

## Aplicação do princípio da relativização dos elementos informáticos

Recentemente, a 5ª Turma do Superior Tribunal de Justiça (AgRg no Habeas Corpus nº 828.054/RS, RN nº 2023/0189615-0) [1], por unanimidade, decidiu que são inadmissíveis no processo penal as provas obtidas de celular quando não forem adotados procedimentos para assegurar a idoneidade e a integridade dos dados extraídos. Isso ocorre porque, segundo o colegiado, as provas digitais podem ser facilmente alteradas, inclusive de maneira imperceptível, demandando, portanto, mais atenção e cuidado na custódia e no tratamento, sob pena de terem seu grau de confiabilidade diminuído ou até mesmo anulado.



*O ministro Joel Ilan Paciornik*

O relator, ministro Joel Ilan Paciornik, pontuou que é indispensável que todas as fases do processo de obtenção das provas digitais sejam documentadas, cabendo a polícia, além da adequação de metodologias tecnológicas que garantam a integridade dos elementos extraídos, o devido registro das etapas da cadeia de custódia, de modo que sejam asseguradas a autenticidade e a integralidade dos dados.

Segundo ele, o material digital de interesse da persecução penal deve ser tratado mediante critérios bem definidos, com indicação de quem foi responsável pelas fases de reconhecimento, coleta, acondicionamento, transporte e processamento, tudo formalizado em laudo produzido por perito, com esclarecimento sobre metodologia empregada e ferramentas eventualmente utilizadas.

### Princípio da relativização dos elementos informáticos

Trata-se da aplicação do princípio da relativização dos elementos informáticos, desenvolvido em 2015 no Curso de Direito Penal Informático [2] pelo professor dr. Spencer Sydow, conhecido não apenas pela criação do ramo do Direito Penal Informático no Brasil, mas também por sua atuação profissional e acadêmica profícua em prol do desenvolvimento dessa ciência.

O referido princípio preceitua que os elementos informáticos são inerentemente voláteis,



dinâmicos e podem ser facilmente manipulados ou alterados. Dessa forma, considerando-se que o meio digital permite a manipulabilidade ideológica (modificação indevida do conteúdo representado em um elemento informático verdadeiro) e formal (modificação do próprio elemento, independentemente de conter elementos ideologicamente verdadeiros) de seus documentos, o princípio em questão busca garantir que a evidência informática seja tratada com cuidado no processo legal.

Cita-se, como exemplo disso, a criação de logs de transações com criptoativos falsificados para criar transações inexistentes, prints de carteiras digitais com saldos manipulados para enganar investidores ou parceiros comerciais, uso de VPNs e IP spoofing para mascarar a localização e identidade dos usuários, e contratos inteligentes falsos contendo código malicioso para desviar fundos ou manipular resultados. Na medida em que essas possibilidades são identificadas, deve-se, necessariamente, aplicar o princípio da relativização dos elementos informáticos ató que as hipóteses de manipulação sejam afastadas.

Trata-se de exemplos que ressaltam a necessidade de se criar rigorosos protocolos de verificação para assegurar a integridade e autenticidade dos elementos probatórios em processos legais. Por esse motivo, Sydow defende que faz-se necessária a criação de um novo paradigma de precaução probatória para que sejam adotados procedimentos pertinentes para salvaguardar a integridade e a autenticidade dos elementos probatórios que estão sendo analisados. Isso se dá porque as bases de investigação e julgamento partem de pressupostos muitas vezes incorretos, não raro incorrendo em análises enviesadas de realidades informáticas, graças à ausência de cuidados elementares nessa esfera [3].

Essa situação se torna ainda mais premente em face do profundo e generalizado desconhecimento de boa parte dos atores processuais (advogados, juizes, promotores, delegados etc.) acerca de diversos elementos informáticos — questão que, no nosso entendimento, é ainda mais crítica ao se tratar de criptoativos e de tecnologia blockchain. Seja por falta de preparo, inexperiência, negligência ou, ainda, simplesmente por falta de conhecimento técnico, percebe-se na prática jurídica atual que questões fundamentais básicas sobre esses temas são tratadas de maneira grosseira, superficial ou simplesmente errônea, situação que compromete gravemente a eficácia do processo penal e, consequentemente, do sistema jurídico nacional.

Não se olvida que a informatização dos meios de vida, a criação imaterial de elementos e a desmaterialização do processo judicial de papel tornaram mais fácil a vida ao mesmo tempo que tornou os negócios mais velozes e mais amplos. Contudo, deve-se lembrar que os métodos informáticos de geração de elementos juridicamente relevantes também trouxeram um lado de questionamento possível dada a ampliação dos mecanismos de manipulação e modificação desses mesmos elementos [4].



Por isso, é de grande relevância que todos os elementos informáticos levado a um procedimento parta do pressuposto da existência de métodos de manipulação e adulteração para que possam ser considerados idôneos. Caso contrário, admitir-se-á o risco de condenações de acusados baseadas em elementos que não foram devidamente analisados, violando-se regras constitucionais basilares.

---

[1] Disponível em

[https://processo.stj.jus.br/processo/julgamento/electronico/documento/mediado/?documento\\_tipo=integra&d](https://processo.stj.jus.br/processo/julgamento/electronico/documento/mediado/?documento_tipo=integra&d)

[2] <https://www.lexml.gov.br/urn/urn:lex:br:redes.virtual.bibliotecas:livro:2020;001178860>

[3] SYDOW, Spencer Toth. Curso de Direito Penal Informático - Partes Geral e Especial. São Paulo: Editora JusPodvim, 2023. p. 131

[4] SYDOW, Spencer Toth. Curso de Direito Penal Informático - Partes Geral e Especial. São Paulo: Editora JusPodvim, 2023. p. 139

**Autores:** Spencer Sydow, Pedro Torres