TEXTO FINAL – PROVA DIGITAL

CAPÍTULO IV

DA PROVA DIGITAL

Art. 298. Na disciplina da prova digital, consideram-se:

I - Dispositivo Eletrônico: equipamento ou dispositivo de tratamento ou guarda de dados que se utilize de qualquer meio ou conexão para a transmissão, emissão ou recepção das informações;

II - Sistema Informático: conjunto de dispositivos eletrônicos que utilizem de tecnologias de informação e comunicação;

III - Protocolos de Rede: conjunto de regras, padrões e especificações técnicas que regulam a transmissão de dados entre dispositivos eletrônicos;

IV - Redes de Dados: infraestrutura de meios, tecnologias e dispositivos eletrônicos de telecomunicações necessária para o tráfego de dados, conexão entre usuários e prestação ou operação de serviços de telecomunicações;

V - Pacotes de dados: conjunto de dados que trafegam por uma rede de dados obedecendo a um determinado protocolo de rede;

VI - Dados: informação multifuncional que pode servir de elemento probatório eletrônico, adequada a conformidade de sua proteção;

VII - Metadados: dados e registros gerados a partir de uma comunicação e que não constituam o seu conteúdo em si, mas sejam capazes de garantir autenticidade e contexto ao documento eletrônico;

VIIII - Dados em Transmissão: dados encapsulados em pacotes trafegando por redes segundo protocolos determinados;

IX - Dados em Repouso: dados que se encontram armazenados em um dispositivo eletrônico ou sistema informático;

X – Prova Digital: a prova nato-digital ou digitalizada;

XI - Prova Nato-Digital: informação gerada originariamente em meio eletrônico;

XII - Prova Digitalizada: informação originariamente suportada por meio físico e posteriormente migrada para armazenamento em meio eletrônico, na forma da lei.

Parágrafo único. O tratamento da prova digital será orientado pelos seguintes fundamentos:

I - direito fundamental à proteção de dados, assegurando-se o seu uso de forma adequada, necessária e proporcional, observado o disposto no § 1º do art. 4º da Lei nº 13.709, de 14 de agosto de 2018;

II - respeito à soberania nacional;

III - a cooperação jurídica internacional;

IV - garantia de autenticidade e da integridade da informação;

V - a preservação da Empresa e sua função social; e

VI - transparência dos meios de tratamento da informação.

Art. 299 Considera-se prova digital todo dado produzido, armazenado ou transmitido em meio eletrônico, hábil ao esclarecimento de determinado fato que diga respeito à prática de crimes.

§1º A informação contida ou transmitida por meios eletrônicos que diz respeito à proveniência dos dados digitais é compreendida como fonte de prova digital.

§ 2º A aquisição de fontes de provas digitais deve ocorrer a partir de técnicas investigativas menos intrusivas, em respeito às garantias fundamentais previstas na Constituição Federal, incluindo devido processo legal e respeito aos direitos fundamentais.

§ 3º A aquisição de fontes de provas digitais deve se limitar ao mínimo necessário, evitando-se obtenção de informações não essenciais à investigação. A aquisição de informações pertencentes a pessoas que não são alvo de investigação devem ser descartadas, sendo vedado o seu tratamento; e

§4º A admissibilidade da prova digital depende da preservação da integridade e autenticidade do dado digital que se pretende conceber como elemento de prova.

§ 5º À prova digital aplicam-se subsidiariamente as disposições relativas às provas em geral.

Art. 300 A admissibilidade da prova digital na investigação e no processo exigirá a disponibilidade dos metadados e a descrição dos procedimentos de custódia e tratamento suficientes para a verificação da sua autenticidade e integridade, além da auditabilidade, repetição e reprodutibilidade.

Parágrafo único. Se da prova digital derivar produto de tratamento de dados por aplicação de operação matemática ou estatística, de modo automatizado ou não, devem estar transparentes os parâmetros e métodos empregados.

Art. 301 Para o fim da investigação ou instrução processual penal, poderão o Ministério Público, a defesa ou o delegado de polícia, requerer ordem judicial

para guarda e acesso à prova digital sob controle de terceiros, observados os requisitos de necessidade, finalidade, adequação, proporcionalidade e qualidade dos dados.

§ 1º Quando formulado pelo delegado de polícia, o Ministério Público será ouvido acerca do pedido.

§2º O requerimento deve individualizar usuários, provedores, dispositivos eletrônicos ou sistemas informáticos, temporalidades, redes de dados e protocolos de rede próprios ao contexto da investigação ou da instrução processual, não podendo ter caráter genérico.

§3º Os dados transmitidos ou encaminhados em suporte físico, pelos provedores, em cumprimento de ordem judicial ou, sendo dados cadastrais, por requisição da autoridade policial e do Ministério Público, devem estar em formato interoperável e com garantia de autenticidade e integridade.

§4º O requerimento e concessão de ordem judicial que franqueou acesso à prova digital sob controle de terceiros deve primar pelos métodos menos intrusivos e pela razoabilidade e adequação do pedido com relação aos objetivos de uso da prova digital.

Art. 302. Os provedores de conexão e aplicação deverão manter, além das informações de guarda legal previstas em lei, os registros de dados pessoais necessários e suficientes para a individualização inequívoca dos usuários de seus serviços pelo prazo de um ano.

Art. 303 Se houver receio de que a prova digital possa perder-se, alterar-se ou deixar de estar disponível, poderá o juiz, a requerimento da defesa, e o delegado de polícia ou o Ministério Público ordenar a quem tenha disponibilidade, controle ou opere os dados, que os guarde pelo prazo de até noventa dias, podendo este prazo ser renovado por decisão judicial fundamentada, observadas a necessidade, finalidade, adequação, proporcionalidade e qualidade dos dados.

§ 1º O requerimento deverá indicar os dados concretos a serem guardados, vedados pedidos genéricos ou inespecíficos.

§ 2º O requerimento realizado por delegado de polícia ou pelo Ministério Público, independentemente de ordem judicial, será comunicado ao juiz competente em até vinte e quatro horas, para validação da medida.

§ 3º A extensão do prazo de guarda da prova digital será realizada por decisão judicial e deverá apresentar fundamentações claras a respeito dos riscos de armazenamento da informação em questão, incluindo:

I - fato ou indício que configura risco de alteração ou perda da prova; e

II - razões que configurem risco concreto a partir da descrição do contexto.

§ 4º O acesso à prova digital dependerá de autorização judicial específica de acordo com o disposto neste capítulo.

Seção I

Dos Meios de obtenção

Art. 304. Constituem meios de obtenção da prova digital, na forma da Lei:

I - a coleta por acesso forçado de sistema informático ou de redes de dados;

II - o tratamento de dados disponibilizados em fontes abertas, independentemente de autorização judicial.

Seção II

Interceptação Telemática

Art. 305. A interceptação telemática poderá ser destinada aos provedores ou serviços de conexão ou aplicação, bem como aos dispositivos eletrônicos ou sistemas informáticos particulares, devendo ser individualizadas as redes de dados e os protocolos de internet envolvidos.

Parágrafo único. A interceptação telemática seguirá subsidiariamente o procedimento estabelecido para a interceptação telefônica.

Seção III

Requisição itinerante

Art. 306 SUPRESSÃO

Seção IV

Coleta por Acesso Forçado

Art. 307. A coleta por acesso forçado a dispositivo eletrônico, sistema informático ou redes de dados, ocorrerá somente após prévia desobediência de ordem judicial determinando a entrega da prova pretendida ou quando impossível identificar o controlador ou provedor em território nacional, e compreenderá os

métodos de segurança ofensiva ou qualquer outra forma que possibilite a exploração, isolamento e tomada de controle.

Parágrafo único. Em caso de dispositivo, sistema informático ou redes de dados que se encontrem em território estrangeiro, somente se procederá por via da cooperação internacional.

Seção V

Decisão judicial e prazo

Art. 308. A ordem judicial para obtenção da prova digital para fins de investigação e processo penal descreverá os fatos investigados com a indicação da materialidade e indícios de autoria delitiva, indicando ainda os motivos, a necessidade e os fins da diligência, estabelecendo os limites da atividade a ser empreendida e o prazo para seu cumprimento.

§ 1º Em caso de monitoramento do fluxo de dados, o prazo da medida não poderá exceder a sessenta dias, permitidas prorrogações por igual período, desde que continuem presentes os pressupostos autorizadores da diligência, até o máximo de trezentos e sessenta dias, salvo quando se tratar de crime permanente, enquanto não cessar a permanência.

§ 2º A obtenção da prova digital pode se dirigir a uma terceira pessoa, desde que haja indícios de que o investigado utilize o dispositivo eletrônico, ou quaisquer outros meios de armazenamento de informação eletrônica, com ou sem o conhecimento do proprietário.

§ 3º A polícia investigativa ou o Ministério Público poderá requisitar a guarda da prova digital sem acesso ao conteúdo pelo prazo de um ano, independentemente de autorização judicial, quando houver perigo na demora, devendo comunicar a medida ao juiz competente em até vinte e quatro horas, para validação da medida.

Seção VI

Mandado judicial

Art. 309. A decisão judicial será instrumentalizada por mandado, dirigido aos seus executores e às pessoas naturais ou jurídicas que irão sofrê-la, suficientemente instruído com:

I - informações sobre os fatos sob investigação;

II - a pessoa natural ou jurídica alvo da diligência, se possível;

III - os dispositivos eletrônicos, sistemas informáticos ou quaisquer outros meios de armazenamento de informação eletrônica, se for o caso;

IV - os provedores de estrutura, de conexão ou de aplicação, potencialmente atingidos;

V - o objeto da medida, os procedimentos autorizados a serem efetuados, os limites da apreensão e o prazo para cumprimento.

Parágrafo único. Será expedido mandado de intimação aos interessados, nos termos do caput, logo após o fim do cumprimento da medida, desde que não prejudique a operação.

Seção VII

Auto Circunstanciado

Art. 310. Ao fim da diligência para obtenção da prova digital, o órgão de investigação lavrará auto circunstanciado, com declaração do lugar, dia e hora em que se realizou, com menção das pessoas que a sofreram e das que nela tomaram parte ou a tenham assistido, com as respectivas identidades, bem como de todos os incidentes ocorridos durante a sua execução, especificando-se os procedimentos adotados e equipamentos utilizados.

Art. 311. Caso a diligência para obtenção da prova digital seja positiva, constará do auto circunstanciado a relação e descrição das coisas e dos dados apreendidos, bem como dos métodos de preservação de sua autenticidade e integridade.

Art. 312. O cumprimento da diligência será comunicado à autoridade judicial competente, no prazo de setenta e duas horas, informando-se do seu resultado e do encaminhamento conferido aos objetos coletados e apresentando-se cópia do auto circunstanciado.

Seção VIII

Cadeia de Custódia Específica

Art. 313. Além do auto circunstanciado, será elaborado o registro da custódia do que foi apreendido na diligência, indicando os custodiantes e as transferências havidas, bem como as demais operações realizadas em cada momento da cadeia.

Art. 314. Os meios de obtenção da prova digital serão implementados por perito oficial ou assistente técnico da área de informática, que deverão proceder conforme as boas práticas aplicáveis aos procedimentos a serem desenvolvidos, cuidando para que se preserve a integridade, a completude, a autenticidade, a auditabilidade e a reprodutibilidade dos métodos de análise.

§ 1º No curso da obtenção, será garantido, independentemente de norma técnica:

I - ambiente controlado com redução de contaminação;

II - espelhamento técnico em duas cópias, com o máximo de metadados e a descrição completa de procedimentos, datas, horários ou outras circunstâncias de contexto aplicáveis;

III - preservação imediata após o ato de espelhamento com emprego de recurso confiável que garanta a integridade da prova.

§ 2º A autoridade judicial, mediante requerimento do órgão de investigação ou do interessado, requisitará aos controladores o encaminhamento de dados pessoais associados à prova digital obtida e que sejam complementares e suficientes para a sua análise contextual.

Art. 315. Uma cópia dos dados resultantes da diligência, feita por espelhamento, será encaminhada e armazenada pela autoridade judicial competente, para eventual confronto. As análises, as pesquisas e os exames periciais devem ser realizados sobre cópia de trabalho.

Parágrafo único. Os terceiros interessados, assim reconhecidos em decisão judicial fundamentada, poderão ter acesso ao conteúdo da cópia do espelhamento, ouvido o titular dos dados e o Ministério Público e mediante compromisso de sigilo.

Art. 316. Salvo expressa determinação judicial em contrário, ou impossibilidade de cumprimento por fundamentada motivação técnica ou operacional da medida desta forma, a apreensão da prova digital ocorrerá por espelhamento, não se fazendo a apreensão de dispositivos eletrônicos, sistemas informáticos ou quaisquer outros meios de armazenamento de informação eletrônica.

Seção IX

Restituição de dispositivos eletrônicos ou sistemas informáticos

Art. 317. Em caso de impossibilidade de apreensão por espelhamento, será garantida aos titulares ou agentes de tratamento atingidos pela apreensão dos dispositivos eletrônicos, sistemas informáticos ou outros meios de

armazenamento de informação eletrônica cópia dos dados coletados. A apreensão não poderá superar o prazo de sessenta dias, salvo por motivo relevante.

Seção X

Sigilo profissional e religioso

Art. 318. Os meios de obtenção da prova digital observarão o sigilo em razão de função, ministério, ofício ou profissão, incluindo, mas não se limitando, o sigilo médico, religioso e o sigilo da relação advogado e cliente, ressalvados os casos em que o exercício da atividade represente ou preste-se a encobrir a atuação delitiva.

Seção XI

Dados íntimos e restrições de acesso à informação

Art. 319. Os dados pessoais sensíveis, íntimos ou sigilosos do investigado, acusado, pessoas a ele relacionadas, bem como das vítimas e pessoas a elas relacionadas que sejam relevantes ao caso, mas que não digam respeito aos demais sujeitos processuais, serão apartados em autos próprios, mantendo-se acessíveis apenas aos interessados, vedada a alteração do espelhamento.

§ 1º Decorridos cinco anos do cumprimento integral da sentença condenatória ou em caso de absolvição ou de decretação de extinção de punibilidade, os dados mencionados no caput serão indisponibilizados, desde que não haja interesse público na preservação ou que não tenham relevância ou pertinência processual, devendo ser intimados os interessados e atualizada a garantia de integridade e anterioridade dos dados remanescentes.

§ 2º Os dados que se enquadrem nas restrições de acesso à informação, nos termos da lei, serão apartados em autos próprios e encaminhados em vinte e quatro horas à autoridade competente, vedada a alteração do espelhamento.

§ 3º Em qualquer caso, poderá o titular de dados pessoais ou legítimo interessado, requerer em autos apartados a imediata indisponibilização de dados pessoais sensíveis que não possuam relação com os fatos em apuração, observado o contraditório.

Art. 320. Aplica-se, no que couber, a disciplina da cadeia de custódia da prova.

Parágrafo único: Verificada a quebra da cadeia de custódia que resulte em desvantagens probatórias à vítima, reconhece-se direito à indenização em face do Estado, sem prejuízo da responsabilização administrativa e penal do agente.

Seção XII

Encontro fortuito

Art. 320. Se, na coleta da prova digital judicialmente autorizada, houver o encontro fortuito de dados relacionados a infração penal, estes deverão ser remetidos como notícia crime ao órgão de investigação.