ESTUDOS CRIMINAIS

Prof. Pedro Coelho

https://profpedrocoelho.com.br/
Instagram: @profpedrocoelhodpu
Youtube: Professor Pedro Coelho
Telegram: https://t.me/profpedrocoelho

PROVAS DIGITAIS NO PROCESSO PENAL

1. Prova X Elementos de Informação.

(a) Função da Prova no Processo Penal.

(b) Magistrado e o processo de cognição indireta.

2. Sociedade Moderna.

- Interconectividade, *modus vivendi* digital, superação de barreiras clássicas, novas perspectivas da intimidade.

- Ambientes virtuais e Redes Sociais em constante contato com informações pessoais **(dados sensíveis)** funcionando como caixa de ressonância de interações.

- Não apenas os nexos constitutivos de sociabilidade são replicados no ambiente digital, como podem servir eles próprios de comprovação de ações realizadas dentro ou fora dele.

3. Conceito de Prova Digital.

É o instrumento jurídico vocacionado a demonstrar a ocorrência de um fato e suas circunstâncias, **tendo ele ocorrido total ou parcialmente em meios digitais ou, se fora deles, esses sirvam como instrumento para sua demonstração (THAMAY, Renan e TAMER, Maurício.** *Provas no direito digital – conceito da prova digital, procedimentos e provas em espécie.* 2ª edição. São Paulo. Ed. Thomson Reuters, 2022, p. 33).

Obs.1: Quais as principais diferenças conceituais da prova digital?

O que difere a prova digital das demais é que o ambiente por ela demonstrado é o virtual, ou seja, um ato que tenha como suporte a utilização do meio digital. Para além de tal possibilidade, **a prova digital também terá serventia para os fatos ocorridos fora dos ambientes virtuais, mas que sua comprovação poderá ser feita por meios digitais**.

4. Prova Digital e a persecução criminal.

(i) Ampliação da utilização do meio digital na rede de contatos de criminosos, de sua instrumentalização para a prática de delitos e prática de condutas lesivas com camuflagem de identificação.

Obs.1: Prática de RANSOMWARE e competência.

É conhecido também como **EXTORSÃO DIGITAL OU CIBERNÉTICA**. Basicamente, trata-se do procedimento em que terceiro, por meio da internet, entra ilegalmente nos sistemas de informações de uma instituição e bloqueia o acesso ao banco de dados, passando a exigir do proprietário o pagamento de determinada quantia para que este possa novamente acessar as informações que lhe pertencem.

O Brasil assumiu o compromisso de reprimir esse delito na Convenção de Budapeste. **NESSE CASO, A COMPETÊNCIA SERÁ DA JUSTIÇA ESTADUAL OU FEDERAL?**

(...) 3. Em se tratando de crime previsto em tratado ou convenção internacional, a competência da Justiça Federal é firmada quando "quando, iniciada a execução no País, o resultado tenha ou devesse ter ocorrido no estrangeiro, ou reciprocamente" (art. 109, inciso V, da Constituição da República), ou se for praticado "em detrimento de bens, serviços ou interesse da União ou de suas entidades autárquicas ou empresas públicas", nos termos do inciso IV, do mesmo dispositivo constitucional. **Basta a presença de uma dessas hipóteses para que seja firmada a competência da Justiça Federal, não sendo necessária a presença concomitante de ambas, como entendeu o Juízo Suscitante.** (...) 6. No caso, **ao contrário do afirmado pelo Juízo Suscitante, há prova da internacionalidade do delito, pois as investigações feitas pela autoridade policial constataram que tanto o registro como o acesso a ao menos um dos e-mails utilizados pelo criminoso, para a prática do delito, foram feitos no estrangeiro**. 7. Firmada a competência da Justiça Federal, nos termos do art. 109, inciso V, da Constituição da República (...) **(CC n. 197.032/AM, relatora Ministra Laurita Vaz, Terceira Seção, julgado em 14/6/2023, DJe de 21/6/2023).**

Obs.2: Calúnia e Difamação pelas redes sociais.

Art. 143 - O querelado que, antes da sentença, se retrata cabalmente da calúnia ou da difamação, fica isento de pena. Parágrafo único. **Nos casos em que o querelado tenha praticado a calúnia ou a difamação utilizando-se de meios de comunicação, a retratação dar-se-á, se assim desejar o ofendido, pelos mesmos meios em que se praticou a ofensa.**

Obs.3: *CyberStalking.*

Art. 147-A. Perseguir alguém, reiteradamente e por qualquer meio, ameaçando-lhe a integridade física ou psicológica, restringindo-lhe a capacidade de locomoção ou, de qualquer forma, invadindo ou perturbando sua esfera de liberdade ou privacidade. Pena – reclusão, de 6 (seis) meses a 2 (dois) anos, e multa. (Incluído pela Lei nº 14.132, de 2021)

5. Caso Anderson Torres e Mauro Cid – Acesso às nuvens e nova tendência investigativa – Importância do Marco Civil da Internet.

- Provas Testemunhais, perícias clássicas e análise documental X VESTÍGIOS DIGITAIS.

- Ferramentas tecnológicas, ambientes virtuais e redes sociais – potencialização e concentração de armazenamento de fotos, documentos, mensagens de texto e de voz, vídeos, e-mails e outros tipos de arquivos.

- Relevância dos provedores no fornecimento de informações.

- Marco Civil da Internet (Lei 12.965/2014):

Art. 7º O acesso à internet é essencial ao exercício da cidadania, e ao usuário são assegurados os seguintes direitos: (...) III - inviolabilidade e sigilo de suas comunicações privadas armazenadas, **salvo por ordem judicial;**

6. Necessidade de Maior Cautela nas Provas Digitais.

6.1. Peculiaridades dessa prova: (i) ***caráter não material*** (ou seja, não palpável; que não possui uma materialidade imediatamente constatável) ***e*** **(ii)** ***sua congênita mutabilidade*** (BADARÓ, Gustavo. ***Os standards metodológicos de produção na prova digital e a importância da cadeia de custódia***. Boletim IBCCRIM – Ano 29 – Nº 343 – junho/2021, p. 7).

6.2. Norma técnica ABNT ISO IEC 27037:2013, vigente no país desde 2014, gerida pela ABNT — órgão brasileiro de normatização técnica. Procedimentos próprios para a custódia das evidências digitais:

(1) a devida identificação dos dispositivos de armazenamento de mídia digital e aqueles que podem conter evidência digital relevante; **(2)** a coleta da evidência digital, que será removida da localização original em que ocupa e será remetida a um ambiente controlado; **(3)** a aquisição, consistente na produção de cópia da evidência digital e documentação dos métodos utilizados; e **(4)** a preservação da evidência, consistente na proteção desta contra possíveis adulterações.

Obs.1: Recomendação da Função HASH pela ABNT + Quebra da Cadeia de Custódia.

(...) 4. A autoridade policial responsável pela apreensão de um computador (ou outro dispositivo de armazenamento de informações digitais) deve copiar integralmente (bit a bit) o conteúdo do dispositivo, gerando uma imagem dos dados: um arquivo que espelha e representa fielmente o conteúdo original. 5.

Aplicando-se **uma técnica de algoritmo hash, é possível obter uma assinatura única para cada arquivo, que teria um valor diferente caso um único bit de informação fosse alterado em alguma etapa da investigação, quando a fonte de prova já estivesse sob a custódia da polícia**. Comparando as hashes calculadas nos momentos da coleta e da perícia (ou de sua repetição em juízo), é possível detectar se o conteúdo extraído do dispositivo foi modificado. 6. É ônus do Estado comprovar a integridade e confiabilidade das fontes de prova por ele apresentadas. É incabível, aqui, simplesmente presumir a veracidade das alegações estatais, quando descumpridos os procedimentos referentes à cadeia de custódia. No processo penal, a atividade do Estado é o objeto do controle de legalidade, e não o parâmetro do controle; isto é, cabe ao Judiciário controlar a atuação do Estado-acusação a partir do direito, e não a partir de uma autoproclamada confiança que o Estado-acusação deposita em si mesmo. 7. No caso dos autos, **a polícia não documentou nenhum dos atos por ela praticados na arrecadação, armazenamento e análise dos computadores apreendidos durante o inquérito, nem se preocupou em apresentar garantias de que seu conteúdo permaneceu íntegro enquanto esteve sob a custódia policial. Como consequência, não há como assegurar que os dados informáticos periciados são íntegros e idênticos aos que existiam nos computadores do réu**. 8. Pela quebra da cadeia de custódia, são inadmissíveis as provas extraídas dos computadores do acusado, bem como as provas delas derivadas, em aplicação analógica do art. 157, § 1º, do CPP **(AgRg no RHC n. 143.169/RJ, relator Ministro Messod Azulay Neto, relator para acórdão Ministro Ribeiro Dantas, Quinta Turma, julgado em 7/2/2023, DJe de 2/3/2023).**

7. Algumas situações concretas de relevância na aplicabilidade da prova digital:

7.1. Impossibilidade de utilização como prova de mensagens obtidas de print screen da tela pela ferramenta Whatsapp Web:

Determinada pessoa entregou à Polícia prints de conversas registradas no WhatsApp Web. Tais conversas demonstravam a ocorrência de crimes contra a Administração Pública. **Vale ressaltar que esses prints foram feitos por um dos integrantes do grupo do aplicativo, ou seja, os prints foram tirados por um dos interlocutores da conversa.** Mesmo assim, **O STJ CONSIDEROU ILÍCITA ESSA PROVA**. Isso porque, para o STJ, **é inválida a prova obtida pelo WhatsApp Web, tendo em vista que nessa ferramenta "é possível, com total liberdade, o envio de novas mensagens e a exclusão de mensagens antigas (registradas antes do emparelhamento) ou recentes (registradas após), tenham elas sido enviadas pelo usuário, tenham elas sido recebidas de algum contato**. Eventual exclusão de mensagem enviada (na opção "Apagar somente para Mim") ou de mensagem recebida (em qualquer caso) não deixa absolutamente nenhum vestígio, seja no aplicativo, seja no computador emparelhado, e, por conseguinte, não pode jamais ser recuperada para efeitos de prova em processo penal, tendo em vista que a própria empresa disponibilizadora do serviço, em razão da tecnologia de encriptação ponta-a-ponta, não armazena em nenhum servidor o conteúdo das conversas dos usuários" **(STJ. 6ª Turma. RHC 99.735/SC, Rel. Min. Laurita Vaz, julgado em 27/11/2018).** Assim, a pessoa que tirou os prints poderia, em tese, ter manipulado as conversas, de maneira não há segurança para se utilizar como prova. Diante disso, **o STJ declarou nulas as mensagens obtidas por meio do print screen da tela da ferramenta WhatsApp Web, determinando-se o desentranhamento delas dos autos, mantendo-se as demais provas produzidas após as diligências prévias da polícia**

realizadas em razão da notícia anônima dos crimes **(STJ, 6ª Turma, AgRg no RHC 133.430/PE, Rel. Min. Nefi Cordeiro, julgado em 23/02/2021).**

7.2. Tecnologia Geo Fencing e a (in)admissibilidade no processo penal.

A determinação judicial de quebra de sigilo de dados informáticos estáticos (registros), relacionados à identificação de usuários que operaram em determinada área geográfica, suficientemente fundamentada, não ofende a proteção constitucional à privacidade e à intimidade. A quebra do sigilo de dados armazenados não obriga a autoridade judiciária a indicar previamente as pessoas que estão sendo investigadas, até porque o objetivo precípuo dessa medida é justamente de proporcionar a identificação do usuário do serviço ou do terminal utilizado. **Logo, a ordem judicial para quebra do sigilo dos registros, delimitada por parâmetros de pesquisa em determinada região e por período de tempo, não se mostra medida desproporcional, porquanto, tendo como norte a apuração de gravíssimos crimes, não impõe risco desmedido à privacidade e à intimidade dos usuários possivelmente atingidos por tal diligência (STJ, 3ª Seção, RMS 61.302-RJ, Rel. Min. Rogerio Schietti Cruz, julgado em 26/08/2020.**

7.3. (IM)Possibilidade de quebra de sigilo de dados informáticos estáticos (registros de geolocalização) nos casos em que haja a possibilidade de violação da intimidade e vida privada de pessoas não diretamente relacionadas à investigação criminal.

Em regra, é possível que o juiz determine a **quebra de sigilo de dados informáticos estáticos** (registros), relacionados à identificação de usuários que operaram em determinada área geográfica, suficientemente fundamentada. **Isso não ofende a proteção constitucional à privacidade e à intimidade**. Ex: determinação ao Google a identificação dos IPs ou Device IDs que tenham se utilizado do Google Maps e/ou do Waze no dia do crime, no período das 19h até as 23h, para realizar consulta do endereço onde ocorreu o delito. ISSO É, EM TESE, VÁLIDO. No entanto, **não é possível que se determine a quebra de sigilo de um universo indeterminado de pessoas quando os dados envolverem informações íntimas (como o acesso irrestrito a fotos e conteúdo de conversas). Assim, será inválida a ordem se o juiz determinou que o Google fornecesse o acesso aos seguintes dados das pessoas estiveram no local: conteúdo dos e-mails do Gmail; conteúdo do Google Fotos e do Google Drive; listas de contatos; históricos de localização, incluindo os trajetos pesquisados; pesquisas feitas no Google; e listas de aplicativos baixados (STJ, 5ª Turma, RMS 68119-RJ, Rel. Min. Jesuíno Rissato (Desembargador convocado do TJDFT), julgado em 15/03/2022).**

8. Conclusão.