# A Internetdas Coisas (*Internet ofThings* – IOT)e a Produção de Provas para a Investigação Criminal.

**Débora Freitas Mendes Pereira**[1]

**"As vezes é do passado que é mais difícil de escapar" (*MinorityReport*)**[2]

Vivemos em um mundo onde nada parece poder fugir do poder datecnologia e os especialistas, com frequência, usam a expressão: "dados são o novo petróleo", para dar a dimensão do atual momento da civilizatório.

Nesse contexto, estamos assistindo a uma verdadeira revolução tecnológica onde nenhum setor estará imune ao conhecimento das técnicas e uso de ferramentas capazes de dar acesso a dados e informações, a exemplo da polícia judiciária, sob pena de restarem obsoletas velhas formas de investigação de crimes, sendo possível verificar a dimensão dessa realidadeconforme palavras de MAGRANI (2018, p. 21) quando diz que nesse ambiente de hiperconectividade existe "...um fluxo contínuo de informações e massiva produção de dados", exigindo preparo técnico para o enfrentamento desta realidade.

Por *internet* das coisas (*Internet ofthings* – IOT) compreende-sea interação máquina-homem e também máquina-máquina,que cada vez mais amplia possibilidades de geração dedados que ficam armazenadas em ambiente virtual, a exemplo das nuvens (*clounds*)e que podem ser acessadas de acordo com regras próprias da *internet* para os mais diversos interesses.

Esses registros virtuais são como digitais que podem servir como elementos de provas em uma investigação criminal, ou mesmo como elementos corroborativos de outras provas coletadas.

Isso já vem acontecendo nos Estados Unidos na América, tanto na área civil como na criminal, onde dispositivos inteligentes estão se tornando uma nova espécie de prova e até de "testemunho", a exemplo do *case*relativo ao assassinato de Nicole VanderHeyden, onde seu

[1]**Delegada de Polícia Civil da Bahia, pós-graduada em Direito Público e em Inteligência de Segurança Pública pela UNIFACS.**

[2]*MinorityReport*, é um filme de 2002, com direção de Steven Spielberg, inspirado no conto homônimo dePhilip K. Dick, que mostra uma realidade distópica de uma sociedade onde um departamento denominado:"pré crimes", prevê a ocorrência de delitosporseres sensitivos que se aliam à inteligência artificial produzindo informações para que policiais possam atuar.

namorado foi desde o início das investigações o principal suspeito, contudo, após análise dos dados de uma "pulseira inteligente", usada pela vítima, os investigadores afastaram as suspeitas contra o mesmo.

No Brasil, nada impede que investigadores possam coletar dados identificados como abertos[3]em conteúdos vinculados à *internet* e a redes sociais, contudo o uso dessas informações como provas deverão obedecer a preceitos de natureza constitucional, a exemplo da preservação da intimidade e da privacidade, não podendo haver violações indevidas, sendo, absolutamente, necessário, em matéria criminal,a devida autorização judicial, quando necessário o acesso a conteúdos que afetem a vida intima e privada do cidadão para uso em procedimento investigatório criminal.

Isto porque o levantamento de provas deve seguir rígidos elementos contidos na lei, bem como não podem estar adstritos a convicções pessoais de quem esteja à frente de uma investigação criminal.A coleta de toda e qualquer prova nesse campo deve se pautar pela objetividade, regras técnicas e conclusões baseadas em regras legais e preexistentes.

Relacionado às técnicas de investigação em meio virtual, no Brasil, ainda são poucos os parâmetros legais estabelecidos pelo legislador a exemplo do que está contido na lei 13.441 de 04 de maio de 2017, **que prevê a infiltração de agentes de polícia judiciária na *internet* com o fim de investigar crimes contra a dignidade sexual da criança e do adolescente.**

Os requisitos previstos na lei, supracitada,que alterou o artigo 190 do Estatuto da Criança e do Adolescente, **para a infiltração de agentes de polícia civil na *internet***a fim de investigar e coletar provas são: "I – será precedida de autorização judicial devidamente circunstanciada e fundamentada, que estabelecerá os limites da infiltração para obtenção de prova, ouvido o Ministério Público; II – dar-se-á mediante requerimento do Ministério Público ou representação de delegado de polícia e conterá a demonstração de sua necessidade, o alcance das tarefas dos policiais, os nomes ou apelidos das pessoas investigadas e, quando possível, os dados de conexão ou cadastrais que permitam a identificação dessas pessoas; III – não poderá exceder o prazo de 90 (noventa) dias, sem prejuízo de eventuais renovações, desde que o total não exceda a 720 (setecentos e vinte) dias e seja demonstrada sua efetiva necessidade, a critério da autoridade judicial. § 1º A autoridade judicial e o Ministério Público poderão requisitar relatórios parciais da operação de infiltração antes do término do prazo de que trata o inciso II do § 1º deste artigo.§ 2º Para efeitos do disposto no inciso I do § 1º deste artigo, consideram-se: I – dados de conexão: informações referentes a hora, data, início, término, duração, endereço de Protocolo de Internet (IP) utilizado e terminal de origem da conexão; II – dados cadastrais: informações referentes a nome e endereço de assinante ou

[3] Dados abertos: são aqueles onde não há restrição de acesso.

de usuário registrado ou autenticado para a conexão a quem endereço de IP, identificação de usuário ou código de acesso tenha sido atribuído no momento da conexão. § 3º A infiltração de agentes de polícia na *internet* não será admitida se a prova puder ser obtida por outros meios."

Nesse sentido, o trabalho operacional de investigação criminal, deverá ser precedido de treinamento técnico e profissional das ferramentase técnicas que serão utilizadas na *internet*para a obtenção das provas, posto que a própria lei indica os requisitos a serem seguidos e a metodologia de investigação e coleta que servirão de baliza de legalidade da prova.

Com relação a proteção do cidadão contra os excessos do setor privado e público na coleta de dados pessoais, o Brasil ainda não possui uma lei geral como a que entrou em vigor na Europa em 25 de maio de 2018 cujo nome é *General Data ProtetionRegulation* (GDPR), contudo tramitam projetos no Congresso Nacional havendo grande clamor para a regulação no setor.

Compreende-se que o Brasil já precisa de uma regulação de proteção de dados e esperam-se normas gerias para breve. Os projetos de lei no Congresso Nacionalforam impulsionadosapós os escândalos de vazamentos de dados do *facebook* e da CambridgeAnalytic, sobretudocom o uso que dados pessoais foram feitos na campanha presidencialque elegeu Donald Trump, tendo sido aprovado em 29/05/2018 o projeto de lei 4060/12 na Câmara dos Deputados, ainda sendo exigido tramitação no Senado. Contudo, o projeto não prevê normas de natural criminal, cuja necessidade a cada dia se farão presentes, a exemplo da regulação de investigação em aplicativos como *whatsapp*e *telegram*, mas a lei de proteção de dadosnorteará as investigações criminais, naturalmente, como normas gerais, até que as especificas sejam editadas.

Fato é que a cada dia a exigência para o conhecimento do modo de se fazer coleta de provas em meio virtual, bem como regulações legais se fazem necessárias, tendo em vista que muitos crimes são praticados em ambiente digital e os registros deixam marcas que podem ser seguidas por um investigador, a exemplo devestígios digitais deixados em redes sociais.

As marcas deixadas por opiniões pessoais, registros de viagens, aquisições patrimoniais, local de moradia, relacionamentos, tudo isso pode significar muito de quem deixasuas marcas na *internet.*

Diante deste quadro se tornou praticamente impossível realizar uma boa investigação criminal sem o uso de ferramentas digitais.

O antigo formato de oitivas em salas fechadas, com depoimentos, declarações e interrogatóriosperderam o mesmo valor que tinham antes, pois serviam para levantamento de informações que eram coletadas de forma ‘braçal” que hoje em dia podem até já serem conhecidas, independente, destas técnicas antigas.

Registre-se que nossos dados são inseridos em bancos de dados de empresas privadas e de órgãos públicos e lá ficam armazenados, a exemplo dos cadastros que fazemos em lojas de departamentos e mercados, onde trocamos a inserção de nosso CPF por descontos em compras, e o uso destas informações deverão se pautar pelo respeito à intimidade dos cidadãos, contudo, investigações criminais com regras previamente estabelecidas para deverão ser autorizadas.

A lei geral de dados da Europa, em vigor desde o dia 25/05/2018 (GDPD), prevê cooperação entre autoridades nacionais e internacionais sobre dados criminais. Essa cooperação denomina-se: *ProtectionDirective for Police and Criminal Justice Authorities* (Diretiva de Proteção para Autoridades Policiais e de Justiça Criminal), objetivando fortalecimento na troca de informações entre *lawenforcements*(acordos legais) de países da união europeia e relativo a entidades supranacionais, como a *Interpol*, e ao mesmo tempo assegurar que os dados cambiados sejam devidamente protegidos.

Esse é o cenário que temos hoje e o que se avizinha e quem não estiver preparado pouco poderá entender e realizar nesse mundo cuja força da tecnologia se impõe.

***

REFERÊNCIAS.


1- MAGRANI, Eduardo. A Internet das Coisas. Editora FGV. 2018.
2- FERRO JÚNIOR, Celso Moreira e outros. A Segurança Pública Inteligente. Editora Kelps. 2008.
3- http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2017/lei/L13441.htm; acesso em 11 de junho de 2018.
4- https://www.conjur.com.br/2018-mar-14/internet-coisas-usada-prova-julgamentos-eua; acesso em 11 de junho de 2018.
5- https://www.jota.info/coberturas-especiais/liberdade-de-expressao/lei-protecao-de-dados-pessoais-29052018; acesso em 12 de junho de 2018;
6- https://www.nexojornal.com.br/expresso/2018/06/07/O-que-diz-o-projeto-de-lei-de-prote%C3%A7%C3%A3o-de-dados-que-tramita-no-Senado; acesso em 12 de junho de 2018.