

CLAUDIO JOEL BRITO LÓSSIO

MANUAL *DESCOMPLICADO* DE DIREITO DIGITAL

Guia para
Profissionais
e Concurseiros
do Direito e
da Tecnologia

4ª edição
revista, atualizada
e ampliada

2024

 EDITORA
*Jus*PODIVM
www.editorajuspodivm.com.br

As aplicações *web* e *desktop* são *softwares*, conforme apresentado logo no início desta escrita e são protegidos por esse diploma legal, veja o artigo 12.

Artigo	Tipo	Exemplo
Artigo 12	Violar direitos de autor de programa de computador.	Utilização de programa pirata. (Cópia não original)

10.6. TIPO PENAL NA LEI DE INTERCEPTAÇÃO TELEFÔNICA¹⁷

Artigo	Tipo
Artigo 10	Interceptação de comunicações sem autorização judicial.

10.7. TIPOS NO CÓDIGO PENAL BRASILEIRO – ADMINISTRAÇÃO PÚBLICA

Neste subtópico estão tipos do Código Penal Brasileiro direcionados à Administração Pública.

Artigo	Tipo	Exemplo
Artigo 154-B	Nos crimes definidos no art. 154-A, somente se procede mediante representação, salvo se o crime é cometido contra a administração pública direta ou indireta de qualquer dos Poderes da União, Estados, Distrito Federal ou Municípios ou contra empresas concessionárias de serviços públicos.	Ataque por <i>ransomware</i> na administração pública.

17. BRASIL **Lei nº 9.296, de 24 de julho de 1996**. “Art. 10. Constitui crime realizar interceptação de comunicações telefônicas, de informática ou telemática, ou quebrar segredo da Justiça, sem autorização judicial ou com objetivos não autorizados em lei.” Regulamenta o inciso XII, parte final, do art. 5º da Constituição Federal. Disponível em: <http://www.planalto.gov.br/ccivil_03/Leis/l9296.htm>. Acesso em: 16 mai. 2018.

Artigo	Tipo	Exemplo
Artigo 266	Interromper ou perturbar serviço telegráfico, radiotelegráfico ou telefônico, impedir ou dificultar-lhe o restabelecimento.	Ataque DDOS.
Artigo 313-A	Inserir ou facilitar, o funcionário autorizado, a inserção de dados falsos, alterar ou excluir indevidamente dados corretos nos sistemas informatizados ou bancos de dados da Administração Pública com o fim de obter vantagem indevida para si ou para outrem ou para causar dano.	Inserção de dados falsos em sistema de informações.
Artigo 313-B	Modificar ou alterar, o funcionário, sistema de informações ou programa de informática sem autorização ou solicitação de autoridade competente.	Modificação ou alteração não autorizada de sistema de informações.
Artigo 325	Revelar fato de que tem ciência em razão do cargo e que deva permanecer em segredo, ou facilitar-lhe a revelação.	Revelação segredo por servidor público.
Artigo 325, § 1º, I	Permite ou facilita, mediante atribuição, fornecimento e empréstimo de senha ou qualquer outra forma, o acesso de pessoas não autorizadas a sistemas de informações ou banco de dados da Administração Pública.	Compartilhamento de senha.

11. PROVAS DIGITAIS

A abordagem sobre as provas estão presentes em nosso Código de Processo Civil, em seu artigo 369, ao afirmar que “as partes têm o direito de empregar todos os meios legais, bem como os moralmente legítimos, ainda que não especificados neste Código, para provar a verdade dos fatos em que se funda o pedido ou a defesa e influir eficazmente na convicção do juiz”.

Segundo Renato Brasileiro, “é o conjunto de atos que são praticados pelas partes, pelo juiz e por terceiros visando proporcionar ao magistrado subsídios suficientes para formar a sua convicção sobre a existência ou não de determinado fato, ou a veracidade ou falsidade de dada afirmação.”

No âmbito digital, Pedro Verdelho, afirma que o mundo virtual é deslocado, apenas sendo possível considerá-lo de uma forma abrangente, à escala planetária, assim em acordo com “a sociedade civil global”, de José Joaquim Gomes Canotilho e Vital Moreira.¹

1. CANOTILHO, José Joaquim Gomes; MOREIRA, Vital. (2007). **CRP:** Constituição da República Portuguesa. *Ibidem*.

Este capítulo poderia até estar junto do que toca a perseguição penal, mas como as provas no direito digital também possuem um caráter de imperiosa relevância, acabou por ficar independente nesta obra.

As provas, evidências, indícios e vestígios farão parte do dia a dia da preservação dos fatos ocorridos no ambiente digital, e há uma diferença entre o que é cada um desses institutos, os quais serão apresentados, iniciando pelo vestígio.

Conforme o Dicionário da Língua Portuguesa, vestígio (lat *vestigiu*) significa: sinal deixado pela pisada ou passagem, tanto do homem como de qualquer outro animal; pegada, rasto. Indício ou sinal de coisa que sucedeu, de pessoa que passou (...).²

Já no Código de Processo Penal, em seu art. 158-A:

§ 3º **Vestígio** é todo objeto ou material bruto, visível ou latente, constatado ou recolhido, que se relaciona à infração penal. (Grifo Nosso)

Assim, em ambiente digital, deve ser observado qualquer vestígio, como alguma alteração no sistema operacional, por exemplo, uma pasta incomum, um processamento alto ou uma elevada utilização de memória, que tornasse necessário que a equipe de resposta a incidentes (e/ou perito) de segurança da informação fosse acionada para levantamento das evidências. Mas no ambiente digital, o que é uma evidência?

-
2. MALLMITH, Décio. **A perícia vale o que vale o perito**. 2020. Disponível em: <<https://criminalisticaforense.wordpress.com/2011/12/11/vestigios-evidencias-e-indicios/#:~:text=239%20do%20CPP%20parece%20sin%C3%B4nimo%20do%20conceito%20de%20evid%C3%A2ncia.&text=Portanto%2C%20conclui%2Dse%20que%20toda,encaminha%3B%20o%20ind%C3%ADcio%20aponta.%E2%80%9D>>. Acessado em: 19 de jan. 2021.

Segundo Mallmith, no âmbito da criminalística, a evidência é o vestígio após análise,³ muito embora no âmbito digital a evidência é o objeto que será feito o processo da recolha para passar pela fase do exame e análise, como a imagem de um dispositivo de armazenamento interno ou nuvem e coleta de dados de *e-mail*, por exemplo.

Já o indício está previsto no Código de Processo Penal, mais precisamente no Art. 239 (CPP): “Considera-se indício a circunstância conhecida e provada, que, tendo relação com o fato, autorize, por indução, concluir-se a existência de outra ou outras circunstâncias.”⁴ Assim, o indício é identificado na fase pós-pericial, e deve compor o relatório pericial, o qual será uma prova pericial.⁵

Figura 28 – Vestígio, Evidência, Indício e Prova



Fonte: Autor.

11.1. PEDRAS DE TOQUE DAS PROVAS DIGITAIS

O termo pedras de toque, é utilizado por Celso Antonio Bandeira de Mello ao abordar os dois princípios basilares do Direito Administrativo. Segundo o Dicio.com.br, pedra de toque é um material que serve para analisar a pureza de metais

3. Idem. Ibidem.

4. BRASIL. **Decreto-Lei nº 3.689, de 03 de outubro de 1941**. Código de Processo Penal. Ibidem.

5. BRASIL. **Decreto-Lei nº 3.689, de 03 de outubro de 1941**. Código de Processo Penal. Disponível em: <http://www.planalto.gov.br/ccivil_03/decreto-lei/del3689.htm>. Acessado em: 19 jan. 2021.

preciosos, servindo para avaliar a essência ou a verdadeira natureza de algo. Com isso no direito digital há duas pedras de toque que envolve o ambiente legal e o informático, que serão apresentados mais adiante.

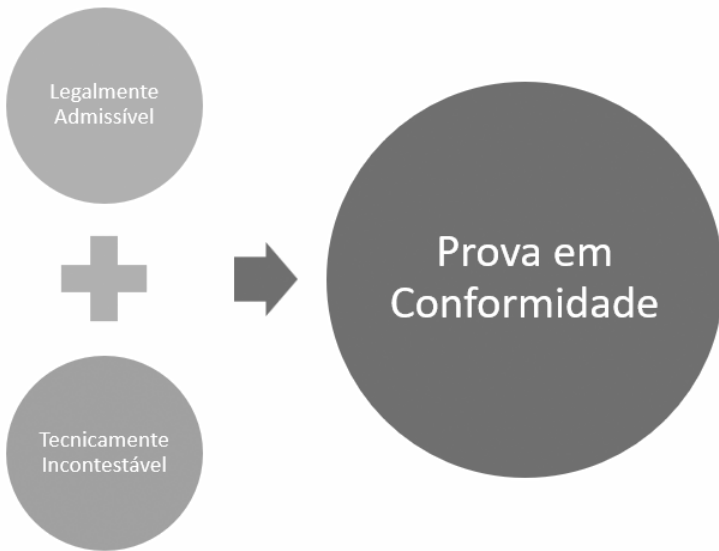
As provas darão convicção para a decisão do juiz e serão criadas a partir dos indícios presentes no relatório pericial, ou no parecer apresentado pelo assistente técnico, que devem possuir narrativas claras constituídas legalmente admissível e tecnicamente incontestável para que tenha o máximo de força possível para o convencimento do magistrado. É muito difícil não existir questionamentos e contestações, mas se a conformidade técnica e legal for plena, a eficácia da prova poderá ser positiva.

É de supra importância que os procedimentos periciais sejam realizados por profissionais que busquem ao máximo a conformidade técnica e legal para que dinheiro e tempo não sejam gastos em vão.

As provas digitais possuem alguns aspectos:

- É frágil e pode ser facilmente alterada ou destruída;
- Pode ser tão encoberta e dissimulada;
- Pode facilmente cruzar fronteiras;
- Depende da hora e local exato onde foi produzida.

As provas devem estar em conformidade legal, para que não sejam desentranhadas do processo. Assim devendo possuir como: PEDRAS DE TOQUE DAS PROVAS DIGITAIS:

Figura 29 – Pedras de Toque das Provas Digitais

Fonte: Autor.

Entre os procedimentos apresentados pelo pacote anti-crime, a cadeia de custódia teve uma evolução enorme, esclarecendo melhor o rito envolvendo o rastreamento do vestígio:

Art. 158-B. A cadeia de custódia compreende o rastreamento do vestígio nas seguintes etapas:

I - reconhecimento: ato de distinguir um elemento como de potencial interesse para a produção da prova pericial;

II - isolamento: ato de evitar que se altere o estado das coisas, devendo isolar e preservar o ambiente imediato, mediato e relacionado aos vestígios e local de crime;

III - fixação: descrição detalhada do vestígio conforme se encontra no local de crime ou no corpo de delito, e a sua posição na área de exames, podendo ser ilustrada por fotografias, filmagens ou croqui, sendo indispensável a sua descrição no laudo pericial produzido pelo perito responsável pelo atendimento;

IV - coleta: ato de recolher o vestígio que será submetido à análise pericial, respeitando suas características e natureza;

V - acondicionamento: procedimento por meio do qual cada vestígio coletado é embalado de forma individualizada, de acordo com suas características físicas, químicas e biológicas, para posterior análise, com anotação da data, hora e nome de quem realizou a coleta e o acondicionamento;

VI - transporte: ato de transferir o vestígio de um local para o outro, utilizando as condições adequadas (embalagens, veículos, temperatura, entre outras), de modo a garantir a manutenção de suas características originais, bem como o controle de sua posse;

VII - recebimento: ato formal de transferência da posse do vestígio, que deve ser documentado com, no mínimo, informações referentes ao número de procedimento e unidade de polícia judiciária relacionada, local de origem, nome de quem transportou o vestígio, código de rastreamento, natureza do exame, tipo do vestígio, protocolo, assinatura e identificação de quem o recebeu;

VIII - processamento: exame pericial em si, manipulação do vestígio de acordo com a metodologia adequada às suas características biológicas, físicas e químicas, a fim de se obter o resultado desejado, que deverá ser formalizado em laudo produzido por perito;

IX - armazenamento: procedimento referente à guarda, em condições adequadas, do material a ser processado, guardado para realização de contraperícia, descartado ou transportado, com vinculação ao número do laudo correspondente;

X - descarte: procedimento referente à liberação do vestígio, respeitando a legislação vigente e, quando pertinente, mediante autorização judicial.

Caso a prova seja obtida ou derivada com vícios na licitude, será considerada ilícita, assim:

Art. 157. São inadmissíveis, devendo ser desentranhadas do processo, as provas ilícitas, assim entendidas as obtidas em violação a normas constitucionais ou legais.

§ 1º São também inadmissíveis as provas derivadas das ilícitas, salvo quando não evidenciado o nexo de causalidade entre umas e outras, ou quando as derivadas puderem ser obtidas por uma fonte independente das primeiras.

§ 2º Considera-se fonte independente aquela que por si só, seguindo os trâmites típicos e de praxe, próprios da investigação ou instrução criminal, seria capaz de conduzir ao fato objeto da prova.

§ 3º Preclusa a decisão de desentranhamento da prova declarada inadmissível, esta será inutilizada por decisão judicial, facultado às partes acompanhar o incidente.

§ 5º O juiz que conhecer do conteúdo da prova declarada inadmissível não poderá proferir a sentença ou acórdão.

A prova ilícita é inadmissível e deverá ser desentranhada do processo, sendo então inutilizada, inclusive, o juiz que tiver conhecido a prova declarada inadmissível, não poderá proferir a sentença ou acórdão.

11.2. ESTUDO DE CASO

Mas, como atribuir a culpa ou dolo a alguém? Através das provas, indícios obtidos nas evidências e, para isso, neste subtópico serão apresentados alguns meios de prova e meios de preservação do conteúdo digital.

No decorrer deste capítulo, será apresentada a narrativa de TÍCIO para proporcionar um maior entendimento. Para tal tipo de abordagem parte-se do crime digital impróprio, assim, serão apresentados alguns procedimentos de preservação do fato ocorrido no ambiente digital.

Fato:

TÍCIO possui uma rede social, FB-SOCIAL, com um perfil público e permitindo também postagem ou comentário por qualquer usuário da rede social.

MÉVIO possui plano de *internet* com o PROVEDOR-X em sua residência. Conectado na rede Wi-Fi de sua casa, cria um perfil falso na rede social FB-SOCIAL, acessa o perfil de TÍCIO e faz ameaças contra a vida de TÍCIO em uma postagem.

Diante do exposto, TÍCIO deverá buscar mais rápido possível realizar alguns procedimentos para preservar o conteúdo que poderá evidenciar a ameaça, a postagem, e aumentando a força com novos procedimentos, visto que poderá ser excluída a qualquer momento por MÉVIO. E agora?

11.2.1. Testemunhas

A prova testemunhal deverá ocorrer em um primeiro momento, pois como a evidência pode ser eliminada a qualquer momento, o tempo torna-se um inimigo da preservação, assim:

TÍCIO deverá chamar as pessoas presentes próximas para testemunharem o ocorrido, pois o testemunho poderá ser a única prova no processo.

Qualquer pessoa poderá ser testemunha, e o depoimento deve ser oral, segundo os Artigos 202 e 204:

Art. 202. Toda pessoa poderá ser testemunha.

Art. 204. O depoimento será prestado oralmente, não sendo permitido à testemunha trazê-lo por escrito.

Parágrafo único. Não será vedada à testemunha, entretanto, breve consulta a apontamentos.⁶

Com o testemunho de pessoas conforme citado, agora TÍCIO deve dar mais força ainda a evidência. Agora deve:

6. BRASIL. **Decreto-Lei nº 3.689, de 03 de outubro de 1941**. Código de Processo Penal. *Ibidem*.

<i>Prints</i> ⁷ da tela no próprio dispositivo, sem recortar o <i>print</i> ;
De outro dispositivo, fazer fotos da tela no dispositivo com a ameaça;
De outro dispositivo, fazer filmagens da tela no dispositivo com a ameaça.

Até então, nada formal, tudo de maneira rápida. Esse outro dispositivo pode ser o particular de cada uma das testemunhas. Lembrando que toda pessoa poderá ser uma testemunha diante de tal situação e, mesmo o depoimento em juízo sendo oral, nada impede de ser utilizado um apontamento.⁸

Devendo as testemunhas estarem completamente cientes que, segundo o Artigo 342: “Fazer afirmação falsa, ou negar ou calar a verdade como testemunha, perito, contador, tradutor ou intérprete em processo judicial, ou administrativo, inquérito policial, ou em juízo arbitral”, constitui crime, tipificado no Código Penal Brasileiro o falso testemunho ou falsa perícia.⁹

11.2.2. Armazenar a URL

Caso TÍCIO possua conhecimento para preservar a URL ou contrate um advogado que atue em direito digital e possua tal competência, (ou tenha lido este livro, hehe). A URL já foi antecipadamente apresentada anteriormente, e o armazenamento dela é fundamental, mas como armazenar a URL?

7. Proporcionar a captura na íntegra da tela do computador ou dispositivo móvel. Em alguns computadores poderá ser o feito através da tecla PrtScr, em *smartphones* normalmente ao pressionar botões de forma combinada. Ex: *power* e volume.

8. BRASIL. **Decreto-Lei nº 3.689, de 03 de outubro de 1941**. Código de Processo Penal. Ibidem.

9. BRASIL. **Decreto-Lei nº 2.848, de 7 de dezembro de 1940**. Código Penal Brasileiro. Disponível em: <http://www.planalto.gov.br/ccivil_03/decreto-lei/Del2848compilado.htm>. Acesso em: 12 mai. 2018.

Em um repositório ou depósitos de páginas *web* e, a preservação poderá ser realizada facilmente, assim apresentando-se o WebArchive – *Waybackmachine*¹⁰, que é um “arquivo” da *internet*. Este armazenamento poderá contribuir para uma investigação pericial posterior.

Copie (Ctrl+C) o endereço da URL na página onde ocorreu a ameaça;
Acesse <<https://web.archive.org/>>;
Vá até “Save Page Now”, Cole (Ctrl+V);
Clique em Save Page.

Pronto, o armazenamento da URL foi concluído com êxito. O próximo passo será o BO/TCO.

11.2.3. Fazer BO/TCO

A partir dessa etapa, é essencial a presença de um advogado que atue com direito digital e saiba contribuir para que todos os detalhes sejam observados. Assim, TÍCIO deve procurar uma Delegacia de Polícia e fazer um Boletim de Ocorrência (BO)/ Termo Circunstanciado de Ocorrência (TCO), dependendo do crime. O BO ou o TCO são a porta de entrada para o início do Inquérito Policial, que tem como objeto da investigação o fato, para achar inicialmente o indiciado, que é o indivíduo com indícios suficientes de autoria.

A função desse inquérito policial é a formação de elementos que propicia ao Ministério Público extrair a justa

10. WAYBACKMACHINE. **Internet Archive**. Disponível em: <<https://web.archive.org/>>. Acesso em: 12 mai. 2018.

causa para a ação penal, caso o crime tenha como base uma ação pública. Caso não seja, então servirá para registrar o fato e representar.

A lista das delegacias especializadas em crimes digitais está disponível no site da SaferNet, e estão localizadas nas capitais dos estados abaixo relacionados:¹¹

- Bahia
- Espírito Santo
- Maranhão
- Mato Grosso
- Minas Gerais
- Pará
- Paraná
- Pernambuco
- Piauí
- Rio Grande do Sul
- São Paulo (1)
- São Paulo (2)
- Sergipe
- Rio de Janeiro
- Tocantins
- Distrito Federal

11. SAFERNET. **Delegacias Cibercrimes**. 2018. Disponível em: <<http://new.safernet.org.br/content/delegacias-cibercrimes>>. Acesso em: 12 jan. 2021.

O Brasil ainda é muito debilitado quando se fala em delegacias voltadas ao combate do crime eletrônico, muito embora haja projetos para implantação de delegacias especializadas em cibercrimes em várias cidades. Caso sua cidade não possua uma delegacia especializada, busque a mais próxima de sua residência, mesmo não sendo voltada para os cibercrimes.

Com isso TÍCIO deverá ir à delegacia fazer:

Fazer BO/TCO na delegacia.

11.2.4. Fazer Ata Notarial

A ata notarial é um instrumento que é lavrado por uma pessoa física, o tabelião de notas, o qual dará a fé pública que lhes foi investida pelo Estado¹² a uma constatação dos fatos observados. A ata notarial está expressa no nosso Código de Processo Civil¹³ e, como falado, esta poderá ser conceituada como o instrumento público lavrado pelo notário e por este conferido, constatado e dado fé que tem por finalidade a produção antecipada de prova tanto para fins administrativos quanto judiciais.¹⁴

12. DIP, Ricardo. **Registros Públicos**. São Paulo: Editora Millenium. 2017, p. 52.

13. BRASIL. **Lei nº 13.105, de 16 de março de 2015**. Código de Processo Civil. “Art. 384. A existência e o modo de existir de algum fato podem ser atestados ou documentados, a requerimento do interessado, mediante ata lavrada por tabelião. Parágrafo único. Dados representados por imagem ou som gravados em arquivos eletrônicos poderão constar da ata notarial.” Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2015/lei/l13105.htm>. Acesso em: 30 mar. 2018.

14. LOUREIRO, Luiz Guilherme. **Registros Públicos: Teoria e Prática**. 8. ed. Salvador: Juspodivm, 2017, p. 1212.

A ata notarial deve ser lavrada publicamente no cartório de notas pelo tabelião de notas, ou seja, o Notário, com a finalidade de constatação de que determinado fato ocorreu, muito embora em alguns casos o Tabelião não possa garantir a autenticidade de algumas situações, visto que pode ser necessária uma perícia para sua concretização.¹⁵ Cabe perceber que o cartório preserva documentos públicos, e uma ata lavrada por uma pessoa poderá ser consultada por qualquer outra que se dirija ao cartório e solicite uma certidão da determinada ata.

Assim, os serviços notariais, incluindo a ata, têm como finalidade garantir a publicidade, autenticidade e segurança dos atos jurídicos, por exemplo, a vontade das partes. Veja alguns dos artigos da Lei 8.935/94, que regulamenta os Atos Notariais:

Art. 1º Serviços notariais e de registro são os de organização técnica e administrativa destinados a garantir a publicidade, autenticidade, segurança e eficácia dos atos jurídicos.

Art. 6º Aos notários compete:

- I - formalizar juridicamente a vontade das partes;
- II - intervir nos atos e negócios jurídicos a que as partes devam ou queiram dar forma legal ou autenticidade, autorizando a redação ou redigindo os instrumentos adequados, conservando os originais e expedindo cópias fidedignas de seu conteúdo;
- III - autenticar fatos.

Segundo o conceito anteriormente citado, a ata notarial é o instrumento para constatação de um fato, e oficializado em um documento com fé pública.

15. Idem. Op. Cit., p. 1213.

O que deverá constar em uma ata notarial de TÍCIO?

Fazer uma ata notarial em cartório, que deve conter:

As URL que identifiquem os fatos (Se possível);

As URL que identifiquem os perfis (Se possível);

Datas;

Horas;

Mensagens;

Prints, vídeos e áudios (Se possível);

E todos os demais dados que achar importante.

As URL do local do ocorrido e do perfil devem ser armazenadas sempre que possível, visto que existem aplicações em dispositivos móveis nos quais não há a possibilidade de coletar a URL e pode ser tentado se existir a mesma aplicação em *desktop* ou para acessar via navegador, para a ata notarial.

Para ganhar tempo, o advogado poderá relatar todo o ocorrido em forma textual para que, ao chegar no cartório para lavrar a ata notarial, esse trabalho seja facilitado para o tabelião de notas como, por exemplo, em casos de ligações telefônicas gravadas.

Como o crime citado foi a ameaça, e com todo esse procedimento realizado, agora o processo inicial já pode ser instaurado. Caso o procedimento fosse um crime próprio que exigisse perícia judicial ou uma possível assistência técnica, o procedimento deverá partir para a análise pericial, seja determinado pela polícia, no caso de crime público incondicionado, ou informado pelo advogado caso seja um crime próprio, mas que necessite representação.

A ata notarial poderá ser uma primeira preservação, mas a *internet* deixa rastros, sempre. Veja então as palavras da professora Patrícia Peck Pinheiro em entrevista para a revista Carta Forense em 2011:¹⁶

Ao contrário do que aparente, o mundo digital não é uma terra sem dono e todos os atos praticados pela internet deixam rastros. Seguindo tais rastros, é possível encontrar os responsáveis, os quais irão sofrer as penalidades cabíveis para cada caso.

Assim, quando a prova deixa rastros, segundo o Código de Processo Penal Brasileiro, em seu artigo 158: “Quando a infração deixar vestígios, será indispensável o exame de corpo de delito, direto ou indireto, não podendo supri-lo a confissão do acusado”. Então, em caso de ausência do exame de corpo de delito, surge também o artigo 564 do Código de Processo Penal: “A nulidade ocorrerá nos seguintes casos: III - por falta das fórmulas ou dos termos seguintes: b) o exame do corpo de delito nos crimes que deixam vestígios, ressalvado o disposto no Art. 167”, onde expressa: “Não sendo possível o exame de corpo de delito, por haverem desaparecido os vestígios, a prova testemunhal poderá suprir-lhe a falta”.

Assim, há uma importância necessária no exame pericial, para que assim o conteúdo probatório do ocorrido no ambiente cibernético seja apresentado. E quando surge por vias dos crimes digitais impróprios, esse exame provavelmente poderá, diante do entendimento do juiz, ser suprido pela prova testemunhal. Então, eis a importância da presença de testemunhas durante tal ilicitude no ambiente cibernético.

16. PINHEIRO, Patrícia Peck. **Direito Digital**. Entrevista concedida à Revista Carta Forense em 02 de fevereiro de 2011. Disponível em: <<http://www.cartaforense.com.br/conteudo/entrevistas/direito-digital/6567>>. Acesso em: 16 mai. 2018.

11.2.5. Elaboração de Parecer por Assistente Técnico

Após a ata lavrada, com a constatação do fato pelo oficial notário, segundo o apresentado no parágrafo anterior, o usuário com seu advogado poderá contratar um assistente técnico especializado em computação forense para assistir no processo e elaborar um parecer técnico.

O parecer elaborado por esse assistente técnico em computação forense extrairá do ambiente digital, os indícios que estão presentes na assistência. Informações que determinarão, de forma clara e com um olhar pericial, o real ocorrido, buscando por meio de procedimentos forense apresentar o fato sucedido, conseqüentemente, instrumentalizando em um parecer técnico e, assim, formando uma legítima prova.

Para comprovar o registro de tempo do fato ocorrido, esse parecer técnico realizado pelo assistente pode ser registrado em serventia extrajudicial, no cartório de registro de títulos e documentos, pelo oficial de registro.¹⁷

O RTD tem como finalidade a conservação de um documento como, por exemplo, um contrato eletrônico, ou até mesmo algo que prove sua autoria, como um programa de computador, tornando esse documento público, não visando proteger apenas o interesse individual.¹⁸ Segundo Artigo 127, *caput* e parágrafo único da Lei nº 6.015/73:

Art. 127. No Registro de Títulos e Documentos será feita a transcrição: Parágrafo único. Caberá ao Registro de Títulos e Documentos a realização de quaisquer registros não atribuídos expressamente a outro ofício.

17. LOUREIRO, Luiz Guilherme. **Registros Públicos**. p. 439.

18. LOUREIRO, Luiz Guilherme. **Registros Públicos**. Op. Cit., p. 440.