UNIVERSIDADE DO SUL DE SANTA CATARINA

DANIEL IVONESIO SANTOS

INTERNET DAS COISAS, A PROVA DO FUTURO: EXAME DA LEGALIDADE DO USO DE DADOS COLETADOS POR DISPOSITIVOS DE INTERNET DAS COISAS, SEM CONSENTIMENTO DO USUÁRIO, COMO PROVA ACUSATÓRIA NO PROCESSO PENAL BRASILEIRO

Florianópolis

2019

DANIEL IVONESIO SANTOS

INTERNET DAS COISAS, A PROVA DO FUTURO: EXAME DA LEGALIDADE DO USO DE DADOS COLETADOS POR DISPOSITIVOS DE INTERNET DAS COISAS, SEM CONSENTIMENTO DO USUÁRIO, COMO PROVA ACUSATÓRIA NO PROCESSO PENAL BRASILEIRO

Trabalho de Conclusão de Curso apresentado ao Curso de Graduação em Direito, da Universidade do Sul de Santa Catarina, como requisito parcial para obtenção do título de Bacharel em Direito.

Orientadora: Prof.ª. Maria Lucia Pacheco Ferreira Marques, Dra.

Florianópolis

2019

DANIEL IVONESIO SANTOS

INTERNET DAS COISAS, A PROVA DO FUTURO: EXAME DA LEGALIDADE DO USO DE DADOS COLETADOS POR DISPOSITIVOS DE INTERNET DAS COISAS, SEM CONSENTIMENTO DO USUÁRIO, COMO PROVA ACUSATÓRIA NO PROCESSO PENAL

Este Trabalho de Conclusão de Curso foi julgado adequado à obtenção do título de bacharel em Direito e aprovado em sua forma final pelo Curso de Direito da Universidade do Sul de Santa Catarina.

Florianópolis, 01 de julho de 2019.

Prof. e orientador Maria Lúcia Pacheco Ferreira Marques, Dra.
Universidade do Sul de Santa Catarina

Prof. Everson Becker Silva, Esp.
Universidade do Sul de Santa Catarina

Prof. Henrique B. Souto Maior Baião, Esp.
Universidade do Sul de Santa Catarina

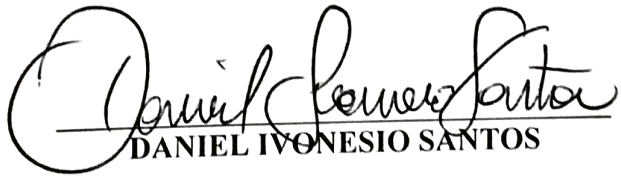
TERMO DE ISENÇÃO DE RESPONSABILIDADE

INTERNET DAS COISAS, A PROVA DO FUTURO:
EXAME DA LEGALIDADE DO USO DE DADOS COLETADOS POR DISPOSITIVOS DE INTERNET DAS COISAS, SEM CONSENTIMENTO DO USUÁRIO, COMO PROVA ACUSATÓRIA NO PROCESSO PENAL BRASILEIRO

Declaro, para todos os fins de direito, que assumo total responsabilidade pelo aporte ideológico e referencial conferido ao presente trabalho, isentando a Universidade do Sul de Santa Catarina, a Coordenação do Curso de Direito, a Banca Examinadora e o Orientador de todo e qualquer reflexo acerca deste Trabalho de Conclusão de Curso.

Estou ciente de que poderei responder administrativa, civil e criminalmente em caso de plágio comprovado do trabalho monográfico.

Florianópolis, 7 de junho de 2019.



DANIEL IVONESIO SANTOS

AGRADECIMENTOS

Agradeço àqueles que tiveram paciência para ouvir minhas angústias, resiliência para encarar acirradas discussões, ponderações, reflexões e críticas, coragem para caminhar e crescer ao meu lado, incentivando-me a aprender novas coisas e se sentindo incentivado por ideias que carrego — ora humanistas demais para uma justiça estéril, ora utópicas demais para um racionalista —, e, por fim, aos que tiveram afetuosidade para me fazer diariamente lembrar a que o direito importa e qual o meu papel nesse contexto de realidades diversas e perversas e da inquietude dos desafios vindouros.

“Se nós continuarmos a desenvolver nossa tecnologia sem sabedoria ou prudência, nosso servo pode provar ser nosso carrasco” (Omar N. Bradley).

RESUMO

Diante do direito fundamental à privacidade e a autodeterminação informativa o presente trabalho tem como objetivo principal examinar a legalidade da utilização de dados coletados por dispositivos de Internet das Coisas, sem o consentimento do usuário, como prova acusatória no processo penal brasileiro. Para a concretização do objetivo geral serão necessários alguns pontos de estudo, entre eles a apresentação da teoria constitucional penal das provas, a apresentação das eras da internet, conceito de Internet das Coisas e suas aplicações práticas em dispositivos, como forma de exploração de seus significados e suas potencialidades enquanto objetos probatórios, e a exposição doutrinária especializada acerca da conceituação do direito fundamental à privacidade, sobretudo em suas perspectivas da proteção de dados e autodeterminação informativa, bem como exposição de qual o cenário atual do Brasil dentro deste contexto. O método de abordagem da pesquisa será o dedutivo, pois a análise a ser realizada terá como ponto de partida o estudo da Internet das Coisas, para que se a entenda e se propicie uma visão de quais possibilidades ela carrega aos seus dispositivos, passando para a teoria do processo penal constitucional, com o objetivo de entender as limitações do uso de provas ilícitas e estudar-se os conceitos de privacidade e sua vertente da autodeterminação informativa para, ao fim, examinar a legalidade do uso de dados coletados por dispositivos de Internet das Coisas como prova acusatória no processo penal brasileiro, quando estes dados forem coletados sem o consentimento do usuário. A pesquisa será feita através do método procedimental monográfico, vez que o tema da pesquisa será estudado de forma profunda e com escopo bem delimitado. A técnica de pesquisa que a viabilizará será a bibliográfica, com aporte na doutrina clássica e atual, como, dentre outros, as obras de Bruno Ricardo Bioni, Daniel J. Solove, Eduardo Magrani, Ada Pellegrini Grinover, Marcelo Batlouni Mendroni e Vicente Greco Filho; e na Constituição da República Federativa do Brasil de 1988, no Código de Processo Penal, Lei 12.965, de 23 de abril de 2014 e Lei 13.709, de 14 de agosto de 2018 e demais dispositivos aplicáveis. Por fim, a hipótese defendida é que há vedação para o uso de dados coletados por dispositivos de Internet das Coisas sempre que o dispositivo tenha sido previamente utilizado pelo usuário coletando dados sem seu consentimento, sendo esta proibição apenas relativizável pelo princípio da proporcionalidade constitucional.

Palavras-chave: Autodeterminação informativa. Internet das Coisas. Privacidade. Proteção de dados.

SUMÁRIO

1 INTRODUÇÃO

O avanço da tecnologia traz ao direito, enquanto ciência jurídica, a necessidade de se debruçar sobre conceitos pré-estabelecidos e analisar a conformidade das teorias, há muito assentadas, com os novos rumos que a sociedade toma e as situações que derivam desse progresso.

A ideia de uma rede de dispositivos interconectados é bastante recente, com pouco mais de três décadas, e a sua atual era, a Internet das Coisas, deve ser analisada sob a óptica constitucional quando passa a permitir aos órgãos acusadores o uso dos dados contextualmente coletados para fins persecutórios e condenações no bojo do processo penal.

O contexto de importância em que se insere a pesquisa é o do expressivo e rápido crescimento da criação e lançamento de dispositivos de Internet das Coisas no mundo inteiro, com a previsão de que haja a movimentação de cifras trilionárias com a exploração desse mercado, mas também parte da verificação já realizada por diversas pesquisas de que há uma tendência alarmante de que a inovação dos dispositivos esteja desacompanhada da necessária preocupação com a segurança e privacidade, sobretudo no que atine aos dados do usuário.

Diante do direito fundamental à privacidade e a autodeterminação informativa o presente trabalho tem como objetivo principal examinar a legalidade da utilização de dados coletados por dispositivos de Internet das Coisas, sem o consentimento do usuário, como prova acusatória no processo penal brasileiro.

Para a concretização do objetivo geral serão necessários alguns pontos de estudo, entre eles a apresentação da teoria constitucional penal das provas, que trará a necessária compreensão acerca dos limites da prova lícita; a apresentação das eras da internet, conceito de Internet das Coisas e suas aplicações práticas em dispositivos, como forma de exploração de seus significados e suas potencialidades enquanto objetos probatórios; e, por fim, a exposição doutrinária especializada acerca da conceituação do direito fundamental à privacidade, sobretudo em suas perspectivas da proteção de dados e autodeterminação informativa, bem como exposição de qual o cenário atual do Brasil dentro deste contexto.

O método de abordagem da pesquisa será o dedutivo, pois a análise a ser realizada terá como ponto de partida o estudo da Internet das Coisas, para que se a entenda e se propicie uma visão de quais possibilidades ela carrega aos seus dispositivos, passando para a teoria do processo penal constitucional, com o objetivo de entender as limitações do uso de provas ilícitas e estudar-se os conceitos de privacidade e sua vertente da autodeterminação informativa para, ao fim, examinar a legalidade do uso de dados coletados por dispositivos de Internet das Coisas

como prova acusatória no processo penal brasileiro, quando estes dados forem coletados sem o consentimento do usuário.

A pesquisa será feita através do método procedimental monográfico, vez que o tema da pesquisa será estudado de forma profunda e com escopo bem delimitado. A técnica de pesquisa que a viabilizará será a bibliográfica, com aporte na doutrina clássica e atual, como, dentre outros, as obras de Bruno Ricardo Bioni, Daniel J. Solove, Eduardo Magrani, Ada Pellegrini Grinover, Marcelo Batlouni Mendroni e Vicente Greco Filho; e na Constituição da República Federativa do Brasil de 1988, no Código de Processo Penal, Lei 12.965, de 23 de abril de 2014 e Lei 13.709, de 14 de agosto de 2018 e demais dispositivos aplicáveis.

A hipótese defendida é que há vedação para o uso de dados coletados por dispositivos de Internet das Coisas sempre que o dispositivo tenha sido previamente utilizado pelo usuário coletando dados sem seu consentimento, sendo esta proibição apenas relativizável pelo princípio da proporcionalidade constitucional.

No segundo capítulo do trabalho apresentar-se-ão as bases históricas do desenvolvimento da internet, de seu início até sua atual era, a da Internet das Coisas, conceituando esta última e apontando exemplos práticos de dispositivos e quais as possibilidades que representam enquanto elementos probatórios no processo penal.

O terceiro capítulo cuidará de apresentar a teoria das provas no processo penal, explicitando-se o seu conceito como elemento de aproximação de uma hipotética verdade histórica. Discorrerá também sobre a interceptação telefônica e de dados e a busca e apreensão como meios de obtenção de provas, sendo esta última o instrumento processual adequado para a obtenção de dados armazenados em dispositivos de Internet das Coisas.

É no quarto capítulo que se cuida de apresentar as bases históricas e dificuldades de conceituar privacidade, trazendo como alternativa à essas sinuosas tentativas o *framework* conceitual de Daniel J. Solove, bem como expor-se-á o desenvolvimento da privacidade sob a perspectiva da autodeterminação informativa e do direito à proteção de dados para, ao final, explicitar o cenário atual da privacidade na Internet das Coisas.

Por fim, as conclusões, que sustentam a validade da hipótese defendida.

2 DA INTERNET À INTERNET DAS COISAS

O presente capítulo trará da evolução da internet, desde sua criação e necessários aperfeiçoamentos nas décadas de 60 e 70, passando pela sua expansão e findando em sua atual e terceira era, a Internet das Coisas, bem como bases conceituais gerais necessárias para a boa compreensão do assunto.

No último subtítulo apresentar-se-ão algumas das possibilidades emergentes de produtos da Internet das Coisas, sejam dispositivos privados, cada vez mais presentes nas residências, ou pertencentes ao poder público, sobretudo aqueles que dão forma às *smart cities*, e que coletam dados de absolutamente todos os indivíduos que participam dessa cidade.

É importante a exposição de exemplos de dispositivos de Internet das Coisas para que ao final, no exame a ser feito, entenda-se a dinâmica interacional destes com seus donos ou usuários, e possa-se delinear contornos claros para os limites à privacidade, de forma a se validar a hipótese defendida.

2.1 BASES HISTÓRICAS

A ideia de uma sociedade futurista, onde os seres humanos livremente interagem com robôs e máquinas e cada vez mais podem contar com as tecnologias disponíveis para otimizar seu dia a dia, melhorar sua performance em atividades cotidianas, reduzir os custos operacionais em grandes empresas e trazer informações cada vez mais customizadas para escolhas mais assertivas já passa da transição do imaginário para o factível.

A computação em si é algo recente, com menos de um século de vida, sendo apenas disseminada a partir dos anos 60, e possibilitada como conhecemos em dispositivos cada vez mais diminutos com o surgimento dos microprocessadores, nos anos 70, e com o movimento de contracultura na Califórnia, que viabilizou a ruptura das máquinas como ferramenta unicamente para astutos programadores e processamento de dados em empresas e as levou para os lares do cidadão americano comum, com o *personal computer* — PC —, ou computador pessoal (LÉVY, 2011, p. 31 - 32).

Mas o conceito de um computador vai muito além da imagem comum que se tem, que é a de *desktops*, os computadores de mesa, e *notebooks*, os computadores portáteis, com todos seus periféricos.

O computador é, nas palavras de Lévy (2011, p. 44) “uma montagem particular de unidades de processamento, de transmissão, de memória e de interfaces para entrada e saída de

informações.", essas suas unidades de montagem são os *hardwares*, que podem compor, além dos corriqueiros computadores pessoais, robôs, relógios inteligentes, celulares, eletrodomésticos, câmeras, sensores corporais e até os nós — pontos de distribuição — da internet (LÉVY, 2011, p. 44).

O avanço das técnicas, entendidas como o "ângulo de análise dos sistemas sociotécnicos globais [...]" (LÉVY, 2011, p. 22), foi o permissivo necessário para o nascimento de dispositivos cada vez mais avançados, mas também para uma revolução tecnoeconômica que moldou a forma como a sociedade se comporta e comunica e propiciou a infraestrutura do ciberespaço, novo ambiente de relacionamento pessoal, onde as pessoas e empresas se comunicam, organizam, transacionam, expandem-se, onde a informação flui e o conhecimento emerge (LÉVY, 2011).

O termo internet foi definido em 24 de outubro de 1995 pela Federal Networking Council (FNC), para se referir:

> [...] ao sistema global que — (i) é logicamente ligado por um espaço de endereço globalmente único baseado em seu Internet Protocol (IP) ou suas extensões subsequentes/continuações; (ii) é capaz de suportar comunicações usando o conjunto de protocolos TCP/IP ou suas extensões subsequentes/continuações, e/ou outro protocolo compatível com o IP; e (iii) fornece, usa ou torna acessível, seja publicamente ou privadamente, serviços de alto nível em camadas nas comunicações e infraestrutura relacionada aqui descrita (LEINER *et al*, 1997, tradução nossa)[1].

Note-se que a internet em si não é apenas a rede acessada pelos navegadores e celulares, mas sim "o conjunto de meios físicos (linhas digitais de alta capacidade, computadores, roteadores, etc.) e programas (protocolo TCP/IP) usados para o transporte da informação." (LÉVY, 2011, p. 265), é "[...] tanto uma coleção de comunidades como de tecnologias [...]"[2] (LEINER *et al*, 1997, tradução nossa), acertadamente F. Khodadadi, A. V. Dastjerdi e R. Buyya (2016, p. 3, tradução nossa) a conceituam como uma "[...] vasta categoria de aplicativos e protocolos construídos sobre redes de computadores sofisticados e

---

[1] "to the global information system that — (i) is logically linked together by a globally unique address space based on the Internet Protocol (IP) or its subsequent extensions/follow-ons; (ii) is able to support communications using the Transmission Control Protocol/Internet Protocol (TCP/IP) suite or its subsequent extensions/follow-ons, and/or other IP-compatible protocols; and (iii) provides, uses or makes accessible, either publicly or privately, high level services layered on the communications and related infrastructure described herein." (LEINER *et al*, 1997).

[2] "[...] as much a collection of communities as a collection of technologies [...]" (LEINER *et al*, 1997).

interconectados, atendendo a bilhões de usuários em todo o mundo a todo momento"[3], embora a web seja seu aspecto mais lembrado.

Foi em 1962 que Joseph Carl Licklider desenvolveu a ideia de uma rede conectada em que pessoas poderiam acessar qualquer informação de onde estivessem, através de interconexões em uma malha global, que o pesquisador chamou de *Galactic Network* (LIMA, 2015, p. 221), essa infraestrutura, em outras palavras, é o que compõe o cerne da ideia da internet como se conhece hoje.

Mas o notável pontapé da internet se deu ao término da década de 60, no contexto da Guerra Fria (PEREIRA, 2006, p. 23), através do projeto de interconexão de bases militares regionais *Advanced Research Projects Agency Network* (Arpanet), "uma rede de computadores de médio e grande porte, criada e desenvolvida [...] pela ARPA" (LÉVY, 2011, p. 261), que gerou uma estrutura nodal capaz de transmitir imagens e sons sem a necessidade de um centro de controle (MAGRANI, 2018, p. 61 - 62), o que foi trivial para o desenvolvimento da inteligência militar e transpôs a mera ideia de Licklider à prática.

Embora o projeto Arpanet não seja o primeiro esforço embrionário para um mundo conectado em redes, vez que antes mesmo de seu surgimento já se faziam pesquisas avançadas de redes de computadores com comutação por pacotes (*pocket switched networks*) na Universidade de Los Angeles e no Instituto de Tecnologia de Massachussets (ROHRMANN, 2005, p. 24), esse tem sido o ponto principal de seu desenvolvimento, de acordo com as narrativas históricas feitas (LEINER *et al*, 1997; MAGRANI, 2018, p. 62).

Em seu início o Arpanet se utilizou do *Network Control Protocol*, ou protocolo NCP, para se estabelecer (LEINER *et al*, 1997). O protocolo NCP utiliza um processo de rede chamado comutação por pacote (*pocket switched networks*) onde cada informação que será transmitida de um computador para outro é quebrada em pequenas unidades, chamadas pacotes, empacotada e encaminhada pela rede, em rotas diversas e complexas, não lineares (ROHRMANN, 2005, p. 40).

A preocupação inicial na constituição da infraestrutura do projeto foi a descentralização dos pontos de informação, garantindo que diante da ameaça de bombas nucleares ou mesmo nos combates das guerras a comunicação americana não ficasse vulnerável

---

[3] "[...] vast category of applications and protocols built on top of sophisticated and interconnected computer networks, serving billions of users around the world in 24/7 fashion." (KHODADADI; DASTJERDI; BUYY, 2016, p. 3).

e prejudicada (PEREIRA, 2006, p. 23), o que trouxe a conformação da rede em nós, mantida até hoje.

Na década de 70, com a ampliação de estudos em colaboração com o Departamento de Defesa dos Estados Unidos da América os nós das redes, que inicialmente eram quatro, expandiram-se rapidamente (MAGRANI, 2018, p. 62), porém, com o crescimento acelerado dos nós das redes o protocolo NCP passou a se tornar inadequado, pois os pacotes, unidades de informação transmitidas de ponta a ponta, eram perdidos no percurso, de forma que não se podia garantir a integridade das mensagens enviadas (LEINER *et al*, 1997).

Nesse sentido, diante dos desafios encontrados com o protocolo NCP, Robert E. Kahn iniciou sua empreitada para desenvolver um novo padrão que comportasse uma arquitetura aberta de comunicação e resolvesse os principais problemas de erro na transmissão de dados, assim, em parceria com Vinton G. Cerf criou o *transmission control protocol*, TCP, posteriormente cindido em TCP e IP (MAGRANI, 2018, p. 62).

O protocolo TCP, apresentado por Vinton G. Cerf e Robert E. Kahn em 1974, em seu artigo "*A Protocol for Packet Network Intercommunication*", permite que máquinas dentro da rede possam se comunicar de forma efetiva, ao enviar informações, por meio de pacotes, de uma ponta à outra, mas com a garantia de que as informações terão sua integridade preservada e, em caso de perda de pacotes, será possível recuperá-las (CERF; KAHN, 1974, p. 637 - 648).

O crescimento exponencial da internet enquanto ambiente digital e com uso mais diversificado se deu na década de 80, com a consolidação do protocolo TCP/IP para comunicação entre as redes de computadores. Foi também nessa época que os primeiros computadores pessoais surgiram, Arpanet 8800 e Apple I e II (MAGRANI, 2018, p. 62), daí a importância da solidez dos protocolos de rede, para que se mantenha estabilidade nos ambientes virtuais.

Mesmo com a ideia do projeto Arpanet bem consolidada esta foi rapidamente desvirtuada já em seus primórdios, com a apropriação da rede e da estrutura por movimentos de estudantes e pesquisadores para criar uma comunicação transversal e cooperativa, afastando-se dos objetivos militares e guiando-se para a conformação que hoje se tem da internet (LÉVY, 2011, p. 226).

E no final da década de 1980 a internet passou por significativo avanço, com a criação da *World Wide Web* (ou *WWW*), responsável por permitir a distribuição eficiente das informações em rede através de hipermídias, fator que atraiu a atenção de *players* públicos e privados, que passaram a investir na internet, despertando interesses além do militar e acadêmico (MAGRANI, 2018, p. 63 - 64).

Além da popularização da *World Wide Web*, que permitiu a disponibilização das informações e interfaces gráficas de uma forma simples e muito mais agradável esteticamente, Rohrmann (2005, p. 7) aponta como outro fator relevante para a escalada da internet a criação de provedores de acesso na década de 90, que permitiam aos usuários conectarem-se à rede mundial diretamente de suas casas, e Huidobro (2001, p. 209 *apud* PEREIRA, 2006, p. 31) rememora o surgimento do navegador Mosaic, que fez com que o número de usuários da internet triplicasse em 18 meses, alcançando os 20 milhões, também como fator determinante desse crescimento.

Passadas as considerações iniciais, é salutar compreender o desenvolvimento da internet até os dias atuais, o que se cuida de fazer adiante.

2.2 AS TRÊS ERAS DA INTERNET

A internet é marcada por três eras distintas, a primeira, conhecida como web 1.0, tem seu início em meados da década de 80, caracterizando-se pela conexão interpessoal, possibilitada pelo protocolo *WWW* e pela criação de milhões de páginas, ainda que estáticas, para disponibilização de informações das formas mais variadas, através de *hiperlinks* (MAGRANI, 2018, p. 64).

A web 2.0 tem como principais características a colaboratividade e interação rápida, dinâmica e fluída entre os usuários, possibilitada pela expansão da blogosfera, das plataformas de criação e curadoria colaborativa de conteúdo e das redes sociais, que ativaram um usuário marcado não apenas pelo consumo passivo (*read web*), mas de consumo, curadoria e produção ativa de materiais informacionais (*read-write web*) (MAGRANI, 2018, p. 65 - 67).

O termo web 2.0 tornou-se popular para designar quaisquer inovações, o que no marketing se convenciona chamar de *buzz word*, para conquistar mercados e vender serviços, porém, Juliano Spyer afirma (2015, p. 92):

> Em sua origem ele deveria distinguir sites ou aplicativos com baixo custo de desenvolvimento, em que o conteúdo surge de baixo para cima (bottom-up) a partir do relacionamento entre participantes (user generated content ou UGT), e que pode combinar as soluções e o conteúdo de mais de um site para produzir uma experiência integrada [...].

Ou seja, há uma verdadeira inversão na forma com que o usuário se insere na rede, agora com um protagonismo muito maior do que na primeira era da internet, e isso possibilita a força da inteligência coletiva para expansões inimagináveis na criação de conteúdo, o que, por si só, não é sinônimo indiscriminado de inovação.

Houve uma transição extremamente tênue entre a primeira e a segunda era da internet, embora marcada pelos avanços substanciais da forma como os recursos preexistentes eram utilizados, que torna difícil identificar uma ou outra era, como bem apontam Cornode e Krishnamurthy (2018 *apud* MAGRANI, 2018, p. 66 - 67):

> [...] É difícil encontrar uma definição precisa e é difícil categorizar muitos sites com o rótulo binário "web 1.0" ou "web 2.0". Mas há uma clara separação entre um conjunto de sites web 2.0 altamente populares, como Facebook e Youtube, e a "web antiga". Essas separações são visíveis quando projetadas em uma variedade de eixos, como o tecnológico (o desenvolvimento de scripts e tecnologia de apresentação usadas para renderizar o site e permitir a interação dos usuários); o estrutural (finalidade e disposição do site) e o sociológico (noções de amigos e grupos).

Nota-se que as características mais sobressalentes para a análise de subsunção de um *site*, por exemplo, a uma ou outra era da internet são aquelas relacionadas com o avanço técnico do desenvolvimento, com linguagens de programação mais avançadas e programadores com mais aptidão para codificar, o que por si só amplia as possibilidades estruturais e dá aos usuários uma nova conformação de uso dos recursos existentes.

A ruptura maior da internet ocorreu da segunda para terceira era, onde passou-se de uma fase de consumo e produção de conteúdo para outra baseada na consolidação de conteúdos dinâmicos através de dados e objetos interligados, o que se costuma chamar de web 3.0 ou Internet das Coisas (MAGRANI, 2018, p. 68 – 70).

No processo de desenvolvimento da internet para uma terceira era a evolução que se percebe, como assevera Rolf H. Weber (2009, p. 522, tradução nossa), é "[...] de uma rede de computadores interconectados para uma rede de objetos interconectados [...]"[4], ou seja, a ideia de rede, antes vinculada às pessoas em seus computadores pessoais, agora se aplica também — e principalmente — aos objetos interconectados e interagindo entre si, sem qualquer necessidade de interferência direta para sua operação.

Adiante será desvelada a terceira era, apresentando-se o conceito de Internet das Coisas e suas principais características definidoras, que a torna merecedora de profundas ponderações no campo das ciências jurídicas.

A expressão *Internet das Coisas*, "é utilizada para designar a conectividade e interação entre vários tipos de objetos do dia a dia, sensíveis à internet." (SANTOS; PEDRO, 2016, p. V *apud* MAGRANI, 2018, p. 44), as *coisas* que nos circundam estão cada vez mais

---

[4] "[...] from a network of interconnected computers to a network of interconnected objects [...]" (WEBER, 2009, p. 522).

conectadas, coletando informações ambientais e dados que nos são disponibilizados ou que são cruzados com outros dispositivos para nos permitir — ao menos na teoria — um maior bem-estar.

Em sua definição embrionária — e primeira aparição do termo —, ainda em 1999, Kevin Ashton, citado por Rose, Eldridge e Chapin (2015, p. 12, tradução nossa), conceituou a Internet das Coisas como "um sistema no qual objetos em um mundo físico podem se conectar à internet por sensores."[5], seria uma nova forma de enxergar e utilizar as coisas que nos rodeiam.

A definição supra se justifica pois à época o visionário da internet cunhou o termo devido aos avanços possibilitados pelos sensores de identificação por radiofrequência (RFIDs), uma das principais tecnologias que viabilizou esses dispositivos (KHODADADI; DASTJERDI; BUYY, 2016, p. 5).

Para Weber (2010, p. 23, tradução nossa) "A internet das coisas (IoC) é uma arquitetura de informação global e emergente baseada na internet para facilitar a troca de bens e serviços em uma cadeia de produção em rede global."[6], nesse ponto é uma nova forma de se lidar com as demandas do dia-a-dia ao permitir que objetos, agindo autonomamente, possam se utilizar de uma rede global à qual estão interconectados para, por exemplo, fazer compras de um item que faltou na despensa de casa antes mesmo de seu dono sentir que algum suprimento acabou.

Porém a definição do termo não é unanimidade, enquanto para alguns autores Internet das Coisas se refere à própria infraestrutura de conexão em rede adaptada para dispositivos que antes não possuíam uma camada digital, para Rose, Eldridge e Chapin (2015, p. 12, 14) o termo se refere ao cenário das múltiplas conexões destes objetos, perpassando a infraestrutura, mas notando um fator primordial, a quase total ausência de interferência do ser humano nesse processo.

Antonio Iera *et al* (2010 *apud* ARSÉNIO *et al*, 2014, p. 2, tradução nossa), nessa toada, conceituam a Internet das Coisas como

> [...] A penetrante presença ao nosso redor de uma variedade de coisas ou objetos — como etiquetas com Identificação por Radiofrequência (RFID), sensores, atuadores, telefones celulares, etc. — que através de esquemas de

---

[5] "[...] a system in which objects in the physical world could be connected to the Internet by sensors." (ROSE; ELDRIDGE; CHAPIN, 2015, p. 12).

[6] "The Internet of Things (IoT) is an emerging global Internet based information architecture facilitating the exchange of goods and services in global supply chain networks." (WEBER, 2010, p. 23).

> endereçamento únicos são capazes de interagir entre si e cooperar com seus [objetos] vizinhos.[7]

De todo modo, ainda que haja divergências conceituais, é inconteste que há uma ruptura tão grande que a segunda era da internet, conhecida pela produção ativa de conteúdo pelo usuário, em uma abordagem *bottom-top*, ou seja, descentralizada e interconectada, passa a perder espaço para uma era onde a maior interação do ser humano com a internet será passiva, através de objetos de seu dia a dia (ROSE; ELDRIDGE; CHAPIN, 2015, p. 14).

Nesse sentido,

> A Internet das Coisas possibilita um estado de rede ubíqua em que cada objeto em nossas vidas diárias poderia ser uma coisa potencialmente conectada na internet, com o seu próprio conjunto de sensores, atuadores e, possivelmente, estes poderiam ter um senso próprio e inteligência para reagir a seu entorno [...] (ARSÉNIO *et al*, 2014, p. 4, tradução nossa).[8]

A propósito, Kevin Ashton em artigo na RFID Journal ressalta a importância de se mudar o paradigma atual, onde os computadores funcionam com dados de entrada transmitidos diretamente pelo ser humano, sobretudo pois o ser humano é limitado em capacidade, velocidade e tempo, permitindo, nesse estágio, que as coisas possam, através de seus sensores, "[...] ver, ouvir e sentir o mundo por elas mesmas, em toda a sua aleatória glória." (ASHTON, 2009, tradução nossa)[9].

Em arremate, o sentido de *coisas* no contexto da internet pode ser resumido à objetos quaisquer que possuem uma camada digital em regra indissociável de si, com três características principais, capacidade computacional, capacidade de comunicação e capacidade de autocontrole (MEIRA, 2016 *apud* MAGRANI, 2018, p. 69).

Se não tem sensores ou atuadores que lhe permitem características de controle, um objeto está no plano da computação e comunicação, é uma máquina em rede; se não tem capacidade de comunicação, é um sistema de controle digital; se não tem capacidades computacionais, é o que antigamente se chamada (e ainda existem hoje) sistemas de telemetria (MEIRA, 2016 *apud* MAGRANI, 2018, p. 69).

---

[7] "[…] the pervasive presence around us of a variety of things or objects – such as Radio-Frequency Identification (RFID) tags, sensors, actuators, mobile phones, etc. – which through unique addressing schemes are able to interact with each other and cooperate with their neighbours." (IERA *et al*, 2010 *apud* ARSÉNIO *et al*, 2014, p. 2).

[8] "IoT enables a state of ubiquitous networking in which every object in our daily lives could be a potential connected thing on the internet, with its own set of sensors, actuators and, possibly, these could even have a sense of purpose and intelligence to react to their surroundings […]" (ARSÉNIO *et al*, 2014, p. 4).

[9] "[...] see, hear and smell the world for themselves, in all its random glory." (ASHTON, 2010).

Roman, Najera e Lopez (2011, p. 52) apontam ainda outras características como inerentes a todos objetos de Internet das Coisas: existência no mundo físico, ou seja, antes de se atingir sua camada digital o objeto é tangível; senso de si, que é a capacidade de decidir e agir autonomamente; conectividade e interatividade, permitindo que os objetos se comuniquem, respondam à estímulos e interajam com outros objetos ou seres humanos; e dinamicidade, a interação é dinâmica e não depende de proximidade física com outro objeto para ocorrer.

Se em um primeiro momento os dispositivos de Internet das Coisas possuíam uma interface muito mais necessitada de *inputs* de dados pelo usuário, a tendência que os autores apontados trazem é para uma independência quase que absoluta desses objetos hiperconectados, é o que se convencionou nomear de Internet das Coisas Inteligentes, ou simplesmente IoIT, sigla que vem do inglês, *Internet of Intelligent Things*.

A Internet das Coisas Inteligentes amplia o paradigma da Internet das Coisas ao se utilizar de sensores inteligentes capazes de dar aos seus objetos capacidade cognitiva para compreender seu entorno e contexto local e agir de forma minimamente autônoma para que não precise de um *hub* onde estes dados são processados e nem a interferência humana para processá-los (ARSÉNIO *et al*, 2014, p. 5).

Nesse sentido a Internet das Coisas Inteligentes "[...] vai além do paradigma da Internet das Coisas de conectar bilhões de coisas, para o paradigma de transformar objetos do dia a dia em coisas inteligentes que se comunicam umas com as outras e com pessoas." (ARSÉNIO *et al*, 2014, p. 33, tradução nossa).[10]

Essa disposição técnico-estrutural das coisas em rede com outras coisas embora seja uma amostra da expansão inevitável da terceira era da internet traz como questionamentos pertinentes para onde ela caminha e quais os perigos que carrega, assim, no próximo item tratar-se-á de aplicações práticas e atuais da Internet das Coisas em dispositivos, permitindo-se um panorama das possibilidades de seu uso.

2.3 APLICAÇÕES PRÁTICAS DA INTERNET DAS COISAS EM DISPOSITIVOS

Passada a exposição conceitual necessária para compreender do que se trata a atual tecnologia da Internet das Coisas, adiante expõe-se algumas das milhões de possibilidades de

[10] "[...] goes further than IoT paradigm of connecting billions of things, into the paradigm of transforming everyday objects into intelligent things that communicate with each other, and with people." (ARSÉNIO *et al*, 2014, p. 33).

dispositivos dessa nova era da internet, bem como questões que já têm sido suscitadas por conta de seu uso.

Talvez o dispositivo mais *clichê* do mundo da Internet das Coisas seja a geladeira que está atenta às necessidades do usuário e, quando algum item termina, automaticamente envia um pedido para o mercado mais próximo para fazer sua reposição, com o cartão de crédito que foi previamente cadastrado pelo seu usuário (NASCIMENTO, 2015 *apud* MAGRANI, 2018, p. 46).

Esse exemplo da geladeira embora seja corriqueiro na literatura e apresentações sobre o tema expõe apenas uma ínfima possibilidade de criação de dispositivos de Internet das Coisas, que podem estar atrelados em indústrias e ramos dos mais diversos, como a agricultura, medicina, logística, segurança pública, etc., bem como podem estar ao alcance das residências e nas mãos de qualquer pessoa, em casas projetadas de forma integrada e inteligente e com controle através de *apps* de celular.

O tênis UA HOVR™ Phantom/SE[11], da empresa americana Under Armour, por exemplo, possui tecnologia que rastreia e analisa os dados do usuário, enquanto ele o utiliza, para que possa melhorar sua performance em corridas e esportes, bem como conhecer informações sobre queima calórica, frequência cardíaca, distâncias percorridas no dia a dia, dentre outras (UA HOVR™..., 2019).

A interface do tênis com o celular é feita através de aplicativos proprietários, cada um desenvolvido para objetivos específicos e com funções específicas. O *app* Map My Fitness, por exemplo, mapeia todos os passos do usuário, gerando visualmente uma relação de todos locais percorridos, sua distância e intensidade da caminhada ou corrida (CONTROLE..., 2019).

O tênis da Under Armour possui sensores embutidos com tecnologia que permitem ao dispositivo se conectar ao celular do usuário com uma simples aproximação, garantindo que todos os dados capturados pelos sensores sincronizem com o aplicativo Map My Fitness e sejam facilmente visualizados (CONTROLE..., 2019).

Ainda que o usuário não esteja no momento de sua caminhada ou corrida com o celular em mãos, os sensores são capazes de armazenar todos os dados no próprio tênis para posterior transmissão ao celular, quando este estiver próximo, isto pois basta calçar o tênis para que ele comece a coletar dados (ALVAREZ, 2019).

---

[11] O modelo pode ser conferido em: https://www.underarmour.com/en-us/mens-ua-hovr-phantom-se-running-shoes/pid3021587-600. Acesso em 10 mar. 2019.

Aqui pode-se traçar o primeiro cenário de preocupação relativo à privacidade e guarda dos dados em um contexto de investigação criminal: o rastreamento geográfico e uso de dados de geolocalização de um dispositivo de Internet das Coisas poderia ser utilizado como indício de participação ou não na cena de um crime.

Um exemplo claro disso foi o de Jeannine Risley, que denunciou à Polícia suposto caso de estupro por um desconhecido enquanto dormia na casa de seu chefe, em Lancaster County, no estado americano da Pensilvânia. Ocorre que através do dispositivo FitBit da suposta vítima, uma pulseira *fitness* que rastreia os movimentos do seu usuário, os detetives do caso descobriram que a versão contada não conferia com os dados e localização rastreados, o que, junto com as demais provas, pôs em xeque a versão da suposta vítima — que posteriormente enfrentou a acusação de denúncia falsa (ROBINSON, 2016).

Em residências inteligentes, com uso de sensores de iluminação, que criam *logs* de passagem pelos cômodos da casa, com as maçanetas inteligentes, que podem identificar tentativas de arrombamento e enviar alertas para outros dispositivos, e mesmo o uso dos dados de redes WAP (SALAMA, 2017) e toda a automatização permitida pela interconexão de dispositivos gerará vários dados que poderiam identificar o percurso feito por um criminoso dentro de um imóvel, e guiar as perícias policiais para encontrar novas provas a serem utilizadas em um processo penal.

Outra das possibilidades é a criação de um sistema de informação de construções que permita a identificação e descrição de cada um dos materiais utilizados em uma residência, como o tipo e as especificidades de madeiras, tintas, alumínios, fiação, vidros e cerâmicas, para que o dono do imóvel possa efetuar eventuais reparos necessários de forma mais eficiente, indo diretamente no ponto crítico ou cujos materiais necessitem ser trocados (ARSÉNIO *et al*, 2014, p. 11).

Um sistema nesses moldes permitiria que a análise forense da trajetória de um projétil fosse facilitada, bem como diminuiria as dificuldades de encontrar pontos de dano decorrentes de um conflito — e que poderiam encaminhar para novas provas.

Também é possível contar com aspiradores inteligentes, como o Roomba 980, da empresa iRobot, que se guiam pelo ambiente para remover as sujeiras, identificando objetos ao seu redor para prosseguir na tarefa sem esbarrar neles, porém, estes são dispositivos que podem estar capturando dados espaciais enquanto limpam o ambiente residencial, criando um mapa detalhado, com cada um dos obstáculos, paredes e mobílias que estão presentes no local (ASTOR, 2017).

Se em um primeiro momento o mapeamento da residência não aparenta trazer maiores implicações para a privacidade, tem-se de por em perspectiva a combinação e compartilhamento desses dados com outros produtos, que poderão fazer deduções acerca do classe social e padrões comportamentais de um indivíduo a partir do tamanho do imóvel, posicionamento dos cômodos e de seus móveis e objetos, como afirma Jamie Lee Williams, advogado da organização não governamental americana *Electronic Frontier Foundation* (ASTOR, 2017).

Carros conectados são outra das oportunidades da Internet das Coisas: através de sensores RFID, *bluetooth* e de conexão com a internet, sobretudo por redes de dados móveis 3G e 4G disponibilizadas por chips celulares, o dono do veículo pode destravar o carro ao se aproximar do veículo com seu celular no bolso, ativar o motor e controlar o automóvel remotamente, bem como checar seus dados de performance, velocidade e geolocalização, serviços e possibilidades que embora surjam de forma tímida têm ganhado espaço na indústria automobilística, de acordo com relatório da *GSM Association* (2015, p. 13 - 14), associação americana representativa da indústria de comunicação móvel.

Os carros além de coletar, armazenar, analisar e enviar os dados de uso para os dispositivos de seu dono, podem se integrar com a cidade inteligente através da infraestrutura urbana para permitir uma melhor fluidez no tráfego, ao, por exemplo, gerar dados que permitam a sincronização de semáforos inteligentes e placas de velocidade de acordo com a intensidade do trânsito na via (GSM ASSOCIATION, 2015, p. 14), diminuindo a interferência humana e otimizando semáforos com dados em tempo real — e não programação fixa, como ocorre hoje em sua maioria.

Há, portanto, um segundo cenário de preocupação. Como esses veículos podem coletar dados de velocidade, percurso e localização e enviar para qualquer outro dispositivo ou aplicativo na nuvem, emerge a possibilidade de a autoridade policial acessar dados coletados pelo automóvel após um acidente, através de um desses dispositivos conectados ao automóvel, e o que pode ser primordial para a solução de um caso de homicídio causado por excesso de velocidade pode, do mesmo modo, ser a chave para a condenação do acusado no processo penal.

Ademais, a integração dos carros com a cidade pode fazer com que sua interceptação seja facilitada através da violação da privacidade dos dados encaminhados para semáforos inteligentes, barreiras de pedágio ou fiscalização, por exemplo.

Saindo das residências e automóveis para as cidades, o combate à criminalidade tem tido grandes avanços com a ajuda da inteligência artificial e da Internet das Coisas, exemplo disso é o reconhecimento facial feito por câmeras urbanas, que possibilita o cruzamento de

dados de diversas fontes para, através de algoritmos extremamente precisos e refinados, identificar acusados de crimes ou condenados com mandados de prisão em aberto no meio de uma multidão (TOLEDO, 2019).

Embora este sistema de vigilância seja promissor, remanesce a dúvida acerca dos *inputs* de dados, ou seja, quais são as fontes primárias dos bancos de dados que alimentam esses sistemas para que possam correlacionar a face de um indivíduo com o que é visto pela câmera no dia a dia da cidade.

A própria utilização do sistema, no cotidiano, também gera uma enxurrada de dados armazenáveis e que podem ser cruzados com aqueles já contidos nos bancos de dados, para trazer maior acurácia nas identificações futuras, e aí há um segundo cenário de preocupação no contexto do processo penal: dados desprotegidos de dispositivos de Internet das Coisas podem gerar cruzamentos ineficazes.

Em julho de 2018 a empresa SenseNets, que opera no ramo do reconhecimento facial para sistemas de segurança pública no mercado chinês, teve dados de 2.5 milhões de pessoas totalmente acessível por não adotar protocolos de segurança na guarda de informações de forma eficiente e compatível com o tamanho dos dados gerados (O'FLAHERTY, 2019).

A preocupação é relevante pois as autoridades chinesas têm utilizado os dados desses sistemas de reconhecimento facial e vigilância urbana, seja qual for sua origem, lícita ou não, para levar a cabo prisões arbitrárias, conforme denunciou o *Human Rights Watch* — Observatório de Direitos Humanos (SHEPHERD, 2018).

Essa perspectiva de violação de direitos humanos com base em presunções aparenta-se como mais um cenário de preocupação a ser vislumbrado, sobretudo considerando o contexto brasileiro, onde a conduta ilícita dos agentes do Estado é frequente, mas os números exatos desse fenômeno são quase uma incógnita diante da inércia do Brasil em reportá-las, conforme recomendado pela Corte Interamericana de Direitos Humanos no caso Favela Nova Brasília vs. Brasil (CIDH, 2017, p. 5), conforme expõe o *Human Rights Watch* (2019) em artigo de 2019.

Por fim, mas sem a mínima pretensão de esgotar o inesgotável, com a Internet das Coisas Inteligentes há uma outra perspectiva possível para robôs, que deixarão de ser vistos como um corpo metálico dotado de certa autonomia para ser uma entidade autônoma cujo corpo se forma com a união de diversos dispositivos que estarão na residência de seu usuário, "o cérebro de um robô estará na nuvem, e seus algoritmos de inteligência artificial podem

controlar, ou 'encarnar', diferentes plataformas robóticas físicas dependendo das necessidades." (ARSÉNIO *et al*, 2014, p. 33, tradução nossa)[12].

Diante dos exemplos dados e atentando-se para as infinitas possibilidades de produtos e serviços que deverão surgir nos mercados brasileiros e internacional nos próximos meses e anos, deve-se examinar quais as implicações que virão embarcadas junto a estes dispositivos no contexto do processo penal, elucubração que só pode ser feita perpassando-se o entendimento das provas e meios de obtenção e as provas ilícitas, o que se fará no capítulo seguinte.

[12] "A robot's brain will be in the cloud, and its AI algorithms may control, or 'incarnate', different physical robotic platforms according to needs." (ARSÉNIO *et al*, 2014, p. 33).

3 PROVAS NO PROCESSO PENAL

3.1 PROVAS E SEUS MEIOS DE OBTENÇÃO NO PROCESSO PENAL

Como ensina Renato Marcão (2018, p. 442), prova é termo que tem origem no latim *probatio*, mas com significados diversos, a depender do seu contexto: "Pode significar, portanto, a atividade probatória levada a efeito por quem atue no processo; o meio de prova utilizado para a demonstração daquilo que se pretende provar; a ação de provar, ou o resultado da atividade probatória" (MARCÃO, 2018, p. 442).

A acepção mais ampla do conceito de prova é "[...] um fato supostamente verdadeiro que se presume deva servir de motivo de credibilidade sobre a existência de outro fato." (BENTHAM, 1959 *apud* NUCCI, 2018, p. 499), Marcelo Mendroni (2015, p. 44), por sua vez, conceitua a prova como "fato considerado demonstrado, certo, incontroverso, favoravelmente ou contrariamente ao pretendido pela parte, ou, [...] 'fatos que servem de prova a outros fatos'.", definições que apontam acertadamente que a prova não é meio de confirmação imediata da verdade, mas retrata uma suposição da realidade (NUCCI, 2018, p. 499)[13].

Mesmo através do cotejo probatório, com os indícios, deduções e valorações de praxe, nada impede que a conclusão a que o juízo chegará seja diametralmente oposta à dinâmica real dos fatos, assim, o estudo das provas objetiva não o alcance de uma verdade histórica, mas a melhor aproximação possível com esta para que o julgamento possa se dar de forma mais justa (NUCCI, 2018, p. 499).

Pacelli (2018, p. 332) explica que

> O processo, portanto, produzirá uma certeza do tipo jurídica, que pode ou não corresponder à verdade da realidade histórica (da qual, aliás, em regra, jamais se saberá), mas cuja pretensão é a de estabilização das situações eventualmente conflituosas que vêm a ser o objeto da jurisdição penal.

E é justamente essa a finalidade da prova, a tentativa de demonstração da ocorrência ou inocorrência de determinada situação fática dentro da dinâmica do contexto do crime, como complementa Vincenzo Manzini (1970 *apud* MARCÃO, 2018, p. 443).

A acusação terá, com o conjunto das provas que levar aos autos, a oportunidade de narrar os fatos tão bem quanto estas se alinhem para uma conclusão clara e certeira, de forma

---

[13] Note-se que embora Mendroni utilize as palavras *certo* e *incontroverso* para adjetivar o fato probatório, em sua doutrina o autor aponta que a certeza se difere da verdade. Enquanto a verdade seria uma realidade fática a certeza e a natureza de ser ou não controverso são apenas crenças advindas do raciocínio lógico-dedutivo.

que é de seu interesse a produção de elementos probatórios invulneráveis, já a defesa, ao se beneficiar do elemento *dúvida*, é de seu interesse expungir qualquer presunção de culpabilidade levantada pelas provas, atacando-as e derruindo-as em suas vulnerabilidades (MENDRONI, 2015, p. 13).

Importante que se frise que não é viável no sistema constitucional brasileiro que o órgão acusador, tendo disponíveis as provas já coletadas, promova a denúncia com base em ilações além da exata medida do elemento de prova que possui, ou seja, o Ministério Público estará sempre adstrito às provas obtidas (MENDRONI, 2015, p. 14).

Nesse sentido o Superior Tribunal de Justiça já se manifestou, em ementa da lavra do Ministro Sebastião Reis Junior no Agravo Regimental no Recurso Especial nº 1.154.376: "[...] Não existe interceptação apenas para sondar, para pesquisar se há indícios de que a pessoa praticou o crime, para descobrir se um indivíduo está envolvido em algum delito." (BRASIL, 2013).

Como as provas são produzidas para possibilitar a "demonstração da verdade que se pretende ver formalmente reconhecida" (MARCÃO, 2018, p. 443), têm que partir de um ponto onde haja, de plano, ao menos indícios suficientes da ocorrência de um delito para que seja permitida autorização para a sua produção ou obtenção.

A prova pode ter três formas, como aponta Mendroni (2015, p. 92; 94) a primeira é a testemunhal, forma de prova indireta onde o indivíduo que presenciou determinado fato utiliza-se de seus sentidos, sobretudo o visual e auditivo, e, através do processamento cerebral das informações testemunhadas, emite juízo de valor sobre um fato, fazendo-se valer de suas experiências pretéritas, o que pode ocasionar um menor grau de fidedignidade com o que de fato se passou no contexto do crime.

A segunda forma é a prova documental, aquela que se materializa em qualquer uma das expressões possíveis que um documento pode assumir (MENDRONI, 2015, p. 95), assim, é preciso abeberar-se na definição de documento para compreendê-la.

Conforme Eraldo Rabello (1996 *apud* MENDRONI, 2015, p. 95), documento é:

> todo papel ou material equivalente, sobre o qual se tenha gravado ou escrito uma mensagem ou declaração inteligíveis, com caracteres gráficos representativos de uma forma qualquer de linguagem humana, e que possa servir de prova de questões ou relações de fato ou de direito.

Portanto, é prova que está vinculada à linguagem gráfica representada em substrato de papel ou que a ele equivale e que traz algum grau de certeza na comprovação de uma relação jurídica ou fática.

Por fim tem-se a prova material, que se conceitua por exclusão, é todo aquele material que não tenha a forma de prova testemunhal ou documental e que deve ser posto à análise pericial para que seja emitido, através de métodos científicos, relatório capaz de apontar sua mais pura substância, ou seja, formatação que se alinha com os fatos que se pretende provar (MENDRONI, 2015, p. 97).

Para o alcance da certeza jurídica o ordenamento brasileiro elenca inúmeros meios de prova, que possibilitam ao operador, dentro dos limites e proteções que a Constituição Federal traz às garantias individuais, chegar o mais próximo possível da verdade histórica (PACELLI, 2018, p. 332).

O título VII do Código de Processo Penal elenca como provas, nos capítulos II ao XI, os exames periciais, o interrogatório e a confissão do acusado, a prova testemunhal, o reconhecimento de pessoas e coisas, a acareação, a prova documental, a prova indiciária e a busca e apreensão, e no capítulo I do mesmo título encontram-se as disposições gerais aplicadas a todos os demais capítulos (BRASIL, 1941), não se olvidando da existência de legislações esparsas que permitem outras formas probantes.

Adiante tratar-se-á da busca e apreensão, prevista no artigo 240 do Código de Processo Penal, e da interceptação telefônica e telemática, meio de prova previsto na Lei 9.296 de 24 de julho de 1996, temas, dentre os meios de prova, pertinentes ao escopo do trabalho.

3.2 INTERCEPTAÇÃO TELEFÔNICA E DE DADOS E A BUSCA E APREENSÃO

A Constituição da República Federativa do Brasil, de 1988, traz em seu artigo 5º um rol de direitos e garantias fundamentais que devem ser prestados pelo Estado, dentre eles o direito à inviolabilidade da privacidade, intimidade e vida íntima:

> Art. 5º Todos são iguais perante a lei, sem distinção de qualquer natureza, garantindo-se aos brasileiros e aos estrangeiros residentes no País a inviolabilidade do direito à vida, à liberdade, à igualdade, à segurança e à propriedade, nos termos seguintes:
> [...]
> X - são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação;
> XI - a casa é asilo inviolável do indivíduo, ninguém nela podendo penetrar sem consentimento do morador, salvo em caso de flagrante delito ou desastre, ou para prestar socorro, ou, durante o dia, por determinação judicial;
> XII - é inviolável o sigilo da correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas, salvo, no último caso, por ordem judicial, nas hipóteses e na forma que a lei estabelecer para fins de investigação criminal ou instrução processual penal; (BRASIL, 1988).

Em que pese os incisos X e XI do artigo 5º da Constituição Brasileira trazerem em seu bojo a proteção da intimidade de forma imediata, o inciso XII do artigo 5º é uma norma constitucional que possui eficácia mista, pois permite a interceptação de comunicações telefônicas em determinadas situações, sendo, no entanto, sua parte final, de limitada eficácia, ou seja, depende da edição de uma normativa infraconstitucional para que possa operar seus efeitos (SARLET, MARINONI, MITIDIERO, 2018, p. 182).

Antes da entrada em vigor de uma lei que atendesse a necessidade regulamentadora emergente da Constituição a interceptação de comunicações telefônicas foi instrumento legitimador de um sem-fim de abusos e violações da privacidade, permitindo o controle e vigilância de vidas civis, sob a batuta estatal, mas também atendendo aos interesses particulares para fins diversos, como espionagem industrial e interceptação para comprovação de casos de infidelidade conjugal (GOMES, CERVI, 1997, p. 85).

Ainda, Gomes e Cervi (1997, p. 85) asseveram que a

> Ausência de um regime jurídico adequado (embora isso fosse constitucionalmente exigido), omissão legislativa, autorizações judiciais "controvertidas" (para se dizer o mínimo), incursões duvidosas no âmbito da intimidade de incontáveis pessoas, desrespeito em conseqüência a vários direitos fundamentais, insegurança jurídica, frustração da atividade persecutória, etc. foram as características do direito brasileiro, no que concerne às interceptações telefônicas, no período que vai de 1988 a julho de 1996.

Apenas em 24 de julho de 1996 foi editada a Lei 9.296, que regulamenta o inciso XII do artigo 5º da Constituição Federal de 1988, ou seja, oito meses após a promulgação da Carta Constitucional (BRASIL, 1996; GOMES, CERVI, 1997, p. 93), no entanto, a lei não surgiu sem embates doutrinários, sendo o de maior relevo ao presente estudo o referente à extensão autorizadora garantida pelo constituinte originário para a criação de uma legislação que também permitisse a interceptação de dados telemáticos para fins de investigação e instrução penais (GOMES, CERVI, 1997, p. 103).

As ponderações surgiram por conta da redação do inciso XII do artigo 5º da Constituição e dos artigos da lei 9.296/1996, que trataram de cuidar especificamente das comunicações telefônicas, ou seja, das comunicações presentes, e não dos registros anteriores que porventura tenham sido gerados por elas e dos dados (GOMES, CERVI, 1997, p. 103), de forma que a reserva geral qualificada não se adere às demais formas de comunicação previstas no artigo supra da Constituição (SARLET, MARINONI, MITIDIERO, 2018, p. 472).

Nesse sentir, a expressão "salvo, no último caso", prevista no artigo 5º, inciso XII da Constituição, autorizadora da violação quando amparada por ordem judicial, quando a lei

regulamentadora assim permita, e com fins de investigação e instrução penais, poderia ser interpretada tanto para se referir unicamente às comunicações telefônicas, não gerando a presunção *juris tantum* de que o sigilo das correspondências, das comunicações telegráficas e de dados estariam sujeitos a qualquer tipo de relativização, mas também poderia se referir a todos estes casos, abrangendo-os (GRECO FILHO, 2015, p. 31).

Percebe-se que a legislação sob análise possui apenas o parágrafo único do artigo primeiro apontando para "[...] interceptação do fluxo de comunicações em sistemas de informática e telemática" (BRASIL, 1996), e tipifica em seu artigo 10 a realização de interceptações telefônica, informática e telemática como crimes, quando feitas sem autorização judicial ou com objetivos ilícitos (BRASIL, 1996), deixando margens de dúvida acerca de sua incidência para os dados pretéritos e outras formas de comunicação, como as telemáticas (GOMES, CERVI, 1997, p. 115).

Duas linhas de ponderação merecem deferência acerca da nebulosidade apontada. Há isolada corrente defensora da inconstitucionalidade da interceptação da comunicação de dados e dados *per se* com base nos permissivos da Lei 9.296/1996 (SARLET, MARINONI, MITIDIERO, 2018, p. 474), sendo Vicente Greco Filho um de seus adeptos.

Greco Filho (2015, p. 31) utiliza-se de interpretação gramatical para concluir que a Constituição não prevê a possibilidade de interceptação de correspondências, comunicações telegráficas e de dados, pois,

> Se a Constituição quisesse dar a entender que as situações são apenas duas, e quisesse que a interceptação fosse possível nas comunicações telegráficas, de dados e das comunicações telefônicas, a ressalva estaria redigida não como "no último caso", mas como "no segundo caso". Ademais, segundo os dicionários, último significa o derradeiro, o que encerra, e não, usualmente, o segundo. (GRECO FILHO, 2015, p. 32).

Para Tercio Sampaio Ferraz Junior (1992 *apud* GRECO FILHO, 2015, p. 32) a proteção constitucional do artigo 5º, XII da Constituição dá guarida unicamente à realização de interceptações de dados telefônicos por ser tipo de comunicação instantânea, que não gera resultados (dados) captáveis *a posteriori*, esvaindo-se as provas no momento de sua oralização, assim, o artigo não permitiria a interceptação de comunicações informáticas e telemáticas (GRECO FILHO, 2015, p. 32), o que não significa que a proteção tenha sido estendida pelo Constituinte às bases físicas de suporte de dados (SARLET, MARINONI, MITIDIERO, 2018,

p. 474), conforme é o entendimento do Superior Tribunal Federal no Recurso Extraordinário 418.416 (BRASIL, 2006)[14].

De outra sorte, o direito à proteção dos dados pessoais não se submete às limitações regulamentadoras do legislador ordinário na lei 9.296/1996, pois não há na Constituição reserva legal que afaste sua plena eficácia, ainda assim, não se olvide de se tratar este ponto sob a mesma perspectiva dispensada pelas doutrinas alemã e espanhola, que formulam o direito à autodeterminação informativa e, observando-se os necessários limites às limitações de direitos fundamentais, como o são a privacidade e intimidade, dão proteção aos dados pessoais (SARLET, MARINONI, MITIDIERO, 2018, p. 478; 480).

A experiência brasileira traz alguns avanços normativos acerca da interceptação de dados e o necessário cuidado a ser dispensado a eles. Greco Filho (2015, p. 33), aliás, aponta a *contrario sensu* do que havia defendido nas edições anteriores de sua obra, que a interceptação de dados quando se trata de comunicação telefônica seria autorizada pela lei 9.296/1996,

> O texto, portanto, não é inconstitucional como sustentamos anteriormente, mas tem de ser interpretado de maneira a ser admissível a interceptação de dados enquanto instrumento de comunicação entre duas pessoas, não importa se via analógica ou digital, ou se o aparelho se chama telefone, *pager*, ou se é via rede mundial de computadores, como o VOIP (*Voice over Internet Protocol*). (GRECO FILHO, 2015, p. 33, grifos do autor).

Há aparente permissão para utilização de dados coletados de dispositivos de Internet das Coisas no processo, quando conferida autorização judicial mediante decisão devidamente fundamentada, embora esteja assentada a inaplicabilidade da lei de interceptação telefônica ao conteúdo dos dados coletados, conforme já mencionado no Recurso Extraordinário 418.416.

Nos diversos casos de fluxo de dados pela internet a legislação mais apropriadamente aplicável, em primeira análise, é a Lei 12.895, de 23 de abril de 2014, que prevê proteções em seu artigo 7º, incisos II e III:

> Art. 7º O acesso à internet é essencial ao exercício da cidadania, e ao usuário são assegurados os seguintes direitos:
> II - inviolabilidade e sigilo do fluxo de suas comunicações pela internet, salvo por ordem judicial, na forma da lei;

---

[14] "Na espécie, ao contrário, não se questiona que a apreensão dos computadores da empresa do recorrente se fez regularmente, na conformidade e em cumprimento de mandado judicial. 3. Não há violação do art. 5º. XII, da Constituição que, conforme se acentuou na sentença, não se aplica ao caso, pois não houve 'quebra de sigilo das comunicações de dados (interceptação das comunicações), mas sim apreensão de base física na qual se encontravam os dados, mediante prévia e fundamentada decisão judicial'. 4. **A proteção a que se refere o art. 5º, XII, da Constituição, é da comunicação 'de dados' e não dos 'dados em si mesmos', ainda quando armazenados em computador**. (cf. voto no MS 21.729, Pleno, 5.10.95, red. Néri da Silveira - RTJ 179/225, 270)." (BRASIL, 2006, grifo nosso)

> III - inviolabilidade e sigilo de suas comunicações privadas armazenadas, salvo por ordem judicial; (BRASIL, 2014)

E o artigo 10, §2º que disciplina acerca da armazenagem e disponibilização dos dados:

> Art. 10. A guarda e a disponibilização dos registros de conexão e de acesso a aplicações de internet de que trata esta Lei, bem como de dados pessoais e do conteúdo de comunicações privadas, devem atender à preservação da intimidade, da vida privada, da honra e da imagem das partes direta ou indiretamente envolvidas.
> §2º O conteúdo das comunicações privadas somente poderá ser disponibilizado mediante ordem judicial, nas hipóteses e na forma que a lei estabelecer, respeitado o disposto nos incisos II e III do art. 7º. (BRASIL, 2014).

Greco Filho (2015, p. 34) aponta que as garantias de sigilo, previstas no artigo 7º, II e III supra, que podem ser quebradas por ordem judicial na forma da lei, têm como fonte normativa direta e supedâneo fundamental para sua relativização a Constituição Federal de 1988.

Na senda da possibilidade aventada, a forma processual adequada para inserir a prova no processo é a busca e apreensão, meio cautelar para obtenção de material a ser utilizado como prova e que não esteja facilmente disponível à Justiça, autorizável quando existente justa causa, fundada em urgência e necessidade (PACELLI, 2018, p. 445), previsto no artigo 240 do Código de Processo Penal, que em seus dois parágrafos aponta as razões autorizadoras:

> Art. 240. A busca será domiciliar ou pessoal.
> § 1º Proceder-se-á à busca domiciliar, quando fundadas razões a autorizarem, para:
> a) prender criminosos;
> b) apreender coisas achadas ou obtidas por meios criminosos;
> c) apreender instrumentos de falsificação ou de contrafação e objetos falsificados ou contrafeitos;
> d) apreender armas e munições, instrumentos utilizados na prática de crime ou destinados a fim delituoso;
> e) descobrir objetos necessários à prova de infração ou à defesa do réu;
> f) apreender cartas, abertas ou não, destinadas ao acusado ou em seu poder, quando haja suspeita de que o conhecimento do seu conteúdo possa ser útil à elucidação do fato;
> g) apreender pessoas vítimas de crimes;
> h) colher qualquer elemento de convicção.
> § 2º Proceder-se-á à busca pessoal quando houver fundada suspeita de que alguém oculte consigo arma proibida ou objetos mencionados nas letras b a f e letra h do parágrafo anterior. (BRASIL, 1941).

Note-se que embora haja um rol bastante específico nas letras do primeiro parágrafo do artigo citado, sua letra "h" expande consideravelmente e quase que irrestritamente os

horizontes legais ao permitir que seja colhido qualquer elemento que possa formar a convicção do juízo na apuração dos fatos.

Como bem aponta Guilherme de Souza Nucci, há diferenças entre busca e apreensão, enquanto "*Busca* significa o movimento desencadeado pelos agentes do Estado para a investigação, descoberta e pesquisa de algo interessante para o processo penal, realizando-se em pessoas ou lugares." (NUCCI, 2018, p. 701, grifo do autor), a "*Apreensão* é medida assecuratória que toma algo de alguém ou de algum lugar, com a finalidade de produzir prova ou preservar direitos" (NUCCI, 2018, p. 701, grifo do autor), de forma que se diferem em suas finalidades, embora frequentemente caminhem juntas.

A doutrina de Marcellus Polastri Lima (*apud* TÁVORA; ALENCAR, 2016, p. 734) leciona, de maneira idêntica a Nucci, que a busca e apreensão embora esteja prevista no capítulo dos meios de prova dentro do Código de Processo Penal não é, em sua natureza jurídica, prova, mas medida acautelatória que objetiva a obtenção ou resguardo da prova para que a mesma seja utilizada no processo e não pereça.

Importante ressaltar que a busca e apreensão deve estar lastreada em mandado específico e pormenorizado, vedando-se a devassa geral no domicílio por conta de sua generalidade, bem como é necessária a justa causa autorizativa (TÁVORA; ALENCAR, 2016, p. 737).

Ocorre que as perspectivas apresentadas, tanto na interceptação telefônica como na busca e apreensão de dispositivos para utilização dos dados que coletou, se relacionam com a geração de dados que o indivíduo conscientemente sabia que estariam sendo gerados e onde houve seu consentimento na produção — embora não na coleta como prova —, bem como mandado anterior e pormenorizado autorizativo, adiante tratar-se-á das provas penais ilícitas para que se possa entender qual a tutela dada pelo direito ao acusado quando este não pode se valer de seu direito à autodeterminação informativa.

3.3 PROVAS ILÍCITAS

A investigação criminal, embora tenha se beneficiado de avanços técnicos que permitem uma maior facilidade na coleta de elementos probatórios, o que significa um alargamento das possibilidades de se encontrar a verdade dita real, deve ser analisada e confrontada com as possibilidades inerentes ao progresso científico e princípios próprios do processo e ordenamento jurídico, e é sob o enfoque legislativo que se insere o questionamento

mais proeminente para o estudo, qual o balanço entre a admissão de provas ilícitas e o ataque a direitos fundamentais (GRINOVER, 1982, p. 92 – 93; 96).

O equilíbrio deve ser perseguido pois o livre convencimento motivado do juiz no âmbito processual penal não é salvaguarda para que aja de forma despótica e com ilimitada liberdade, admitindo a qualquer custo elementos que julgue pertinentes para se alcançar a verdade e esclarecer o caso, mesmo quando coletados com violação dos ditames legais (GRINOVER, 1982, p. 58).

É em realidade de todo o oposto, já que a natureza do sistema do livre convencimento motivado impõe que os ritos para a produção de provas sejam observados, de forma que estes não se revestem em formalismo inútil, mas levam ao processo as mínimas fronteiras éticas que devem ser respeitadas para que se garanta ao acusado e as partes a ordem, afastando-as de arbítrios (GRINOVER, 1982, p. 58 - 59), assim, "inimiga declarada do arbitrário, a forma é irmã gêmea da liberdade" (IHERING, 1943 *apud* GRINOVER, 1982, p. 59, tradução nossa)[15].

O entendimento das provas ilícitas é necessário para que adiante se possa abordar a importância da salvaguarda da privacidade e da autodeterminação informativa no contexto do processo penal, bem como as previsões normativas da Lei 13.709 de 14 de agosto de 2018, que dispõe sobre a proteção de dados pessoais, assim, para se alcançar um horizonte no problema, traçar-se-ão algumas bases teóricas e conceituais mínimas.

A ideia de provas ilícitas remonta às *exclusionary rules* norte-americanas, cláusulas normativas que tornam nulos os elementos de convicção coletados pelo agente do estado que age sem a observância das garantias e direitos constitucionais do cidadão, objetiva-se, com isso, coibir abuso estatal e garantir a integridade das Cortes, ao não chancelar os arbítrios (MENDRONI, 2015, p. 162; 165).

Grinover (1982, p. 126) aponta que a invocação das *exclusionary rules* pressupõe a obtenção da prova com violação dos direitos constitucionais do próprio acusado — jamais de terceiros — e que a ilicitude seja praticada por um agente do Estado ou um particular em conluio com um agente estatal.

Enquanto as *exclusionary rules* surgiram com as experiências práticas, característica do sistema de *common law* dos Estados Unidos da América, é mérito do direito

---

[15] "ennemie jurée de l'árbitraire, la forme est la soeur jumelle de la liberté" (IHERING, 1943 *apud* GRINOVER, 1982, p. 59).

germânico, através da *Beweisverbote*, o avanço no assunto das proibições (MENDRONI, 2015, p. 165).

A *Beweisverbote* nasce do aprofundamento teórico e tentativa de sistematização das proibições com vistas à proteção da dignidade humana, para que não se a fulmine, o que pode ser visto como movimento inerente ao sistema romano-germânico do *civil law*, é meio processual que garante a preservação de bens jurídicos individuais constitucionalmente previstos através da imposição da tutela do direito material (MENDRONI, 2015, p. 165).

Diferentemente das *exclusionary rules*, por essa tutela faz-se uma ponderação valorativa das circunstâncias e do caso concreto, tendo como norte o princípio da proporcionalidade constitucional, *Verhältnismäßigkeitsgrundsatz*, "Significa dizer que, em análise comparativa de âmbito constitucional – violação/proteção de direito –, há que se aferir qual tem maior peso para então se viabilizar a conclusão a respeito da proibição ou não da apresentação e apreciação da prova em Juízo." (MENDRONI, 2015, p. 165 – 166).

Não fosse assim, teríamos como caminho jurídico lógico que toda a prova levada aos autos deveria ser admitida, independente se sua obtenção se deu com a violação de outras normas, priorizando-se uma suposta busca da verdade real, pois só assim se aproximaria daquilo que ocorreu no contexto do crime e quem de fato o cometeu (MENDRONI, 2015, p. 166 – 167).

> Diferentemente das *exclusionary rules*, as teorias alemãs da *Beweisverbote* não buscam a prevenção pela repressão; mas sim a análise do caso concreto em termos comparativos com as situações de direito e garantia individual que se procurou proteger, em evidente análise de valoração. (MENDRONI, 2015, p. 170, grifo do autor).

Como ensina Mendroni (2015, p. 169), as provas proibidas (*Beweisverbote*) podem se valer da aplicação de três teorias, a primeira, e a menos prestigiada, é a Teoria da esfera jurídica (*Die Rechtskreistheorie des BGH*), que entende que as provas mesmo colhidas em condições que por definição seriam ilícitas não serão, em tese, proibidas nos autos, até que a parte que se sinta prejudicada por ela interponha o recurso cabível à corte constitucional[16], tudo em privilégio ao princípio do *pas de nullité sans grief*, cabendo a análise à alta corte.

A segunda teoria, como prossegue Mendroni (2015, p. 170), é a teoria da proteção do efeito ou da finalidade (*Die Schutzzwecklehre*), segundo a qual a prova proibida poderá ser admitida para preservar seus efeitos se apenas da sua valoração, ou seja, na sentença, houver violação do bem jurídico que a proibição tutela, portanto, admitir-se-ia prova proibida para

---

[16] Mendroni (2015, p. 169) explica que o recurso cabível ao caso para demonstrar o prejuízo é o *Revision*, direcionado à mais alta corte alemã, *Der Bundesgerichtshof* (ou BGH).

preservar o alcance de sua finalidade. Assim como a primeira, essa teoria trata claramente da proibição após a admissão, ou seja, por uma análise valorativa da prova carreada, e também não obteve grande espaço nos tribunais alemães.

Por fim, Mendroni (2015, p. 169) traz a teoria mais aceita e utilizada, a teoria da ponderação (*Die Abwägungslehre*), e que se trata da aplicação de um juízo de ponderação para a análise da prova proibida em relação ao caso e aos interesses tutelados no processo e ordenamento, tendo-se em mente o princípio da proporcionalidade constitucional (*Verhältnismaßigkeitsgrun dsatz*) e observando-se os interesses da sociedade e de seus cidadãos.

> Nestes termos, as provas são proibidas em teoria, em face das previsões legais, mas podem ser não só admitidas nos autos como também levadas à valoração em plano de julgamento dependendo dos pesos e contrapesos que se verificam em face de uma situação concreta. (MENDRONI, 2015, p. 169).

Nesse sentido, as teorias alemãs, que comungam do sistema jurídico de base brasileiro, o *civil law*, trazem ensinamentos que se mostram pertinentes para o estudo e em muito o Brasil à elas se atém quando seus tribunais reafirmam as análises casuísticas e o princípio da proporcionalidade constitucional em seus julgados, no entanto, a proporcionalidade da doutrina alemã não pode ser vista de forma acrítica.

Grinover (1982, p. 112 – 113) alerta que a ponderação com base no princípio da proporcionalidade acarreta em subjetividade perigosa, de forma que alguns doutrinadores apenas têm aceito o referido princípio como a medida mais excepcional do sistema constitucional, "situações tão extraordinárias, que a inadmissibilidade da prova ilícita poderia produzir resultados desproporcionais, desusuais e repugnantes" (CAPPELLETTI, 1973 *apud* GRINOVER, 1982, p. 113).

Partindo para a conceituação, Nucci (2018, p. 508) sustenta que provas ilícitas é gênero do qual são integrantes duas espécies, a das provas obtidas com violação às normas Constitucionais e aquelas obtidas com violação da legislação infraconstitucional, incluindo os procedimentos processuais, removendo a categoria de provas ilegítimas.

Por sua vez, Avolio (1995, p. 39) entende cabível a divisão em provas ilícitas e ilegítimas, conceituando a prova ilegítima como a que fere normas de direito processual em sua colheita, ou seja, não há respeito ao procedimental definido em lei, enquanto a prova ilícita ou ilicitamente obtida viola dispositivos de ordem material, como os previstos na legislação infraconstitucional, mas principalmente os previstos explicitamente e implicitamente na Constituição, "porque, como vimos, a problemática da prova ilícita se prende sempre à questão

das liberdades públicas, onde estão assegurados os direitos e garantias atinentes à intimidade, à liberdade, à dignidade humana" (AVOLIO, 1995, p. 39).

Em entendimento idêntico Távora e Alencar (2016, p. 624) apontam que as provas se classificam em ilícitas, correspondentes às que foram produzidas com violação de norma ordinária ou princípio constitucional de natureza material, e ilegítimas, sendo as que violam normas processuais ordinárias e os princípios constitucionais relacionados, ambas são espécies do gênero provas vedadas.

Pietro Nuvolone (1966 *apud* GRINOVER, 1982, p. 97) leciona que quando a proibição do uso de determinada prova se der em função da lógica do processo terá natureza processual, e sua violação constituirá ato ilegítimo, enquanto que a violação da proibição que ocorra em decorrência dos direitos individuais garantidos pelo ordenamento, ainda que também sirvam a interesses processuais, terá natureza substancial e configurará ato ilícito.

Com essa lição de Nuvolone Grinover (1982, p. 99) define prova ilícita como: "[...] A fonte de prova colhida infringindo-se normas ou princípios colocados pela Constituição e pelas leis, freqüentemente para proteção das liberdades públicas e especialmente dos direitos de personalidade e daquela sua manifestação que é o direito à intimidade", note-se que a doutrinadora ítalo-brasileira trata como ilícita a coleta da *fonte* de prova violando-se direitos, e não a prova em si.

Embora utilize-se corriqueiramente a expressão *provas ilícitas* — o que se fará no correr do presente estudo — o que são verdadeiramente ilícitos são os meios empregados para a coleta da prova, como bem explica Mendroni (2015, p. 38):

> [...] ilícitos são os "meios" e não as "provas". Os meios são dinâmicos e as provas são estáticas. As provas têm ou não o poder de demonstrar outro fato. O meio como as provas são obtidas é que pode ser ilícito. Uma gravação em CD ou fita cassete de uma conversa de outras (terceiras) pessoas jamais é – em si – ilícita. É prova de algum fato ou não. Se a gravação foi realizada com autorização judicial, terá sido produzida através de meio lícito, se feita clandestinamente, terá sido produzida através de meio ilícito.

Os elementos de prova são um material bruto que só passa a ter qualquer valor jurídico quando juntado aos autos, antes disso pode existir no plano fático, materializado em um substrato ou na memória de um indivíduo que estava presente na cena em que se praticou um crime, mas é imprestável para qualquer fim, seja condenatório ou absolutório, segundo a máxima romana *quod non est in actis non est in mondo* (o que não está nos autos, não está no mundo) (MENDRONI, 2015, p. 39; 42).

Através de um ato processual o material passa a integrar os autos, e é este o meio hábil necessário para que venha a fazer parte do sistema jurídico e que possa ser utilizado para

cotejo probatório na sentença, daí que se subtrai que ilícitos são os meios, ou seja, os atos processuais que carreiam ao processo o elemento de prova, antes a prova é apenas material bruto e sem valor processual (MENDRONI, 2015, p. 42 – 44).

A questão da ilicitude da prova, porém, não se encerra apenas na legitimidade do *meio* probatório, mas também deve ser analisada quanto ao *resultado* que se alcança, pois ainda que o meio seja legítimo e autorizado o resultado que se alcança pode se fundar em violação de direitos (PACELLI, 2018, p. 349), nessa senda,

> Em tema de prova, portanto, mesmo quando não houver vedação expressa quanto ao meio, será preciso indagar ainda acerca do resultado da prova, isto é, se os resultados obtidos configuram ou não violação de direitos. E se configurarem, se a violação foi e se poderia ter sido autorizada. (PACELLI, 2018, p. 349).

Ademais, nem sempre a ilegitimidade do meio deve ser analisada apenas através do choque com as legislações ordinárias e Constituição, isso pois os meios ilícitos "abrangem não somente os que forem expressamente proibidos por lei, mas também os imorais, antiéticos, atentatórios à dignidade e à liberdade da pessoa humana e aos bons costumes, bem como os contrários aos princípios gerais de direito" (NUCCI, 2018, p. 502).

A vedação à admissibilidade das provas ilícitas no processo está prevista no artigo 5ª, LVI da Constituição Federal, que assim preconiza: "LVI: são inadmissíveis, no processo, as provas obtidas por meios ilícitos" (BRASIL, 1988), bem como no *caput* do artigo 157 do Código de Processo Penal, com a redação dada pela lei 11.690 de 2008: "Art. 157. São inadmissíveis, devendo ser desentranhadas do processo, as provas ilícitas, assim entendidas as obtidas em violação a normas constitucionais ou legais." (BRASIL, 1941).

Porém, como explica Eugênio Pacelli (2018, p. 336 – 337), nem sempre a vedação das provas ilícitas se deu como atualmente, sobretudo diante da existência do altamente aclamado princípio da busca da verdade real, que garantiu ao juiz, até a promulgação da Constituição Federal de 1988, uma postura absolutamente inquisitiva e amplo engajamento na iniciativa de produção de provas, "ainda que sem previsão legal, autorizadas que estariam pela nobreza de seus propósitos: a verdade." (PACELLI, 2018, p. 337).

A proibição de utilização das provas ilícitas no bojo do processo tem como objetivo principal, após a promulgação da Constituição Federal de 1988, evitar que o Estado, detentor tanto do poder jurisdicional encapado na figura do Juiz natural quanto do poder persecutório, na figura dos Promotores naturais, cometa arbitrariedades e adote práticas contrárias aos valores da Constituição para alcançar a condenação de um acusado (PACELLI, 2018, p. 348), assim, "A norma [...] presta-se, a um só tempo, a tutelar direitos e garantias individuais, bem como a

própria qualidade do material probatório a ser introduzido e valorado no processo" (PACELLI, 2018, p. 348).

O que surge da discussão da utilização das provas ilícitas como meio probatório legítimo é se elas são admissíveis quando *obtidas* de forma ilícita, e pode-se apontar duas correntes, a primeira, sustentada por Carnelutti, Cordero, Leone, entre outros, conclui que a prova ilícita será admissível no processo, enquanto a ilegítima deverá ser imediatamente desentranhada deste, já a segunda corrente sustentada por, entre outros, Allorio e Nuvolone, infere que a prova ilícita deve ser tida como ilegal, por conta da unidade jurídica do ordenamento, que prevê como regra geral a nulidade do que é de plano inválido, ou seja, ataca as normas e princípios constitucionais e infraconstitucionais (GRINOVER, 1982, p. 104 – 110).

Partindo das premissas supras, adiante se discorrerá sobre o direito fundamental à privacidade, em sua esfera da autodeterminação informativa, e o direito à proteção de dados, como fatores determinantes para a análise da licitude da prova.

4 PRIVACIDADE E PROTEÇÃO DE DADOS

4.1 BASES HISTÓRICAS E CONCEITOS DE PRIVACIDADE

Alessandro Barbosa Lima (2015, p. 221) muito bem ressalta que as questões afeitas à privacidade sempre caminharam ao lado do desenvolvimento tecnológico, e com a internet e todos os avanços inerentes a ela, bem como com o acelerado movimento mercadológico de criação de inúmeros dispositivos de Internet das Coisas não poderia ser diferente.

Adiante tratar-se-á do desenvolvimento da ideia de privacidade, revisitando-se suas bases históricas e conceitos clássicos para a apresentação de uma definição a ser seguida no curso do presente trabalho, e em um segundo momento, serão apresentados os aspectos atuais da privacidade e da proteção de dados no Brasil.

O termo privacidade é uma das palavras polissêmicas que suscita inúmeros debates para uma conformação adequada entre seu significado no campo teórico e a realidade da prática jurídica, isso é bastante compreensível pelas inúmeras e extensas possibilidades de se compreender o conceito, que pode ser ao mesmo tempo pontual, vago, genérico, facilmente ressignificado contextualmente, visto sob perspectivas coletiva ou individualista, e mesmo trazer respostas carregadas de inúmeras outras perguntas (SOLOVE, 2008, p. 1 – 2; 7).

O ponto de partida do conceito de privacidade remonta ao surgimento dos direitos de personalidade na Grécia e Roma antigas, sociedades que se afastaram de uma proteção unicamente da integridade física do ser humano e passaram a tutelar sua integridade moral. Note-se que a noção que se tinha de privacidade àquela época era divergente da que se tem atualmente, sobretudo por conta dos valores da sociedade (BIONI, 2018, p. 51).

O corpo nu, por exemplo, era sinal de força e civilização em Atenas (SENNETT, 1994 *apud* SOLOVE, 2008, p. 53), na Roma Antiga homens e mulheres tomavam banho juntos e na idade média os banhos passaram a fazer parte das festas, sendo atribuído ao cristianismo a objurgação do corpo despido, que passou a ser visto como impuro (SOLOVE, 2008, p. 53).

A ideia de privacidade ganha impulso com o jusnaturalismo no século XVII, e a conformação da ciência jurídica à laicidade, removendo-se divindades dos parâmetros justificantes de direitos fundamentais (BIONI, 2018, p. 51 – 52).

Com o arrefecimento da dogmática naturalista diante de sua quase sucumbência às dificuldades trazidas pela dinâmica jusracionalista, sempre em busca de dogmas elevados em abstracionismos, mas com rigor objetivo-matemático para a criação de suas premissas, ocorreu

uma mudança de eixo nas ordens jurídicas, que passaram a se guiar para a proteção patrimonialista (BIONI, 2018, p. 53).

A família foi um ativo comercial importante da burguesia em expansão, através de seus membros, honrados por seguirem determinadas normas sociais impostas à época, criava-se uma rede de contatos para possibilitar o comércio de forma mais ampla. Havia clara confusão entre o pessoal e profissional, inclusive com as casas utilizadas como extensão dos negócios, o que passou a se desfazer no início do século XIX, tanto com o individualismo como com a promoção da vida privada dos membros familiares (SOLOVE, 2008, p. 51 – 52; 59).

Ocorre que a moldura da sociedade patriarcal não se desfez com essa mudança para uma perspectiva individualista, e a condução dos assuntos da vida privada para longe dos olhos do Estado possibilitou no âmbito doméstico a manutenção de dinâmicas sociais machistas que punham (ou mantinham) a mulher em seu patamar de submissão e sofrendo de agressões sem qualquer tipo de interferência pública (SOLOVE, 2008, p. 52).

Coube à história o papel de repensar o pouco protagonismo dos direitos de personalidade, após as experiências escravistas e nazifascistas pelo mundo, e reposicionar o ser humano como *centro gravitacional*[17] da tutela jurídica (BIONI, 2018, p. 55 – 56), ainda assim, mesmo com a mudança paradigmática, o que se considera privado ou não continuou se alterando na defluência dos períodos históricos e de acordo com cada contexto social, sobretudo por conta dos avanços tecnológicos, das mudanças nas estruturas da sociedade e suas instituições e nos estilos de vida (SOLOVE, 2008, p. 50).

A título exemplificativo, a Declaração Universal dos Direitos Humanos de 1948 trouxe em seu artigo 12 a proteção da privacidade nas esferas do domicílio, da família, da reputação de um indivíduo, e em suas correspondências (OHCHR, 2019).

Atualmente a privacidade é alçada como direito fundamental nas ordens constitucionais globais, ainda que de forma indireta, como no caso de países como Canadá, França, Alemanha, Japão e Índia, para citar alguns, bem como recebeu atenção de uma gama de legislações e diretivas, como as do acordo de Cooperação Econômica Ásia-Pacífico, a Lei de Proteção de Dados da Argentina, de 2000, a Diretiva de Proteção de Dados da União Europeia (SOLOVE, 2008, p. 2 – 3), bem como o Regulamento Geral Sobre a Proteção de

---

[17] Como exposto pelo autor, até então, com a queda da força jusnaturalista diante do exacerbo pela dogmática racionalista, o centro gravitacional e de interesse para a tutela jurídica era apenas a propriedade privada, como bem exemplifica em citação de Antônio Menezes de Cordeiro, através do Código Civil Francês de primórdios do século XX, que "apenas se preocupava com o patrimônio e com os aspectos patrimoniais, deixando os direitos de personalidade, entendidos como todos os que não se reportem a bens" (CORDEIRO, 2011 *apud* BIONI, 2018, p. 54).

Dados da União Europeia (UNIÃO EUROPÉIA, 2016) e a novel Lei Brasileira de Proteção de Dados, sancionada em 14 de agosto de 2018 (BRASIL, 2018).

No Brasil, no entanto, ainda que infraconstitucionalmente existam legislações que tutelem a privacidade, não há explicitamente um direito à privacidade positivado na Constituição Federal de 1988, mas um rol de direitos fundamentais autônomos que estariam sob o conceito lato — ou guarda-chuva — da privacidade, como os previstos em seu artigo 5º, incisos X e XII (TAVARES, 2018, p. 543).

Enquanto alguns doutrinadores têm uma perspectiva bastante catastrófica e alarmista sobre o conceito de privacidade, vislumbrando o fim de quaisquer limites entre o público e o privado bem como a total aniquilação do termo, outros apontam que é um conceito que está em desenvolvimento, ainda que esse desenvolvimento possa eventualmente apontar para a sua extinção futuramente, mas que em muitas das vezes fica muito mais preso ao campo abstrato do que reflete nas práticas e cuidados da vida cotidiana (SOLOVE, 2008, p. 3 – 5).

O que as teorias têm em comum, no entanto, é a incansável e falha busca por encontrar um núcleo duro[18] definidor do que seja a privacidade em si, fazendo com que o termo seja aplicável em inúmeros contextos com base na sua perspectiva mais íntima (SOLOVE, 2008, p. 8).

O juiz americano Richard Posner (1981 *apud* SOLOVE, 2008, p. 5, tradução nossa), por exemplo, aponta que a privacidade dá aos indivíduos "poder de ocultar informações sobre si que outros poderiam utilizar de forma desvantajosa [negativa]."[19], e o doutrinador Fred Cate (1997 *apud* SOLOVE, 2008, p. 5) aduz que a privacidade é

> [...] um construto antissocial... que conflita com outros valores importantes dentro da sociedade, como o interesse da sociedade em facilitar a liberdade de expressão, prevenção e punição de crimes, proteger a propriedade privada e conduzir operações governamentais eficientemente.[20]

Essa tensão entre interesses individuais e coletivos é o que torna a discussão premente e, mesmo sendo assunto recorrente e amplamente debatido, atualíssima, pois relembra o impacto da expansão da tecnologia e se abebera nos valores de determinada sociedade para

---

[18] Nas palavras do autor, "the 'essential' or 'core' characteristics of privacy" (SOLOVE, 2008, p. 9).

[19] "[...] power to conceal information about themselves that others might use to [the individuals'] disadvantage." (POSNER, 1981 *apud* SOLOVE, 2008, p. 5).

[20] "[...] an antisocial construct... [that] conflicts with other important values within the society, such as society's interest in facilitating free expression, preventing and punishing crime, protecting private property, and conducting government operations efficiently." (CATE, 1997 *apud* SOLOVE, 2008, p. 5).

dar respostas para as suas inquietudes da forma mais adequada — ao menos em tese — às suas conformações constitucionais.

Por sua vez, ao buscar-se uma definição mais acertada e apegada aos contextos jurídicos preocupa-se em trazer às vidas pessoais impacto significativo, que vá além do abstracionismo, e que possa servir inclusive de parâmetro limitador da atuação dos agentes do Estado e das pretensões da sociedade.

Nesse sentir, no entanto, há um verdadeiro paradoxo, como bem aponta Rodrigo Pereira de Mello referenciando-se nos ensinamentos de Lawrence H. Tribe (*apud* MELLO, 2000, p. 44, tradução nossa),

> [...] entre o reconhecimento do direito à privacidade [por parte da sociedade], como valor fundamental do homem, e o seu objeto próprio: é o reconhecimento pelos homens que vivem em sociedade de um repúdio às pretensões que a sociedade possa ter sobre o homem.

Pois se por um lado há legítimo interesse da sociedade em ter respostas estatais para suas demandas, sobretudo aquelas criminais, por outro não se pode concluir que há irrestrita outorga de poderes para que o Estado se movimente na concretização destas pretensões, pois estaria incorrendo em violações porventura mais graves, em um ponto de vista difuso, do que o próprio crime cometido.

Retornando à conceituação do termo, Rohrmann (2005, p. 139) destaca a posição constitucional americana, decorrente dos *Bill of Rights*, que entende a privacidade como o direito à anonimidade e o "direito de ser deixado a sós" (ROHRMANN, 2005, p. 139), ponderando que, no entanto, esse não é um direito absoluto, devendo ser analisado à luz das expectativas de privacidade em determinado momento da vida do analisado, bem como frente aos demais direitos constitucionais tutelados.

Pereira, em contraponto, aponta uma linha de distinção entre intimidade e privacidade, conceitos que se misturam em muitas das doutrinas, o que ataca a definição trazida por Rohrmann em referência à ideia constitucional americana de anonimidade, cujo patriarca é Thomas M. Cooley (PEREIRA, 2006, p. 112).

Para o autor a intimidade é "a possibilidade do indivíduo de viver em tranqüilidade e em solidão" (PEREIRA, 2006, p. 112), é "tudo quanto diga respeito única e exclusivamente à pessoa em si mesma, a seu modo de ser e de agir em contextos mais reservados ou de total exclusão de terceiros" (TAVARES, 2018, p. 544). enquanto em sua acepção mais moderna a privacidade consiste na "[...] liberdade de exercer um direito de controle sobre os dados

referidos a uma pessoa, que já saíram da esfera própria para converterem-se em elemento de um arquivo eletrônico" (GÓMEZ, 1997 *apud* PEREIRA, 2006, p. 119, tradução nossa)[21].

Note-se que a definição de privacidade referida por Rohrmann seria equivalente à de intimidade, de forma que não põe fim e nem traz caminhos para um conceito mais claro do termo, enquanto Pereira (2006, p. 120) aponta que privacidade[22] e intimidade embora em certa medida se correspondam, não possuem significados equivalentes.

O emblemático caso levado à Corte Suprema Americana, *Roe v. Wade*, que trouxe como assunto o direito de a mulher decidir se aborta ou não, trouxe como plano de fundo a privacidade, que no julgamento foi estendida ao "direito de a pessoa fazer escolhas significativas para sua vida sem a interferência indevida de terceiros" (ROHRMANN, 2005, p. 139), essa é uma concepção extremamente abrangente carreada pelo direito americano, englobando desde esterilizações até o uso de métodos contraceptivos e, como citado, a decisão pelo aborto (PEREIRA, 2006, p. 124).

Para Schwartz (2004, p. 2058) o caso citado expõe uma das facetas da privacidade, a *privacidade decisória*[23], que é, em sua concepção, a privacidade relacionada à não interferência no direito de se tomar uma decisão, mas também ressalta uma segunda faceta, a privacidade informacional[24], aquela relacionada ao "[...] uso, transferência e processamento dos dados pessoais gerados na vida diária."[25] (SCHWARTZ, 2004, p. 2058, tradução nossa).

Jerry Kang (1998 *apud* ROHRMANN, 2005, p. 140) conclui que "num corolário da decisão acima [de *Roe v. Wade*], a pessoa tem o direito de decidir o fluxo a ser tomado por seus dados pessoais (e, conseqüentemente, por suas informações).", o que aponta uma inter-relação entre as extensões decisória e informacional da privacidade, facetas que estão vinculadas.

No mesmo sentido da concepção moderna trazida por Garrido Gómez, André Ramos Tavares (2018, p. 543) assim a conceitua:

> Pelo direito à privacidade, apenas ao titular compete a escolha de divulgar ou não seu conjunto de dados, informações, manifestações e referências individuais, e, no caso de divulgação, decidir quando, como, onde e a quem.

---

[21] "[...] libertad de ejercer un derecho de control sobre los datos referidos a una persona, que hayan salido ya de la esfera própria para convertirse en elemento de um archivo electrónico" (GÓMEZ, 1997 *apud* PEREIRA, 2006, p. 119).

[22] O autor utiliza o termo "*privacy*".

[23] Livre tradução do termo utilizado pelo autor, *decisional privacy*, em seu artigo "Property, Privacy, and Personal Data".

[24] Livre tradução do termo utilizado pelo autor, *information privacy*, na obra citada anteriormente.

[25] "[...] use, transfer, and processing of the personal data generated in daily life." (SCHWARTZ, 2004, p. 2058).

> Esses elementos são todos aqueles que decorrem da vida familiar, doméstica ou particular do cidadão, envolvendo fatos, atos, hábitos, pensamentos, segredos, atitudes e projetos de vida.

A ideia de privacidade defendida por Garrido Gómez e por André Ramos Tavares se aproxima da faceta informacional conceituada por Schwartz, embora este autor a conceitue de forma mais abrangente e não apenas em sua acepção de controle de dados, mas em todo fluxo de comunicação, transferência e processamento, como já mencionado.

Sem embargos, Daniel J. Solove (2008, p. 24 - 29) aponta que a teorização de privacidade unicamente como o controle que os indivíduos têm de sua informação pessoal, como a visão que traz Gómez, é bastante restrita ao não endereçar os seus aspectos não informacionais, como os da faceta decisória, defendida por Schwartz, além de vaga, pela definição imprecisa de *controle* e de quais as informações que são protegidas por esse direito de controle, partindo-se, em regra, da premissa que é apenas o indivíduo o responsável por definir o que se quer manter afastado do conhecimento público — esquecendo-se do contexto social e os valores que a sociedade busca proteger.

Um exemplo claro de como as doutrinas do controle de informação trazem mais questionamentos do que soluções pode ser visto com a conceituação de *informação* proposta por Richard Parker (1974 *apud* SOLOVE, 2008, p. 25, tradução nossa): "controle sobre quem pode nos ver, ouvir-nos, tocar-nos, sentir nosso cheiro, sentir nosso gosto, em suma, controle sobre quem pode nos sentir é o núcleo da privacidade"[26], que preceitua que qualquer contato interpessoal é informação e, portanto, seria invasão de privacidade se não autorizado pelo dono do corpo (SOLOVE, 2008, p. 25).

Também fica evidenciada as limitações que podem surgir a depender da concepção de controle que se defenda. O ser humano vivendo em sociedade, seja ela digital ou não-digital, produz inúmeras informações que, ao passo que são íntimas, também se relacionam com a vida de outras pessoas participantes de seu contexto e fazem parte da história de uma determinada região, razão pela qual a informação pessoal "[...] raramente pertence a apenas um indivíduo; ela é frequentemente formada em relação com outros." (SOLOVE, 2008, p. 27 – 28, tradução nossa) [27], e não poderia ser tratada da perspectiva do direito de propriedade (SOLOVE, 2008, p. 27).

---

[26] "Control over who can see us, hear us, touch us, smell us, and taste us, in sum, control over who can sense us, is the core of privacy." (PARKER, 1974 *apud* SOLOVE, 2008, p. 25).

[27] "[...] rarely belongs to just one individual; it is often formed in relationships with others." (SOLOVE, 2008, p. 27).

A seguir traz-se duas perspectivas de privacidade relevantes ao trabalho, bem como o *framework* conceitual desenvolvido pelo teórico da privacidade Daniel J. Solove como alternativa viável para sua definição e que a atinja de forma ao mesmo tempo precisa, mas sem ser limitadora e excludente, e ampla, mas sem vagueza, para nortear o exame a ser feito no presente trabalho.

4.1.1 PRIVACIDADE COMO AUTODETERMINAÇÃO INFORMATIVA

A autodeterminação informativa é, no sistema normativo brasileiro, um dos fundamentos da disciplina de proteção de dados pessoais, conforme dispõe o artigo 2º, inciso II da Lei 13.709, de 14 de agosto de 2018: "Art. 2º A disciplina da proteção de dados pessoais tem como fundamentos: [...] II - a autodeterminação informativa;" (BRASIL, 2018).

Emergente como uma das inúmeras facetas conceituais possíveis da privacidade, sendo, dentre todas, entre as mais relevantes para o estudo, sobretudo pela defesa que traz aos direitos positivos de escolha, surgiu no direito germânico, quando do julgamento da Lei do Censo de 1983 (*Volkszählunsgesetz*) pelo Tribunal Constitucional Alemão (BIONI, 2019, p. 101).

A referida lei determinou que os cidadãos deveriam fornecer dados pessoais que serviriam para fins estatísticos de análise da densidade e distribuição demográfica, porém, seus dispositivos foram redigidos de forma vaga e ampla, permitindo o cruzamento dos dados fornecidos com outras informações para fins administrativos genéricos, abrindo-se possibilidades inclusive para a promoção de execuções administrativas (BIONI, 2019, p. 101).

Diante da incerta finalidade da lei e a insegurança jurídica que causou, inúmeras reclamações foram levadas ao Tribunal Constitucional Alemão que, analisando a matéria considerou parcialmente inconstitucional a legislação censitária, apontando que a mesma deve destinar os dados coletados dos cidadãos unicamente para os fins estatísticos, ainda, anonimizando-os (BIONI, 2019, p. 101) e reforçando um direito fundamental à autodeterminação informativa (*Grundrecht auf informationelle Selbstbestimmung*)[28].

Segundo Bioni (2019, p. 101) como razão de decidir "estabelece-se a importante construção de que o cidadão deve ter o controle sobre os seus dados pessoais, a fim de que ele possa autodeterminar as suas informações.", estatuindo-se a autodeterminação como parcela do

[28] Caso: BVerfGE 65, 1.

desenvolvimento da personalidade do indivíduo, e isso vai além da simples ideia de consentimento, como esclarece Leonardo Martins (2005 *apud* BIONI, 2019, p. 103):

> Quem não consegue determinar com suficiente segurança quais informações sobre sua pessoa são conhecidas em certas áreas de seu meio social, e quem não consegue avaliar mais ou menos o conhecimento de possíveis parceiros na comunicação, pode ser inibido substancialmente em sua liberdade de planejar ou decidir com autodeterminação [...]

Ricard Martínez Martínez (2007, p. 47, tradução nossa) aponta, nessa toada, que o direito fundamental à autodeterminação informativa "[...] oferece proteção contra a coleta, armazenamento, utilização e transmissão ilimitada de dados pessoais e 'garante o direito do indivíduo de decidir basicamente por si mesmo sobre a divulgação e utilização de seus dados pessoais'"[29].

E reforça Lucas Murillo de la Cueva (1993 *apud* MARTÍNEZ, 2007, p. 49, tradução nossa):

> O controle que cada um de nós temos sobre a informação que nos interessa pessoalmente, seja íntimo ou não, para preservar, deste modo e, em última análise, nossa própria identidade, nossa dignidade e liberdade. Na sua formulação como um direito, implica necessariamente poderes que permitem ao seu titular definir os aspectos da sua vida que não são públicos, que ele não deseja sejam conhecidos, bem como poderes que lhe assegurem que os seus dados pessoais manuseados por terceiros sejam precisos, completos e atuais, e que foram obtidos de forma leal e lícita.[30]

Nem sempre é de um panorama do consentimento que a autodeterminação informativa deve ser entendida, no caso da lei germânica supra a questão se posiciona mais adequadamente no campo da escolha cônscia, crítica e informada de como os dados pessoais deveriam ser usados diante da definição dos propósitos e finalidades da coleta pela lei (BIONI, 2019, p. 105), e é dessa forma que esse direito deve ser entendido.

---

[29] "[...] ofrece protección frente a la recogida, el almacenamiento, la utilización y la transmisión ilimitada de los datos de carácter personal y «garantiza la facultad del individuo de decidir basicamente por sí mismo sobre la difusión y la utilización de sus datos personales »" (MARTÍNEZ, 2007, p. 47).

[30] "el control que a cada uno de nosotros nos corresponde sobre la información que nos concierne personalmente, sea íntima o no, para preservar de este modo y en último extremo la propia identidad, nuestra dignidad y libertad. En su formulación como derecho, implica necesariamente poderes que permitan a su titular definir los aspectos de su vida que no sean públicos, que desea que no se conozcan, así como facultades que le aseguren que los datos que de su persona manejan terceros informaticamente son exactos, completos y actuales, y que se han obtenido de modo leal y lícito". (LA CUEVA, 1993 *apud* MARTÍNEZ, 2007, p. 49).

4.1.2 PRIVACIDADE COMO PROTEÇÃO DE DADOS

O direito à privacidade se desenvolveu como forma de demarcar os limites entre a vida pública e privada, como já exposto, ainda que a própria definição do que é público e privado seja oscilante para cada período e contexto histórico.

A esfera privada é a da reflexão sem influências, é o refúgio que permite ao indivíduo abstrair as concepções sociais para pensar de forma crítica sobre seus permeares, sem necessitar curvar-se ao totalitarismo do senso comum, das opiniões pré-concebidas e dos padrões comportamentais, pois "Somente com a fuga da 'pressão social', os indivíduos conseguiriam desenvolver cada qual sua subjetividade para, posteriormente, projetá-la em meio à sociedade" (BIONI, 2019, p. 94).

Nessa perspectiva é que Bioni (2019, p. 96) aponta que se tem a construção do direito à privacidade como um direito de liberdade negativa, ou seja, é do titular do direito a decisão dos limites de sua exposição à opinião pública acerca dos fatos que pertencem à esfera de sua vida privada.

O avanço da privacidade de uma concepção estática, onde as limitações são apriorísticas, para uma concepção dinâmica, onde há controle das informações, é o que engloba nesse conceito guarda-chuva — de forma não limitadora e restritiva — o direito à proteção de dados pessoais, e altera as lentes para um direito de liberdade positiva, onde o titular das informações passa ter papel ativo na determinação do que quer ou não quer comunicar e, se comunicado, o que quer revogar do conhecimento social amplo (BIONI, 2019, p. 97).

Essa ampliação para uma perspectiva dinâmica surgiu, em grande medida, pelos avanços da biotecnologia e da internet, que facilitaram o acesso e divulgação de dados sensíveis de forma externa, alargando as possibilidades de violação da esfera privada e possibilitando a visualização da privacidade como proteção aos dados (Mulholland, 2019, p. 489).

Bioni (2019, p. 97, grifos do autor) esclarece que:

> A *esfera privada* não seria algo já posto à espera de uma violação, mas um espaço a ser construído *a posteriori* e dinamicamente mediante o controle das informações pessoais. Haveria, por isso, uma mudança qualitativa representada pela transposição do eixo antes focado no trinômio "pessoa-informação-sigilo" ao eixo agora composto por quatro elementos – "pessoa-informação-circulação-controle".

Mas ainda que se busque uma aproximação da privacidade e proteção de dados, alerta Bioni (2019, p. 98 – 99), não se pode confundir e equiparar as duas tutelas como se idênticas fossem, deve-se buscar uma ampliação normativa que possibilite tutelar a proteção de dados, e afastar-se do erro dogmático de enxergar a proteção de dados como uma evolução da

privacidade, vez que "o direito à proteção de dados pessoais angaria autonomia própria. É um novo direito da personalidade que não pode ser amarrado a uma categoria específica, em particular ao direito à privacidade." (BIONI, 2019, p. 98).

Embora privacidade e direito à proteção de dados se tangenciem em inúmeros momentos, este supera a dicotomia entre público-privado e aponta para a necessária expansão dos olhares para o assunto, de forma que sua alocação se torna adequada no rol dos direitos de personalidade (BIONI, 2019, p. 100).

A proteção de dados, segundo Rodotà (2018, p. 14), se configura como a tutela de um amplo conjunto de direitos que garantem ao indivíduo gozar das facetas da cidadania do novo milênio, com uma roupagem vinculada às novas tecnologias e seus avanços.

Para a Lei 13.709, de 14 de agosto de 2018 o dado pode ser classificado de três formas, conforme incisos I, II e III do artigo 5º:

> I - dado pessoal: informação relacionada a pessoa natural identificada ou identificável;
> II - dado pessoal sensível: dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural;
> III - dado anonimizado: dado relativo a titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento; (BRASIL, 2018).

A Internet das Coisas é uma fonte inesgotável de dados, como ensina Caitlin Mulholland (2019, p. 485), isso pois permite que objetos se interliguem a outros objetos e coletem, transmitam, armazenem e compartilhem informações contextuais, o que, por conseguinte, também garante os mesmos poderes às empresas que disponibilizam estas tecnologias e que passam a ter participação indireta em toda a cadeia de interação das coisas com os seres humanos.

Bem alerta Mulholland (2019, p. 486):

> Para o mundo "prático", a internet das coisas traz benefícios de tamanha ordem – ainda que alguns deles possam ser considerados fúteis – que o usuário do bem conectado sequer imagina quais são as consequências jurídicas eventuais – e maléficas – que podem surgir no que diz respeito à proteção de privacidade e de dados pessoais.

A questão emergente, portanto, é se existem políticas claras de proteção de dados e da privacidade dos usuários, que vão além dos *defaults* de mercado e se as pessoas gostariam de abrir mão de seus dados em troca do uso das coisas ou o fazem por conta da conveniência e falta de padrões normativos, mesmo sem saber que estão comercializando sua vida privada (MULHOLLAND, 2019, p. 486).

Não se pode limitar a questão das violações porventura existentes apenas de uma perspectiva do consentimento ou sua revogação, manifestados pela autodeterminação informativa, sendo premente a tutela jurídica se direcionar também às razões do consentimento, se o consentimento foi esclarecido, se o proprietário da coisa entendeu o que ter seus dados coletados, armazenados, utilizados e compartilhados significa e se teve ciência das finalidades da coleta e limites dos termos de adesão do próprio produto (MULHOLLAND, 2019, p. 492).

Como aponta Mulholland (2019, p. 487), abeberando-se dos ensinamentos de Rodotà, o "corpo eletrônico" merece tanta tutela jurídica quanto aquela que o corpo físico já possui, para que as pessoas não sejam reduzidas a meras fontes econômicas mineráveis, com valor econômico definido pelos dados que possui ou gera, é nessa perspectiva que o tópico seguinte aponta um *framework* conceitual que se afasta da singela tentativa de conceituar privacidade e posiciona sua lente para os problemas que dela decorrem.

4.1.3 *FRAMEWORK* CONCEITUAL DE PRIVACIDADE DE DANIEL J. SOLOVE

Daniel Solove (2008, p. 40) teoriza em sua densa obra que conceituar a privacidade depende de quatro dimensões, a primeira é a *metódica*, que privilegia a busca por pluralidades na definição de privacidade, afastando-se da procura por um denominador comum que subsuma as situações cotidianas ao conceito de privacidade defendido, o que se alcança com o método de semelhança de família proposto pelo filósofo Ludwig Wittgenstein.

Em apartada síntese, no método tradicional de conceituação parte-se da premissa de que o termo a ser definido possui características centrais às quais estarão sempre conectadas outras características periféricas, enquanto a teoria de Wittgenstein assume a possibilidade de outras conformações de conceituação, sobretudo aduz que é possível que determinados conceitos contem com uma malha de interrelação entre suas características, sem que partam de uma generalização apriorística (SOLOVE, 2008, p. 42 – 44).

O autor exemplifica com uma família:

> [...] em uma família, cada criança pode ter certas características similares à cada pai, e as crianças podem compartilhar características similares umas com as outras, mas eles [os pais e as crianças] podem não se assemelhar uns com os outros da mesma maneira. Mesmo assim, todos eles se parecem uns com os outros.[31] (SOLOVE, 2008, p. 42 – 43, tradução nossa).

[31] "[...] in a family, each child may have certain features similar to each parent, and the children may share similar features with each other, but they may not all resemble each other in the same way. Nevertheless, they all bear a resemblance to each other." (SOLOVE, 2008, p. 43 – 43)

Nesse sentido não se pretende definir privacidade buscando um eixo comum que ligue todas as situações, mas apropriar-se das relações que as situações possam ter para, assim, chegar em uma definição de privacidade.

A segunda dimensão para a conceituação de privacidade é a da generalidade, o conceito de privacidade deve partir de uma visão pragmática, pois através de análises que estejam nutridas de perspectivas contextuais e experienciais serão gerados resultados que redundarão em amplitude capaz de chegar à natureza dos problemas e, assim, na conformação teórica do termo (SOLOVE, 2008, 46 – 49; 75).

O pragmatismo "[...] afasta-se da abstração e da insuficiência, das soluções verbais, das más razões *a priori*, dos princípios fixos, dos sistemas fechados e dos pretensos absolutos e origens. Ele se volta para a concretude e adequação, para os fatos, para a ação e para o poder." (JAMES, 1991 *apud* SOLOVE, 2008, p. 47, tradução nossa)[32], portanto, ao aproximar-se das noções de Wittgenstein o pragmatismo permite *iniciar* o entendimento da privacidade por meio de situações contextuais específicas (SOLOVE, 2008, p. 47).

A análise contextual é importante pois o conceito de privacidade é dinâmico e sofre alterações, e como tal as aspirações sociais têm relevância nessas mudanças, por exemplo, "por um longo tempo as comunicações eram bastante inseguras, e seu estado dificilmente poderia ser rotulado como 'privado'. O desejo social, entretanto, era que as comunicações fossem privadas mesmo quando não fossem [de fato privadas]." (SOLOVE, 2008, p. 64, tradução nossa)[33].

O terceiro aspecto dimensional é a variabilidade, pois, segundo o autor, a sociedade muda e altera a sua compreensão acerca do que é privado ou não, aceitando determinados comportamentos e reprovando outros, e um conceito não poderia se imiscuir de considerar que cada contexto histórico e social, e mesmo a dicotomia entre oriente e ocidente é suficiente para trazer percepções distintas acerca do que seja privacidade em seus mais diversos ramos e aspectos cotidianos (SOLOVE, 2008, p. 50 – 67).

---

[32] "[...] turns away from abstraction and insufficiency, from verbal solutions, from bad a priori reasons, from fixed principles, closed systems, and pretended absolutes and origins. He turns towards concreteness and adequacy, towards facts, towards action and towards power." (JAMES, 1991 *apud* SOLOVE, 2008, p. 47, grifo do autor).

[33] "For a long time, communications were quite insecure, and their status could hardly be labeled 'private.' The social desire, however, was for communications to be private even when they were not. We make things private with the tools of law and technology." (SOLOVE, 2008, p. 64).

Note-se que enquanto a generalidade emerge da análise de problemas práticos específicos, em busca de uma teoria, a variabilidade atribui papel de relevo ao contexto em que os problemas específicos se desenvolvem e ocorrem (SOLOVE, 2008, p. 46 – 67).

Por fim, o autor traz a dimensão focal, pela qual aduz que a privacidade não pode ser conceituada pela ótica abstrata da natureza da informação ou assunto tratado,

> A privacidade não é uma propriedade inerente das coisas; depende de condições que podem se ligar a informações ou assuntos particulares. A privacidade não é uma preferência individual, mas é moldada pelas atitudes das pessoas. Tampouco a privacidade é meramente uma expectativa da sociedade; é um desejo normativo. (SOLOVE, 2008, p. 75, tradução nossa)[34].

A questão deve ser vista partindo dos problemas que se quer sejam resolvidos pelo direito, focando-se naquilo que traz preocupações e gera ao cidadão comum o desejo de proteção, independente destas violações serem tratadas sob a alcunha da privacidade ou não (SOLOVE, 2008, p. 77).

Diante dessas premissas assenta-se a taxonomia proposta pelo teórico, tendo como objetivo não *conceituar* especificamente privacidade, mas verificar quais problemas que podem causar sua violação para posteriormente fazer generalizações, com a abordagem pragmática, assim, foram definidos quatro eixos de atividades nocivas, "[...] (1) coleta da informação, (2) processamento da informação, (3) disseminação da informação, e (4) invasão" (SOLOVE, 2008, p. 103, tradução nossa)[35].

Os problemas relacionados à coleta da informação são aqueles causados por uma interrupção no processo de coleta de dados, podem se dar pela vigilância do indivíduo ou seu interrogatório não consentido (SOLOVE, 2008, p. 106).

Por sua vez, os problemas relacionados ao processamento da informação, referem-se à forma como os dados já coletados são utilizados, podendo violar a privacidade por diversas formas: agregação de uns dados aos outros; pela identificação do indivíduo pertencedor dos dados através de características objetivas ou subjetivas; por inseguranças na forma como os dados são armazenados e processados; por uso dos dados legitimamente coletados para fins secundários não informados ao seu dono; e, por fim, pela exclusão, que é a impossibilidade do

---

[34] "Privacy is not an inherent property of things; it depends upon conditions that can attach to particular information or matters. Privacy is not an individual preference, yet it is shaped by people's attitudes. Nor is privacy merely a societal expectation; it is a normative desire." (SOLOVE, 2008, p. 75).

[35] "[...] (1) information collection, (2) information processing, (3) information dissemination, and (4) invasion." (SOLOVE, 2008, p. 103).

possuidor dos dados ter acesso à eles e o conhecimento de quais dados foram efetivamente coletados sobre si (SOLOVE, 2008, p. 117 – 118; 123; 130 – 131; 133).

Já os problemas acerca da disseminação da informação referem-se à revelação dos dados coletados, grupo que inclui a quebra de confidencialidade; a revelação de informações, que se diferenciam da quebra por não ocorrer com o rompimento do liame de confiança, mas com a disseminação não autorizada de informações; e o aumento da acessibilidade dos dados, que facilita a descoberta de informações de terceiros armazenadas em determinados locais, através de sua publicação online, fazendo, assim, que sejam mais facilmente disseminadas do que seriam se se mantivessem em seu substrato físico (SOLOVE, 2008, p. 136; 140 – 142; 149 – 150).

Ainda na disseminação da informação há o subgrupo da exposição, entendida como a exibição de atributos psicológicos e físicos de determinado indivíduo a outros, sendo que geralmente são atributos que se encontram em um contexto repugnante socialmente, como o corpo nu dilacerado ou um indivíduo com fezes e urina próximos a si. (SOLOVE, 2008, p. 147 – 148).

A chantagem é mais uma das formas com que se permite a quebra da privacidade mediante disseminação da informação, pois se trata de uma relação de dominação baseada no poder que o chantagista tem sobre a sua vítima ao coagi-la, mediante ameaça, a fazer ou deixar de fazer algo, sob pena de ter seus dados injustamente divulgados (SOLOVE, 2008, p. 151 – 153).

Tem-se também a apropriação e a distorção no grupo da disseminação da informação, enquanto esta se refere à alteração da percepção que os outros têm de determinado indivíduo aquela se refere ao uso que determinado indivíduo faz da identidade de um terceiro como se sua fosse (SOLOVE, 2008, p. 155; 160).

Por fim, tem-se o último grupo, o da invasão, que é discutida por duas linhas bastante similares, a primeira é a da intrusão, entendida como a invasão *em geral* na vida de um indivíduo, afetando seu direito de ser deixado a sós e ter um espaço reservado para a sua solidão ou mesmo interação cotidiana, e a segunda a da interferência decisional, cuja diferença para a anterior se dá no escopo, vez que é tipo de invasão mais restrita, praticada pelo governo ou Estado contra o indivíduo impedindo-o de gozar de seu direito de decidir. (SOLOVE, 2008, p. 161 – 165; 167 – 169).

Esse *framework* acaba por contemplar as três concepções de privacidade principais e anteriormente expostas, o direito de ser deixado a sós, o direito ao controle, acesso, correção, disponibilização e armazenagem dos dados pessoais, à sua livre escolha, o que enaltece a

autodeterminação informativa, e, por fim, o direito à autonomia existencial, por meio da liberdade de fazer escolhas pessoais sensíveis de caráter existencial. (RODOTÀ, 2008, p. 92)

Passada a dificultosa tarefa de conceituar, ou, mais apropriadamente, entender de que se trata a privacidade, o que se fez explorando os tortuosos caminhos e discussões conceituais e, posteriormente, partindo do *framework* de Daniel J. Solove e sua abordagem pragmática, aponta-se no tópico seguinte o cenário atual da privacidade na Internet das Coisas.

4.2 CENÁRIO ATUAL DA PRIVACIDADE NA INTERNET DAS COISAS

Segundo dados da HP em seu relatório de estudo intitulado "Internet of things research study report", citado por Eduardo Magrani (2018, p. 93), 70% dos dispositivos de Internet das Coisas possuíam, em 2014, quando publicado o estudo, falhas de segurança que os poriam em propensão ao ataque de um hacker, sendo os problemas maiores relacionados à privacidade, insuficiência de proteção dos dados em seu transporte, softwares de segurança inadequados, entre outros.

Rose, Eldridge e Chapin (2015) expõem que até 2025 o impacto econômico da Internet das Coisas será massivo, alcançando cerca de 100 bilhões de dispositivos interconectados, com impacto de 11 trilhões de dólares. Tony Danova (2013) aponta análise mais otimista, feita pela Morgan Stanley, para a empresa do setor financeiro o número de dispositivos de Internet das Coisas pode alcançar já em 2020 a marca dos 75 bilhões, dados que apresentam a dimensão da evolução — e do problema que a acompanha.

Muitos dos dispositivos que estarão futuramente disponíveis serão apenas a adaptação de objetos analógicos convencionais para a era da Internet das Coisas, adicionando a eles uma camada digital para sua conexão em rede com outros objetos, o que acaba por criar uma Internet das Coisas Inúteis.

A Internet das Coisas Inúteis é um conceito crítico que pontua a desnecessidade de tornar qualquer objeto analógico em digital, vez que nem sempre a conversão o tornará mais simples e, muitas vezes, trará ainda um custo elevado e injustificável para sua produção (MAGRANI, 2018, p. 47).

O conceito de Internet das Coisas Inúteis é de relevância para a compreensão dos problemas, vez que a conversão de produtos analógicos em digitais, que não criam engajamento substancial e são brevemente descartados ou deixados de lado pelo consumidor, apenas para que possam ostentar o rótulo de produtos inteligentes (*smart products*) ou *high techs*, "além de encarecer o produto e deixá-lo sujeito a falhas que não teria a priori, pode gerar riscos também

em relação à segurança e à privacidade." (ROMAN; ZHOU; LOPEZ, 2010 *apud* MAGRANI, 2018, p. 49, grifo do autor).

No contexto da *big data*, ou seja, com volume massivo de dados comportamentais do usuário, que possibilitam conhece-lo e prever seus interesses antes mesmo de sua ação, a propagação de informações e dados por dispositivos tende a ser cada vez maior e mais rápida, e as brechas de privacidade, como tal, tendem a crescer com um mercado acelerado, sem tempo para pormenores de segurança, pois um dia pode ser decisivo para que o lançamento de um dispositivo de IoC seja bem ou malsucedido.

Assim, os usuários são perfilados e rastreados por dispositivos de IoC que se encontram — ou tendem a estar — em qualquer lugar e coisa, disponíveis a qualquer momento, em serviços e objetos personalizados ou de uso comunitário, e mesmo nos ambientes em si, todos capazes de coletar dados consideráveis e adquirir informações automaticamente (ROMAN; NAJERA; LOPEZ, 2011).

A conectividade dos objetos à internet permite remotamente que seu estado seja determinado através de sua localização e informações físicas e processuais, advindas de sensores, garantindo que o mundo real seja observado de formas que antes não eram possíveis e por um preço ínfimo (MATTERN; FLOERKEMEIER, 2010, p. 242 - 243), tudo através da coleta de dados.

Não se olvide de dizer, como bem explicita Lévy (2011) que a gama de dados de cada usuário disponíveis pode representar uma ameaça à sua privacidade, pois o espaço digital tem sido tratado como um verdadeiro mercado, onde há constante disputa de interesses e comércio das informações adquiridas, um verdadeiro "banco de dados universal onde poderiam ser encontrados e consumidos, mediante pagamento, todas as mensagens, todas as informações, todos os programas, todas as imagens, todos os jogos imagináveis." (LÉVY, 2011, p. 208).

Nesse sentido a privacidade pode ser relativizada por interesses diversos, sejam apenas financeiros, que dá às grandes empresas o poder de traçar estratégias de venda mais bem elaboradas ao conhecer intimamente cada um de seus clientes ou possíveis clientes, sejam aqueles que perpassem a aquisição de informações, que trazem um plano de fundo de cruzamento ou utilização de dados para persecução penal ou mesmo tributária.

Acerca da segurança dos dados Eduardo Magrani (2018, p. 92) aponta que "[...] ainda não há um consenso entre os fabricantes de produtos de IoT. Os próprios desenvolvedores ainda não têm uma noção completa do que é realmente necessário em termos de segurança", e nesse ínterim do desenvolvimento e aperfeiçoamento técnico dos protocolos de segurança e

privacidade os dados de uso das coisas vão sendo acumulados e tratados, muitas vezes precariamente.

Assim, o lento desenvolvimento de objetos de IoC adequados à curadoria de dados sensíveis, comparando-se com o exponencial lançamento de objetos diariamente, bem como toda a sua interconectividade acabam por tornar a segurança e privacidade do usuário frágeis e a necessidade de se questionar até onde o Estado pode interferir nisso se mostra premente (MAGRANI, 2018, p. 91 - 92), sobretudo em questões de regulamentação e coleta de dados pelo próprio Estado.

Enquanto os Estados-Nação já passam a se adequar para a atual era da internet e adaptam seus ambientes e mesmo as cidades (*smart cities*) para essa realidade, ainda pouco se fala sobre como devem se portar na persecução penal, em situações de conflito, diante de dados, tanto públicos quanto privados, que podem ser elemento de convicção em uma acusação.

A experiência brasileira ainda está adstrita à poucas legislações, como a recente Lei Geral de Proteção de Dados Pessoais, o Marco Civil da Internet, bem como a legislação regulamentadora do artigo 5º, inciso XII da Constituição, qual seja, Lei 9.296, de 24 de julho de 1996, que cuida das interceptações telefônicas e telemáticas.

O Brasil também é signatário da Convenção Americana sobre Direitos Humanos, conforme Decreto nº 678, promulgado em 6 de novembro de 1992, sendo nela prevista, em seu artigo 11.2 que: "ninguém pode ser objeto de ingerências arbitrárias ou abusivas em sua vida privada, em sua família, em seu domicílio ou em sua correspondência, nem ofensas ilegais à sua honra ou reputação" (BRASIL, 1992), no entanto, há pouca repercussão interna dos casos julgados pela Corte Interamericana de Direitos Humanos, que tem jurisdição obrigatória no Estado Brasileiro (GRECO FILHO, 2015, p. 16 – 17), dificultando-se o controle de convencionalidade para casos relacionados às provas ilícitas.

A resposta para o problema de pesquisa, após todo o apanhado teórico, direciona-se para o embate entre o direito à proteção dos dados, pelas perspectivas da autodeterminação informativa e privacidade, e a possibilidade que o Estado tem, de perpassar direitos fundamentais em prol do interesse coletivo e utilizar nos autos dados que são coletados de forma não-autorizada, questão principal do trabalho e que o concluirá no tópico seguinte.

5 CONCLUSÃO

A lei de interceptação telefônica enquanto regulamentadora da parte final do inciso XII do artigo 5º da Constituição Federal de 1988 ousou cuidar especialmente das questões concernentes ao fluxo das comunicações telefônicas, fazendo brevíssimas menções às comunicações informáticas e telemáticas.

Se em 1988 o telefone era majoritariamente instrumento de conversação por transferência sonora a realidade atual já diverge, permitindo-se chamadas por voz e vídeo e a transmissão de dados das mais diversas naturezas por aplicativos que estão na palma das mãos de grande parcela dos indivíduos, de forma que os apontamentos *en passant* relativos às comunicações informáticas e telemáticas poderiam ser entendidos apenas em uma perspectiva do avanço das técnicas de telecomunicação.

Acerca dos dados preteritamente coletados ou mesmo da existência de limites estanques para o juiz autorizar a sua coleta, especialmente os registros telefônicos, objeto da lei 9.296/1996, deve-se ter em mente que a legislação ficou à mercê das interpretações jurisprudenciais e doutrinárias, que têm corrente majoritária entendendo pela aplicação da lei referida não apenas no contexto telefônico (mesmo que com seus avanços), mas na interceptação do fluxo de informação de quaisquer dados informáticos e telemáticos.

O ponto chave do estudo, no entanto, vai além do fluxo comunicacional e preocupa-se especialmente com a busca e apreensão dos dados de dispositivos de Internet das Coisas, mas não quaisquer dados, especificamente os que foram coletados na origem sem o consentimento do acusado no processo penal e sem sua ciência das finalidades secundárias de coleta.

Embora ainda haja muitos dispositivos de Internet das Coisas que adotam uma postura menos autônoma acerca da coleta de dados, dependendo de *inputs* e configurações iniciais predefinidas por seu usuário para que continuem suas atividades-fim, e aqueles com graves problemas na segurança e privacidade dos dados, a perspectiva que se tem é que a indústria passe a investir em dispositivos que poderão agir por si sós, sem a interferência da — em um contexto de inteligências artificiais — limitada e ineficiente inteligência e capacidade humana.

O ponto principal para análise da tutela da privacidade e proteção de dados nesses dispositivos deve se dar partindo da ausência de consentimento informado vasto o suficiente para que o mesmo colete, compartilhe, utilize e armazene informações contextuais referentes ao usuário, o que viola de início a autodeterminação informativa deste.

O uso de dados coletados pelos dispositivos de IoT como prova não é feito mediante sua interceptação, mas com a busca e apreensão de coisa e os dados que nela estejam contidos, e a primeira razão fundamentadora para a vedação do uso dos dados referidos se faz por equiparação aos cenários de interceptação telefônica.

É a ordem judicial que torna a ilicitude da interrupção do fluxo comunicacional na interceptação telefônica legítima e prestáveis seus dados coletados como elementos de convicção, portanto, antes de autorizada a interceptação não é lícita a disponibilização do teor das conversas realizadas sem o consentimento das partes para tal.

No entanto, mesmo autorizada a interceptação, esta tem prazo certo de ocorrência, não podendo ser feita *ad aeternum*, sob pena de se violar tanto as previsões do artigo 5º da Lei 9.296, de 24 de julho de 1996, quanto a própria existência de justa causa e dos limites da ordem emanada da autoridade judiciária.

Já quanto ao conteúdo pretérito, a autorização não o abrangerá, apenas o seu registro, que, como é dado *per se*, e não fluxo de dado, não conta com a proteção da legislação aplicável à interceptação telefônica, como proficuamente têm entendido os tribunais superiores, ou seja, a interceptação é pós-delitual ou ocorre mediante autorização que capte o momento do delito.

A situação do estudo é particular pois difere-se da lógica que se tem na interceptação da comunicação telefônica. Nela o usuário livremente se comunica com outro, através de seu aparelho telefônico ou dispositivo com função equiparada, exercendo seu direito fundamental de liberdade negativa, e, diante do mandamento judicial, um terceiro alheio àquela relação comunicador-receptor livremente estabelecida, toma conhecimento dos assuntos tratados, relativizando o direito à privacidade de todos os envolvidos.

Embora na interceptação telefônica o indivíduo interceptado não tenha ciência de que ocorre a interrupção do fluxo de comunicação enquanto se comunica, este está ciente de que o conteúdo de sua fala está sendo transmitido e captado, v. g., pelo receptor do telefonema. Já nos dispositivos de Internet das Coisas cujas camadas de privacidade não possuam grandes possibilidades de customização por seu usuário, ou quando as definições padrões de fábrica violam a privacidade, ou mesmo quando o usuário consente de forma desinformada, haverá devassa do conteúdo contextualmente captado ao não se concluir pela sua vedação como prova acusatória.

O mapeamento de um local onde investiga-se a ocorrência de crime e o uso de dados de *tracking* de calçados conectados à rede ou da voz captada por uma televisão podem colocar o acusado imediatamente dentro da cena de um crime, e quando o usuário desses dispositivos

apenas buscava aspirar sua residência, coletar seus dados de cadência ou assistir ao seu filme preferido, não conferindo qualquer autorização além das pretendidas, há violação da privacidade, conforme *framework* de Daniel J. Solove, em relação à coleta dos dados, que ocorre mediante inautorizada vigilância; quanto ao seu processamento, por ser utilizado para fins secundários aos autorizados pelo usuário do dispositivo de IoT; e por ter ocorrido a invasão mediante intrusão e interferência decisional do Estado — esta entendida em conjunto com o padrão da jurisprudência alemã acerca da autodeterminação informativa.

Não se pode vigiar o tempo todo uma pessoa, pela simples possibilidade de ser um suspeito de um crime, e é dessa premissa que se partiria ao permitir o uso de dados captados indeterminadamente, sem que o usuário possa determinar-se nesse contexto de coleta.

Assim, a busca e apreensão de dados armazenados em dispositivos de Internet das Coisas, ao ocorrer em um cenário onde o seu adquirente sequer sabe quais dados seus já foram captados pelo objeto, pois não tem controle direto sobre aquela inteligência artificial ou dispositivo senão os parametrizados pelo seu fabricante, permitiria a coleta de elemento de prova que surgiu com violação ao direito de privacidade ao passo que a autodeterminação informativa não pode ser exercida pelo usuário em relação aos seus próprios dados.

Embora haja a possível relativização de direitos constitucionais, sobretudo quando colidem, para que o sistema constitucional alcance uma maior efetividade, as causas previstas ordinariamente para a coleta de dados armazenados, mediante busca e apreensão, não devem se estender aos dados coletados de forma manifestadamente ilícita e sem anterior autorização judicial e a proporcionalidade constitucional deve ser vista casuisticamente, sempre atentando-se à rigorosa excepcionalidade de admissão de provas ilícitas como elementos de convicção no processo penal.

Convém que o entendimento do judiciário em relação ao uso dos dados coletados em violação às legislações ordinárias, notadamente a Lei Geral de Proteção de Dados Pessoais em seu artigo 2º, incisos I e II, pois, se direcione de forma à vedar sua coleta, vez que os mesmos são pretéritos à qualquer autorização judicial e surgiram sem que o acusado tivesse qualquer tipo de ciência e consentimento na origem.

Apegando-se à corrente defendida por Nuvolone, que parte da premissa de que sempre que a fonte de prova for obtida de forma ilícita a prova será inadmissível, chega-se à conclusão de que o fator que se tem como preponderante para determinar a licitude se vincula à forma com que a fonte de prova é obtida.

Aprofundando a afirmativa delineiam-se premissas para o caso do uso de dados coletados por dispositivos de Internet das Coisas sem a autorização de seu proprietário:

1. O dispositivo de Internet das Coisas coleta dados contextuais do indivíduo;
2. A coleta de dados contextuais pode ou não ser autorizada pelo indivíduo;
3. A falta de autorização extrapola o consentimento e direito de o indivíduo decidir, conforme artigo 2º, I e II da Lei Geral de Proteção de Dados;
4. A ordem jurídica brasileira considera como fundamento da proteção de dados a autodeterminação afirmativa;
5. por sua vez, os dados coletados violaram a autodeterminação afirmativa;

Os dados em si são *fontes* de prova, sua coleta é meio de obtenção da fonte de prova, sendo esta coleta ilegal por violar a autodeterminação informativa a prova não pode ser convalidada em lícita como regra do sistema jurídico.

Outra das razões para assim entender possui caráteres eminentemente sociológicos e criminológicos. A Internet das Coisas amplia a vigilância dos usuários ao permitir a coleta parametrizada de inúmeros dados, como de voz, dados corporais e aqueles captados por sensores de condições ambientais e de geolocalização, e as violações à privacidade ocorrem justamente pela falta de padrões de desenvolvimento que possam minimamente garanti-la durante o uso destes objetos.

Partindo dessa premissa, ao se permitir o uso de dados captados de forma não autorizada como prova acusatória em um processo penal estar-se-ia legitimando um constante estado de vigilância, onde o detentor do rumo (determinação conforme a finalidade) das informações das vidas civis deixa de ser o próprio usuário ao qual os dados se referem.

Ainda na mesma senda teórica, a assimetria da informação traz seu peso na conformação do problema. A Internet das Coisas Inúteis é um conceito notado facilmente na prática dos mercados internacionais de massa, cuja única preocupação tem sido converter objetos analógicos para o mundo digital com a máxima rapidez e o menor dos custos, e essa percepção atiça a necessária compreensão do que essa dinâmica econômica representa.

A criação de produtos baratos para que as *coisas*, mesmo que inúteis, cheguem às casas de qualquer pessoa, a fluidez e velocidade da inovação, o marketing que difunde a ideia de facilidade e comodidade para o dia a dia, a ausência de padrões de desenvolvimento de software e hardware claros, dentre inúmeros outros fatores empurram para o lado a necessária preocupação com as possibilidades que o dispositivo carrega de fábrica para as definições das camadas mínimas de privacidade, opções que apenas grandes empresas tendem a prestar mais atenção no lançamento de produtos.

Este cenário de convalidação de lícito em ilícito, mesmo sem a expressão da autodeterminação, fará com que a privacidade e o direito à proteção de dados deixem de ser

direitos fundamentais, mas bens que apenas o dinheiro poderá comprar, pois só aqueles que adquiram produtos bem desenvolvidos e que tenham acesso às formas de definir como seus dados são capturados que poderão, mesmo com a apreensão de seus dispositivos, se ver livres de uma condenação que se fundamente nos dados apreendidos.

Por fim, o horizonte do problema é muito maior e, mesmo com a validade da hipótese defendida as respostas estão ainda distantes, sobretudo pois dessas conclusões traçadas surgem novas perguntas, como qual a forma adequada de comprovar o consentimento e autodeterminação; onde se insere a tutela jurídica sob o viés doutrinário da autodeterminação quando os dados captados são os de terceiros, e quais os limites da autodeterminação quando se analisa o interesse público.

A conclusão a que se chega acerca do tema é que embora se tenha fundamentação hábil para sustentar a ilicitude de uso de dados coletados de dispositivos de Internet das Coisas quando não houve consentimento do usuário na coleta, a questão deve ser ampliada com fins de sistematizá-la para que se torne, quando desemboquem os problemas no Judiciário, uma tese madura à apreciação, sobretudo por se tratar de assunto que se vincula a tecnologias — e problemas — bastante recentes e têm tido pouca apreciação da doutrina clássica, cujo enfoque da ilicitude da prova penal acaba por ser discutido apenas em relação aos meios de sua coleta, e não às suas origens e resultados probatórios.

REFERÊNCIAS

ALVAREZ, Edgar. **Under Armour's HOVR connected shoes aim to make you a smarter runner**. 2019. Disponível em: https://www.engadget.com/2019/02/01/under-armour-hovr-infinite-mapmyrun-smart-running-shoes/. Acesso em: 10 mar. 2019.

ARSÉNIO, A. *et al*. Internet of Intelligent Things: Bringing Artificial Intelligence into Things and Communication Networks. *In:* XHAFA F.; BESSIS N. (editores). **Inter-cooperative Collective Intelligence**: Techniques and Applications. Studies in Computational Intelligence. Berlim: Springer, 2014. Cap. 1. p. 1 – 37. 440 p.

ASHTON, Kevin. **The 'internet of things' thing**: In the real world, things matter more than ideas. 2009. Disponível em: https://www.rfidjournal.com/articles/view?4986. Acesso em: 25 fev. 2019.

AVOLIO, Luiz F. Torquato. **Provas ilícitas** – interceptações telefônicas e gravações clandestinas. São Paulo: Editora RT, 1995.

BIONI, Bruno Ricardo. **Proteção de dados pessoais**: a função e os limites do consentimento. Rio de Janeiro: Forense, 2019. 316 p.

BRASIL. [Constituição (1988)]. **Constituição da República Federativa do Brasil**. Brasília, DF: Presidência da República, 1988. Disponível em: http://www.planalto.gov.br/ccivil_03/Constituicao/Constituicao.htm. Acesso em: 5 abr. 2019.

BRASIL. **Decreto 678, de 6 de novembro de 1992**. Promulga a Convenção Americana sobre Direitos Humanos (Pacto de São José da Costa Rica), de 22 de novembro de 1969. Brasília, DF: Presidência da República, 1992. Disponível em: http://www.planalto.gov.br/ccivil_03/decreto/D0678.htm. Acesso em: 27 abr. 2019.

BRASIL. **Decreto-Lei 3.689, de 3 de outubro de 1941**. Código de Processo Penal. Brasília, DF: Presidência da República, 1941. Disponível em: http://www.planalto.gov.br/ccivil_03/decreto-lei/del3689compilado.htm. Acesso em: 4 maio 2019.

BRASIL. **Lei nº 13.709, de 14 de agosto de 2018**. Dispõe sobre a proteção de dados pessoais e altera a Lei nº 12.965, de 23 de abril de 2014 (Marco Civil da Internet). Brasília, DF: Presidência da República, 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Lei/L13709.htm. Acesso em: 5 abr. 2019.

BRASIL. **Lei nº 9.296, de 24 de julho de 1996**. Regulamenta o inciso XII, parte final, do art. 5° da Constituição Federal. Brasília, DF: Presidência da República, 1996. Disponível em: http://www.planalto.gov.br/ccivil_03/LEIS/L9296.htm. Acesso em: 22 abr. 2019.

BRASIL. Superior Tribunal de Justiça. **Agravo Regimental no Recurso Especial nº 1.154.376**, Ministério Público Federal. Relator: Min. Sebastião Reis Júnior. 29 de maio de 2013. Disponível em: https://ww2.stj.jus.br/processo/pesquisa/. Acesso em 11 mai. 2019.

BRASIL. Supremo Tribunal Federal. **Recurso Extraordinário nº 418.416, Luciano Hang**. Relator: Min. Menezes Direito. 04 de abril de 2006. Disponível em:

http://stf.jus.br/portal/diarioJustica/verDiarioProcesso.asp?numDj=242&dataPublicacaoDj=19/12/2006&incidente=2205705&codCapitulo=5&numMateria=43&codMateria=1. Acesso em: 22 abr. 2019.

CERF, Vinton G.; KAHN, Robert E. A Protocol for Packet Network Intercommunication. **IEEE Transactions on Communications**, vol. 22, nº. 5, Mai. 1974, p. 637 – 648.

CIDH. **Corte Interamericana de Direitos Humanos**: Caso Favela Nova Brasília vs. Brasil. 2017. Disponível em: http://www.corteidh.or.cr/docs/casos/articulos/seriec_333_esp.pdf. Acesso em: 22 mar. 2019.

CONTROLE Todos os Treinos. **MapMyFitness**. 2019. Disponível em: https://www.mapmyfitness.com. Acesso em: 7 abr. 2019.

DANOVA, Tony. **Morgan Stanley:** 75 Billion Devices Will Be Connected To The Internet Of Things By 2020. 2013. Disponível em: https://www.businessinsider.com/75-billion-devices-will-be-connected-to-the-internet-by-2020-2013-10. Acesso em: 19 fev. 2019.

GRECO FILHO, Vicente. **Interceptação telefônica**: considerações sobre a Lei n. 9.296/96. 3. ed. rev., atual. e ampl. São Paulo: Saraiva, 2015. *E-book*. Acesso restrito via Minha Biblioteca.

GRINOVER, Ada Pellegrini. **Liberdades Públicas e Processo Penal**: As Interceptações Telefônicas. 2. ed. atual. São Paulo: Ed. Revista dos Tribunais, 1982. 288 p.

GOMES, Luiz Flávio; CERVINI, Raúl. **Interceptação telefônica**: lei 9.296, de 24.07.96. São Paulo: Editora Revista dos Tribunais, 1997. 280 p.

GSM Association. **How China is scaling the internet of things**: An insight report from the GSMA Connected Living Programme. 2015. Disponível em: https://www.gsma.com/newsroom/wp-content/uploads/16531-China-IoT-Report-LR.pdf. Acesso em: 22 mar. 2019.

HUMAN RIGHTS WATCH. **Brazil**: Events of 2018. 2019. Disponível em: https://www.hrw.org/world-report/2019/country-chapters/brazil#4368e7. Acesso em 22 mar. 2019.

KHODADADI, F.; DASTJERDI, A. V.; BUYYA, R. Internet of things: an overview. *In:* BUYYA, Rajkumar; DASTJERDI, Amir Vahid (editores). **Internet of Things:** Principles and Paradigms. Massachusetts: Morgan Kaufmann, 2016. 354 p.

LEINER, Barry M. *et al*. **Brief History of the Internet**. 1997. Disponível em: https://www.internetsociety.org/internet/history-internet/brief-history-internet/. Acesso em: 9 mar. 2019.

LÉVY, Pierre. **Cibercultura**. 3. ed. São Paulo: Editora 34, 2011. 272 p. Tradução de: Carlos Irineu da Costa.

LIMA, Alessandro Barbosa. Privacidade. *In*: AVORIO, Andre; SPYER, Juliano (orgs.). **Para entender a Internet**. 2. ed. rev. e ampl. *[s.l.]*: Não Zero, 2015. Cap. 57. p. 221 – 223.

MAGRANI, Eduardo. **A internet das coisas**. Rio de Janeiro: FGV Editora, 2018. 192 p.

MARCÃO, Renato. **Curso de Processo Penal**. 4. ed. rev., atual. e ampl. São Paulo: Saraiva Educação, 2018. 1240 p.

MARTÍNEZ, Ricard Martínez. El derecho fundamental a la protección de datos: perspectivas. **Revista de Internet, Derecho y Política**. Catalunha, V. 0, nº. 5, Nov. 2007, p. 47 – 61. Disponível em: https://idp.uoc.edu/articles/10.7238/idp.v0i5.440/galley/3346/download/. Acesso em 28 mai. 2019.

MATTERN, Friedemann; FLOERKEMEIER, Christian. From the Internet of Computers to the Internet of Things. **Lecture Notes In Computer Science**, *[s.l.]*, p. 242 - 259, 2010. Springer Berlin Heidelberg. Disponível em: https://vs.inf.ethz.ch/publ/papers/Internet-of-things.pdf. Acesso em: 25 fev. 2019.

MELLO, Rodrigo Pereira de. **Provas ilícitas e sua interpretação constitucional**. Porto Alegre: Sergio Antonio Fabris Editor, 2000. 160 p.

MENDRONI, Marcelo Batlouni. **Provas no Processo Penal**. Estudo Sobre a Valoração das Provas Penais. 2. ed. São Paulo: Editora Atlas, 2015. 179 p.

MULHOLLAND, Caitlin. A Tutela da Privacidade na Internet das Coisas (IOT). *In:* REIA, Jhessica (orgs.) *et al.* **Horizonte Presente**: Tecnologia e Sociedade em Debate. Belo Horizonte: Casa do Direito; FGV — Fundação Getúlio Vargas, 2019. p. 485 – 495.

NUCCI, Guilherme de Souza. **Curso de Direito Processual Penal**. 15. ed. Rio de Janeiro: Forense, 2018. *E-book*. Acesso restrito via Minha Biblioteca.

O'FLAHERTY, Kate. **China Facial Recognition Database Leak Sparks Fears Over Mass Data Collection**. 2019. Disponível em: https://www.forbes.com/sites/kateoflahertyuk/2019/02/18/china-facial-recognition-database-leak-sparks-fears-over-mass-data-collection/#669e1c6efb40. Acesso em 10 mar. 2019.

OHCHR. **Universal Declaration of Human Rights**. 2019. Disponível em: https://www.ohchr.org/EN/UDHR/Pages/Language.aspx?LangID=por acesso em: 21 abr. 2019.

PACELLI, Eugênio. **Curso de processo penal**. 22. ed. rev., atual. e ampl. São Paulo: Atlas, 2018. *E-book*. Acesso restrito via Minha Biblioteca.

PEREIRA, Marcelo Cardoso. **Direito à intimidade na internet**. Curitiba: Jurá Editora, 2006. 280 p.

ROBINSON, Wesley. **Watch 'Today' segment on how Fitbit helped expose woman's false rape claim in Lancaster County**. 2016. Disponível em: https://www.pennlive.com/news/2016/04/watch_today_segment_on_how_fit.html. Acesso em 10 mar. 2019.

RODOTÀ, Stefano. **A vida na sociedade da vigilância**: a privacidade hoje. Rio de Janeiro: Renovar, 2008.

ROHRMANN, Carlos Alberto. **Curso de Direito Virtual**. Belo Horizonte: Del Rey, 2005. 276 p.

ROMAN, Rodrigo; NAJERA, Pablo; LOPEZ, Javier. Securing the Internet of Things. **Computer**, *[s.l.]*, v. 44, n. 9, p. 51-58, set. 2011. Institute of Electrical and Electronics Engineers (IEEE). Disponível em: https://ieeexplore.ieee.org/document/6017172. Acesso em: 21 fev. 2019.

ROSE, Karen; ELDRIDGE, Scott; CHAPIN, Lyman. **The Internet of things**: an overview. Understanding the issues and challenges of a more connected world. *[s.l.]* Internet Society, 2015. Disponível em: https://www.internetsociety.org/wp-content/uploads/2017/08/ISOC-IoT-Overview-20151221-en.pdf. Acesso em: 25 fev. 2019.

SALAMA, Usama. **Investigating IoT Crime in the Age of Connected Devices**. 2017. Disponível em: https://securityintelligence.com/investigating-iot-crime-in-the-age-of-connected-devices. Acesso em 27 mar. 2019.

SARLET, Ingo Wolfgang; MARINONI, Luiz Guilherme; MITIDIERO, Daniel. **Curso de Direito Constitucional**. 7. ed. rev., atual. e ampl. São Paulo: Saraiva Educação, 2018. *E-book*. Acesso restrito via Minha Biblioteca.

SCHWARTZ, Paul M. Property, Privacy, and Personal Data. **Harvard Law Review**, *[s.l.]*, v. 117, n. 7, p. 2056 – 2128, maio 2004. JSTOR.

SHEPHERD, Christian. **'Big data' predictions spur detentions in China's Xinjiang - Human Rights Watch**. 2018. Disponível em: https://uk.reuters.com/article/uk-china-rights-xinjiang/big-data-predictions-spur-detentions-in-chinas-xinjiang-human-rights-watch-idUKKCN1GB0CZ. Acesso em: 10 mar. 2019.

SOLOVE, Daniel J. **Understanding Privacy**. England: Harvard University Press, 2008. 257 p.

SPYER, Juliano. Web 2.0. *In:* AVORIO, Andre; SPYER, Juliano (orgs.). **Para entender a Internet**. 2. ed. rev. e ampl. *[s.l.]*: Não Zero, 2015. Cap. 23. p. 91 – 92.

TAVARES, André Ramos. **Curso de Direito Constitucional**. 16. ed. rev. e atual. São Paulo: Saraiva Educação, 2018. *E-book*. Acesso restrito via Minha Biblioteca.

TÁVORA, Nestor; ALENCAR, Rosmar Rodrigues. **Curso de direito processual penal**. 11. ed. rev., ampl. e atual. Salvador: Editora Juspodivm, 2016. 1834 p.

TOLEDO, Mario. **Câmeras de reconhecimento facial começam a funcionar em Copacabana**. 27 fev. 2019. Disponível em: http://agenciabrasil.ebc.com.br/geral/noticia/2019-02/cameras-de-reconhecimento-facial-comecam-funcionar-em-copacabana. Acesso em 7 abr. 2019.

UA HOVR™ Phantom/SE. **Under Armour**. 2019. Disponível em: https://www.underarmour.com/en-us/mens-ua-hovr-phantom-se-running-shoes/pid3021587-600. Acesso em 7 abr. 2019.

UNIÃO EUROPÉIA. Parlamento Europeu e Conselho da União Europeia. **Regulamento 2016/679 de 27 de abril de 2016**. Relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados). Disponível em:

https://publications. europa.eu/pt/publication-detail/-/publication/3e485e15-11bd-11e6-ba9a-01aa75ed71a1. Acesso em: 27 mar. 2019.

WEBER, Rolf H.. Internet of things – Need for a new legal environment? **Computer Law & Security Review**, *[s.l.]*, v. 25, n. 6, p.522-527, nov. 2009. Elsevier BV. Disponível em: https://www.sciencedirect.com/science/article/pii/S0267364909001514. Acesso em 24 fev. 2019.