

# O protagonismo dos sistemas de tecnologia da informação na interceptação telefônica: a importância da cadeia de custódia<sup>1</sup>

*The protagonism of information technology systems in telephone interception: the importance of the chain of custody*

## **Antonio Eduardo Ramires Santoro<sup>2</sup>**

Professor Universidade Federal do Rio de Janeiro, IBMEC/RJ e Universidade Católica de Petrópolis – Rio de Janeiro/RJ. Doutor pela UFRJ  
antoniosantoro@antoniosantoro.com.br  
 lattes.cnpq.br/9190879263950156 |  orcid.org/0000-0003-4485-844X

## **Natália Lucero Frias Tavares<sup>3</sup>**

Mestranda em Direito na Universidade Católica de Petrópolis – Petrópolis/RJ. Bolsista CAPES.  
natalialuceroadv@gmail.com  
 lattes.cnpq.br/0410822851348833 |  orcid.org/0000-0002-0153-1298

## **Jefferson de Carvalho Gomes<sup>4</sup>**

Mestrando em Direito na Universidade Católica de Petrópolis – Petrópolis/RJ  
jefferson.gomes@me.com  
 lattes.cnpq.br/6557505957098162 |  orcid.org/0000-0003-0491-0397

<sup>1</sup> Versão revista e ampliada, com a introdução de pesquisa empírica, de trabalho publicado nos Anais do I Encontro de Internacionalização do CONPEDI – Barcelona – 2014. Disponível em: <<http://www.conpedi.org.br/wp-content/uploads/2016/01/NOVO-Miolo-CONPEDI-vol-15-em-moldes-gráficos-1-1.pdf>>. Acesso em: 30 abr. 2017.

<sup>2</sup> Professor Titular de Direito Processual Penal do IBMEC/RJ. Professor Adjunto de Direito Processual Penal e Prática Penal da Faculdade Nacional de Direito da Universidade Federal do Rio de Janeiro - FND/UFRJ. Professor Adjunto do Programa de Pós-Graduação em Direito (Mestrado) da Universidade Católica de Petrópolis - UCP. Coordenador do Grupo de Pesquisa “O Sistema Penal sob Olhar Crítico” da UFRJ/UCP. Pós-Doutor em Direito Penal e Garantias Constitucionais pela Universidad Nacional de La Matanza - Argentina. Doutor e Mestre em Filosofia pela UFRJ. Mestre em Direito Penal Internacional pela Universidad de Granada - Espanha. Especialista em Direito Penal Econômico pela Universidade de Coimbra - Portugal. Especialista em Direito da Economia pela Fundação Getúlio Vargas. Graduado em Direito pela UERJ. Licenciando em História pela UNIRIO. Advogado criminalista.

<sup>3</sup> Mestranda em Direito da Universidade Católica de Petrópolis. Bolsista CAPES. Pós-graduada em Direito e Processo Penal e Criminologia pela Universidade Cândido Mendes (2014) e graduada em Direito pela Universidade do Estado do Rio de Janeiro (2011). Advogada criminalista e pesquisadora do Grupo de Pesquisa “O Sistema Penal sob Olhar Crítico” da UFRJ/UCP.

<sup>4</sup> Mestrando em Direito pela Universidade Católica de Petrópolis (UCP). Especialista em Criminologia, Direito e Processo Penal pela Universidade Cândido Mendes (UCAM). Bacharel em Direito pela Universidade Estácio de Sá (UNESA).

---

**RESUMO:** As mudanças tecnológicas levaram ao processo penal novas formas de obtenção de informações, dentre elas, a interceptação das comunicações telefônicas. A Lei nº 9.296/96 introduziu, nesse subsistema probatório, novos atores, que não existiam no sistema penal tradicional, os quais interferem diretamente na produção da informação valorável pelo julgador. A lei é silente quanto à forma de execução da medida, bem como do rastreamento da informação, relegando tal tarefa às empresas de tecnologia da informação. Temendo os riscos associados a uma possível produção de evidências defeituosas, o presente trabalho versa sobre a importância da cadeia de custódia como garantia de rastreabilidade e fiabilidade. Com o intuito de conhecer o rito para obtenção da informação por meio da interceptação telefônica e da constatação a respeito de sua idoneidade, aliou-se um estudo teórico-bibliográfico à análise dos dados sobre esse meio de obtenção de prova fornecidos pelo CNJ, seguida de análise dos sistemas de tecnologia da informação desenvolvidos para execução da medida de interceptação das comunicações.

**PALAVRAS-CHAVE:** interceptação das comunicações; meios de obtenção de prova atípicos; sistemas de tecnologia da informação; cadeia de custódia; sistemas guardião e vigia.

**ABSTRACT:** *Due to technological advances, new means of obtaining information have been brought up to the field of criminal procedure, among them, the interception of telephone communication. Law 9.296/96 has introduced new actors on to the probative subsystem that play a direct part on the production/gathering of information that may be taken in consideration by the judge. The inexistence of proper procedural regulation that delimitates the manner in which such investigation must be carried out, the defense finds grave difficulty to try and trace the source of the proof. Fearing the risks associated with the production of defective evidence, the present study focuses on the importance of the chain of custody as a mean to track and assure the reliability of set information. With the purpose of knowing the rite to obtain the data through telephone interception and the verifying its credibility, a theoretical-bibliographic study was carried out and combined with an analysis of the statistics on means of investigation of proof provided by the CNJ and, finally, followed by an analysis of the technology systems developed to carry out the interception of communications measure.*

**KEYWORDS:** *telephone interception; atypical means of obtaining evidence; IT companies; chain of custody; surveillance system.*

**SUMÁRIO:** Introdução; 1. Terminologias da prova: interceptação telefônica como meio de obtenção de prova atípico; 2. A inter-

venção do CNJ na regulação, controle e elaboração de estatísticas a respeito do sobreuso da interceptação telefônica no Brasil: onde está a cadeia de custódia?; 3. Sistemas de Tecnologia da Informação (TI) que captam e armazenam os dados colhidos dos monitoramentos das comunicações; 3.1. Identificação dos Sistemas de recepção e armazenamento de dados; 3.2. A operação da interceptação; 3.3. Funcionamento e algumas funcionalidades dos Sistemas de recepção e armazenamento de dados; Considerações Finais; Referências

---

## INTRODUÇÃO

O processo penal vem sofrendo mudanças práticas nos métodos de obtenção de informações, sobretudo com a introdução de novas tecnologias, que vulneram os direitos fundamentais. Inobstante este trabalho tenha por referência o processo penal brasileiro, não são poucos os autores estrangeiros que apontam essa tendência de utilização de métodos não tradicionais para formação do conhecimento sobre os fatos na Espanha<sup>5</sup>, Alemanha<sup>6</sup>, Itália<sup>7</sup>, Portugal<sup>8</sup>, Argentina<sup>9</sup>, entre outros.

---

<sup>5</sup> MUÑOZ CONDE, Francisco. *De las prohibiciones probatorias al derecho procesal penal del enemigo*. Buenos Aires: Hammurabi, 2008. Ainda do mesmo autor: *Valoración de las grabaciones audiovisuales en el proceso penal*. 2ª ed. Buenos Aires: Hammurabi, 2007; ABEL LLUCH, Xavier e RICHARD GONZÁLEZ, Manuel. *Estudios sobre prueba penal volumen III: Actos de investigación y medios de prueba en el proceso penal: diligencias de instrucción, entrada y registro, intervención de comunicaciones, valoración y revisión de la prueba en vía de recurso*. Madri: La Ley Actualidad, 2013; BACIGALUPO, Enrique. *El debido proceso penal*. Buenos Aires: Hammurabi, 2007.

<sup>6</sup> ROXIN, Claus. *La prohibición de autoincriminación y de las escuchas domiciliarias*. Buenos Aires: Hammurabi, 2008. Mais especificamente sobre as investigações genéticas como meio de prova: GÖSSEL, Karl Heinz. *El derecho procesal penal en el Estado de Derecho*. Obras completas. Tomo I. Santa Fe: Rubinzal-Culzoni, 2007.

<sup>7</sup> CONTI, Carlotta; TONINI, Paolo. *Il diritto delle prove penali*. Milão: Giuffrè, 2012.

<sup>8</sup> COSTA ANDRADE, Manuel da. *Sobre as Proibições de prova em processo penal*. Coimbra: Coimbra, 2006; AGUILAR, Francisco. *Dos Conhecimentos Fortuitos Obtidos Através de Escutas Telefônicas*. Coimbra: Almedina, 2004; VALENTE, Manuel Monteiro Guedes. *Escutas Telefônicas: da excepcionalidade à vulgaridade*. 2ª ed. Coimbra: Almedina, 2008.

<sup>9</sup> HENDLER, Edmundo S. *Las garantías penales y procesales: enfoque histórico-comparado*. Buenos Aires: Editores del Puerto, 2004; PASTOR, Daniel

Há hoje mais aparelhos celulares que habitantes no Brasil e os dados do Conselho Nacional de Justiça indicam que em média há autorização judicial de monitoramento de mais de vinte mil linhas telefônicas por mês<sup>10</sup>, o que pode dar ideia da profusão da utilização da interceptação telefônica como método de coleta de elementos cognitivos.

Não se pode olvidar que no sistema de valoração de provas adotado pela Lei nº 11.690/2008, que alterou o Código de Processo Penal, esse meio de investigação de prova inverte a lógica do sistema acusatório, entre outros, por dois motivos.

Em primeiro lugar, apesar da regra geral segundo a qual o juiz não pode fundamentar a sentença exclusivamente nos elementos informativos colhidos na investigação, há uma ressalva para a possibilidade de justificar uma eventual condenação apenas nas provas cautelares, não repetíveis e antecipadas, dentre as quais está a interceptação telefônica<sup>11</sup>. Essa previsão vulnera, na prática, o direito fundamental ao contraditório, uma vez que a informação é produzida e submetida à valoração judicial sem a influência da defesa que, no máximo, exerce um contraditório diferido ou *a posteriori*, o que de fato não se pode chamar de contraditório.

Em segundo lugar, as regras de determinação da competência no Brasil implicam em que o juiz que tenha deferido o pedido de interceptação telefônica ou determinado sua realização de ofício (o que é esbarrecedoramente possível de acordo com o art. 3º da Lei nº 9.296/96) será competente para a ação principal. Aliás, a rigor, o que o art. 1º da Lei nº 9.296/96 diz é precisamente que o juiz competente para a ação principal será competente para deferir ou determinar a medida de interceptação telefônica. Isso, no mínimo, coloca a imparcialidade do juiz em situação constrangedora. Essa regra brasileira da prevenção como

---

(Diretor); GUZMÁN, Nicolás (coordenador). *Neopunitivismo y neoinquisición: un análisis de políticas e prácticas penales violatorias de los derechos fundamentales del imputado*. Buenos Aires: Ad Hoc, 2008.

<sup>10</sup> Esse dado será exposto em seguida no decorrer do trabalho.

<sup>11</sup> SCHREIBER, Simone. Algumas reflexões sobre a medida cautelar de interceptação telefônica, vinte anos depois. In: SANTORO, Antonio Eduardo Ramires; MIRZA, Flávio (orgs.) *Interceptação Telefônica: os 20 anos da Lei nº 9.296/96*. Belo Horizonte: D'Plácido, 2016. p. 445-463.

determinadora da competência<sup>12</sup> implica na exposição do juiz aos elementos cognitivos que possibilitam a formação da convicção e antecipam na consciência do julgador a decisão a ser tomada, de tal sorte que novos conjuntos de elementos cognitivos acabam por se submeter a procedimentos psicológicos de afastamento ou redução da dissonância cognitiva com a prevalência dos elementos conhecidos previamente<sup>13</sup>.

Isso implica na constatação de que medidas cautelares probatórias afetam diretamente direitos fundamentais do cidadão, pois impedem o exercício completo do direito ao contraditório e, em razão de regras de determinação da competência, comprometem a imparcialidade pela submissão do juiz ao conhecimento de elementos cognitivos prévios e unilaterais. Desta forma, face à profusão das referidas medidas, faz-se necessário questionar até que ponto as decisões penais provenientes de tais circunstâncias são legítimas.

Para Luigi Ferrajoli, tanto do ponto de vista epistemológico, como político ou jurídico, o que se exige é “que a legitimidade das decisões penais se condicione à verdade empírica de suas motivações”<sup>14</sup>. Não se pode ignorar que seja possível, mesmo nessas circunstâncias, ou seja, diante da formação da convicção judicial a partir de dados colhidos sem passar pelo filtro do contraditório, admitir que exista alguma compatibilidade empírica da decisão com os dados. O problema está exatamente na idoneidade dos dados.

---

<sup>12</sup> MAYA, André Machado. A prevenção como regra de exclusão da competência no processo penal: uma (re)leitura necessária a partir da jurisprudência do tribunal europeu de direitos humanos e da corte constitucional da Espanha. In: *Anais do XVII Congresso Nacional do CONPEDI*, realizado em Brasília – DF, nos dias 20, 21 e 22 de novembro de 2008, p. 4289-4308.

<sup>13</sup> Nesse sentido vale a leitura de: FESTINGER, Leon. *Teoria da dissonância cognitiva*. Tradução Eduardo Almeida. Rio de Janeiro: Zahar editores, 1975. Sobre a influência que os elementos cognitivos da investigação exercem sobre a formação da convicção judicial: SCHÜNEMANN, Bernd. O juiz como um terceiro manipulado no processo penal? Uma confirmação empírica dos efeitos perseverança e aliança. In: SCHÜNEMANN, Bernd. *Estudos de direito penal, direito processual penal e filosofia do direito*. Tradução Luís Greco. São Paulo: Marcial Pons, 2013.

<sup>14</sup> FERRAJOLI, Luigi. *Direito e razão: teoria do garantismo penal*. 4ª ed. Trad. Ana Paula Zomer Sica, Fauzi Hassan Choukr, Juarez Tavares e Luiz Flávio Gomes. São Paulo: Revista dos Tribunais, 2014, p. 70.

Nesse contexto, o juiz estaria julgando com base empírica nas evidências, no sentido que é atribuído a este termo por Rui Cunha Martins<sup>15</sup>, que se lhe apresentam à consciência, mas não com base na prova colhida de acordo com a formalidade que impõe o processo penal, incluindo todo regramento necessário para que estes dados adquiram democraticidade e, portanto, possam efetivamente condicionar a decisão penal condenatória.

O processo, segundo Michele Taruffo, sob uma perspectiva metodológica, pode ser analisado pela sua dimensão epistêmica “como um ‘modelo epistemológico’ do conhecimento dos fatos com base nas provas”<sup>16</sup>. E ressalta:

Em todo e qualquer procedimento de caráter epistêmico tem importância decisiva o método, ou seja, o conjunto das modalidades com que são selecionadas, controladas e utilizadas as informações que servem para demonstrar a veracidade das conclusões. No âmbito do processo isso equivale a fazer referência sobretudo às regras que disciplinam a produção das provas e sua utilização, ou seja, ao “direito das provas” e à equivalente noção anglo-americana da *law of evidence*.<sup>17</sup>

Portanto, resta claro que o processo penal se legitima pela busca do conhecimento da verdade com base nas provas<sup>18</sup>. Certo de que os fatos estão no passado, as provas nada mais são do que signos transmitidos, são materiais semióticos que representam a única via de acesso ao conhecimento<sup>19</sup> e que, como em todo procedimento de caráter epistêmico, devem ser obtidas com estrita observância do método de produção e utilização.

---

<sup>15</sup> MARTINS, Rui Cunha. *O ponto cego do direito*. São Paulo: Atlas, 2013, p. 159-186.

<sup>16</sup> TARUFFO, Michele. *Uma simples verdade: o juiz e a construção dos fatos*. Tradução Vitor de Paula Ramos. São Paulo: Marcial Pons, 2012, p. 160.

<sup>17</sup> *Ibid*, p. 164.

<sup>18</sup> Sobre o tema verdade, ver: KHALED JR., Salah H. A produção analógica da verdade no processo penal. *Revista Brasileira de Direito Processual Penal*, Porto Alegre, vol. 1, p. 166-184, 2015.

<sup>19</sup> ANDRÉS IBÁÑEZ, Perfecto. *Prueba y convicción judicial en el proceso penal*. Buenos Aires: Hammurabi, 2009, p 49.

Ignorar a dimensão epistêmica do processo pode gerar distorções insanáveis.

O que caracteriza o meio de prova ou do meio de obtenção de prova é seu procedimento, não seu resultado. O rito probatório caracterizador do meio vai desde o requerimento de produção, passando pela sua admissão e produção, até sua valoração. O completo ritual de obtenção da prova confere natureza a ela.

A elaborada ritualística da prova não está na lei processual para satisfazer caprichos ou tornar o processo um complexo emaranhado de atos enfadonhos. Cada regra de produção probatória cumpre uma função de garantia e deve ser respeitada.

Os problemas que se propõem nesse contexto são: há um procedimento para obtenção da informação por meio da interceptação telefônica? Qual o rito que deve ser seguido e quem deve executá-lo? Se não há rito, quais os mecanismos para garantir a idoneidade da informação obtida?

Trabalhamos com a hipótese de que não há um procedimento para execução das medidas de interceptação telefônica e que não estão criados mecanismos de controle da idoneidade da informação obtida.

A metodologia utilizada na pesquisa foi dividida em três etapas: (1) etapa teórico-bibliográfica, em que foram utilizados, sobretudo, os seguintes marcos teóricos: Geraldo Prado, especialmente o livro “Prova penal e sistema de controles epistêmicos: a quebra da cadeia de custódia das provas obtidas por métodos ocultos”, Antonio Magalhães Gomes Filho, em seu artigo “Notas sobre a terminologia da prova (reflexos no processo penal brasileiro)” e Antonio Scarance Fernandes, em seu artigo “Tipicidade e sucedâneos de prova”; (2) etapa estatística, em que foram utilizados os dados das interceptações telefônicas obtidos diretamente junto à Ouvidoria do Conselho Nacional de Justiça obtidos do Sistema Nacional de Controle das Interceptações Telefônicas; (3) etapa empírica, em que foram utilizadas as informações extraídas do Manual de Configuração e Operação do Sistema Guardião (Versão Release 1.6.8 e Versão do Aplicativo 3.2.8.78 – julho de 2013) da empresa Dígito Tecnologia Ltda.

## 1. TERMINOLOGIAS DA PROVA: INTERCEPTAÇÃO TELEFÔNICA COMO MEIO DE OBTENÇÃO DE PROVA ATÍPICO

Ponto fundamental à compreensão do problema diz respeito à compreensão terminológica referente ao tema probatório. Sabe-se que o termo prova é usado de forma indiscriminada para designar uma variada gama de significados, daí a sua natureza polissêmica tanto no trato comum, como no discurso jurídico.

Entretanto, faz-se necessário realizar algumas distinções para efetiva compreensão da proposta de pesquisa realizada neste trabalho. A primeira é compreensão do que vem a ser *elemento de prova e resultado da prova*.

Elementos de prova, no inglês *evidence*, são os “(...) dados objetivos que confirmam ou negam uma asserção a respeito de um fato que interessa à causa”<sup>20</sup> e sobre os quais o juiz vai realizar um procedimento inferencial para chegar a alguma conclusão sobre os fatos. São as informações valoráveis pelo juiz. Já o resultado da prova, no inglês *proof*, é a própria conclusão que o julgador extrai dos diversos elementos de prova existentes, por meio de um procedimento intelectual para estabelecer a veracidade ou não dos fatos alegados. Estes fatos alegados são chamados de objeto de prova.

Há que se distinguir, ainda, *fonte de prova, meio de prova e meio de investigação de prova*.

Fonte de prova são as pessoas ou coisas que podem fornecer uma informação apreciável sobre o objeto de prova, ou seja, os fatos alegados. Daí porque as fonte podem ser reais (documentos *lato sensu*) ou pessoais (testemunhas, acusado, vítima, perito, assistentes técnicos).

Meios de prova são instrumentos ou atividades endoprocessuais que se desenvolvem perante o juiz, com conhecimento e participação das partes, pelos quais as fontes de prova introduzem elementos de prova no processo. Diferenciam-se dos meios de investigação de prova,

---

<sup>20</sup> GOMES FILHO, Antonio Magalhães. Notas sobre a terminologia da prova (reflexos no processo penal brasileiro). In: YARSHELL, Flávio Luiz; ZANOIDE DE MORAES, Maurício (orgs.). *Estudos em homenagem à Professora Ada Pellegrini Grinover*. São Paulo: DPJ, 2005, p. 307.

também chamados meios de pesquisa da prova ou meios de obtenção de prova, que são atividades extraprocessuais, que podem ser produzidos na fase investigatória, sem a participação do investigado, baseado no fator “surpresa”<sup>21</sup> e não podem ser repetidos.

Nosso Código de Processo Penal não distingue entre meios de prova e meios de investigação de prova. O *Codice di Procedura Penale*<sup>22</sup> italiano distingue no Livro III, Título II os meios de prova (testemunhal, confronto ou acareação, reconhecimento, reprodução judicial, pericial e documental) e no Título III os meios de pesquisa da prova (inspeções, buscas, sequestros e interceptações das conversas ou comunicações).

Todavia, a Lei nº 12.850/2013 adotou claramente esta nomenclatura e fez um elenco dos meios de obtenção de prova admitidos nas investigações no seu art. 3º e regulamentou algumas delas.

A interceptação das comunicações telefônicas, conquanto esteja no rol dos meios de obtenção de prova da Lei nº 12.850/2013, está regulada pela Lei nº 9.296 de 1996. De fato, a interceptação telefônica é um meio de investigação ou de pesquisa ou de obtenção da prova, cuja aptidão para levar ao processo elementos probatórios deve ser analisada cuidadosamente.

Em primeiro lugar, há que se distinguir se a interceptação das comunicações telefônicas é um meio de investigação de prova típico ou atípico. Neste ponto é importante pontuar que meios típicos não se caracterizam meramente por estarem previstos em lei, pois, como pontua Scarance, apoiado na lição de Antonio Laronga, “a prova típica é aquela prevista e dotada de procedimento próprio para sua efetivação; a prova atípica, por conseguinte, é aquela que, prevista ou não, é destituída de procedimento para sua produção.”<sup>23</sup>

Nesse sentido seriam típicos aqueles meios cuja previsão e procedimento estão regulamentados, seja o procedimento próprio ou por

---

<sup>21</sup> TONINI, Paolo. *A prova no processo penal italiano*. Trad. Alexandra Martins e Daniela Mróz. São Paulo: Revista dos Tribunais, 2002, p. 242.

<sup>22</sup> Disponível em: <[http://www.polpenuil.it/attachments/048\\_codice\\_di\\_procedura\\_penale.pdf](http://www.polpenuil.it/attachments/048_codice_di_procedura_penale.pdf)>. Acesso em: 13 abr. 2017.

<sup>23</sup> SCARANCE FERNANDES, Antonio. Tipicidade e sucedâneos de prova. In: SCARANCE FERNANDES, Antonio; GAVIÃO DE ALMEIDA, José Raul; ZANOIDE DE MORAES, Maurício (coords.). *Provas no Processo Penal: estudo comparado*. São Paulo: RT, 2012, p. 15.

remissão. De outro lado, não estando previsto o meio ou, ainda que previsto, se seu procedimento não estiver regulamentado ou for objeto de remissão, está-se diante de um meio atípico.

Ora, o art. 5º da Lei nº 9.296 de 1996 prevê não apenas que a decisão que defere a medida deve ser fundamentada, mas que o juiz deve indicar “a forma de execução da diligência”.

Dessa forma, como observou Geraldo Prado, quando a legislação silencia sobre o procedimento probatório, a exigência de motivação da “decisão que defere o emprego de métodos ocultos de investigação importa”<sup>24</sup> não apenas na indicação dos elementos que convencem acerca da sua adequação, mas “ainda, na definição dos meios de sua execução e fiscalização”<sup>25</sup>.

Isso significa que o procedimento da interceptação das comunicações telefônicas não é regulamentado, sendo deixado ao juiz, no ato decisório, fazê-lo. Isso implica em que a interceptação das comunicações é um meio de investigação de prova atípico.

Daí surge um questionamento, os elementos de prova obtidos pelos meios de prova atípicos são de regra admitidos porque submetem-se ao contraditório judicial, mas os meios de investigação de prova atípicos são aptos a obter elementos de prova ou apenas a descobrir e resguardar a fonte de prova?

A resposta de Scarance Fernandes merece transcrição:

O problema da ilicitude coloca-se mais em relação aos meios de investigação ou de obtenção de prova. Como, quase sempre, eles importam restrição ou ameaça de restrição a direitos individuais, a regra deve ser a tipicidade, dependendo a obtenção da fonte de prova de lei que indique as hipóteses em que a restrição será possível e os limites em que será permitida. Somente quando o meio de investigação de prova atípico não interfira em direito individual será possível a sua utilização.<sup>26</sup>

<sup>24</sup> PRADO, Geraldo. *Prova penal e sistema de controles epistêmicos: a quebra da cadeia de custódia das provas obtidas por métodos ocultos*. 1ª ed. São Paulo: Marcial Pons, 2014, p. 78.

<sup>25</sup> *Ibid.*

<sup>26</sup> SCARANCE FERNANDES, *op. cit.*, p. 28-29.

A interceptação das comunicações telefônicas é um meio de investigação de prova atípico, vez que carece de uma regulamentação metodológica de obtenção, que interfere diretamente no direito individual à inviolabilidade das comunicações, à privacidade e à intimidade.

Essa omissão legislativa pode implicar na adoção de uma alternativa epistemológica autoritária pela aplicação de um subjetivismo inquisitivo<sup>27</sup>, a menos que se definam mecanismos de estabelecimento prévio das “regras do jogo”, às quais todos os atores do sistema penal, inclusive o juiz, devam se submeter.

Como aludido, segundo Geraldo Prado, na ausência de regulamentação legal, cabe ao juiz fazê-lo<sup>28</sup>. Essa foi a técnica utilizada pelo legislador pátrio no que concerne ao procedimento para execução da diligência. Basta ver que a Lei nº 9.296/96, que regulamentou o art. 5º, XII CRFB/88, para tratar dos casos de autorização da interceptação telefônica e telemática como meio de obtenção de prova no processo penal brasileiro dispôs no art. 5º que cabe ao juiz, na decisão que defere ou determina a medida, definir “a forma de execução da diligência”.

De se observar que é a autoridade policial quem deve conduzir os procedimentos de interceptação, cientificando o ministério público, que poderá acompanhar a sua realização, segundo o art. 6º da referida Lei.

Assim, inobstante não se possa deixar de lembrar o atropelo dos princípios do contraditório e da imparcialidade da jurisdição, estão definidas as posições (porém não totalmente as tarefas de cada um) dos atores tradicionais do sistema penal, com o devido alijamento da defesa.

A novidade é que a Lei nº 9.296/96 traz à cena dois novos atores para este subsistema probatório: (1) as concessionárias de serviço público de telefonia e provedores de acesso e (2) o sistema de tecnologia da informação (TI) que trata os dados colhidos dos monitoramentos das comunicações (e seus operadores privados). Isso ocorre, respectivamente, no artigo 7º e no parágrafo 1º do art. 6º, ambos da Lei nº 9.296/96.

O art. 7º afirma que a autoridade policial (não a autoridade judicial, nem o ministério público) poderá requisitar serviços e técnicos especializados às concessionárias de serviço público.

---

<sup>27</sup> FERRAJOLI, op. cit., p. 46-47.

<sup>28</sup> Ibid.

O parágrafo 1º do art. 6º apenas afirma que “no caso de a diligência possibilitar a gravação da comunicação interceptada, será determinada sua transcrição”. Muito embora este dispositivo nada fale sobre sistemas de TI, quando faz menção à possibilidade de gravação, torna esse procedimento obrigatório sempre que tiver sido possível. Acontece que em 1996, quando a Lei entrou em vigor, poderia não ser possível em todos os casos, mas hoje, com o avanço tecnológico, isso é sempre possível e entra em cena o sistema de TI utilizado para realizar a tarefa como parte da engrenagem probatória no processo penal.

Todavia, essas poucas menções legais às concessionárias de serviço público de telefonia e ao sistema de tecnologia da informação que trata os dados colhidos dos monitoramentos das comunicações não são suficientes para descrever com precisão o papel que devam desempenhar. Falta regulamentar de maneira uniforme os procedimentos de execução dessas medidas invasivas, incluindo a atividade de cada um dos atores do sistema penal e dos novos atores desse subsistema probatório.

## **2. A INTERVENÇÃO DO CNJ NA REGULAÇÃO, CONTROLE E ELABORAÇÃO DE ESTATÍSTICAS A RESPEITO DO SOBREUSO DA INTERCEPTAÇÃO TELEFÔNICA NO BRASIL: ONDE ESTÁ A CADEIA DE CUSTÓDIA?**

A falta de uma regulamentação legal sobre a execução da medida de interceptação telefônica, bem como a prática judicial de omitir na decisão que defere a interceptação o procedimento a ser utilizado no caso concreto, fez com que o Conselho Nacional de Justiça, criado pela Emenda Constitucional nº 45/2004 para controlar a atuação administrativa e financeira do Poder Judiciário e do cumprimento dos deveres funcionais dos juízes, criasse o Sistema Nacional de Controle de Interceptações Telefônicas e editasse a Resolução nº 59, de 09 de setembro de 2008<sup>29</sup>, com o objetivo de disciplinar e uniformizar as rotinas visando ao aperfeiçoamento do procedimento de interceptação telefônica nos órgãos jurisdicionais do Poder Judiciário.

---

<sup>29</sup> Disponível em: <[http://www.cnj.jus.br/images/stories/docs\\_cnj/resolucao/rescnj\\_59consolidada.pdf](http://www.cnj.jus.br/images/stories/docs_cnj/resolucao/rescnj_59consolidada.pdf)>. Acesso em: 13 abr. 2017.

Essa providência, tomada por um órgão que não tem atribuições legislativas, desvela o vácuo deixado no ordenamento pelas normas que disciplinam a interceptação telefônica e, conquanto sua constitucionalidade esteja sendo questionada pela Procuradoria-Geral da República por meio da ADI nº 4.145<sup>30</sup>, a referida Resolução vem sendo aplicada e o Sistema Nacional de Controle das Interceptações Telefônicas está funcionando, gerando dados para conhecimento da utilização da interceptação telefônica no Brasil.

Os dados fornecidos pelo CNJ são estarrecedores. O CNJ colhe os dados de todas as interceptações realizadas no Brasil e elabora um quadro numerado de 1 a 11, por mês.

| Ano  | Total 1 | Total 2 | Total 3 | Total 4  | Total 5  | Total 6 |
|------|---------|---------|---------|----------|----------|---------|
| 2008 | 3.808   | 7.269   | 1.236   | 3.442    | 16.589   | 827     |
| 2009 | 39.645  | 113.197 | 12.832  | 39.278   | 214.138  | 15.379  |
| 2010 | 53.372  | 113.458 | 12.471  | 40.353   | 214.883  | 15.177  |
| 2011 | 54.165  | 115.634 | 12.615  | 44.441   | 233.054  | 14.531  |
| 2012 | 51.796  | 130.519 | 12.943  | 47.568   | 247.617  | 19.584  |
| 2013 | 47.980  | 113.051 | 12.367  | 49.432   | 242.451  | 26.124  |
| 2014 | 45.521  | 98.849  | 11.810  | 47.884   | 240.195  | 25.988  |
| 2015 | 41.798  | 93.985  | 11.102  | 48.935   | 268.555  | 22.811  |
| Ano  | Total 7 | Total 8 | Total 9 | Total 10 | Total 11 |         |
| 2008 | 218     | 331     | 75      | 311      | 100      |         |
| 2009 | 2.724   | 6.183   | 1.569   | 5.665    | 5.184    |         |
| 2010 | 2.319   | 5.082   | 1.293   | 4.838    | 4.732    |         |
| 2011 | 2.310   | 4.252   | 922     | 3.088    | 4.011    |         |
| 2012 | 1.968   | 4.617   | 773     | 3.676    | 4.744    |         |
| 2013 | 2.307   | 4.582   | 946     | 3.460    | 11.977   |         |
| 2014 | 2.431   | 4.671   | 1.123   | 4.127    | 14.806   |         |
| 2015 | 2.732   | 5.002   | 1.328   | 6.878    | 18.170   |         |

**QUADRO 1.** Dados do Sistema Nacional de Controle de Interceptações Telefônicas do CNJ entre os anos de 2008 e 2015

<sup>30</sup> A favor da constitucionalidade da norma: BOTTINO DO AMARAL, Thiago; CYRINO, André Rodrigues. Memorial apresentado pelo Instituto dos Advogados Brasileiros Ação Direta de Inconstitucionalidade nº 4.145. In: SANTORO, Antonio Eduardo Ramires; MIRZA, Flávio (org.) *Interceptação Telefônica: os 20 anos da Lei nº 9.296/96*. Belo Horizonte: D'Plácido, 2016. p. 557-585.

O CNJ apresenta os dados mês a mês de janeiro de 2008 até maio de 2016<sup>31</sup>, porém, para uma visualização mais fácil e didática, organizou-se um quadro reunindo os dados anualmente.

O quadro acima apresenta os dados, por ano, de 2008 a 2015, em que constam: a quantidade de ofícios expedidos, sendo a quantidade de primeiros ofícios expedidos para interceptação de uma linha telefônica (total 1) e a quantidade de ofícios expedidos enquanto as interceptações telefônicas estão em andamento (total 2), ou seja, aqueles que foram renovados; a quantidade de procedimentos criminais de interceptação telefônica instaurados (total 3) e a quantidade de procedimentos criminais de interceptação telefônica em andamento (total 4); quantidade de telefones monitorados (total 5); quantidade de VOIP monitorado (total 6) – não só telefone; a quantidade de primeiros ofícios expedidos para interceptação de dados – e-mails (total 7) e a quantidade de ofícios expedidos enquanto as interceptações de dados – e-mails – estão em andamento (total 8), ou seja, aqueles que foram renovados; a quantidade de procedimentos criminais de interceptação de dados – e-mails – instaurados (total 9) e a quantidade de procedimentos criminais de interceptação de dados – e-mails – em andamento (total 10); a quantidade de e-mails interceptados (total 11).

Na verdade os dados começaram a ser coletados em 2008, depois da chamada “CPI dos grampos” e da Resolução nº 59 de 2008, o que, como pode se observar, não foi feito de maneira imediata e uniforme.

Não é difícil perceber que somando as linhas telefônicas interceptadas (total 5), as linhas de VOIP interceptadas (total 6) e os endereços de e-mail interceptados (total 11), há por ano mais de 300.000 (trezentas mil) interceptações de comunicações.

Para uma análise estatística qualitativa do ano em que os dados foram obtidos, tomemos os dados de janeiro a maio de 2016, selecionando maio, como exemplo:

---

<sup>31</sup> Esses dados foram coletados pelos autores diretamente na ouvidoria do CNJ no mês de julho de 2016.

| Mês       | Total 1 | Total 2 | Total 3 | Total 4  | Total 5  | Total 6 |
|-----------|---------|---------|---------|----------|----------|---------|
| Janeiro   | 2.469   | 5.925   | 836     | 3.707    | 17.701   | 1.109   |
| Fevereiro | 2.901   | 6.746   | 827     | 3.542    | 18.881   | 1.709   |
| Março     | 3.370   | 7.385   | 938     | 3.483    | 20.232   | 1.384   |
| Abril     | 3.357   | 7.489   | 907     | 3.476    | 20.883   | 1.349   |
| Maiο      | 3.094   | 7.270   | 818     | 3.220    | 20.860   | 1.196   |
| Total     | 15.191  | 34.815  | 4326    | 17.428   | 98.557   | 6.747   |
| Mês       | Total 7 | Total 8 | Total 9 | Total 10 | Total 11 |         |
| Janeiro   | 178     | 312     | 83      | 492      | 1.370    |         |
| Fevereiro | 203     | 389     | 101     | 240      | 961      |         |
| Março     | 220     | 475     | 104     | 272      | 907      |         |
| Abril     | 217     | 489     | 131     | 308      | 983      |         |
| Maiο      | 188     | 435     | 117     | 298      | 702      |         |
| Total     | 1006    | 2100    | 536     | 1610     | 4.923    |         |

**QUADRO 2.** Dados do Sistema Nacional de Controle de Intercepções Telefônicas do CNJ no ano de 2016, mês a mês, de janeiro a maio

A quinta coluna mostra a quantidade de telefones que estariam interceptados naquele mês no Brasil, totalizando 20.860 telefones, a sexta coluna mostra a interceptação de 1.196 VOIP, e a décima primeira coluna mostra que foram interceptados 702 endereços de e-mail, totalizando 22.758 instrumentos de comunicação interceptados.

Diante dos dados obtidos, podemos afirmar que o número total de interceptações telefônica e de dados varia de aproximadamente entre 22.000 e 25.000 por mês. Em alguns meses verifica-se um número de interceptações superior a 25.000, como aconteceu no mês de julho de 2015, em que foram interceptadas 25.491 linhas telefônicas, 2.221 VOIPs e 1.510 endereços de e-mail.

Diante de tamanha intervenção do sistema probatório penal na intimidade e privacidade de mais de 20.000 (vinte mil) cidadãos brasileiros por mês e mais de 300.000 (trezentos mil) por ano e do inegável

potencial de formação da convicção judicial com base nos dados colhidos por estes sistemas a partir de evidências que, a despeito de não submetidas ao contraditório, são comumente consideradas suficientes (e até mesmo preferenciais) para emitir uma decisão condenatória, é importante questionar a idoneidade dessas informações.

Saber se as informações são empiricamente verificáveis implica, antes de mais nada, poder confiar que os dados armazenados e submetidos à valoração judicial guardam fidedignidade e não foram manipulados ou que não foram passíveis de manipulação. A preservação de cada uma das etapas da operação que realizou a interceptação das comunicações de um cidadão é a única maneira de assegurar a integridade do procedimento probatório, ou seja, deve ser preservada a cadeia de custódia para permitir à defesa rastrear as fontes de prova<sup>32</sup>.

Essa preservação das evidências das medidas de interceptação das comunicações não pode estar restrita à apresentação da mídia em que se encontram gravados os arquivos de áudio, mas deve incluir a preservação do próprio sistema de TI, bem como dos registros de atividades de todos os atores do sistema penal, tradicionais (como polícia e ministério público), mas também os novos (como as concessionárias de serviço público de telefonia e os operadores do sistema de tecnologia da informação que trata os dados colhidos dos monitoramentos das comunicações).

Geraldo Prado já havia assinalado essa necessidade ao afirmar que “os suportes técnicos que resultam da operação, portanto, devem ser preservados. A razão adicional, de natureza constitucional, está vinculada ao fato de que apenas dessa maneira é possível assegurar à defesa, oportunamente, o conhecimento das fontes de prova.”<sup>33</sup>

---

<sup>32</sup> Sobre o tema, ver: EDINGER, Carlos. Cadeia de custódia, rastreabilidade probatória. *Revista Brasileira de Ciências Criminais*, São Paulo, v. 24, n. 120, p. 237-257., mai./jun. 2016; MACHADO, Vitor Paczek; JEZLER JUNIOR, Ivan. A prova eletrônico-digital e a cadeia de custódia das provas: uma (re)leitura da súmula vinculante 14. *Boletim IBCCRIM*, São Paulo, v. 24, n. 288, p. 08-09., nov. 2016; CARVALHO, Jefferson Lemes. Cadeia de Custódia e sua relevância na persecução penal. *Brazilian Journal of Forensic Sciences, Medical Law and Bioethics*, vol. 5, p. 371-382.

<sup>33</sup> PRADO, op. cit., p. 79.

Um dos requisitos para manter um sistema de gestão da qualidade é precisamente “cumprir os procedimentos preconizados para manter a cadeia de custódia das evidências”<sup>34</sup>, o que deve ocorrer desde o “recebimento até o acautelamento final”.

No entanto, a despeito das mais de vinte mil linhas telefônicas, e-mails e VOIPs interceptados por mês no Brasil, a Lei nº 9.296/96 não regulamenta sua forma de execução, tampouco a cadeia de custódia. O CNJ, inobstante tenha editado a Resolução nº 59/2008, nada falou sobre a cadeia de custódia, o que acaba deixando tal questão às empresas que desenvolvem e comercializam os sistemas de tecnologia de informação.

Diante dessa realidade impõe-se questionar: os manuais dos sistemas e o funcionamento dos próprios sistemas de TI que captam e armazenam os dados colhidos dos monitoramentos das comunicações são compatíveis ou estão em conflito com o ordenamento legal? Os manuais dos sistemas e o funcionamento dos sistemas de TI permitem concluir que os dados captados e armazenados são empiricamente idôneos a serem valorados pelo juiz? Há cadeia de custódia desses dados diante dos procedimentos adotados pelos sistemas de tecnologia da informação? Se houver, eles são suficientes ou há etapas no procedimento que dependem de agentes diversos?

Importa, portanto, conhecer o funcionamento dos sistemas de tecnologia de informação que captam e armazenam os dados colhidos em interceptações das comunicações.

### **3. SISTEMAS DE TECNOLOGIA DA INFORMAÇÃO (TI) QUE CAPTAM E ARMAZENAM OS DADOS COLHIDOS DOS MONITORAMENTOS DAS COMUNICAÇÕES**

#### **3.1. IDENTIFICAÇÃO DOS SISTEMAS DE RECEPÇÃO E ARMAZENAMENTO DE DADOS**

Pelo que se tem notícia, há no Brasil basicamente três sistemas de TI utilizados para recepção e armazenamento dos dados objetos de monitoramento: o Sistema Guardião desenvolvido e comercializado

---

<sup>34</sup> GARRIDO, Rodrigo Grazinoli; ARAUJO, Katia. Sistemas de Gestão da Qualidade em Laboratórios de Genética Forense. *Revista Espacios*, vol. 35, nº 5, ano 2014, p. 3.

pela empresa Dígito Tecnologia Ltda., o Sistema Sombra desenvolvido e comercializado pela empresa Federal Tecnologia de Software Ltda.-EPP e o Sistema Wytron desenvolvido e comercializado pela empresa Wytron Technology Corp. Ltda.

Dados colhidos do Processo nº 0.00.000.001328/2012-95, que tramitou junto ao Conselho Nacional do Ministério Público e se tratava de um Pedido de Providência formulado pelo Conselho Federal da Ordem dos Advogados do Brasil, consistente no requerimento de auditoria e inspeção nos sistemas de escuta e monitoramento de interceptações telefônicas utilizados pelas unidades do ministério público brasileiro<sup>35</sup>, mostram que, a partir das consultas feitas às 30 unidades do ministério público brasileiro, 8 (oito) adquiriram o Sistema Guardiã (o ministério público federal e o ministério público dos estados de Goiás, Mato Grosso, Rio Grande do Norte, Rio Grande do Sul, São Paulo, Santa Catarina e o Distrito Federal); 6 (seis) adquiriram o Sistema Wytron (o ministério público dos estados de Alagoas, Amapá, Ceará, Maranhão, Pará e Rondônia); 3 (três) adquiriram o Sistema Sombra (o ministério público dos estados da Bahia, Mato Grosso do Sul e Paraíba); 4 (quatro) utilizam o Sistema Guardiã disponibilizado ou cedido por órgãos do Poder Executivo (o ministério público dos estados do Espírito Santo, Minas Gerais, Amazonas e Tocantins); 9 (nove) não possuem ou não têm acesso a qualquer um desses sistemas (o ministério público militar, o ministério público do trabalho e o ministério público dos estados de Sergipe, Pernambuco, Acre, Paraná, Piauí, Roraima e Rio de Janeiro).

Portanto, das 30 (trinta) unidades do ministério público, 21 (vinte e uma) adquiriram ou utilizam sistemas de TI que se destinam a receber e armazenar dados obtidos de interceptações telefônicas ou de dados. Destas 21 (vinte e uma) unidades que operam sistemas de monitoramento de comunicações, 12 (doze) “não dispõem de ato normativo versando sobre procedimentos e rotinas adotadas”<sup>36</sup> e 18 (dezoito) recorrem a policiais civis e/ou militares na operação.

---

<sup>35</sup> Disponível em: <<http://s.conjur.com.br/dl/relatorio-guardiao-mp-cnmp.pdf>>. Acesso em: 13 abr. 2017.

<sup>36</sup> Decisão proferida no processo 0.00.000.001328/2012-95, que tramitou junto ao Conselho Nacional do Ministério Público. Disponível em: <<http://s.conjur.com.br/dl/relatorio-guardiao-mp-cnmp.pdf>>. Acesso em: 13 abr. 2017.

No que se refere à aquisição desses sistemas pelos Departamentos de Polícia Federal dos Estados não há dados tão precisos quanto esses constantes do processo que tramitou no Conselho Nacional do Ministério Público, mas dados do Portal da Transparência do governo federal demonstram que as empresas Dígito Tecnologia Ltda., Federal Tecnologia de Software Ltda.-EPP e Wytron Technology Corp. Ltda. comercializaram com o Departamento de Polícia Federal, sendo, ademais, amplamente divulgada a contratação do Sistema Guardião pelas Superintendências da Polícia Federal de Santa Catarina, Paraná, São Paulo e Rio de Janeiro.

### **3.2. A OPERAÇÃO DA INTERCEPTAÇÃO**

Quanto à operação desses Sistemas, a Dígito e a Federal afirmam que seus sistemas, Guardião e Sombra, respectivamente, não permitem a interceptação telefônica sem a participação das operadoras de telefonia, portanto só realizam monitoramento passivo. Assim, são as operadoras de telefonia que encaminham as informações interceptadas ao Sistema de monitoramento.

Na prática, as operadoras “abrem um *link*” de tal forma que a chamada telefônica ou o fluxo de dados seja desviado para um outro canal de recepção diverso do destinatário e o direciona para o sistema de TI utilizados para recepção e armazenamento dos dados objetos de monitoramento (Guardião, Sombra ou Wytron, por exemplo).

Assim, se o interlocutor A (não interceptado) liga para o interlocutor B (interceptado), esta ligação irá se completar, mas o fluxo se duplicará em dois *links*, um para o interlocutor, outro para o sistema de TI responsável pelo monitoramento.

Aqui está um primeiro, porém muito grave problema. É que diversamente do que dispõe a legislação, quem verdadeiramente conduz a interceptação não é a autoridade policial, como determina o art. 6º da Lei nº 9.296/96, mas a operadora de telefonia. São precisamente as concessionárias de serviço público de telefonia ou os provedores de acesso (no caso de desvio de dados, como e-mail e VOIP) que controlam quem será objeto de interceptação e qual a duração, pois, uma vez que os sistemas de monitoramento são passivos, é a operadora que abre e fecha o *link* e, portanto, determina o tempo de interceptação.

Diante das informações prestadas pelas empresas desenvolvedoras dos sistemas de TI responsáveis pelo monitoramento das comunicações, as operadoras de telefonia e os provedores de acesso desempenham, na prática, um papel proeminente na execução das medidas cautelares de interceptação. No entanto, o sistema legal ignora esse novo ator desse subsistema probatório, não dispensando sequer uma única regulamentação para sua atuação, muito menos discutindo a adequação ou inadequação da sua posição protagonista na coleta de informações dentro da investigação penal.

Ademais, as operadoras de telefonia também não fazem o desvio da chamada para o canal de recepção do sistema de TI dedicado ao monitoramento das comunicações sem o auxílio de uma ferramenta. Há um sistema chamado Vigia, desenvolvido pela empresa Suntech que gerencia “todo o processo de interceptação legal e retenção de dados para qualquer serviço ou subsistema de comunicação de qualquer tecnologia ou vendedor”. De acordo com o desenvolvedor, “com o Vigia é possível interceptar a comunicação em praticamente todos os tipos de rede e reter dados de comunicação sem notificar os assinantes ou prejudicar o serviço”<sup>37</sup>.

Desta forma, o Sistema Vigia e os sistemas de TI dedicados ao monitoramento e armazenamento das comunicações (Guardião, Sombra ou Wytron) não se sobrepõem, ao contrário, são complementares. Na verdade o Sistema Vigia é o sistema ativo, ele é quem de fato realiza a interceptação e o desvio da chamada para o sistema passivo que recebe e armazena os dados.

Importa ressaltar que os Sistemas passivos de TI que recebem, monitoram e armazenam os dados interceptados são adquiridos e operados pelas autoridades públicas responsáveis pela investigação (ministério público, polícia federal, secretarias de segurança dos estados, etc.), ao passo que o Sistema Vigia tem como clientes exatamente as operadoras de telefonia (Claro, Oi, Vivo, Tim, Nextel, Embratel, GVT, Movistar),

---

<sup>37</sup> Disponível em: <<http://www.suntech.com.br/pt/solucoes/lawful-interception/vigia/>>. Acesso em: 16 jun. 2014. Essa página hoje está desativada, mas a informação a respeito do sistema pode ser obtida na página da Câmara dos Deputados, disponível em: <<http://www2.camara.leg.br/camaranoticias/noticias/121746.html>>. Acesso em: 16 mai. 2017.

o que aliás é divulgado em seu sítio eletrônico na internet<sup>38</sup>. Isso apenas corrobora o fato de que operadoras de telefonia e provedores de acesso são atores do sistema penal e precisam ser assim compreendidos para que suas ações sejam excluídas ou regulamentadas.

É ainda imprescindível que se compreenda quais as possibilidades de que os operadores das empresas desenvolvedoras desses sistemas (aqui leia-se todos eles, Vigia, Guardiã, Sombra, Wytron, ou qualquer outro com a mesma funcionalidade), que prestam serviços de suporte técnico, tenham acesso aos mecanismos de funcionamento e aos dados armazenados. Isso porque qualquer um que possa ter acesso, inclusive remoto, ao sistema para solucionar eventual problema técnico, precisa ser devidamente conhecido para configuração da cadeia de custódia.

### **3.3. FUNCIONAMENTO E ALGUMAS FUNCIONALIDADES DOS SISTEMAS DE RECEPÇÃO E ARMAZENAMENTO DE DADOS**

A pesquisa se baseou no acesso ao Manual de Configuração e Operação do Sistema Guardiã (Versão Release 1.6.8 e Versão do Aplicativo 3.2.8.78 – julho de 2013) da empresa Dígitro Tecnologia Ltda, obtido diretamente junto à empresa em formato impresso.

Importa dizer que este trabalho não pretende fazer qualquer apanhado sobre o funcionamento do sistema informático, mas apenas traçar em linhas gerais algumas funcionalidades que interessam para garantia do direito fundamental à prova e ao contraditório.

Assim, as chamadas direcionadas pela operadora de telefonia ou os dados desviados ingressam na plataforma que realiza a gravação em um determinado suporte (HD) e as informações referentes àquela chamada são armazenados em um banco de dados relacional, que podem ser acessados e manipulados. Em outras palavras, o *Hard Disk* (HD) em que ficam armazenados os áudios é diverso daquele em que estão armazenados os dados (metadados), mas são relacionados de tal forma que para cada áudio há os correspondentes dados dos metadados que, quando acionados remetem por *hiperlink* diretamente ao áudio vinculado.

---

<sup>38</sup> Disponível em: <<http://www.suntech.com.br/pt/clientes/>>. Acesso em: 16 jun. 2014. Ver comentário na nota anterior.

Isso implica em que, malgrado se afirme que não é possível fazer exclusão de um áudio do sistema, qualquer alteração de dados na base gera um apagamento lógico, ou seja, não havendo mais relação entre dados e áudio o acionamento do *hyperlink* não será direcionado ao áudio e, portanto, o áudio fisicamente existe, mas não é encontrado.

Ademais, o módulo de *backup* do sistema permite alguns tipos de *backup* (manual ou por agendamento), mas se não gerado é possível que haja sobrescrição, ou seja, a gravação por cima, o que implica também na possibilidade de perda definitiva de áudios. Isso fica muito claro quando, no início do Manual, a Dígito informa que não se responsabiliza por perdas de informações, devido a não observação por parte do cliente, de procedimentos de *backup*, orientando para que regularmente armazene os dados também em mídia eletrônica (CD, DVD, etc.), de forma a possuir contingência externa.

É possível inserir no sistema durante a operação alguns dados cadastrais, como os alvos do monitoramento, os telefones monitorados, os alvarás judiciais que autorizam a interceptação com a data da expedição, o período e a data de validade.

Todavia, esse cadastro, como já dito antes, não torna o sistema ativo, porquanto ele não irá captar as chamadas de determinados alvos e telefones, que continuam a depender do desvio a ser realizado pela operadora de telefonia.

O problema é que o cadastro de alvará judicial não permite ao sistema bloquear a gravação das chamadas após o término do período de validade da autorização judicial, de tal sorte que esta gestão do período de interceptação fica a cargo exclusivo das operadoras de telefonia.

Há no sistema a possibilidade de ter acesso aos *logs* de eventos que, segundo o manual, se selecionada essa opção, será apresentada uma janela com informações estratégicas da execução do programa, recolhidas durante a utilização do Guardiã, que são utilizadas para que se possa fazer a telemanutenção do sistema.

Essa funcionalidade, embora não tenha finalidade de controle da utilização do sistema para rastreamento dos agentes que manusearam ou manipularam a prova, deveria ser utilizado para tal. Alie-se essa ferramenta aos *logs* de gravação, que fornecem o histórico de gravações e revelam qualquer problema no processo de conversão das

gravações, bem como ao histórico de *backup*, teremos um rastreamento pelo próprio sistema.

Há dois problemas: o primeiro é que esse rastreamento só forneceria informações até o *backup* e o segundo é que não há sequer notícia de uma única autorização judicial conhecida que dê à defesa (ou seus eventuais assistentes técnicos) acesso ao sistema de *logs* do sistema de TI.

Com efeito, rastrear apenas até o *backup* é insuficiente quando nos deparamos com perda de áudios nas medidas cautelares de interceptações telefônicas e nos obriga a voltar à questão da cadeia de custódia. Em outras palavras, ainda que o sistema de TI responsável pela recepção e armazenamento das ligações telefônicas ou dados interceptados permita rastrear as etapas da operação até a geração do *backup* para assegurar a integridade do procedimento probatório, é imprescindível que após a geração seja criada uma rotina por lei ou fixada na decisão que defere a interceptação, para permitir à defesa do acusado rastrear as fontes de prova e exercer o seu direito ao contraditório e à defesa. A não observância da rotina, implica na quebra da cadeia de custódia e, por conseguinte, na perda da prova.

Ainda que a exata rotina de custódia da fonte de prova fosse definida, seria imprescindível que o acesso ao sistema de TI responsável pela recepção e armazenamento das ligações telefônicas ou dados interceptados fosse garantido à defesa. No entanto, ao argumento de que não se pode dar acesso à defesa por colocar em risco o sistema e o sigilo de outras operações em andamento (numa presunção de má-fé da defesa e seus eventuais assistentes técnicos), nega-se tal direito sem sequer conceber a criação de mecanismos que possam garantir esse acesso sem prejuízo dos demais interesses envolvidos.

## CONSIDERAÇÕES FINAIS

Sem dúvida o avanço tecnológico promove mudanças nos métodos de obtenção de informações nas persecuções penais com o aporte de técnicas como a interceptação das comunicações telefônicas e de dados, que vem sendo utilizada em profusão.

As interceptações das comunicações telefônicas e de dados são provas produzidas por métodos ocultos cuja definição dos meios de execução e

fiscalização são deixados pelo art. 5º da Lei nº 9.296/96 à definição do juiz e, portanto, devem ser considerados meios de obtenção de provas atípicos.

A Lei nº 9.296/96 traz à cena dois novos atores para o sistema penal: (1) as concessionárias de serviço público de telefonia e provedores de acesso e (2) o sistema de tecnologia da informação (TI) que trata os dados colhidos dos monitoramentos das comunicações (e seus operadores privados).

Diante da inexistência de definição de procedimentos para execução da medida de interceptação das comunicações, o Conselho Nacional de Justiça criou o Sistema Nacional de Controle de Interceptações Telefônicas e editou a Resolução nº 59, de 09 de setembro de 2008, com o objetivo de disciplinar e uniformizar as rotinas visando ao aperfeiçoamento do procedimento de interceptação telefônica nos órgãos jurisdicionais do Poder Judiciário.

Os dados do CNJ constantes do Sistema Nacional de Controle de Interceptações Telefônicas revelam que mais de vinte mil linhas telefônicas, e-mails e VOIPs são monitorados por mês no Brasil.

A preservação de cada uma das etapas da operação que realizou a interceptação das comunicações de um cidadão (cadeia de custódia) é a única maneira de assegurar a integridade do procedimento probatório, permitindo que a defesa rastreie e conheça as fontes de prova. Por conta disso é necessário que sejam preservados os suportes técnicos utilizados na interceptação das comunicações, no entanto, nem a Lei nº 9.296/96, nem a Resolução nº 59/2008 do CNJ, tampouco os sistemas de tecnologia da informação, estabelecem os procedimentos de rastreamento e preservação das informações.

No Brasil, os órgãos públicos responsáveis pela investigação utilizam três sistemas de TI para recepção e armazenamento dos dados obtidos pelas interceptações: o Sistema Guardião desenvolvido e comercializado pela empresa Dígitro Tecnologia Ltda., o Sistema Sombra desenvolvido e comercializado pela empresa Federal Tecnologia de Software Ltda.-EPP e o Sistema Wytron desenvolvido e comercializado pela empresa Wytron Technology Corp. Ltda. Esses sistemas de TI utilizados para recepção e armazenamento dos dados obtidos pelas interceptações são passivos, pois quem redireciona a chamada para suas plataformas são as operadoras de telefonia e os provedores de acesso.

O sistema de TI utilizado por todas as operadoras para fazer a gestão da interceptação é o Vigia, desenvolvido pela empresa Suntech. Esse é o sistema ativo de desvio de chamadas.

Embora o sistema Guardião permita realizar cadastro de dados referentes ao alvará judicial e sua validade, o sistema não bloqueia o recebimento do direcionamento de chamadas após a expiração do prazo, portanto apenas a operadora e seus empregados controlam a observância do período de interceptação.

Inobstante as empresas desenvolvedoras dos sistemas de TI utilizados para recepção e armazenamento dos dados obtidos pelas interceptações afirmem que o sistema não realiza apagamentos de áudios, no Guardião isso pode ocorrer em duas hipóteses: apagamento lógico (quando é apagado algum dado relacionado com um áudio, que passa a não ser mais encontrado) e sobrescrição (quando o HD excede sua capacidade de armazenamento e os novos áudios começam a sobrescrever os antigos se não for realizado o procedimento de *backup*).

O Guardião permite o conhecimento de *logs* de eventos, *logs* de gravação acesso ao sistema e o histórico de *backups*, todavia isso não permite à defesa rastrear as fontes de prova porque (1) esse rastreamento só forneceria informações até o *backup* e (2) não há sequer notícia de uma única autorização judicial conhecida que dê à defesa (ou seus eventuais assistentes técnicos) acesso ao sistema de *logs* do sistema.

Nesse sentido, o sistema de interceptação das comunicações telefônicas e de dados introduz indevidamente dois novos atores, cuja atuação não é regulamentada, e não define procedimentos e rotinas que garantam à defesa rastrear as fontes de prova para o legítimo exercício do direito ao contraditório e à ampla defesa.

Em palavras finais, a única forma de garantir a idoneidade das informações obtidas pela medida de interceptação telefônica é pela cadeia de custódia, o que não é assegurado no sistema estabelecido pela Lei nº 9.296/96, nem pela Resolução nº 59/2008, tampouco pelo funcionamento dos sistemas de TI.

## REFERÊNCIAS

ABEL LLUCH, Xavier; RICHARD GONZÁLEZ, Manuel. *Estudios sobre prueba penal volumen III: Actos de investigación y medios de prueba en el proceso penal:*

diligencias de instrucción, entrada y registro, intervención de comunicaciones, valoración y revisión de la prueba en vía de recurso. Madri: *La Ley Actualidad*, 2013.

AGUILAR, Francisco. *Dos Conhecimentos Fortuitos Obtidos Através de Escutas Telefônicas*. Coimbra: Almedina, 2004.

ANDRÉS IBÁÑEZ, Perfecto. *Prueba y convicción judicial en el proceso penal*. Buenos Aires: Hammurabi, 2009.

BACIGALUPO, Enrique. *El debido proceso penal*. Buenos Aires: Hammurabi, 2007.

BOTTINODO AMARAL, Thiago; CYRINO, André Rodrigues. Memorial apresentado pelo Instituto dos Advogados Brasileiros Ação Direta de Inconstitucionalidade nº 4.145. In: SANTORO, Antonio E. R.; MIRZA, Flávio (org.). *Interceptação Telefônica: os 20 anos da Lei nº 9.296/96*. Belo Horizonte: D'Plácido, 2016.

CARVALHO, Jefferson Lemes. Cadeia de Custódia e sua relevância na persecução penal. *Brazilian Journal of Forensic Sciences, Medical Law and Bioethics*, volume 5, p. 371-382.

CONTI, Carlotta; TONINI, Paolo. *Il diritto delle prove penali*. Milão: Giuffrè, 2012.

COSTA ANDRADE, Manuel da. *Sobre as Proibições de prova em processo penal*. Coimbra: Coimbra, 2006.

EDINGER, Carlos. Cadeia de custódia, rastreabilidade probatória. *Revista Brasileira de Ciências Criminais*, São Paulo, v. 24, n. 120, p. 237-257, mai./jun. 2016.

FERRAJOLI, Luigi. *Direito e razão: teoria do garantismo penal*. 4a ed. Trad. Ana Paula Zomer Sica, Fauzi Hassan Choukr, Juarez Tavares e Luiz Flávio Gomes. São Paulo: Revista dos Tribunais, 2014.

FESTINGER, Leon. *Teoria da dissonância cognitiva*. Trad. Eduardo Almeida. Rio de Janeiro: Zahar, 1975.

GARRIDO, Rodrigo Grazinoli; ARAUJO, Katia. Sistemas de Gestão da Qualidade em Laboratórios de Genética Forense. *Revista Espacios*, vol. 35, nº 5, 2014.

GOMES FILHO, Antonio Magalhães. Notas sobre a terminologia da prova (reflexos no processo penal brasileiro). In: YARSHELL, Flávio Luiz; ZANOIDE DE MORAES, Maurício (orgs.). *Estudos em homenagem à Professora Ada Pellegrini Grinover*. São Paulo: DPJ, 2005.

GÖSSEL, Karl Heinz. *El derecho procesal penal en el Estado de Derecho*. Obras completas. Tomo I. Santa Fe: Rubinzal-Culzoni, 2007.

HENDLER, Edmundo S. *Las garantías penales y procesales: enfoque histórico-comparado*. Buenos Aires: Editores del Puerto, 2004.

KHALED JR., Salah H. A produção analógica da verdade no processo penal. *Revista Brasileira de Direito Processual Penal*, Porto Alegre, vol. 1, p. 166-184, 2015. <https://doi.org/10.22197/rbdpp.v1i1.9>

MACHADO, Vitor Paczek; JEZLER JUNIOR, Ivan. A prova eletrônico-digital e a cadeia de custódia das provas: uma (re)leitura da súmula vinculante 14. *Boletim IBCCRIM*, São Paulo, v. 24, n. 288, p. 08-09, nov. 2016.

MARTINS, Rui Cunha. *O ponto cego do direito*. São Paulo: Atlas, 2013.

MAYA, André Machado. A prevenção como regra de exclusão da competência no processo penal: uma (re)leitura necessária a partir da jurisprudência do tribunal europeu de direitos humanos e da corte constitucional da Espanha. In: *Anais do XVII Congresso Nacional do CONPEDI*, realizado em Brasília – DF, nos dias 20, 21 e 22 de novembro de 2008.

MUÑOZ CONDE, Francisco. *De las prohibiciones probatorias al derecho procesal penal del enemigo*. Buenos Aires: Hammurabi, 2008.

MUÑOZ CONDE, Francisco. *Valoración de las grabaciones audiovisuales en el proceso penal*. 2ª ed. Buenos Aires: Hammurabi, 2007.

PASTOR, Daniel (Diretor); GUZMÁN, Nicolás (coordenador). *Neopunitivismo y neoinquisición: un análisis de políticas e prácticas penales violatorias de los derechos fundamentales del imputado*. Buenos Aires: Ad Hoc, 2008.

PRADO, Geraldo. *Prova penal e sistema de controles epistêmicos: a quebra da cadeia de custódia das provas obtidas por métodos ocultos*. 1ª ed. São Paulo: Marcial Pons, 2014.

ROXIN, Claus. *La prohibición de autoincriminación y de las escuchas domiciliarias*. Buenos Aires: Hammurabi, 2008.

SCARANCA FERNANDES, Antonio. Tipicidade e sucedâneos de prova. In: SCARANCA FERNANDES, Antonio; GAVIÃO DE ALMEIDA, José Raul; ZANOIDE DE MORAES, Maurício (coord.). *Provas no Processo Penal: estudo comparado*. São Paulo: RT, 2012.

SCHREIBER, Simone. Algumas reflexões sobre a medida cautelar de interceptação telefônica, vinte anos depois. In: SANTORO, Antonio Eduardo Ramires; MIRZA, Flávio (org.). *Interceptação Telefônica: os 20 anos da Lei nº 9.296/96*. Belo Horizonte: D'Plácido, 2016.

SCHÜNEMANN, Bernd. O juiz como um terceiro manipulado no processo penal? Uma confirmação empírica dos efeitos perseverança e aliança. In: SCHÜNEMANN, Bernd. *Estudos de direito penal, direito processual penal e filosofia do direito*. Trad. Luís Greco. São Paulo: Marcial Pons, 2013.

TARUFFO, Michele. *Uma simples verdade: o juiz e a construção dos fatos*. Tradução Vitor de Paula Ramos. São Paulo: Marcial Pons, 2012.

TONINI, Paolo. *A prova no processo penal italiano*. Trad. Alexandra Martins e Daniela Mróz. São Paulo: Revista dos Tribunais, 2002.

VALENTE, Manuel Monteiro Guedes. *Escutas Telefônicas: da excepcionalidade à vulgaridade*. 2ª ed. Coimbra: Almedina, 2008.

## DADOS DO PROCESSO EDITORIAL

(<http://www.ibraspp.com.br/revista/index.php/RBDPP/about/editorialPolicies>)

- Recebido em: 09/04/2017
- Controle preliminar e verificação de plágio: 10/04/2017
- Avaliação 1: 16/04/2017
- Avaliação 2: 23/04/2017
- Avaliação 3: 23/04/2017
- Avaliação 4: 24/04/2017
- Decisão editorial preliminar: 25/04/2017
- Retorno rodada de correções: 16/05/2017
- Decisão editorial 2: 17/05/2017
- Retorno rodada de correções 2: 19/05/2017
- Decisão editorial final: 22/05/2017

## Equipe editorial envolvida

- Editor-chefe: 1 (VGV)
- Editor-associado: 1 (MMGV)
- Revisores: 4

## COMO CITAR ESTE ARTIGO:

SANTORO, Antonio E. R.; TAVARES, Natália L. F.; GOMES, Jefferson C. O protagonismo dos sistemas de tecnologia da informação na interceptação telefônica: a importância da cadeia de custódia. *Revista Brasileira de Direito Processual Penal*, Porto Alegre, vol. 3, n. 2, p. 605-632, mai./ago. 2017. <https://doi.org/10.22197/rbdpp.v3i2.76>



Esta obra está licenciada com uma Licença *Creative Commons Atribuição-NãoComercial 4.0 Internacional*.