - Não estava com o sigilo.

O SR. DEPUTADO PAULO ABI-ACKEL - ... o telefone... ela não tinha o seu sigilo quebrado. Então não há, e aqui estamos sempre falando...

O SR. RENATO LIRA DA COSTA - Em hipótese.

O SR. DEPUTADO PAULO ABI-ACKEL - ... em hipótese, claro. Então não há, talvez até em face da excepcional competência e capacidade do programa, não há risco de ocorrência, por parte do investigador, de um procedimento irregular, na medida em que ele promove uma escuta clandestina, uma escuta oficial num telefone que não tem a escuta autorizada e ela não se torna clandestina? Então aí vem a pergunta seguinte: o procedimento não se torna meio clandestino e meio oficial? Essa é a última pergunta que eu tenho para fazer ao senhor.

O SR. RENATO LIRA DA COSTA - Concordo com o senhor. Agora, nenhuma tecnologia vai coibir uma ação do ser humano quando ele se dispõe a fazê-lo. Por exemplo, o Word é o processador de textos mais conhecido no mundo. O senhor pode escrever um relatório da sua CPI, uma pessoa pode escrever um poema, e outro pode escrever uma série de atrocidades contra alguém. Nós não vamos conseguir inibir o ser humano. O Presidente falou aqui ao meu lado, comentou, enquanto o senhor estava falando, e que é a pura verdade: o sistema só

vai trabalhar com dados conhecidos. Se esses dados foram inseridos pelo ambiente de investigação da instituição, por exemplo, eu vou levar para o meu Estado, a Polícia Militar do Rio de Janeiro ou a Secretaria de Segurança vai pedir formalmente, por exemplo, dados ao Departamento de Trânsito sobre registro de veículos. Aquilo vai ser entregue, vai entrar na base corporativa. Muitas vezes o investigador, segundo aqueles critérios que o Marcelo falou de visões específicas sobre a base de dados, ele vai poder ver que um carro foi vendido de mim para uma outra pessoa que está sendo investigada, mas ele não vai conseguir alterar aquela informação, ele poderá só ter a visão. A questão do telefone, ela poderá ter sido gravada, e daí eu tenho o áudio dela, que está lá no fundo, ou na conta reversa que veio da operadora, porque ou eu liguei para ela, ou ela ligou para mim, ou uma outra pessoa de que foi pedida também a conta reversa manteve esse vínculo até chegar o encadeamento até ela. Quer dizer, eu não posso confirmar, eu posso entender e aceitar a sua preocupação. Eu só não posso confirmá-la, porque isso vai depender muito da pessoa que estará utilizando, mas existem *logs*, existem restrições de acesso. Uma série de medidas do ambiente de tecnologia existem, não específicas só do *software*. São restrições de rede, restrições de acesso. Eu posso, através do próprio sistema operacional, dizer que uma pessoa só vai acessar o sistema se estiver dentro da instituição e não fora, ou no horário de expediente, de 8h às 5h, ou de 9h às 6h — fora daquele horário ela não acessa nem o Windows —, ou só de uma determinada máquina, com determinado endereço IP. Então, isso não é particular ao *software.* Eu entendo, porque eu já fui desenvolvedor de *softwares* na segurança pública — quando eu estive na Secretaria de Segurança Pública do Rio de Janeiro, eu trabalhava na parte de desenvolvimento de *software* —, que se nós formos tentar buscar todos os bloqueios, o *software* não vai acontecer. Ele vai perder toda a leveza, toda a flexibilidade que ele tem que ter para poder trabalhar com investigação. Ele não pode ser muito amarrado. Ele tem, sim, que se preocupar em registrar tudo o que acontece dentro dele, para que possa ser auditado mais tarde, a qualquer momento.

O SR. PRESIDENTE (Deputado Marcelo Itagiba) - Não havendo mais perguntas, vou agradecer a presença ao Sr. Marcelo e ao Sr. Renato Lira. Os

esclarecimentos foram importantíssimos para esta Comissão Parlamentar de Inquérito. V.Sas. estão dispensados, com os agradecimentos desta Comissão.

Vou passar agora a ouvir o Sr. Raimundo Pinheiro de Castro Vieira Júnior, a quem convido para tomar assento a esta Mesa. *(Pausa.)*

V.Sa. já foi compromissado na forma da lei, razão pela qual eu lhe passo a palavra, por 20 minutos, para fazer a sua exposição inicial. Em seguida, ouviremos o Relator e o autor do requerimento.

O SR. MARCELO PINHEIRO DE CASTRO VIEIRA JÚNIOR - Obrigado, Sr. Presidente. Eu pediria 5 minutos para tomar as providências tecnológicas aqui. Só 1 minuto. (*Pausa*.)

O SR. PRESIDENTE (Deputado Marcelo Itagiba) - Vou passar a presidência por um momento ao Deputado Paulo Abi-Ackel e já retorno. (*Pausa*.)

O SR. PRESIDENTE (Deputado Paulo Abi-Ackel) - Com os cumprimentos da Mesa, concedo a palavra ao Sr. Raimundo Pinheiro de Castro Vieira Júnior, por até 20 minutos, para usá-la como melhor lhe convier.

O SR. RAIMUNDO PINHEIRO DE CASTRO VIEIRA JÚNIOR - Obrigado, Sr. Presidente. Sr. Relator, Deputado Nelson Pellegrino, Deputado Marcelo Itagiba, Deputado Jorginho Maluly, é com muita honra que estamos aqui presentes no sentido de prestar informações e procurar agregar valores a trabalho de tão relevante importância desta Comissão. Nós, ao contrário de prestarmos informações sobre tecnologias de grampo ou de escuta, estamos aqui para prestar esclarecimentos e informações sobre tecnologia de criptografia de voz, que, aplicada na área de telefonia, surte o efeito contrário, ou seja, minimiza os aspectos do grampo, porque, através dos níveis de criptografia praticados, a gente consegue ocultar o conteúdo de determinadas conversas que forem feitas sob a égide de uma tecnologia criptografada eficaz e consegue, evidentemente, garantir o sigilo, questão hoje bastante — vamos dizer — fragilizada dentro das questões tecnológicas e do próprio expediente de toda a Nação. (*Segue-se exibição de imagem*.) Temos aqui uma tecnologia que trazemos para apresentar como um exemplo de tecnologia utilizada na área de criptografia de voz, dentre outros que existem no Brasil e no exterior, em todo o mundo. A nossa tecnologia chama-se “Enigma”. Essa tecnologia “Enigma” é aplicada primeiramente no padrão de telefonia celular, GSM, e tem

interface com um outro equipamento que trabalha com a mesma tecnologia de criptografia, chamado *Line Cript*, que vamos apresentar para V.Exas., que faz a integração do sistema de telefonia celular, telefonia móvel, com o sistema de telefonia fixa, através de centrais telefônicas que recebem esse equipamento e que, portanto, passam a funcionar como centrais telefônicas seguras. Esta é uma pequena apresentação do Grupo BELCON, que é o fabricante dessa tecnologia — eles são especialistas em promover plataformas seguras e inteligentes de comunicação: hardware e software; têm filiais em Munique, Londres, Seul e Taipei. Aqui, no Brasil, funcionamos como seus distribuidores exclusivos. A especialidade dela é proteção criptográfica em telefonia móvel e fixa e produtos de segurança, sendo que os produtos de segurança não chegaram para nós, como distribuidores, e nós ficamos restritos à questão exclusivamente da telefonia. Esses produtos de telefonia móvel celular, que são o "Enigma", GSM, e o Dispositivo para linha fixa, que é o *Line Cript*, são o foco das nossas exposições hoje para os senhores. O Grupo BELCON fornece produtos revolucionários, inovadores em serviços de segurança e privacidade em chamadas telefônicas da rede celular GSM e da rede RDSI, que é a rede SDN que temos aqui no Brasil, e é muito utilizada pelos organismos de segurança, porque é uma rede que permite tráfego com maior flexibilidade e com maior banda de informações, tanto de dados, quanto de voz. Aí nós temos alguns conceitos sobre privacidade e segredo. O medo crescente de invasão de privacidade em escuta telefônica atinge hoje executivos, homens de negócios e personalidades públicas. Militares, departamentos de defesa, agentes de segurança, policiais e autoridades necessitam urgentemente de dispositivos de comunicação segura e livre de intrusos. Negócios e corporações aumentaram drasticamente seus sistemas de segurança devido ao monitoramento ilegal de suas comunicações de voz e transmissão de dados. Sempre que uma chamada telefônica é efetuada através da rede pública de telecomunicações uma porta sempre fica aberta a intrusos. Então, vamos iniciar a apresentação da solução do telefone celular móvel e do *Line Cript,* que é a linha fixa e SDN. O telefone celular GSM e *Line Cript* são tecnologia alemã de última geração. A BELCON e a RONAN apresentam esse produto no Brasil, que é hoje considerado pelos analistas o produto mais seguro na área de criptografia de voz no Brasil. Tema de segurança de privacidade em

chamadas via celular e rede fixa de RDSI. A criptografia de voz que o sistema enigma nos assegura é em tempo real, ou seja, ela não produz *delay*, você fala em tempo real, não fica ouvindo aquele eco. Ela produz um excelente nível de clareza e de qualidade de transmissão. A plataforma dele é uma plataforma segura, um processador *Intel Strong Arm* que fica justamente acoplado à base interna do chassis do telefone, ou seja, ele permite que o *software* da criptografia funcione com um sistema exclusivo dentro da plataforma do telefone, um sistema exclusivo de leitura e de processamento de todas as transações de criptografia. Ele tem um módulo de alta performance, ele tem codec integrado, que permite a ele fazer transações inclusive de celular para ingresso à Internet etc. A segurança dele é baseada em cartão inteligente, no s*mart card*, que é um *chip* que é inserido na plataforma onde tem um microprocessador que faz a leitura e o processamento das transações telefônicas. Ele permite o gerenciamento de usuário em grupos fechados, ou seja, em VPMs. Você pode fazer uma rede de quantos telefones forem necessários para que todos eles falem entre si num modo seguro exclusivamente. *(Pausa na gravação)* de criptografia utilizados nesse sistema são algoritmos randômicos. Eles são algoritmos que são gerados por esse microprocessador com os dados da tabela de algoritmos do *chip* e eles são processados randomicamente e aleatoriamente. Isso faz com que você tenha um nível de incriptação muito complicado para que você venha fazer uma decriptação com poucas horas de processamento num equipamento poderoso. As informações do fabricante são de que para se fazer uma decriptação de uma transação telefônica gerada por 2 equipamentos dessa natureza demoraria alguns anos/hora, ou seja, entre 15 a 17 anos, para que esses computadores pudessem realmente processar essas informações. E daí nós vamos chegar, mais na frente, nas questões legais. Essa é a estrutura interna do processamento das transações telefônicas criptografadas, onde nós temos o *chip* com o módulo de identidade do assinante, padrão GSM, que é o *chip* da operadora, e abaixo nós temos o módulo de identidade do sistema de criptografia. Eu inclusive vou pegar o telefone aqui fisicamente e vou mostrar para os senhores, que acredito que seja até melhor dessa natureza. O telefone funciona com o *chip* da operadora, que garante — nós chamamos o *chip* de tráfego — o tráfego das transações telefônicas e de voz e de dados na rede telefônica normal. É um *chip*

de qualquer operadora. E ele está habilitado como qualquer celular desses comuns que nós utilizamos em claro. E o *chip* da criptografia que está inserido aqui justamente onde fica o microprocessador de leitura e de operação das transações. Quando nós utilizamos esse sistema em claro — em claro que nós chamamos é justamente com uma ligação comum, que é feita exclusivamente através de geração e transmissão através do *chip* da operadora, nós utilizamos a tecla *send* normal. E quando nós fazemos uma transação telefônica, uma chamada telefônica para um outro equipamento desse, para um outro número que tem o mesmo equipamento, que tem o sistema de criptografia implantado nele, porque ele pode estar sem o *chip*, daí ele perde a função de criptografia, você comanda por aqui, por uma chave específica, que vai gerar um processamento, um protocolo anterior ao lançamento da chamada telefônica regular e vai preparar, através desse protocolo prévio, a abertura de chaves criptográficas para a transação pública. Ou seja, ele vai criar uma transação através da rede telefônica convencional e, dentro dessa rede convencional, ele vai preparar o ambiente para que seja fechado o protocolo de criptografia dos 2 aparelhos. Portanto, ele entra com os protocolos criptográficos com uma razão de aproximadamente 1.021 *bits*, 1.024 *bits*, ou seja, muito elevada, e garante essa primeira barreira inicial, gerando o ambiente onde vai ser feita, onde vai ser processada a chamada telefônica criptografada. A partir do fechamento da rede pública, que eu vou mostrar para os senhores aqui — depois eu vou voltar —, os assinantes trocam chaves públicas que verificam a autenticidade uma da outra e depois eles passam para os pares de chaves do SIM *card* da criptografia. Então, nessa troca de chave pública, como eu já havia falado, nós alcançamos a segurança da transmissão, ou seja, a preparação de todo o ambiente criptográfico para que seja processada a chamada segura. Eu vou, inclusive, encurtar um pouco aqui essas informações todas porque elas constam nesse *folder* que eu produzi e que deixei aqui disponível para os senhores. E gostaria também de ofertar para que seja disponibilizado para os demais Parlamentares que por outros motivos não puderam comparecer aqui à sessão. Bom, aqui tem o processo de geração de chamadas, que é a continuidade daquela transação inicial, onde existe a troca, o reconhecimento e a verificação das autenticidades de cada um, vamos dizer assim, dos aparelhos que estão participando daquela chamada. A cada chamada novas chaves são geradas,

que é o processo randômico que eu expliquei para os senhores minutos atrás. A chave da chamada é transferida, usando o canal de dados seguro, e essa chave é única para toda a conversação e é destruída em ambos aparelhos Enigma no final de cada chamada, que é a chave segura da inicial. Aqui nós temos a criptografia, o processo da criptografia da voz. Assim que a chave da chamada é gerada e trocada com outro usuário Enigma, essa chave, então, é usada pelo protocolo de criptografia IDEA com algoritmo específico para a proteção da voz contra escutas ou gravações. A comparação do SIM *card* da criptografia com os padrões de segurança elevados. Nós temos as chaves IDEA com 128 *bits* nas transações particulares, ou seja, após abertas as transações da chave pública com 1.024 *bits*, que é nível militar, ela traz para 128 *bits,* que permanece até o final da conversação telefônica, quando ela é desativada e destruída, para que ela não seja mais utilizada. Então, aquela chave que foi utilizada durante a proteção daquela chamada telefônica, ela é destruída nos 2 aparelhos. Ela pode até vir a ser reeditada, mas não mais com aquela identidade. Os senhores entenderam. Aqui dados técnicos do equipamento. Ainda estamos falando do equipamento Enigma: módulo de criptografia de 32 *bits* com microprocessador StrongARM Intel, *flash* de 2 MB, criptografia de segurança com cartão inteligente *smart card*, troca de chaves com o RSA algoritmo com 1.024 *bits* de chave pública e privada, codificação da voz algoritmos de 128 *bits* na chave de chamada, ou *data rate* com 9.6 KB por segundo. A freqüência de rede, ele funciona em 2 bandas. Ele funciona em GSM 900 MHz e em 1.800 MHz. Esse equipamento não funciona nos Estados Unidos, onde a freqüência de banda é diferente. E demais especificações técnicas: duração da bateria, 320 horas; as dimensões, ele tem dimensões aproximadamente similares à de qualquer celular comum, só um pouco mais robusto; as suas características não apresentam muitas inovações na parte do *design*, mas obviamente o conteúdo é um conteúdo bastante eficaz. Continuação dos dados técnicos. E aqui nós temos um, vamos dizer, um esquema, que é um esquema da interoperacionalidade entre o Enigma e o Line Crypt, que é o equipamento de interface da telefonia fixa. Uma vez utilizando o Line Crypt, você tem a possibilidade de integrar a telefonia celular à telefonia fixa com o mesmo padrão de criptografia, mantendo estável aquela segurança e aquela proteção das informações que você vai trocar durante aquela transação telefônica. Aqui é mais ou

menos um esquema informando como é que você pode fazer essa transação. Tudo passa através das ERBs, das Estações Rádio Base, que são as antenas repetidoras. E é interessante frisar aqui que as operadoras, todas elas, mantêm as suas ERBs, as suas Estações Rádio Base, com um padrão tecnológico que tem que suportar um determinado tráfego de informações e de chamadas telefônicas calculadas por eles pelas demandas diárias que eles têm. De maneira que essas ERBs, elas têm que ter uma atualização tecnológica que passa de analógica para digital. Se você não tiver operando como *(falha na gravação)* que tenha as suas ERBs com a tecnologia digitalizada, vai ter problemas no sentido do tráfego da sua ligação. Por quê? Porque ela não trafega como dados, ela trafega como voz. *(Falha na gravação.)* A voz encriptada, ela tem uma ocupação de banda um pouco maior do que a voz simples que trafegaria em uma ligação convencional. Então, é preciso que a operadora, ao optar pela utilização *(falha na gravação)*... Ao optar pela utilização do sistema criptografado Enigma, ele também opte por uma operadora que tenha essas qualificações tecnológicas compatíveis com a utilização da tecnologia. Basicamente, esse esquema pode nos mostrar entre uma ligação do fixo e uma interface do Line Crypt, através da própria operadora de telefonia fixa. Então, ele manda para a operadora o sinal, o sinal vem em GSM, ele comuta na central, na operadora fixa, e ele entra numa linha ISDN na central telefônica fixa. Basicamente, esses são os aspectos da telefonia criptografada que nós estamos hoje praticando aqui no nosso País, com bastante dificuldade, inclusive, na questão da apresentação e da comercialização com o Estado brasileiro, pois não conseguimos ainda ter sucesso nas vendas com o Estado, porque esbarramos no processo licitatório. E o processo licitatório, com base especificamente na Lei nº 8.666, prevê ou a dispensa de licitação, ou, no caso, a licitação, se houvesse...

O SR. DEPUTADO NELSON PELLEGRINO - Qual especialização?

O SR. RAIMUNDO PINHEIRO DE CASTRO VIEIRA JÚNIOR - ... se houvesse concorrentes similares. Mas a cultura da aquisição de equipamentos de segurança e de contra-inteligência ainda não existe no nosso país implantada dentro do serviço público federal. Embora até organismos do Governo já tenham conhecido, tomado conhecimento dessa tecnologia, eles não conseguiram formular critérios legais para a aquisição disso. Uma, porque também tem que dar

notoriedade ao processo de compra. E uma vez alertado, através da notoriedade de que vai utilizar aquilo, começam os questionamentos e começam também os *hackers*, aquelas pessoas que buscam quebrar as chaves de segurança criptográfica, a concentrar mais ainda os seus esforços, porque aquela autoridade vai anunciar que vai usar, ou aquele empresário. Mas basicamente é isso. Eu estou às ordens, disponível para o que os senhores...

O SR. PRESIDENTE (Deputado Paulo Abi-Ackel) - Agradeço ao Sr. Raimundo Pinheiro de Castro Vieira Júnior as explicações até aqui.

Imediatamente, para inquirir o senhor depoente, concedo a palavra ao ilustre Deputado Relator, Nelson Pellegrino.

O SR. DEPUTADO NELSON PELLEGRINO - Sr. Presidente, Sr. Raimundo Castro Júnior, primeiro, queria agradecer pela contribuição.

Eu teria apenas umas indagações complementares.

A informação que eu tenho desse equipamento é que ele só funciona de ponta a ponta.

O SR. RAIMUNDO PINHEIRO DE CASTRO VIEIRA JÚNIOR - Sim.

O SR. DEPUTADO NELSON PELLEGRINO - Ele só é 100% seguro se for de ponta a ponta.

O SR. RAIMUNDO PINHEIRO DE CASTRO VIEIRA JÚNIOR - Exatamente.

O SR. DEPUTADO NELSON PELLEGRINO - Se tem um aparelho emissor e tem um aparelho receptor com a mesma tecnologia para poder decodificar a mensagem. É isso?

O SR. RAIMUNDO PINHEIRO DE CASTRO VIEIRA JÚNIOR - Exatamente.

O SR. DEPUTADO NELSON PELLEGRINO - Então, ele só funcionaria assim.

O SR. RAIMUNDO PINHEIRO DE CASTRO VIEIRA JÚNIOR - Exatamente. Ele só funciona de um aparelho Enigma para outro...

O SR. DEPUTADO NELSON PELLEGRINO - Enigma.

O SR. RAIMUNDO PINHEIRO DE CASTRO VIEIRA JÚNIOR - ... equipamento Enigma.

O SR. DEPUTADO NELSON PELLEGRINO - Essa relação pode ser feita de um fixo para um móvel?

O SR. RAIMUNDO PINHEIRO DE CASTRO VIEIRA JÚNIOR - De um fixo para um móvel através de um...

O SR. DEPUTADO NELSON PELLEGRINO - Ambos têm capacidade de decodificação?

O SR. RAIMUNDO PINHEIRO DE CASTRO VIEIRA JÚNIOR - Ambos. Através do sistema Line Crypt, que é o sistema complementar, ou seja, o sistema conversor do sinal do equipamento móvel, do celular, para o fixo, e vice-versa, porque você pode gerar também...

O SR. DEPUTADO NELSON PELLEGRINO - Mas esse sistema tem que ser adquirido à parte, ou a operadora faz essa...

O SR. RAIMUNDO PINHEIRO DE CASTRO VIEIRA JÚNIOR - Não, não. Nenhuma...

O SR. DEPUTADO NELSON PELLEGRINO - Ou o sistema que é vendido já faz essa...

O SR. RAIMUNDO PINHEIRO DE CASTRO VIEIRA JÚNIOR - Não. O sistema é vendido por...ele é modular. Ou você compra só a solução...

O SR. DEPUTADO NELSON PELLEGRINO - Móvel.

O SR. RAIMUNDO PINHEIRO DE CASTRO VIEIRA JÚNIOR -... móvel...

O SR. DEPUTADO NELSON PELLEGRINO - Ou só a fixa.

O SR. RAIMUNDO PINHEIRO DE CASTRO VIEIRA JÚNIOR -... ou só a fixa. Mas obviamente que a fixa, não teria sentido você comprar só a fixa, porque você teria que também deixar canais abertos, porque ela já permite, dentro do projeto original dela, que você utilize tecnologia móvel, entrando e saindo, através do sistema Line Crypt. Então, você teria que ter o Line Crypt como integrador e mantenedor da segurança interna da sua...

O SR. DEPUTADO NELSON PELLEGRINO - Mas se eu quiser integrar o sistema móvel com o sistema fixo eu tenho que adquirir...

O SR. RAIMUNDO PINHEIRO DE CASTRO VIEIRA JÚNIOR - Perfeitamente. O senhor tem que adquirir as duas...

O SR. DEPUTADO NELSON PELLEGRINO - Tenho que adquirir as 2 soluções?

O SR. RAIMUNDO PINHEIRO DE CASTRO VIERA JÚNIOR - As 2 soluções.

O SR. DEPUTADO NELSON PELLEGRINO - As soluções se comunicam entre si, elas falam entre si.

O SR. RAIMUNDO PINHEIRO DE CASTRO VIERA JÚNIOR - Exatamente.

O SR. DEPUTADO NELSON PELLEGRINO - Elas têm um sistema que...

O SR. RAIMUNDO PINHEIRO DE CASTRO VIERA JÚNIOR - Elas são da mesma tecnologia, do mesmo fabricante.

O SR. DEPUTADO NELSON PELLEGRINO - O mesmo sistema de decodificação é a base dos 2 sistemas.

O SR. RAIMUNDO PINHEIRO DE CASTRO VIERA JÚNIOR - A tecnologia é idêntica.

O SR. DEPUTADO NELSON PELLEGRINO - Bom, a outra dúvida que remanesceu, só para dar uma contribuição — isso vai ser objeto até de indagação minha mais adiante —, na quinta-feira passada, nós tivemos o depoimento aqui de um agente da ABIN.

O SR. RAIMUNDO PINHEIRO DE CASTRO VIERA JÚNIOR - O diretor do CEPESC?

O SR. RAIMUNDO PINHEIRO DE CASTRO VIERA JÚNIOR - Isso. Que fez uma série de considerações sobre desenvolvimento de *softwares.* Eu fiz algumas perguntas para ele, a partir de algumas informações que eu tinha também por outras fontes. Eu estou entendendo que esse sistema faz a criptografia da comunicação na comunicação entre um aparelho e outro.

O SR. RAIMUNDO PINHEIRO DE CASTRO VIERA JÚNIOR - Exclusivamente.

O SR. DEPUTADO NELSON PELLEGRINO - Então é um aparelho que quer proteger o conteúdo da comunicação que é emitida.

O SR. RAIMUNDO PINHEIRO DE CASTRO VIERA JÚNIOR - Exatamente.

O SR. DEPUTADO NELSON PELLEGRINO - Então, por exemplo, se eu sou uma autoridade policial e peço a interceptação da sua linha telefônica...

O SR. RAIMUNDO PINHEIRO DE CASTRO VIERA JÚNIOR - Ela vai ser interceptada.

O SR. DEPUTADO NELSON PELLEGRINO - Porque vai na origem da operadora?

O SR. RAIMUNDO PINHEIRO DE CASTRO VIERA JÚNIOR - Ela vai na operadora...

O SR. DEPUTADO NELSON PELLEGRINO - Quando ela sai da operadora, ela já está... Quando ele sai do aparelho, está criptografado, ou quando ele sai da operadora?

O SR. RAIMUNDO PINHEIRO DE CASTRO VIERA JÚNIOR - Veja, primeiro eu gostaria de explicar, voltar um pouquinho atrás, bem rápido, porque nós sabemos que o nosso tempo já está avançado. E a aqui, hoje, a história de quem ri por último não ri melhor, porque a gente acabou não tendo tanto tempo para poder fazer uma explicação. Mas estamos à disposição da Comissão, dos senhores, para contribuirmos sempre que for necessário. O que eu gostaria de enfatizar aqui é o seguinte, respondendo à pergunta de V.Exa. Que as demandas judiciais que resultam na solicitação de quebra de sigilo ou de interceptação do sigilo telefônico, quando no caso de os usuários utilizarem esse tipo de equipamento aqui — este nosso —, a interceptação vai existir, normal, eles vão gerar o grampo, e vão acessar tranqüilamente a conversação...

O SR. DEPUTADO NELSON PELLEGRINO - O conteúdo.

O SR. RAIMUNDO PINHEIRO DE CASTRO VIERA JÚNIOR - É, o conteúdo dela. Só que eles vão acessar e vão gravar uma transação telefônica criptografada. Então ela não será audível, ela não será decriptada.

O SR. DEPUTADO NELSON PELLEGRINO - Então, para entender: a partir do momento em que a minha fala sai desse aparelho, ela já sai criptografada?

O SR. RAIMUNDO PINHEIRO DE CASTRO VIERA JÚNIOR - Quando chega no outro... Ela já sai criptografada.

O SR. DEPUTADO NELSON PELLEGRINO - Não, só para entender: esse aparelho vai emitir um sinal para uma ERB, que é uma estação?

O SR. RAIMUNDO PINHEIRO DE CASTRO VIERA JÚNIOR - Exatamente, exatamente.

O SR. DEPUTADO NELSON PELLEGRINO - A ERB vai transmitir para a estação central, que, por sinal, vai transmitir para outra ERB em que o meu aparelho estiver?

O SR. RAIMUNDO PINHEIRO DE CASTRO VIERA JÚNIOR - Mas dentro do protocolo da transação de chaves públicas que foi gerado, que é um protocolo que protege.

O SR. DEPUTADO NELSON PELLEGRINO - Isso. Mas esse aparelho, pelo que eu estou entendendo, pela explicação, quando ele já emite a minha voz, ela já vai criptografada para a ERB; a ERB passa ela criptografada para a central; e a central passa criptografada para outra ERB, que o meu aparelho está na ponta, ele passa para esse aparelho, e o meu aparelho, que está na outra ponta, decodifica.

O SR. RAIMUNDO PINHEIRO DE CASTRO VIERA JÚNIOR - Exatamente.

O SR. DEPUTADO NELSON PELLEGRINO - Ele tem a capacidade de decodificar.

O SR. RAIMUNDO PINHEIRO DE CASTRO VIERA JÚNIOR - De decodificar.

O SR. DEPUTADO NELSON PELLEGRINO - Então, significa dizer que, pelo protocolo convencional, se eu tenho uma ordem de interceptação daquele aparelho celular, teoricamente a operadora não teria condições de...

O SR. RAIMUNDO PINHEIRO DE CASTRO VIERA JÚNIOR - Operacionalmente, não.

O SR. DEPUTADO NELSON PELLEGRINO - Ter audível o conteúdo daquela fala, porque ela está criptografada.

O SR. RAIMUNDO PINHEIRO DE CASTRO VIERA JÚNIOR - Exatamente.

O SR. DEPUTADO NELSON PELLEGRINO - Aí, como seria esse processo de cumprimento da ordem judicial?

O SR. RAIMUNDO PINHEIRO DE CASTRO VIERA JÚNIOR - Então, o processo...

O SR. DEPUTADO NELSON PELLEGRINO - Eu falo isso, Sr. Raimundo, pelo seguinte...

O SR. RAIMUNDO PINHEIRO DE CASTRO VIERA JÚNIOR - Entendi.

O SR. DEPUTADO NELSON PELLEGRINO - Porque a gente já discutiu, o sigilo telefônico está protegido pela Constituição.

O SR. RAIMUNDO PINHEIRO DE CASTRO VIERA JÚNIOR - Exatamente.

O SR. DEPUTADO NELSON PELLEGRINO - Mas a Constituição estabeleceu exceção, que é o caso de interceptação legal.

O SR. RAIMUNDO PINHEIRO DE CASTRO VIERA JÚNIOR - Com certeza.

O SR. DEPUTADO NELSON PELLEGRINO - Então, eu digo, porque esse aparelho está para garantir o seu direito constitucional de você não ser legalmente interceptado. Mas um traficante pode comprar um aparelho como esse, digamos assim, em tese.

O SR. RAIMUNDO PINHEIRO DE CASTRO VIERA JÚNIOR - Não. Sim, ele não pode comprar...

O SR. DEPUTADO NELSON PELLEGRINO - O criminoso pode até... poder que a Polícia Federal intercepte.

O SR. RAIMUNDO PINHEIRO DE CASTRO VIERA JÚNIOR - Ele pode até ter acesso a esse tipo de aparelho. Inclusive, foram 2 documentos que nós anexamos ao final desse parecer jurídico sobre a licitude do uso da criptografia. Nós anexamos, ao final, 2 termos de compromisso que são firmados com qualquer comprador desse telefone — que foi implementado, inclusive, por nós, por uma questão do cuidado justamente com essas questões todas legais, uma vez que a minha posição na empresa é a de regulatório e de relações institucionais. Então, nós, depois de conversarmos muito com várias pessoas e com vários juristas sobre essa questão, nos precavemos e, inclusive, comunicamos à ANATEL. Esse equipamento é homologado pela ANATEL, é importado e homologado pela ANATEL.

O SR. DEPUTADO NELSON PELLEGRINO - A importação, pelo que a gente viu, a ANATEL não interfere na importação.

O SR. RAIMUNDO PINHEIRO DE CASTRO VIEIRA JÚNIOR - Não.

O SR. DEPUTADO NELSON PELLEGRINO - Ela interfere na certificação para que ele possa ser utilizado pelo sistema.

O SR. RAIMUNDO PINHEIRO DE CASTRO VIEIRA JÚNIOR - No território nacional.

O SR. DEPUTADO NELSON PELLEGRINO - Então, ele só pode ser habilitado numa operadora se ele tiver sido certificado anteriormente pela ANATEL, aquele problema de banda, aquele negócio todo.

O SR. RAIMUNDO PINHEIRO DE CASTRO VIEIRA JÚNIOR - Exatamente. Por isso, ele tem o selo da ANATEL em todos os equipamentos. Voltando à sua pergunta...

O SR. DEPUTADO NELSON PELLEGRINO - Então, só para entender, todo usuário desse equipamento assina um contrato com a empresa...

O SR. RAIMUNDO PINHEIRO DE CASTRO VIEIRA JÚNIOR - É, um termo.

O SR. DEPUTADO NELSON PELLEGRINO - ... onde estão estabelecidas as condições que garantam não só o sigilo do conteúdo da conversa dele, excepcionando, em caso de interceptação legal, onde vocês estariam autorizados a quê? A fornecer o...

O SR. RAIMUNDO PINHEIRO DE CASTRO VIEIRA JÚNIOR - A desabilitar a função criptográfica dele.

O SR. DEPUTADO NELSON PELLEGRINO - Ah, entendi.

O SR. RAIMUNDO PINHEIRO DE CASTRO VIEIRA JÚNIOR - Entendeu? Então, a partir do momento...

O SR. DEPUTADO NELSON PELLEGRINO - Mas, aí, eu quero fazer uma pergunta também, só para entender. A partir do momento que vocês fazem essa desabilitação, é só para efeito da operadora, ou essa desabilitação permite que qualquer um possa interceptar, de forma ilegal?

O SR. RAIMUNDO PINHEIRO DE CASTRO VIEIRA JÚNIOR - Não, ele passa a ser, ele passa a ser...

O SR. DEPUTADO NELSON PELLEGRINO - Passa a ser um aparelho comum?

O SR. RAIMUNDO PINHEIRO DE CASTRO VIEIRA JÚNIOR - Ele passa a ser um aparelho comum, porque eu desabilitei a função do *software* de criptografia.

O SR. DEPUTADO NELSON PELLEGRINO - Então ele pode ser objeto de uma interceptação legal, como também uma ilegal, porque ele perdeu a função dele?

O SR. RAIMUNDO PINHEIRO DE CASTRO VIEIRA JÚNIOR - Exatamente, ele perdeu a função dele. Então ele vai ficar desprotegido, está certo? O que acontece nesse caso?

O SR. DEPUTADO NELSON PELLEGRINO - Contra interceptações legais e ilegais também.

O SR. RAIMUNDO PINHEIRO DE CASTRO VIEIRA JÚNIOR - E as ilegais também, porque as ilegais não tem como você controlar. Então o que acontece, Excelência? Esse *chip* de criptografia nos permite um controle, através do fabricante, para que nós possamos quebrar a função criptográfica dessa licença. Cada *chip* desse é comercializado e industrializado como um licença de *software*. E, quando ele é vendido, ele é vendido juntamente com o aparelho telefônico, exclusivamente, porque ele não tem aplicabilidade nem funcionalidade...

O SR. DEPUTADO NELSON PELLEGRINO - É o *chip* que é criptografado?

O SR. RAIMUNDO PINHEIRO DE CASTRO VIEIRA JÚNIOR - O *chip* é que é o sistema de criptografia.

O SR. DEPUTADO NELSON PELLEGRINO - Para poder evitar o clone, inclusive.

O SR. RAIMUNDO PINHEIRO DE CASTRO VIEIRA JÚNIOR - É. O aparelho tem o outro lado, que é o lado da interpretação, é o lado da decriptação. Então, esse microcomputadorzinho que tem aqui, esse *microchip* que tem aqui, ele é que processa, que entende e que gera todas as transações.

O SR. DEPUTADO NELSON PELLEGRINO - Certo. Bom, pelo que entendi também, a cada momento a chave muda o código dela?

O SR. RAIMUNDO PINHEIRO DE CASTRO VIEIRA JÚNIOR - Não, veja...

O SR. DEPUTADO NELSON PELLEGRINO - A cada ligação, ela vai mudando o código, para justamente evitar...

O SR. RAIMUNDO PINHEIRO DE CASTRO VIEIRA JÚNIOR - Exatamente. Enquanto V.Exa. digita um número e aperta o *send* da criptografia, ele vai gerar um protocolo de chaves públicas e vai trocar aquelas informações com a rede, para justamente preparar o ambiente de passagem da chamada criptográfica. Quando ele protege essa passagem, essa passagem natural, depois da transação da voz e tudo, ela é feita através de um sistema randômico de chaves. Então, ele pode utilizar todas as chaves ou 10 chaves ou 20 chaves do sistema de algoritmos dele dentro daquela transação telefônica, mas nunca se fará de forma repetitiva. Então, isso é o que faz com que a decriptação dele seja muito difícil. Não é impossível, obviamente.

O SR. DEPUTADO NELSON PELLEGRINO - Uma outra discussão que nós fizemos aqui com o técnico da ABIN é que ele disse que o CEPESC tinha desenvolvido uma solução de criptografia para a telefonia fixa e estava desenvolvendo uma para a telefonia celular.

O SR. RAIMUNDO PINHEIRO DE CASTRO VIEIRA JÚNIOR - PCP.

O SR. DEPUTADO NELSON PELLEGRINO - E a da telefonia fixa já estava sendo utilizada pelos órgãos públicos. E eu perguntei a ele se era muito cara essa solução. Digamos que a CPI recomendasse que as operadoras de telefonia fixa do Brasil passassem a adotar esse sistema como instrumento de proteção do sigilo dos seus clientes. Ele disse que não era tão caro assim, mas que podia ser oferecido um serviço como um *plus*, como o bina que algumas operadoras oferecem. Essa tecnologia hoje, quanto custaria, tanto para fixo quanto para celular?

O SR. RAIMUNDO PINHEIRO DE CASTRO VIEIRA JÚNIOR - Essa tecnologia hoje, o equipamento telefônico com o *software* de criptografia, na parte móvel, hoje está em torno de 3.500, 3.800 dólares, e o sistema Line Crypt, que é o do fixo, está em torno de 2.500 dólares.

O SR. DEPUTADO NELSON PELLEGRINO - Se tivesse volume de escala, isso poderia reduzir?

O SR. RAIMUNDO PINHEIRO DE CASTRO VIEIRA JÚNIOR - Sim, sim, sim.

O SR. DEPUTADO NELSON PELLEGRINO - Muito?

O SR. RAIMUNDO PINHEIRO DE CASTRO VIEIRA JÚNIOR - Significativamente, pelos aspectos da importação e dos impostos. Inclusive, se for uma venda institucional e o Estado for o comprador, o Estado pode perfeitamente diminuir a carga tributária ou até se isentar da carga tributária e nós virmos a praticar preços...

O SR. DEPUTADO NELSON PELLEGRINO - Mas digamos que fosse objeto das recomendações da Comissão Parlamentar de Inquérito, para garantir o sigilo telefônico constitucional, que as operadoras de telefonia fixa e as operadoras de telefonia móvel adotassem o sistema de criptografar as ligações, como um instrumento de dar segurança.

O SR. RAIMUNDO PINHEIRO DE CASTRO VIEIRA JÚNIOR - Bom, aí, seria um volume bastante grande, e isso dependeria, obviamente, nas questões

econômicas, do modelo do negócio desenhado. Se nós estivermos falando, por exemplo, num modelo de negócio em que a operadora vai fazer a aquisição dos equipamentos e vai disponibilizar aos seus assinantes, numa conta institucional, o que é bastante comum acontecer isso, a operadora dar o telefone, não esse, mas dar o telefone celular para o cliente que tem uma conta grande ou uma conta institucional, e, aí, ela vai cobrar pelos serviços diretos, prestados, inclusive vai poder cobrar um *plus* pela garantia da segurança de informações trafegadas naquela linha telefônica. Aí, nós estaríamos falando numa redução bastante significante, porque a compra seria um volume bastante significativo.

O SR. DEPUTADO NELSON PELLEGRINO - A informação que esse mesmo técnico da ABIN nos deu, ele usou uma figura de linguagem de que a relação entre a tecnologia e aqueles que querem quebrá-la é uma relação de gato e rato, se é que eu entendi isso, que as empresas criam a tecnologia hoje e, no mesmo dia, não é nem no dia seguinte, já começam estudos para tentar quebrá-la. Em algumas feiras internacionais até se oferecem equipamentos e tal, essa coisa toda. Entendeu? É como se aquele..., se você faz um vírus, e a empresa tem que estudar como combater aquele vírus eletrônico.

Do ponto de vista do estudo, em média, quanto tempo se leva para quebrar uma tecnologia dessa?

O SR. RAIMUNDO PINHEIRO DE CASTRO VIEIRA JÚNIOR - Eu já havia falado anteriormente, entre 15 e 17 anos. É a informação do fabricante, de que seria o tempo...

O SR. DEPUTADO NELSON PELLEGRINO - Qualquer código criptografado, a média para quebrar é essa?

O SR. RAIMUNDO PINHEIRO DE CASTRO VIEIRA JÚNIOR - Não, da tabela de algoritmos utilizada nessa tecnologia.

O SR. DEPUTADO NELSON PELLEGRINO - Essa tecnologia, o volume de tabela de algoritmos, as análises combinatórias levariam de 10 a 15 anos para decifrar aquele código?

O SR. RAIMUNDO PINHEIRO DE CASTRO VIEIRA JÚNIOR - Aproximadamente de 15 a 17 anos, entendeu?

O SR. DEPUTADO NELSON PELLEGRINO - Para conseguir decifrar aquele código, quebrar ele...

O SR. RAIMUNDO PINHEIRO DE CASTRO VIEIRA JÚNIOR - É, utilizar...

O SR. DEPUTADO NELSON PELLEGRINO - Para poder, a partir daí...

O SR. RAIMUNDO PINHEIRO DE CASTRO VIEIRA JÚNIOR - Exatamente.

O SR. DEPUTADO NELSON PELLEGRINO - ... poder ter um instrumental para poder tornar audível o conteúdo daquela...

O SR. RAIMUNDO PINHEIRO DE CASTRO VIEIRA JÚNIOR - Daquela transação que foi submetida ao processamento.

O SR. DEPUTADO NELSON PELLEGRINO - Isso é uma convenção internacional, essa é uma opinião internacionalmente... Digamos assim, é consensual isso ou tem questionamento em relação a essa informação?

O SR. RAIMUNDO PINHEIRO DE CASTRO VIEIRA JÚNIOR - Não, veja, é consensual dependendo do tipo das tabelas de algoritmos utilizadas no conjunto da criptografia, é o que vai dar realmente a facilidade de quebra ou não. Hoje nós temos, como o senhor mesmo citou, essa relação de gato e rato. Eu retorno a alguns minutos da minha palavra aqui para repetir a questão da notoriedade da compra de equipamentos criptografados ou de proteção de dados ou até mesmo de voz, como é o nosso caso. Ela desperta, imediatamente, quando o mercado, vamos dizer assim, de quebra desses protocolos se aguça, imediatamente, quando ele toma conhecimento, ele se aguça e ele começa a pôr os *hackers* dele para trabalhar, porque eles têm que quebrar, têm que quebrar, têm que quebrar. E acontece que eles quebram, sim.

O SR. DEPUTADO NELSON PELLEGRINO - Mas, em média, isso acontece em quanto tempo?

O SR. RAIMUNDO PINHEIRO DE CASTRO VIEIRA JÚNIOR - Para os *hackers*, dentro do que nós vemos diariamente, pode acontecer a qualquer instante. Essa relação temporal não existe mensurada...

O SR. DEPUTADO NELSON PELLEGRINO - Então, essa tecnologia, o *hacker* pode começar a estudar hoje...

O SR. RAIMUNDO PINHEIRO DE CASTRO VIEIRA JÚNIOR - Qualquer tecnologia.

O SR. DEPUTADO NELSON PELLEGRINO - Então, esse código de criptografia pode ser quebrado?

O SR. RAIMUNDO PINHEIRO DE CASTRO VIEIRA JÚNIOR - Pode, sim senhor. Nós temos, na história dos *hackers*, invasões a complexos superimportantes de...

O SR. DEPUTADO NELSON PELLEGRINO - E todos têm um código criptografado de defesa?

O SR. RAIMUNDO PINHEIRO DE CASTRO VIEIRA JÚNIOR - Todos têm o código criptografado de defesa. Por exemplo, a NASA já recebeu várias invasões, inclusive por *hackers* brasileiros, que são os mais temidos no mercado internacional, e os *hackers* russos, hoje. Então, esses 2, brasileiros e russos, são *experts* em quebra de qualquer sistema, tanto faz ser da Microsoft, um Windows Vista e tudo. O cara pega uma cópia, vai lá e cria uma coisa que chamamos de *cracking*, ele vai fazer o crackeamento com uma quebra daquela chave criptografada de acesso, e ele torna cópias piratas regulares, oficiais, e o sistema reconhece como oficiais. E, então, milhares e milhares de computadores hoje no mundo têm programas não legais instalados, a exemplo aqui do Brasil, em que nós temos, em qualquer esquina, qualquer técnico de computador tem 10 discos de CD, com 10 programas, e ele oferece gratuitamente ou por qualquer cruzeiro. Então, essa questão é uma questão difícil de se afirmar. Ela pode acontecer a qualquer instante, mas, por meio da tecnologia hoje, nós temos a quebra dela, e esse produto está conosco no mercado há praticamente um ano. E os testes que a gente vem fazendo, inclusive o próprio fabricante, porque tem muita vontade de entrar no mercado brasileiro, tem patrocinado lá fora a submissão dessa tecnologia a diversos tipos de sistema de quebra, e ninguém conseguiu quebrar...

O SR. DEPUTADO NELSON PELLEGRINO - Ou seja, até hoje... Essa tecnologia tem quanto tempo já desenvolvida?

O SR. RAIMUNDO PINHEIRO DE CASTRO VIEIRA JÚNIOR - Essa tecnologia tem 6 anos.

O SR. DEPUTADO NELSON PELLEGRINO - Seis anos. Nesses 6 anos ela foi quebrada? Tem registro de quebra?

O SR. RAIMUNDO PINHEIRO DE CASTRO VIEIRA JÚNIOR - Não, não tem registro de quebra.

O SR. DEPUTADO NELSON PELLEGRINO - Quantos aparelhos hoje licenciados no Brasil?

O SR. RAIMUNDO PINHEIRO DE CASTRO VIEIRA JÚNIOR - Licenciados no Brasil, nós temos uma população pequena, temos cerca de 40, 50 equipamentos.

O SR. DEPUTADO NELSON PELLEGRINO - E tudo privado? Não tem nada do Poder Público?

O SR. RAIMUNDO PINHEIRO DE CASTRO VIEIRA JÚNIOR - Tudo privado, tudo privado. O perfil do usuário desse equipamento é o mercado financeiro. Aliás, eu gostaria de explanar aqui, em 1 minuto só, que essa tecnologia teve origem por uma necessidade de uma instituição financeira bastante conhecida no mundo inteiro, que é o Deutsche Bank, de proteger as transações bancárias com os seus clientes corporativos, que movimentavam, através de mesas de operações de aplicação e tudo, movimentavam cifras bilionárias entre os mercados, as bolsas financeiras da Europa, dos Estados Unidos e tudo, e precisavam ter um critério de segurança para o comando dessas operações. E ele disponibilizou essa tecnologia, mandou produzir essa tecnologia, para colocar à disposição dos seus clientes. Foi o primeiro exercício da utilização de protocolos de criptografia para o mercado corporativo, ou seja, para o mercado privado, que não fossem as comunidades de inteligência e contra-inteligência, que eram os que usavam exclusivamente.

O SR. DEPUTADO NELSON PELLEGRINO - Pela exposição de V.Sa., eu entendi que nem todos as operadoras conseguem...

O SR. RAIMUNDO PINHEIRO DE CASTRO VIEIRA JÚNIOR - É, nem todas as operadoras conseguem manter esse padrão tecnológico que garanta uma perfeita...

O SR. DEPUTADO NELSON PELLEGRINO - Que possa transitar no sistema.

O SR. RAIMUNDO PINHEIRO DE CASTRO VIEIRA JÚNIOR - Exatamente, mas existem duas aqui no Brasil que... nós já como distribuidores, e eu na qualidade de relações institucionais, já fizemos algumas reuniões e já conseguimos com que eles se comprometessem conosco de manter um padrão tecnológico alinhado à necessidade da tecnologia.

O SR. DEPUTADO NELSON PELLEGRINO - Sr. Presidente, eu me dou por satisfeito. Queria agradecer as contribuições do Sr. Raimundo Castro.

O SR. PRESIDENTE (Deputado Paulo Abi-Ackel) - Com a palavra o ilustre Deputado, participativo, Deputado Jorginho Maluly, autor do requerimento.

O SR. DEPUTADO JORGINHO MALULY - Sr. Presidente Paulo Abi-Ackel, nobre Relator, Dr. Raimundo, pela hora, já são 21h10min, estamos aqui desde às 15h aproximadamente, são 6 horas de CPI, todos estão cansados....

O SR. RAIMUNDO PINHEIRO DE CASTRO VIEIRA JÚNIOR - Eu estou aqui desde o meio-dia.

O SR. DEPUTADO JORGINHO MALULY - Eu, na verdade, saí da minha casa às 5h da manhã para pegar o avião.

O SR. RAIMUNDO PINHEIRO DE CASTRO VIEIRA JÚNIOR - Imagino, pegou o avião.

O SR. DEPUTADO JORGINHO MALULY - Eu moro no interior de São Paulo, até chegar aqui. Tanto é que os heróis aqui ficaram eu, o Relator, por obrigação do ofício; eu, autor do requerimento, e o Paulinho, por carinho e consideração conosco, está aí nos prestigiando, além do interesse que tem. E os funcionários, que são obrigados a ficar, mas acho que devem ter uma horinha extra aí para poder... Não tem não? Então, danou-se. Mas então, vamos ser direto, curto e grosso.

O SR. RAIMUNDO PINHEIRO DE CASTRO VIEIRA JÚNIOR - Pois não.

O SR. DEPUTADO JORGINHO MALULY - Primeiro, obrigado pela sua presença aqui atendendo ao nosso convite.

Queria que o senhor falasse em concorrência, quem são seus concorrentes no Brasil, se é que existe o principal concorrente, alternativas, se existe outra alternativa dessas tecnologias. O senhor já disse que está aqui no Brasil há um ano, se eu não entendi errado, há um ano.

O SR. RAIMUNDO PINHEIRO DE CASTRO VIEIRA JÚNIOR - Exatamente.

O SR. DEPUTADO JORGINHO MALULY - Um ano?

O SR. RAIMUNDO PINHEIRO DE CASTRO VIEIRA JÚNIOR - Cerca de um ano.

O SR. DEPUTADO JORGINHO MALULY - O senhor disse que custa de 3,8 mil dólares aproximadamente o móvel e 2,5 mil o fixo, era uma pergunta que eu ia fazer. Eu ia perguntar quanto, o senhor disse que tem por volta de 40 apenas.

O SR. RAIMUNDO PINHEIRO DE CASTRO VIEIRA JÚNIOR - É.

O SR. DEPUTADO JORGINHO MALULY - Acho que é pouquíssimo.

O SR. RAIMUNDO PINHEIRO DE CASTRO VIEIRA JÚNIOR - Comercializados até hoje é pouquíssimo.

O SR. DEPUTADO JORGINHO MALULY - Deveríamos fazer isso crescer.

Queria que o senhor falasse um pouquinho mais dos critérios na venda dos seus clientes e se o senhor já desabilitou alguém nesse período que o senhor está aqui, dentro desse compromisso aqui assumido, se o senhor já teve que ser, vamos dizer assim, indelicado ou teve que agir no sentido de atacar o mau uso da sua tecnologia.

No mais, eu agradeço. Eu acho que é importante ter esse instrumento de proteção a essa devassa que é feita na vida do brasileira hoje. Ninguém está seguro mais para nada. Espero realmente que isso se popularize um pouco mais e que possa ter um acesso melhor, mais amplo. Por exemplo, acho que a PETROBRAS deve utilizar-se desse tipo de tecnologia. Estamos falando de poços e poços de petróleo cada vez mais sendo descobertos. Se existe alguma coisa nesse sentido em termos de troca de *e-mail*, de arquivo de computador, nesse sigilo.

O SR. RAIMUNDO PINHEIRO DE CASTRO VIEIRA JÚNIOR - Existe.

O SR. DEPUTADO JORGINHO MALULY - Se o senhor puder tocar um pouco rapidamente para não se estender demais. Isso aí pela moda que roubaram os *notebooks* da PETROBRAS, com informações valiosíssimas.

Enfim, acho que esse é o caminho. E eu me dou por satisfeito, quando eu o convidei para vir aqui. E o deixo à vontade para comentar alguma coisa rapidamente nesse sentido, mas eu estou bem satisfeito e agradeço.

Obrigado, Sr. Presidente.

O SR. PRESIDENTE (Deputado Paulo Abi-Ackel) - Parabenizando os trabalhos da CPI e agradecendo ao depoente pela grande colaboração que prestou nesta noite e pedindo desculpa pela hora já avançada, nada mais havendo a tratar...

(Intervenção fora do microfone. Inaudível.)

O SR. PRESIDENTE (Deputado Paulo Abi-Ackel) - Desculpe, meu caro Deputado, parece que o senhor tem alguma solicitação para esclarecimento...

O SR. DEPUTADO JORGINHO MALULY - Não, eu só queria que ele dissesse, pelo que o Relator comentou, esse termo de compromisso, se ele já se utilizou alguma vez para desabilitar alguém. Acho que seria importante, já que são tão poucos. E um pouquinho mais: se eles fazem uma peneira bem criteriosa para vender. No mais era só isso, Sr. Presidente. Eu também me dou por satisfeito.

O SR. PRESIDENTE (Deputado Paulo Abi-Ackel) - Com a palavra o depoente.

O SR. DEPUTADO NELSON PELLEGRINO - Pode fazer uma resposta genérica. Pode dizer já teve uns 2 ou 3, não precisa dizer quem foi o cliente, entendeu? E a outra pergunta era sobre...

(Intervenção fora do microfone. Inaudível.)

O SR. DEPUTADO NELSON PELLEGRINO - Ah, sim.

O SR. PRESIDENTE (Deputado Paulo Abi-Ackel) - Com a palavra o depoente.

O SR. RAIMUNDO PINHEIRO DE CASTRO VIEIRA JÚNIOR - Muito obrigado, Sr. Presidente, nobre Deputado Jorginho Maluly, a quem eu gostaria de agradecer imensamente pela oportunidade que nos está sendo dada, V.Exa. traz, no seu histórico genético familiar, uma existência nesta Casa nobre participação...

O SR. DEPUTADO JORGINHO MALULY - Com muito orgulho.

O SR. RAIMUNDO PINHEIRO DE CASTRO VIEIRA JÚNIOR - Muito orgulho.

O SR. DEPUTADO JORGINHO MALULY - Como o Deputado Paulo Abi-Ackel da mesma maneira.

O SR. RAIMUNDO PINHEIRO DE CASTRO VIEIRA JÚNIOR - Com certeza. A quem inclusive admiro e sou amigo pessoal do pai dele, entendeu?

O SR. PRESIDENTE (Deputado Paulo Abi-Ackel) - Muito obrigado, muito obrigado, Deputado.

O SR. RAIMUNDO PINHEIRO DE CASTRO VIEIRA JÚNIOR - De maneira que responderei às suas perguntas da seguinte forma: primeiro, nós já tivemos necessidade de desabilitar, sim, uma licença. Uma licença de um profissional executivo, de uma estrutura financeira grande, que, viajando, teve perdido ou seja

roubado, não sei, o seu equipamento. E ele entrou em comunicação conosco, e nós tivemos que proceder à desabilitação. E esse processo todo, entre nós recebermos a comunicação dele e entrarmos em contato com o fabricante, e o fabricante queimar o *chip* dele lá, foi de aproximadamente 6 horas, considerando os fusos horários entre a Inglaterra, que é o escritório, o *general office* da Tresor, que, embora seja alemã, comercializa tudo através da Inglaterra. Então, essa primeira questão já respondida. Segundo lugar, a dificuldade que encontramos hoje junto às organizações que são organizações institucionais públicas ou de economia mista, é justamente o critério da legislação, da 8.666, que não prevê a aquisição de equipamentos de segurança, salvo algumas instituições que tenham o benefício da legislação específica, da aquisição de equipamentos para a questão da segurança nacional. E daí estamos falando exclusivamente da Presidência da República, da ABIN, da própria Polícia Federal, que teriam condição talvez, acredito eu, de utilizar essa legislação como embasamento da aquisição de tecnologias dessa natureza. Portanto, as visitas que já fizemos tanto institucionalmente quanto comercialmente com o nosso pessoal da área comercial junto a PETROBRAS e outros organismos do Governo, em todas elas morreram a expectativa de conclusão da negociação justamente pela necessidade de se dar a publicidade da compra, mesmo que fosse num processo licitatório, porque temos concorrentes, sim. O nosso concorrente principal que tem o equipamento dessa natureza e que custa bem mais caro chama-se Rohde & Schwarz. A Rohde & Schwarz é uma empresa que fornece equipamentos desde o SIVAM até o centro de tecnologia de guerra eletrônica do Exército brasileiro.

O SR. DEPUTADO NELSON PELLEGRINO - A Siemens fabrica esse equipamento também?

O SR. RAIMUNDO PINHEIRO DE CASTRO VIEIRA JÚNIOR - Quem?

O SR. DEPUTADO NELSON PELLEGRINO - A Siemens.

O SR. RAIMUNDO PINHEIRO DE CASTRO VIEIRA JÚNIOR - A Siemens não. Embora a plataforma dele seja Siemens. A plataforma do telefone é Siemens, mas a Siemens não fabrica esse...

O SR. DEPUTADO NELSON PELLEGRINO - Ela só fornece a plataforma.

O SR. RAIMUNDO PINHEIRO DE CASTRO VIEIRA JÚNIOR - Ela só fornece a plataforma, só componentes. Então, a Rohde & Schwarz é um dos nossos concorrentes, mas existem análises por parte de autoridades até da própria inteligência de que todo sistema criptografado deve manter um nível de segurança quanto à proteção do grupo de algoritmos que compõem as chaves da criptografia utilizada no sistema ou naquela tecnologia. E essa guarda dessas informações é chamada de *back door*. Então, por exemplo, a maioria das agências de inteligência dos países tem a informação de componentes algoritmos como o *back door* de tecnologias dessa natureza. Então, por exemplo, no caso de um outro estado estrangeiro vir a utilizar uma tecnologia fabricada por exemplo, pela Rohde & Schwarz. A Rohde & Schwarz depositou as coordenadas todas tecnológicas de composição algoritma da tecnologia criptografada dele na agência de inteligência dos Estados Unidos. Então, é provável que uma comunicação entre um Chefe de Estado do Equador ou que seja do Brasil, entendeu, possa ser decriptada imediatamente por conta dessa informação, desse *back door*, que dá a fragilidade do sistema. Alguns especialistas que analisaram a nossa tecnologia aqui no Brasil nos asseguraram que, dada essa forma randômica utilizada, garantiram-nos, o fabricante garante isso inclusive por escrito nos nossos contratos, esse tempo para que fosse decriptado e nos garantem também que, como o processo é aleatório, eles não têm como depositar essas informações.

O SR. DEPUTADO NELSON PELLEGRINO - Só para efeito de compreensão, não é minha especialidade, mas o técnico da ABIN disse que eles tinham desenvolvido um sistema próprio brasileiro.

O SR. RAIMUNDO PINHEIRO DE CASTRO VIEIRA JÚNIOR- Sim.

O SR. DEPUTADO NELSON PELLEGRINO - Eles tinham feito um sistema próprio. Estava desenvolvido para telefonia fixa e estava desenvolvido para telefonia celular. É evidente que essas ligações serão feitas pelo Presidente da República, essas ligações serão feitas pelos Ministros de Estado e envolvem um conteúdo de segurança nacional.

O SR. RAIMUNDO PINHEIRO DE CASTRO VIEIRA JÚNIOR - Com certeza.

O SR. DEPUTADO NELSON PELLEGRINO - Pelo que estou entendendo, a sede da empresa detém o código.

O SR. RAIMUNDO PINHEIRO DE CASTRO VIEIRA JÚNIOR - A sede da empresa?

O SR. DEPUTADO NELSON PELLEGRINO - Detém, digamos assim, as informações que permitem a quebra do sistema.

O SR. RAIMUNDO PINHEIRO DE CASTRO VIEIRA JÚNIOR - Em alguns....

O SR. DEPUTADO NELSON PELLEGRINO - Então, o Estado brasileiro adquirir uma tecnologia dessa, como a tecnologia mãe é produzida fora do País, qual a segurança que o Estado brasileiro teria de saber que uma empresa estrangeira que é detentora...

O SR. RAIMUNDO PINHEIRO DE CASTRO VIEIRA JÚNIOR - Exatamente.

O SR. DEPUTADO NELSON PELLEGRINO - Ou seja, se essa empresa poderia desenvolver, digamos assim, uma solução que fosse sob o controle...

O SR. RAIMUNDO PINHEIRO DE CASTRO VIEIRA JÚNIOR - Personalizada.

O SR. DEPUTADO NELSON PELLEGRINO - Isso.

O SR. RAIMUNDO PINHEIRO DE CASTRO VIEIRA JÚNIOR - É possível sim.

O SR. DEPUTADO NELSON PELLEGRINO - Que ela mesma não tivesse informação, que ela não tivesse condição de quebrar, a não ser...

O SR. RAIMUNDO PINHEIRO DE CASTRO VIEIRA JÚNIOR - Exatamente, exatamente. E nesse caso específico, ela própria, como fabricante, embora ela tenha informação das chaves que ela criou e colocou aqui dentro, ela não tem o controle da..

O SR. DEPUTADO NELSON PELLEGRINO - Da combinação.

O SR. RAIMUNDO PINHEIRO DE CASTRO VIEIRA JÚNIOR - Das combinações e das mutações que ela sofre.

O SR. DEPUTADO NELSON PELLEGRINO - Então, a única forma de quebrar é retirando a ...

O SR. RAIMUNDO PINHEIRO DE CASTRO VIEIRA JÚNIOR - É submeter ao processamento em grandes computadores e aguardar até ter... Então, eles fizeram essa tecnologia sem o tal do *back door*, está entendendo?

O SR. DEPUTADO NELSON PELLEGRINO - Agora, o Deputado Jorginho Maluly fez uma pergunta. Não precisa determinar quem foi, mas já teve caso de alguma autoridade brasileira pedir para suspender a criptografia para poder interceptar?

O SR. RAIMUNDO PINHEIRO DE CASTRO VIEIRA JÚNIOR - Não, ainda não. Ainda não.

O SR. DEPUTADO NELSON PELLEGRINO - Não tem nenhum caso?

O SR. RAIMUNDO PINHEIRO DE CASTRO VIEIRA JÚNIOR - Até porque dado ao nosso próprio perfil, que acredito que é bastante visível, nós nos preocupamos muito com essa questão de quem é que vai utilizar a tecnologia nossa, quem é que vai comprar, entendeu? Isso não impede que, por exemplo, um diretor de bancos tenha ligações criminosas com qualquer segmento do crime organizado e ele adquire em nome do banco que seja um banco de bastante idoneidade, que não esteja sob suspeita de nada, e amanhã esse telefone esteja sendo utilizado por um, não digo...

O SR. DEPUTADO NELSON PELLEGRINO - Alguém que tá lavando dinheiro.

O SR. RAIMUNDO PINHEIRO DE CASTRO VIEIRA JÚNIOR - Não digo um marginal de baixo calão, mas...

O SR. DEPUTADO NELSON PELLEGRINO - Não, alguém que pode lavar dinheiro.

O SR. RAIMUNDO PINHEIRO DE CASTRO VIEIRA JÚNIOR - Esteja ocultando transações ilegais, esteja...

O SR. DEPUTADO NELSON PELLEGRINO - Lavagem de dinheiro

O SR. DEPUTADO JORGINHO MALULY - Futebol.

O SR. RAIMUNDO PINHEIRO DE CASTRO VIEIRA JÚNIOR - Futebol, né, Deputado?

O SR. DEPUTADO NELSON PELLEGRINO - Lavagem de dinheiro, pode ter algum executivo de um banco da área financeira que esteja lavando dinheiro para alguém.

O SR. RAIMUNDO PINHEIRO DE CASTRO VIEIRA JÚNIOR - Exatamente. De qualquer forma, ele tem esse critério, ele tem... critério não, desculpe, ele tem esse perfil de dar essa proteção dúbia.

O SR. DEPUTADO NELSON PELLEGRINO - Então, é um equipamento que, digamos assim, teria um filtro, não é qualquer um que pode adquirir.

O SR. RAIMUNDO PINHEIRO DE CASTRO VIEIRA JÚNIOR - Não, nós não vendemos para qualquer um.

O SR. DEPUTADO NELSON PELLEGRINO - É uma política da empresa não vender para qualquer um.

O SR. RAIMUNDO PINHEIRO DE CASTRO VIEIRA JÚNIOR - É uma política...

O SR. DEPUTADO NELSON PELLEGRINO- Não é um equipamento que está livremente para o marcado, não é qualquer um que pode comprar.

O SR. RAIMUNDO PINHEIRO DE CASTRO VIEIRA JÚNIOR - É uma política da empresa, é uma política minha, enquanto pessoa física, que descendo de uma linhagem militar muito patriota, entendeu, e muito conhecedora. Somos uma família de juristas, advogados, juízes e procuradores, entendeu? E nós temos muito critério quanto a essa questão da manutenção da licitude nos nossos atos. E eu, como diretor da empresa, embora não seja sócio, eu jamais permitiria que houvesse um envolvimento de qualquer tipo de ilicitude dessa natureza. Então, nós somos muito criteriosos na análise prévia que nós fazemos, e fazemos isso com bastante critério mesmo, entendeu? Nós não vamos atrás de questões creditícias, de SPC, de SERASA, não sei o quê, mas nós vamos atrás... E inclusive temos hoje no mercado "n" empresas que prestam esses serviços de análise de riscos não só financeiros, mas de riscos operacionais e até mesmo criminosos. E a gente se vale dessas informações, desse levantamento.

O SR. DEPUTADO JORGINHO MALULY - Só queria deixar registrado que eu acho muito pouco 40 aparelhos. Mesmo que o Governo não compre, o Brasil tem pelo menos 200 empresas de grande porte que devem ter seus interesses preservados em licitações, pesquisa.

O SR. RAIMUNDO PINHEIRO DE CASTRO VIEIRA JÚNIOR - Com certeza.

O SR. DEPUTADO JORGINHO MALULY - Enfim, eu fico surpreso com esse número. Pensei que era... tinha certeza que eram poucos, mas não na ordem das dezenas. Eu pensei que fosse na ordem das centenas.

O SR. RAIMUNDO PINHEIRO DE CASTRO VIEIRA JÚNIOR - É. O que eu poderia afirmar para o senhor, Deputado, é que nós estamos trabalhando junto ao nosso pessoal de vendas para que essa cultura venha a ser, dentro do menor espaço de tempo, amplificada, para que realmente esse tipo de criptografia, de tecnologias de proteção da informação, dentro do critério hoje universal da segurança da informação, possa estar presente realmente na vida do empresário brasileiro.

O SR. DEPUTADO JORGINHO MALULY - O que me causa estranheza, por exemplo, os depoimentos hoje, aqui mesmo, que tem equipamentos que fazem a escuta, estão na contramão, que custam de 3 a 5 milhões e são comprados sem licitação.

O SR. RAIMUNDO PINHEIRO DE CASTRO VIEIRA JÚNIOR - E são comprados sem licitação.

O SR. DEPUTADO JORGINHO MALULY - Você vai comprar 50 aparelhos de 3 mil dólares, são 150 mil dólares.

O SR. RAIMUNDO PINHEIRO DE CASTRO VIEIRA JÚNIOR - Deputado, só...

O SR. DEPUTADO JORGINHO MALULY - É 10% desse valor aí.

O SR. RAIMUNDO PINHEIRO DE CASTRO VIEIRA JÚNIOR - Só uma conjectura. Nós temos hoje um critério cultural, mutante, porque temos visto aí os nossos conceitos todos da nossa vida social estarem sempre aceitando, se flexionando ou enrijecendo, entendeu, diante de determinadas circunstâncias. E a questão da segurança e da proteção da informação hoje é vista, primeiro, com um impacto primeiro pelo lado do mal: você sempre vai querer proteger uma informação porque ela é oriunda...

O SR. DEPUTADO JORGINHO MALULY - De ato ilícito.

O SR. RAIMUNDO PINHEIRO DE CASTRO VIEIRA JÚNIOR - ...de ato ilícito. O Parlamentar, que é um representante do povo, não tem o direito social, embora ele tenha todas as prerrogativas para ter a necessidade da proteção das

informações dele, porque ele trabalha com informações que são estratégicas, são informações de Estado, e ele utiliza uma tecnologia dessa, e é publicado na imprensa que ele a está utilizando...

O SR. DEPUTADO JORGINHO MALULY - Está morto.

O SR. RAIMUNDO PINHEIRO DE CASTRO VIEIRA JÚNIOR - ...está morto: *"Está se escondendo, está roubando, está fazendo isso, está matando..."*, entendeu. Infelizmente.

O SR. DEPUTADO JORGINHO MALULY - Nós estamos muito desvalorizados e desrespeitados.

O SR. RAIMUNDO PINHEIRO DE CASTRO VIEIRA JÚNIOR - Infelizmente, a imagem...

O SR. DEPUTADO JORGINHO MALULY - Esse é um desafio nosso.

O SR. RAIMUNDO PINHEIRO DE CASTRO VIEIRA JÚNIOR - A imagem requer realmente esse desafio. E eu tenho certeza de que V.Exas., que são portadores de uma herança genética bastante honrosa, vão saber dar uma boa solução a essa questão, legislando para que venha ser viável e ser realmente possível, entendeu, essa proteção da informação. Muito obrigado a todos.

O SR. PRESIDENTE (Deputado Paulo Abi-Ackel) - O Deputado Relator tem alguma pergunta mais a fazer?

O SR. DEPUTADO NELSON PELLEGRINO - Eu queria elogiar o Deputado Jorginho Maluly, seu requerimento permitiu dar uma contribuição significativa a esta Comissão Parlamentar de Inquérito. Tenho certeza de que o conteúdo das informações foram muito importantes para termos uma compreensão melhor. Isso seguramente vai interferir no meu relatório.

Hoje foi um dia meio prejudicado, mas tudo que foi aqui objeto de depoimento está sendo gravado, vai ser depois taquigrafado, vai servir de base para o relatório.

Agradeço as contribuições do Sr. Raimundo Castro. Foram contribuições importantes. Trouxeram contribuições inclusive adicionais, algumas questões que poderão constar do nosso relatório. Os elementos que foram trazidos nesta tarde foram importantes na convicção do Relator.

Muito obrigado.

O SR. PRESIDENTE (Deputado Paulo Abi-Ackel) - Deputado Jorginho Maluly, mais alguma consideração a fazer?

O SR. DEPUTADO JORGINHO MALULY - Não, Presidente, pode encerrar.

O SR. PRESIDENTE (Deputado Paulo Abi-Ackel) - Não havendo mais nada a tratar, prestando as minhas homenagens e agradecendo a presença ao Dr. Raimundo Pinheiro de Castro Vieira Júnior e sua importante contribuição a esta CPI, estou encerrando os trabalhos, antes convocando os Srs. Deputados para a próxima reunião ordinária a realizar-se amanhã, dia 05 de março, às 14h30min, no Plenário nº 11, do Anexo II, para tomada de depoimento dos senhores: Dr. Mozart Valadares Pires, Presidente da Associação dos Magistrados Brasileiro; Dr. Walter Nunes da Silva Júnior, Presidente da Associação dos Juízes Federais do Brasil; Dr. Antônio Carlos Alpino Bigonha, Presidente da Associação Nacional dos Procuradores da República; Dr. José Carlos Consenzo, Presidente da Associação Nacional dos Membros do Ministério Público.

Em nome do Presidente, agradeço aos Srs. Relatores, Sr. Deputado, senhores funcionários da Comissão, senhor depoente.

Está encerrada a presente reunião.