2023

CÍNTIA ROSA PEREIRA DE LIMA

PREFÁCIO DE NELSON ROSENVALD

SISTEMA DE RESPONSABILIDADE CIVIL PARA CARROS AUTÔNOMOS

EDITORA FOCO

2023

CÍNTIA ROSA PEREIRA DE LIMA

PREFÁCIO DE NELSON ROSENVALD

SISTEMA DE RESPONSABILIDADE CIVIL PARA CARROS AUTÔNOMOS

EDITORA FOCO

Dados Internacionais de Catalogação na Publicação (CIP) de acordo com ISBD

L732s Lima, Cíntia Rosa Pereira de
Sistema de responsabilidade civil para carros autônomos / Cíntia Rosa Pereira de Lima. - Indaiatuba, SP : Editora Foco, 2023.

240 p. ; 16cm x 23cm.

Inclui bibliografia e índice.

ISBN: 978-65-5515-808-3

1. Direito. 2. Direito civil. 3. Responsabilidade civil. 4. Carros autônomos. I. Título.

2023-1532 CDD 347 CDU 347

Elaborado por Vagner Rodolfo da Silva – CRB-8/9410

Índices para Catálogo Sistemático:

1. Direito civil 347
2. Direito civil 347

CAPÍTULO 2
INTERNET DAS COISAS E SUA APLICAÇÃO NA AUTOMAÇÃO DOS CARROS

The consumer "Internet of Things" is suddenly reality, not science fiction. Electronic sensors are now ubiquitous in our smartphones, cars, homes, electric systems, health-care devices, fitness monitors, and workplaces. [...] For example, insurers can price automobile coverage more accurately by using sensors to measure exactly how you drive (e.g., Progressive's Snapshot system), which should theoretically lower the overall cost of insurance.

Scott R. Peppet (Universidade de Colorado, Estados Unidos)[1]

Internet das Coisas ou *Internet of Things (IoT)*, na expressão inglesa consagrada em nível global, vem chamando a atenção de empresas e do Governo haja vista os enormes benefícios sociais e econômicos. Este interesse pode ser evidenciado com a consolidação de consórcios para desenvolver esta tecnologia a ser aplicada em diversos segmentos do mercado e das chamadas "Cidades Inteligentes" ("Smart Cities").[2] Por exemplo, a aquisição da *Nest* pela *Google* por 3,2 bilhões de dólares

1. PEPPET, Scott R. Regulating the Internet of Things: First Steps Toward Managing Discrimination, Privacy, Security, and Consent. *Texas Law Review*, v. 93, p. 85-176, 1º mar. 2014. Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2409074. Acesso em: 12 fev. 2020. p. 85: "O consumo de 'Internet das Coisas' é uma realidade, deixou de ser ficção científica. Os sensores eletrônicos agora são onipresentes em nossos *smartphones*, carros, residências, sistemas elétricos, dispositivos de saúde, monitores de *fitness* e locais de trabalho. [...] Por exemplo, as seguradoras podem precificar a cobertura de automóveis com mais precisão usando sensores para medir exatamente como você dirige (por exemplo, o sistema *Progressive's Snapshot*), o que teoricamente deve reduzir o custo total do seguro." (tradução livre)
2. Entretanto, a Internet das Coisas pode ser uma solução em diversos segmentos, tais como: *Connected Cars, Smart Homes, Smart Industry, Smart Health, Smart Transport, Smart Banking, Smart Investment, Smart Insurance, Smart Farmsmart Supply Chains, Smart Retail*, e etc.

e as subsequentes aquisições da *Dropcam* pela *Nest* revelam o potencial lucrati da aplicação da *IoT*. De fato, estima-se que esta tecnologia possa representar u ganho econômico na ordem de 7,1 trilhões de dólares até 2020.[3]

A corrida pela Internet das Coisas destas grandes empresas ressalta o inte resse econômico devido ao valor adicionado que a *IoT* viabiliza. Isto porque a soluções com base em Internet das Coisas coletam, armazenam e processam uma quantidade enorme de informações, geralmente, muito úteis para o aprimoramento de serviços e produtos. Atentos a estes fatos, diversos países passaram a regular a Internet das Coisas com o objetivo de incentivar a inovação e garantir a proteção a direitos fundamentais equilibrando os interesses econômicos envolvidos. Neste sentido, o art. 170 da CF/88 impõe ao Governo brasileiro uma abordagem da Internet das Coisas com base no desenvolvimento econômico e na proteção da propriedade privada, soberania nacional, livre concorrência, busca pelo pleno emprego, tutela do consumidor e do meio ambiente, dentre outros.

A ideia básica da *IoT* é a conexão generalizada entre vários objetos, utilizando ferramentas como identificação por radiofrequência (*RFID*),[4] etiquetas, sensores, telefones celulares, para atingir objetivos comuns. Destaca-se que os sensores desempenham um importante papel na medida em que eles cooperaram com os sistemas *RFID* para melhorar os resultados acompanhando o *status* das coisas, ou seja, sua localização, temperatura, movimentos etc. E, por fim, a conexão de todos estes dados com a *web* viabiliza a análise de enorme quantidade de dados de maneira muito rápida e com resultados bem assertivos (*Big Data Analitics)*. Por isso, muitos passaram a identificar esta nova fase da *IoT* como "Web of Things".[5]

Assim, o Decreto 9.854, de 25 de junho de 2019, que estabelece o Plano Nacional de Internet das Coisas no Brasil, é uma medida preliminar para auxiliar na regulação da Internet das Coisas em diversos setores no país, tais como:

---

3. WORTMANN, Felix; FLÜCHTER, Kristina. Internet of Things Technology and Value Added. *Business Information System Engineering*, v. 57, issue 3, p. 221-224, 27 de março de 2015. Disponível em: https://www.researchgate.net/publication/276439592. Acesso em: 10 fev. 2020. p. 221.
4. Sobre o conceito de *RFID* cf. ATZORI, Luigi; IERA, Antonio; MORABITO, Giacomo. The Internet of Things: A survey. *Computer Networks*, Campus Elsevier, 31 maio 2010. 19 páginas. Disponível em: https://www.cs.mun.ca/courses/cs6910/*IoT*-Survey-Atzori-2010.pdf. Acesso em: 20 jan. 2020. p. 04: "From a physical point of view a RFID tag is a small microchip attached to an antenna (that is used for both receiving the reader signal and transmitting the tag ID) in a package which usually is similar to an adhesive sticker. Dimensions can be very low: Hitachi has developed a tag with dimensions 0.4 mm x 0.4 mm x 0.15 mm."
5. CIRANI, Simone; FERRARI, Gianluigi; PICONE, Marco; VELTRI, Luca. *Internet of Things: architectures, protocols and standards*. New Jersey: John Wiley & Sons, 2019. p. 97: "The Web of Things (WoT) provides an application layer that simplifies the creation of the *IoT*. By bringing the patterns of the web to the *IoT*, it will be possible to create robust applications in the long term and to build an infrastructure designed to scale indefinitely over time. WoT applications will bring to the *IoT* the same usability as the World Wide Web did with the Internet. The WoT will use a mix of HTTP and CoAP protocols, according to the specific application requirements and deployment scenarios."

agronegócio, automóveis e mobilidade urbana, cidades inteligentes, educação, energia, finanças e seguros.

Quanto aos transportes, os carros conectados (conceituados no capítulo 3 desta obra) é um exemplo de aplicação da *IoT* para viabilizar a interconexão entre os carros e entre estes a infraestrutura viária. Para compreender esta aplicação, é mister assimilar a origem, conceito, aplicações e perspectivas regulatórias da Internet das Coisas, objeto deste capítulo.

2.1 ORIGEM E EVOLUÇÃO DA INTERNET DAS COISAS

Originariamente, a concepção da comunicação entre as coisas surgiu da evolução das tecnologias que viabilizavam o intercâmbio de dados entre equipamentos ("machine-to-machine" = M2M tecnologies),[6] baseadas nos protocolos IP, cujo objetivo era otimizar a atividade industrial reduzindo os custos e aumentando a segurança, *e. g.* auxiliando no gerenciamento de estoque e etc. Em outras palavras, é a conexão entre sensores e outros dispositivos usando sistemas de tecnologia da informação e comunicação (TIC) via redes com ou sem fio, também conhecida como *Internet dos Objetos (Internet of Objects = IoO)*.

Hoje, o maior segmento que tem usado esta tecnologia é a indústria automotiva viabilizando os carros telemáticos ou conectados. A Internet das Coisas estrutura-se a partir do mesmo racional descrito acima, ou seja, o intercâmbio de informações, porém, com um complemento, qual seja, a conexão de todas as coisas em um contexto mais amplo: a Internet. Podendo-se dizer que a *IoT* é uma extensão da Internet ("The IoT is not a new Internet, it is an extension to the existing Internet").[7]

6. O Decreto 9.854/2019 que a seguir será analisado traz um conceito sobre "comunicação de máquina à máquina", no art. 8º: "são considerados sistemas de comunicação máquina a máquina as redes de telecomunicações, incluídos os dispositivos de acesso, para transmitir dados a aplicações remotas com o objetivo de monitorar, de medir e de controlar o próprio dispositivo, o ambiente ao seu redor ou sistemas de dados a ele conectados por meio dessas redes.

§ 1º Para fins do disposto no caput, os sistemas de comunicação máquina a máquina não incluem os equipamentos denominados máquinas de cartão de débito e/ou crédito, formalmente considerados terminais de transferência eletrônica de débito e crédito, classificados na posição 8470.50 da Tabela de Incidência do Imposto sobre Produtos Industrializados – TIPI, aprovada pelo Decreto 8.950, de 29 de dezembro de 2016.

§ 2º Compete à Agência Nacional de Telecomunicações regulamentar e fiscalizar o disposto neste artigo, observadas as normas do Ministério da Ciência, Tecnologia, Inovações e Comunicações."

7. HÖLLER, Jan; TSIATSIS, Vlasios; MULLIGAN, Catherine; KARNOUSKOS, Stamatis; AVESAND, Stefan; BOYLE, David. *From Machine-to-Machine to the Internet of Things*: Introduction to a New Age of Intelligence. Oxford: Elsevier, 2014. p. 11-12: "A typical M2M system solution consists of M2M devices, communication networks that provide remote connectivity for the devices, service enablement and application logic, and integration of the M2M application into the business processes provided by an Information Technology (IT) system of the enterprise [...]".

A expressão "Internet of Things" foi usada pela primeira vez há quase 20 anos, sendo atribuída ao chefe do Laboratório de Identificação Automática do Instituto de Tecnologia de Massachusetts (MIT),[8] Kevin Ashton,[9] cujas pesquisas pretendiam desenvolver uma rede de infraestruturas de identificação por radiofrequência (*RFID*).[10] O objetivo destas pesquisas era o desenvolvimento de um código eletrônico para identificar produtos (*Electronic Product Code™ – EPC*) e para viabilizar o uso disseminado de *RFID* em redes comerciais modernas em todo o mundo a partir de padrões globais para a indústria (*EPCglobal Network™*).[11]

Desde então, a Internet das Coisas tem extrapolado bastante estes objetivos iniciais. Atualmente, a *IoT* é uma ferramenta importante para a chamada "Smart Industry" *(Industry 4.0)*, que utiliza a Internet das Coisas para otimizar a produção e a distribuição dos bens produzidos; "Smart Homes", com uma diversidade de aplicações desde termostatos e sensores que se comunicam até a *Smart Tv* e geladeiras, que coletam informações e alertam o morador sobre os inconvenientes de passar tantas horas em frente à televisão ou sobre os alimentos que estão acabando; "Smart Transport", para rastrear os veículos e disponibilizar um sistema de pagamento de estacionamento e etc.; "Smart Health", auxilia no monitoramento de pacientes com doenças crônicas que demandam atenção constante; e "Smart Cities", que auxilia nos sistemas de administração de trânsito em tempo real. Tudo isso graças ao gerenciamento destas ferramentas cada vez mais eficiente, o avanço na comunicação de banda larga, o aumento de memória, o desenvolvimento de tecnologias de microprocessador, dentre outros.

O fortalecimento da Internet das Coisa em escala global e sua aplicação no mercado devem-se ao barateamento dos sensores de sistemas micro eletromecânicos, que convertem dados físicos, tais como movimento, calor, pressão ou localização, em dados digitalizados. Inicialmente, por volta da década de 1980, estes sensores custavam cerca de 25 dólares por unidade; hoje, eles custam menos de um dólar por unidade. Alguns estimam que, até 2025, mais de um trilhão de dispositivos baseados em sensores estarão conectados à Internet ou um ao outro.[12]

A tendência atual é desenvolver diversas plataformas que irão sustentar a conexão de qualquer coisa viabilizando o oferecimento de serviços pela Internet,

8. Cf. http://www.autoidlabs.org/.
9. WEBER, Rolf H. Internet of Things – New security and privacy challenges. *Computer Law & Security Review*, v. 2 6, Campus Elsevier, 2010. p. 23.
10. WORTMANN, Felix; FLÜCHTER, Kristina. Internet of Things Technology and Value Added. *Business Information System Engineering*, v. 57, issue 3, p. 221-224, 27 mar. 2015. Disponível em: https://www.researchgate.net/publication/276439592. Acesso em: 10 fev. 2020. p. 221.
11. ATZORI, Luigi; IERA, Antonio; MORABITO, Giacomo. Op. cit., p. 02.
12. PEPPET, Scott R. Op. cit., p. 98.

inclusive os carros, por isso, alguns falam em "Internet of Everything".[13] Estima-se que em 2025, a quantidade de sensores conectados aos mais diversos bens chegará a 6,2 trilhões de novos dispositivos conectados por ano.[14] Os carros conectados, como serão analisados no capítulo 3, resultam da aplicação da Internet das Coisas viabilizando a comunicação interativa entre os automóveis ("vehicle-to-vehicle" - V2V), bem como a conexão destes com toda a infraestrutura viária ("vehicle-to-infrastructure" – V2I).

Assim, o avanço da Internet das Coisas está marcado pelo grande volume de dados associado às ferramentas de inteligência artificial, cujo conceito é complexo por envolver diversas camadas da economia informacional e segmentos do mercado, inclusive o Governo que tende a ser um exemplo em soluções com base em *IoT* a fim de assegurar mais eficiência aos serviços públicos.

2.2 TERMINOLOGIA, CONCEITO E CARACTERÍSTICAS DA INTERNET DAS COISAS

A União Internacional de Telecomunicações (*International Telecommunication Union)*[15] define Internet das Coisas como uma infraestrutura global para a sociedade informacional, que permite serviços avançados interconectando coisas (físicas e virtuais) com base em dados existentes e em tecnologias interoperáveis de informação e comunicação.

A União Europeia, por sua vez, usa o termo Internet das Coisas para se referir aos objetos que possuem algum sistema de identificação e operações de funcionalidades virtuais em espaços usando interfaces inteligentes para se conectarem e comunicarem dentro de vários ambientes.[16]

13. O termo foi usado pelo CEO da Cisco, John Chambers, quando entrevistado pela Revista Forbes: PEARL, Robert. Cisco CEO John Chambers: American Health Care Is at a Tipping Point. Disponível em: https://www.forbes.com/sites/robertpearl/2014/08/28/cisco-ceo-john-chambers-american-health-care-is-at-a-tipping-point/#273d43ec79f2. Acesso em: 11 fev. 2020: "He envisions a world that's connected by what he calls the 'Internet of Everything.' According to Chambers, it's about "bringing together people, process, data and things to make networked connections more relevant and valuable than ever before."
14. PEPPET, Scott R. Op. cit., p. 89.
15. *Recommendation ITU-T Y.2060*. Disponível em: https://www.itu.int/rec/T-REC-Y.2060-201206-I. Acesso em: 10 fev. 2020. "3.2.2 Internet of things (IoT): A global infrastructure for the information society, enabling advanced services by interconnecting (physical and virtual) things based on existing and evolving interoperable information and communication technologies."
16. *IoT* European Research Cluster (IERC). Enabling Consumer Connectivity Through Consensus Building. Disponível em: http://standardsinsight.com/ieee company detail/. Acesso em: 12 jan. 2020. consensus-building "A dynamic global network infrastructure with self-configuring capabilities based on standard and interoperable communication protocols where physical and virtual 'things' have

No Brasil, o Decreto 9.854/2019 traz, no art. 2º, o conceito de Internet das Coisas e outros termos fundamentais para a compreensão do tema, *in verbis*:

> Art. 2º Para fins do disposto neste Decreto, considera-se:
>
> I – *Internet das Coisas – IoT* – a infraestrutura que integra a prestação de serviços de valor adicionado com capacidades de conexão física ou virtual de coisas com dispositivos baseados em tecnologias da informação e comunicação existentes e nas suas evoluções, com interoperabilidade;
>
> II – *coisas* – objetos no mundo físico ou no mundo digital, capazes de serem identificados e integrados pelas redes de comunicação;
>
> III – *dispositivos* – equipamentos ou subconjuntos de equipamentos com capacidade mandatória de comunicação e capacidade opcional de sensoriamento, de atuação, de coleta, de armazenamento e de processamento de dados; e
>
> IV – *serviço de valor adicionado* – atividade que acrescenta a um serviço de telecomunicações que lhe dá suporte e com o qual não se confunde novas utilidades relacionadas ao acesso, ao armazenamento, à apresentação, à movimentação ou à recuperação de informações, nos termos do disposto no art. 61 da Lei 9.472, de 16 de julho de 1997.

Pode-se concluir que Internet das Coisas é uma rede mundial de objetos interconectados endereçados de forma única, com base na comunicação padrão de protocolos.[17] Estas definições tomam por base a interconexão entre as coisas, a conexão das coisas com a Internet ou, ainda, os objetivos genéricos da *IoT*, quais sejam, a coleta de informações, o seu compartilhamento e armazenamento.

Para a implementação de um produto conectado, como os carros conectados, sob o ponto de vista tecnológico, a Internet das Coisas demanda uma combinação de vários componentes de *software* e *hardware* organizados em multicamadas de três ordens: 1ª) dos produtos e dos equipamentos; 2ª) da conectividade entre eles; e 3ª) do armazenamento em nuvem das informações coletadas. Justamente esta diversificação dos agentes econômicos envolvidos que desafia a regulação efetiva da Internet das Coisas.

A partir das definições apresentadas, pode-se dizer que uma das características da *IoT* é a ampla conexão em três aspectos: – comunicação entre pessoas; – comunicação entre pessoas e objetos; e – comunicação entre os objetos.

Além desta, a *IoT* resulta em serviços de valor agregado, o que movimenta bilhões de dólares e este número só tende a crescer. Em 2016, as oportunidades de mercado que a Internet das Coisas viabilizou foram avaliadas em 15,3 bilhões de dólares. Isto justifica os elevados investimentos para o desenvolvimento e im-

---

identities, physical attributes and virtual personalities and use intelligent interfaces, and are seamlessly integrated into the information network."

17. ATZORI, Luigi; IERA, Antonio; MORABITO, Giacomo. Op. cit., p. 02.

plantação desta tecnologia.[18] Este valor agregado deve-se ao compartilhamento das informações coletadas entre as empresas, desde que observados os requisitos legais, e são avaliadas com base no seu potencial de colaborar para o aprimoramento de produtos e serviços.

Outra característica da *IoT* é a ubiquidade, pois esta tecnologia viabiliza a conexão (*any network*) de quaisquer objetos (*anything*), utilizados cotidianamente com funcionalidades distintas (*any context*), por qualquer pessoa (*anybody*), em qualquer lugar (*anywhere*), a qualquer momento (*anytime*).[19]

Outrossim, a Internet das Coisas apresenta outras características, a saber: – *invisível*, pois os sensores e chips estão ficando cada vez menores, o que passa imperceptível ao usuário que esteja usando uma solução com base em *IoT*; – *ambiguidade*, uma vez que tudo e todos podem estar conectados; – *identificável*, na medida em que todas estas coisas conectadas podem revelar a identidade do usuário, bem como outras informações pessoais; – *ultra conectividade*, pois a Internet das Coisas se insere no contexto de *Big Data*, ou seja, diversas conexões que geram um volume elevado de dados; – *autonomia e imprevisibilidade*, isto é, ressaltando o comportamento autônomo e imprevisível dos objetos conectados a partir dos algoritmos inteligentes que são agregados às ferramentas de *IoT* para oferecer soluções; – *inteligência incorporada*, justamente em função do uso destes algoritmos inteligentes, a *IoT* contribui para os comportamentos emergentes; – *descentralização das operações*, ou seja, a diversidade dos segmentos de mercado, além do Governo, impede a centralização das soluções com base em Internet das Coisas; – *dificuldade em determinar os direitos autorais* daqueles envolvidos nas soluções *IoT* porque é comum congregar pesquisas desenvolvidas por vários órgãos; – *acessibilidade dos dados*; e – *vulnerabilidade*.[20]

No entanto, para poder usufruir destas vantagens econômicas, os agentes devem garantir segurança destes sistemas, por exemplo, os carros conectados exigem que as aplicações de *IoT* em semáforos inteligentes estejam sempre em bom funcionamento, e em todas as camadas dos múltiplos agentes econômicos, pois a falta de energia pode prejudicar este sistema de sinalização de trânsito podendo causar graves acidentes. Para evitar, é preciso diagnosticar possíveis vulnerabilidades do sistema e estabelecer alternativas para recuperar eventuais falhas do sistema.

---

18. HÖLLER, Jan; TSIATSIS, Vlasios; MULLIGAN, Catherine; KARNOUSKOS, Stamatis; AVESAND, Stefan; BOYLE, David. Op. cit., p. 39.
19. TZAFESTAS, Spyros G. Ethics and Law in the Internet of Things World. *In: Smart Cities*, v. 1, issue 1, p. 98-120, 2018. Disponível em: https://doi.org/10.3390/smartcities1010006. Acesso em: 12 jan. 2020. Op. cit., p. 99.
20. Cf. TZAFESTAS, Spyros G. Op. cit., p. 110-111.

Além disso, as informações coletadas durante o funcionamento de um carro conectado tais como os lugares frequentados pelos passageiros, o itinerário realizado, associado a tantas outras informações mesmo não estruturadas podem gerar uma superexposição dos indivíduos.[21] A fim de eliminar estes possíveis danos, o sistema de *IoT* aplicado aos carros conectados deve estabelecer outros componentes para o gerenciamento de identidade, a autenticação, a autorização e a confiança de que o tratamento de dados esteja sendo realizado de acordo com os preceitos legais, em especial a Lei Geral de Proteção de Dados, no Brasil; e o Regulamento Geral Europeu sobre Proteção de Dados (GDPR), na Europa. Neste sentido, as soluções de *IoT* apresentam ferramentas para o registro do usuário (*device authentication/authorization*), ferramentas de configuração (*device configuration*), ferramentas de monitoramento (*device monitoring*), ferramentas para detectar falhas (*device fault diagnosis*) e ferramentas para resolver eventuais problemas com o funcionamento da aplicação com base em *IoT* (*device troubleshooting*).[22]

Diante da necessidade do envolvimento de diversas camadas da economia informacional para a implementação de soluções com base em *IoT*, somada à circulação transfronteiriça destas informações, não é tarefa fácil estabelecer um modelo regulatório eficiente que concilie todos os interesses conflitantes e que seja tecnológica e economicamente viável.

2.3 PERSPECTIVAS REGULATÓRIAS DA INTERNET DAS COISAS

As vantagens da utilização da Internet das Coisas, para além do incremento à economia de maneira geral, são socialmente visíveis. Por exemplo: a otimização na produção agrícola, como auxiliar no monitoramento do plantio e da colheita detectando necessidades do solo e adaptando o ambiente para cada tipo de plantação; a automação industrial complementada pela Internet das Coisas trará mais segurança aos trabalhadores, diminuindo drasticamente os acidentes de trabalho; a segurança alimentar na medida em que sensores poderão monitorar os produtos a partir de um sistema de identificação por radiofrequência (*RFID*), podendo rastrear os alimentos por toda a cadeia de consumo, inclusive, com a possibilidade de viabilizar efetivamente a transparência nas relações de consumo ao detectar a origem dos alimentos; a automação dos veículos, pois os

21. PEPPET, Scott R. Op. cit., p. 90: "Even Internet of Things devices far more innocuous than the Breathometer can generate data that present difficult issues. Sensor data capture incredibly rich nuance about who we are, how we behave, what our tastes are, and even our intentions. Once filtered through "Big Data" analytics, these data are the grist for drawing revealing and often unexpected inferences about our habits, predilections, and personalities. I can tell a lot about you if I know that you often leave your oven on when you leave the house, fail to water your plants, don't exercise, or drive recklessly."
22. TZAFESTAS, Spyros. Op. cit., p. 100.

carros conectados entre si e com a infraestrutura viária podem detectar sit
perigosas com maior antecedência o que permite adotar soluções mais efi
para evitar os acidentes de trânsito.

Todavia, a Internet das Coisas traz uma série de desafios, tais com
fesa da soberania nacional, pois muitas destas aplicações de Internet das
usam programas privados (proprietários) desenvolvidos por empresa de
países que teriam acesso às informações de toda a sociedade brasileira;
ção de dados e privacidade, uma vez que o intercâmbio de informações
coisas pressupõe a coleta, o tratamento e o armazenamento de dados p
a segurança cibernética, porque a Internet das Coisas aumenta a expos
equipamentos utilizados vez que viabiliza o acesso não autorizado a es
mas por *hackers*.

Scott R. Peppet[23] detectou quatro pontos principais que devem s
tados no contexto da Internet das Coisas, a saber: 1) uma possível disc
tendo em vista que a análise de *Big Data* aliada às funcionalidades d
resultar em informações sensíveis, como convicção religiosa, orienta
filiação partidária de determinada pessoa; 2) a inviabilidade da manu
procedimentos de anonimização de dados o que potencializa os dan
dade e à proteção de dados; 3) a vulnerabilidade dos dispositivos qu
violados por *hackers*; e 4) a ineficiência das políticas de privacidade
de dados para o uso de sensores contidos nos mais diversos dispos

Observe-se que o amplo acesso às mais diversas aplicações foi f
plataformas de banda larga móveis, o que contribuiu para gerar un
de informações coletadas sobre uma pessoa jamais imaginada. Info
localização, nível de educação, emprego, saúde, dados fiscais (CPF
de crédito (*credit scoring*), padrões de compra, histórico de pes
taformas de busca), *status* de relacionamento, fotos, curtidas na
todas elas são armazenadas, interconectadas e interligadas nu
empresarial de comunicações convergentes. Este contexto revela
direito à proteção de dados pessoais e o direito à privacidade, o q
a atenção do legislativo e das agências reguladoras de diversos

Neste sentido, destaca-se que a constante preocupação d
propostas regulatórias da *IoT* é justamente com a proteção à
dados pessoais na medida em que os riscos são evidentes comc
uso de etiquetas *RFID* para rastrear pessoas, hipótese que sus
e legais. Os possíveis danos a estes direitos são acentuados a pa
em massa de sensores em vários ambientes, inclusive em s

23. Op. cit., p. 117.

carros conectados entre si e com a infraestrutura viária podem detectar situações perigosas com maior antecedência o que permite adotar soluções mais eficientes para evitar os acidentes de trânsito.

Todavia, a Internet das Coisas traz uma série de desafios, tais como: a defesa da soberania nacional, pois muitas destas aplicações de Internet das Coisas usam programas privados (proprietários) desenvolvidos por empresa de outras países que teriam acesso às informações de toda a sociedade brasileira; a proteção de dados e privacidade, uma vez que o intercâmbio de informações entre as coisas pressupõe a coleta, o tratamento e o armazenamento de dados pessoais; a segurança cibernética, porque a Internet das Coisas aumenta a exposição dos equipamentos utilizados vez que viabiliza o acesso não autorizado a estes sistemas por *hackers*.

Scott R. Peppet[23] detectou quatro pontos principais que devem ser enfrentados no contexto da Internet das Coisas, a saber: 1) uma possível discriminação tendo em vista que a análise de *Big Data* aliada às funcionalidades da *IoT* pode resultar em informações sensíveis, como convicção religiosa, orientação sexual, filiação partidária de determinada pessoa; 2) a inviabilidade da manutenção dos procedimentos de anonimização de dados o que potencializa os danos à privacidade e à proteção de dados; 3) a vulnerabilidade dos dispositivos que podem ser violados por *hackers*; e 4) a ineficiência das políticas de privacidade e de proteção de dados para o uso de sensores contidos nos mais diversos dispositivos.

Observe-se que o amplo acesso às mais diversas aplicações foi facilitado pelas plataformas de banda larga móveis, o que contribuiu para gerar uma quantidade de informações coletadas sobre uma pessoa jamais imaginada. Informações sobre localização, nível de educação, emprego, saúde, dados fiscais (CPF), classificação de crédito (*credit scoring*), padrões de compra, histórico de pesquisa (nas plataformas de busca), *status* de relacionamento, fotos, curtidas nas redes sociais, todas elas são armazenadas, interconectadas e interligadas numa plataforma empresarial de comunicações convergentes. Este contexto revela a fragilidade do direito à proteção de dados pessoais e o direito à privacidade, o que tem chamado a atenção do legislativo e das agências reguladoras de diversos países.

Neste sentido, destaca-se que a constante preocupação das diretrizes e das propostas regulatórias da *IoT* é justamente com a proteção à privacidade e aos dados pessoais na medida em que os riscos são evidentes como a possibilidade do uso de etiquetas *RFID* para rastrear pessoas, hipótese que suscita conflitos éticos e legais. Os possíveis danos a estes direitos são acentuados a partir da implantação em massa de sensores em vários ambientes, inclusive em *smartphones*, porque

23. Op. cit., p. 117.

potencializam a coleta de dados e informações pessoais de forma constante. Outro ponto a ser enfrentado são as ferramentas de análise destes dados, que podem criar perfis dos usuários, ainda que aparentemente anônimos.[24]

Quanto à segurança da informação, estes sistemas devem prever mecanismos para elaborar um relatório de impacto à proteção de dados pessoais e à privacidade, bem como notificar à ANPD sobre vulnerabilidades à proteção dos dados pessoais e da privacidade nos termos do art. 48 da LGPD.

O modelo regulatório da Internet das Coisas tem sido preferencialmente a autorregulação, pois como destacado *supra* esta é uma realidade complexa que congrega diversas camadas da economia informacional, desde as empresas de telecomunicações às provedoras de diversas aplicações. No entanto, como a Internet das Coisas opera com dados pessoais, todas estas soluções estão sujeitas à LGPD e aos regulamentos da ANPD. O ideal é estabelecer alguns padrões e princípios a serem seguidos por todos os agentes, sem excluir a possibilidade de se elaborarem códigos de boas práticas para as soluções de *IoT*.[25]

Além disso para assegurar a eficiência de qualquer regulação sobre a matéria, bem como a viabilidade de um Plano Nacional para a Internet das Coisas, alguns obstáculos devem ser superados, notadamente: – proteção à privacidade e aos dados pessoais; – medidas eficazes para a cibersegurança; – modelos de negócios sustentáveis; – estrutura governamental; e – a dificuldade de se estabelecer um padrão de interoperatividade.

A União Europeia, atenta aos entraves para uma regulação eficiente sobre *IoT*, criou em março de 2015 a *Alliance for Internet of Things Innovation*,[26] cujo primeiro relatório apresentado em abril de 2016 caracteriza-se por oferecer diretrizes gerais pautado pelo incentivo à Internet das Coisas, pela abordagem antropocêntrica e a construção de um mercado único para a Internet das Coisas.

No Brasil, semelhantemente, optou-se por uma regulação preliminar para preparar o terreno para a futura regulação da Internet das Coisas no país. Neste sentido, o Decreto 9.854/2019, que instituiu o "Plano Nacional de Internet das

24. HÖLLER, Jan; TSIATSIS, Vlasios; MULLIGAN, Catherine; KARNOUSKOS, Stamatis; AVESAND, Stefan; BOYLE, David. Op. cit., p. 31: "Concepts like Provenance of Data and Quality of Information (QoI) become important, especially considering aggregation of data and analytics. As there is a risk of relying on inaccurate or even faulty information in a decision process, the issue of accountability, and even liability, becomes an interest." Cf. FROOMKIN, A. Michael. The Death of Privacy? *Stanford Law Review*, v. 52, p. 1461-1543, 2000. Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2715617. Acesso em: 10 mar. 2020. p. 1.481.
25. WEBER, Rolf H. Op. cit., p. 25: "So far, the regulatory model in the *IoT* is based on selfregulation through manifold business standards, starting from technical guidelines and leading to fair information practices."
26. Cf. https://ec.europa.eu/digital-single-market/en/internet-of-things.

Coisas", não pode ser visto como uma regulação exaustiva, mas sim o primeiro passo para a implementação sustentável da *IoT* no país.

2.4 PLANO NACIONAL DE INTERNET DAS COISAS: DESAFIOS AO *ENFORCEMENT* DO DECRETO 9.854/2019

O Decreto 9.854, de 25 de junho de 2019, em vigor desde a data de sua publicação, revogou o Decreto 8.234, de 2 de maio de 2014, que estabelecia um conceito sobre comunicação entre máquinas e atribuía à ANATEL (Agência Nacional de Telecomunicações) a função de fiscalizar e regulamentar estas ferramentas, sujeita às normas do Ministério das Comunicações.[27]

O atual Decreto 9.854/2019 tem por finalidade implementar e desenvolver a Internet das Coisas no Brasil, observadas a livre concorrência, a livre circulação de dados, as diretrizes de segurança da informação e de proteção de dados pessoais (art. 1º). Como visto, importante referência feita à necessária proteção aos dados pessoais tendo em vista a coleta e o tratamento de dados pessoas em larga escala pelas funcionalidades da *IoT*. Portanto, a LGPD deve ser respeitada por todas as empresas e aplicações que utilizam Internet das Coisas, equilibrando os interesses em jogo nos termos do art. 170 da CF/88.

Os objetivos do Plano Nacional de Internet das Coisas, conforme o art. 3º do referido Decreto são: – melhorar a qualidade de vida e eficiência dos serviços a partir da implementação de soluções de *IoT*; – a capacitar profissionais para o desenvolvimento de aplicações de *IoT* e a gerar empregos na economia digital; – aumentar a produtividade e competitividade das empresas brasileiras desenvolvedoras de *IoT*, por meio da promoção de um ecossistema de inovação neste setor; – buscar parcerias com os setores público e privado para a implementação da *IoT*; e – aumentar a integração do País no cenário internacional, por meio da participação em fóruns de padronização, da cooperação internacional em pesquisa, desenvolvimento e inovação e da internacionalização de soluções de *IoT* desenvolvidas no País.

Nota-se uma preocupação do Governo brasileiro com o mercado de trabalho, devendo buscar mecanismos para capacitar os cidadãos para enfrentar essa

27. A antiga redação do Decreto 8.234, de 02 de maio de 2012: "Art. 1º Para fins do disposto no art. 38 da Lei 12.715, de 17 de setembro de 2012, são considerados sistemas de comunicação máquina a máquina os dispositivos que, sem intervenção humana, utilizem redes de telecomunicações para transmitir dados a aplicações remotas com o objetivo de monitorar, medir e controlar o próprio dispositivo, o ambiente ao seu redor ou sistemas de dados a ele conectados por meio dessas redes. [...] § 3º Compete à Anatel regulamentar e fiscalizar as disposições previstas neste artigo, observado o disposto nas normas do Ministério das Comunicações."

Coisas", não pode ser visto como uma regulação exaustiva, mas sim o primeiro passo para a implementação sustentável da *IoT* no país.

2.4 PLANO NACIONAL DE INTERNET DAS COISAS: DESAFIOS AO *ENFORCEMENT* DO DECRETO 9.854/2019

O Decreto 9.854, de 25 de junho de 2019, em vigor desde a data de sua publicação, revogou o Decreto 8.234, de 2 de maio de 2014, que estabelecia um conceito sobre comunicação entre máquinas e atribuía à ANATEL (Agência Nacional de Telecomunicações) a função de fiscalizar e regulamentar estas ferramentas, sujeita às normas do Ministério das Comunicações.[27]

O atual Decreto 9.854/2019 tem por finalidade implementar e desenvolver a Internet das Coisas no Brasil, observadas a livre concorrência, a livre circulação de dados, as diretrizes de segurança da informação e de proteção de dados pessoais (art. 1º). Como visto, importante referência feita à necessária proteção aos dados pessoais tendo em vista a coleta e o tratamento de dados pessoas em larga escala pelas funcionalidades da *IoT*. Portanto, a LGPD deve ser respeitada por todas as empresas e aplicações que utilizam Internet das Coisas, equilibrando os interesses em jogo nos termos do art. 170 da CF/88.

Os objetivos do Plano Nacional de Internet das Coisas, conforme o art. 3º do referido Decreto são: – melhorar a qualidade de vida e eficiência dos serviços a partir da implementação de soluções de *IoT*; – a capacitar profissionais para o desenvolvimento de aplicações de *IoT* e a gerar empregos na economia digital; – aumentar a produtividade e competitividade das empresas brasileiras desenvolvedoras de *IoT*, por meio da promoção de um ecossistema de inovação neste setor; – buscar parcerias com os setores público e privado para a implementação da *IoT*; e – aumentar a integração do País no cenário internacional, por meio da participação em fóruns de padronização, da cooperação internacional em pesquisa, desenvolvimento e inovação e da internacionalização de soluções de *IoT* desenvolvidas no País.

Nota-se uma preocupação do Governo brasileiro com o mercado de trabalho, devendo buscar mecanismos para capacitar os cidadãos para enfrentar essa

27. A antiga redação do Decreto 8.234, de 02 de maio de 2012: "Art. 1º Para fins do disposto no art. 38 da Lei 12.715, de 17 de setembro de 2012, são considerados sistemas de comunicação máquina a máquina os dispositivos que, sem intervenção humana, utilizem redes de telecomunicações para transmitir dados a aplicações remotas com o objetivo de monitorar, medir e controlar o próprio dispositivo, o ambiente ao seu redor ou sistemas de dados a ele conectados por meio dessas redes. [...] § 3º Compete à Anatel regulamentar e fiscalizar as disposições previstas neste artigo, observado o disposto nas normas do Ministério das Comunicações."

nova dinâmica de aplicação da Internet das Coisas em diversos setores por meio de cursos técnicos e profissionalizantes, bem como curso de nível superior. Desta forma, o Brasil terá melhores condições de se inserir no capitalismo informacional, para não ser refém do fenômeno do "colonialismo digital". Além disso, o Decreto estabelece uma diretriz importante, qual seja, a análise antropocêntrica para o desenvolvimento e a implementação da Internet das Coisas na medida em que se justifica para a melhoria da qualidade de vida e a eficiência dos serviços.

Cabe ao Ministro de Estado da Ciência, Tecnologia, Inovações e Comunicações (art. 4º) indicar os setores priorizados para aplicações de soluções de *IoT*, sendo que o Decreto determina *a priori* quais setores obrigatoriamente serão priorizados (saúde, cidades, indústrias e rural).

Como destacado no início deste capítulo, as áreas priorizadas no Decreto vão ao encontro da tendência global em aplicação da *IoT*. A área da saúde (*Smart Health*) é uma das principais preocupações, pois as soluções de *IoT* viabilizam monitoramento constante de pacientes em estado grave, por exemplo, além de diagnosticar com precisão e antecedência possíveis agravamentos do estado de saúde das pessoas. Outra área priorizada são as cidades (*Smart Cities*), hoje muito populosas e intensamente urbanizadas, sendo que as soluções em *IoT* auxiliam no gerenciamento do trânsito da cidade, transportes públicos, iluminação pública de maneira que os recursos possam ser aplicados com mais eficiência e, portanto, maior economia. Na indústria (*Smart Industry*) as soluções de *IoT* associadas à automação do processo industrial são valiosas ferramentas para o aumento da produção com otimização da administração de estoque, por exemplo. Por fim, o agronegócio poderá ser beneficiado com as soluções de *IoT*, realçando o potencial brasileiro neste setor extremamente importante à economia do país.

Os carros conectados não foram expressamente previstos no Decreto 9.854/2019, mas o Ministro de Estado da Ciência, Tecnologia, Inovações e Comunicações deve considerar este um setor importante, pois impacta diretamente na melhoria da qualidade de vida das pessoas, eficiência do serviço, além dos setores expressamente previstos no Decreto, ou seja, saúde, cidades, indústria e rural. Observe-se que otimizando o tempo no trânsito e diminuindo os acidentes, o sistema de carros conectados desafoga os serviços hospitalares que estão abarrotados de pacientes, muitos dos quais são vítimas de acidentes de trânsito. Otimizando o sistema de colheitas no campo e transporte de mercadorias, os lucros contribuirão para o fortalecimento da indústria e do agronegócio brasileiro. Por fim, os carros conectados contribuem para uma gestão de tráfego de maneira muito mais eficiente nas cidades, além dos serviços públicos de forma geral.

O ato do Ministro de Estado da Ciência, Tecnologia, Inovações e Comunicações deve observar os critérios de "oferta, de demanda e de capacidade de

desenvolvimento local" nos termos do § 1º do art. 4º. Aind
ato do Ministro destacando o setor automotivo, as empres
próximo capítulo já estão investindo nestas tecnologias. Po
o ato do Ministro priorizar os carros conectados, além das
Decreto, é que os carros conectados tornar-se-ão referênci
mecanismos de fomento à pesquisa científica, ao desenvolvir
à inovação; e – o apoio ao empreendedorismo de base tecnoló

Além disso, os órgãos e as entidades públicas com prc
à *IoT* poderão aderir ao Plano Nacional de Internet das Cois
destes benefícios por meio de acordo de cooperação técnica
da Ciência, Tecnologia, Inovações e Comunicações (§ 3º do
9.854/2019).

O Brasil deve se adequar à economia informacional, pa
que integração o plano de ações para viabilizar o Plano Nacio
Coisas nos termos do art. 5º do Decreto são:

I – ciência, tecnologia e inovação;
II – inserção internacional;
III – educação e capacitação profissional;
IV – infraestrutura de conectividade e interoperabilidade;
V – regulação, segurança e privacidade; e
VI – viabilidade econômica.

Outro ponto importante do Plano Nacional de Internet d
foi a identificação de projetos para facilitar a sua implement
ordenados pelo Ministério da Ciência, Tecnologia, Inovaçõe
(art. 6º), são eles: I – Plataformas de Inovação em Internet da
tros de Competência para Tecnologias Habilitadoras em Int
III – Observatório Nacional para o Acompanhamento da Tran

Por fim, o art. 7º do Decreto 9.854/2019 criou um ó
"Câmara de Gestão e Acompanhamento do Desenvolvime
Comunicação Máquina a Máquina e Internet das Coisas –
colegiado (não deliberativo nos termos do § 1º do art. 7º), dis
mínimo para votação. Percebe-se, portanto, que este órgão é
cuja missão é assessorar e acompanhar a implementação do
Internet das Coisas.

O art. 7º do referido Decreto estabelece as competências

I – monitorar e avaliar as iniciativas de implementação do Plano N
Coisas;

desenvolvimento local" nos termos do § 1º do art. 4º. Ainda que não exista um ato do Ministro destacando o setor automotivo, as empresas, como se verá no próximo capítulo já estão investindo nestas tecnologias. Porém, a vantagem de o ato do Ministro priorizar os carros conectados, além das áreas indicadas no Decreto, é que os carros conectados tornar-se-ão referência para: – o acesso a mecanismos de fomento à pesquisa científica, ao desenvolvimento tecnológico e à inovação; e – o apoio ao empreendedorismo de base tecnológica (§ 2º do art. 4º).

Além disso, os órgãos e as entidades públicas com projetos relacionados à *IoT* poderão aderir ao Plano Nacional de Internet das Coisas para se valerem destes benefícios por meio de acordo de cooperação técnica com o Ministério da Ciência, Tecnologia, Inovações e Comunicações (§ 3º do art. 4º do Decreto 9.854/2019).

O Brasil deve se adequar à economia informacional, para tanto, os temas que integração o plano de ações para viabilizar o Plano Nacional de Internet das Coisas nos termos do art. 5º do Decreto são:

I – ciência, tecnologia e inovação;

II – inserção internacional;

III – educação e capacitação profissional;

IV – infraestrutura de conectividade e interoperabilidade;

V – regulação, segurança e privacidade; e

VI – viabilidade econômica.

Outro ponto importante do Plano Nacional de Internet das Coisas do Brasil foi a identificação de projetos para facilitar a sua implementação que serão coordenados pelo Ministério da Ciência, Tecnologia, Inovações e Comunicações (art. 6º), são eles: I – Plataformas de Inovação em Internet das Coisas; II – Centros de Competência para Tecnologias Habilitadoras em Internet das Coisas; e III – Observatório Nacional para o Acompanhamento da Transformação Digital.

Por fim, o art. 7º do Decreto 9.854/2019 criou um órgão denominado "Câmara de Gestão e Acompanhamento do Desenvolvimento de Sistemas de Comunicação Máquina a Máquina e Internet das Coisas – Câmara IoT", um colegiado (não deliberativo nos termos do § 1º do art. 7º), dispensado o quórum mínimo para votação. Percebe-se, portanto, que este órgão é apenas consultivo cuja missão é assessorar e acompanhar a implementação do Plano Nacional de Internet das Coisas.

O art. 7º do referido Decreto estabelece as competências deste órgão, a saber:

I – monitorar e avaliar as iniciativas de implementação do Plano Nacional de Internet das Coisas;

objetivos do Plano Nacional de Internet das Coisas;

III – discutir com os órgãos e entidades públicas os temas do plano de ação de que trata o art. 3º;

IV – apoiar e propor projetos mobilizadores; e

V – atuar conjuntamente com órgãos e entidades públicas para estimular o uso e o desenvolvimento de soluções de IoT.

Portanto, não se trata de uma agência reguladora, pois não tem função regulatória, fiscalizatória ou sancionatória. Ademais, o exercício da função não é remunerado, pois é considerado prestação de serviço público relevante (§ 1º do art. 7º). O órgão é composto por representantes do Ministério da Ciência, Tecnologia, Inovações e Comunicações, que a presidirá; Ministério da Economia; Ministério da Agricultura, Pecuária e Abastecimento; Ministério da Saúde; e Ministério do Desenvolvimento Regional (§ 2º do art. 7º), que serão indicados pelos respectivos ministérios e designados pelo Secretário de Empreendedorismo e Inovação do Ministério da Ciência, Tecnologia, Inovações e Comunicações (§ 4º do art. 7º).

Este órgão poderia fazer uma assessoria melhor se tivesse representantes de outros setores como mercado, sociedade civil e comunidade científica. Todavia, tal lacuna pode ser sanada, pois o § 5º do art. 7º do Decreto 9.854/2019 permite que o Secretário de Empreendedorismo e Inovação do Ministério da Ciência, Tecnologia, Inovações e Comunicações convide representantes de associações e de entidades públicas e privadas para participar das reuniões da Câmara *IoT*. Todavia, ressalte-se que esta participação é fundamental para resultar em medidas efetivas em uma área tão segmentada como a Internet das Coisas, sendo a indústria automotiva um exemplo de sua aplicação, com os chamados "carros conectados".

2.5 INTERNET DAS COISAS: O EXEMPLO DE SUA APLICAÇÃO NOS CARROS CONECTADOS E MOBILIDADE URBANA

A *IoT* permite que as coisas estejam conectadas, viabilizando uma integração mais sólida e rápida entre vários objetivos, desde os mais simples, como televisão, até os mais complexos como os carros conectados podem se comunicar de maneira mais controlada e inteligente, por isso, o adjetivo "objetos inteligentes" (exemplo, *Smart Tv, Smart Cities, Smart Cars,* e etc.). Neste contexto, toda essa interconexão gera mais dados e informações, que podem ser utilizados para otimizar os sistemas de mobilidade urbana e o funcionamento dos carros autônomos, inclusive.

O diferencial da Internet das Coisas está justamente no volume de dados com que esta tecnologia trabalha para realizar diversos tipos de análises das informações coletadas resultando em predições muito eficazes.[28] Levando esta ferramenta para o contexto do tráfego de veículos, esta tecnologia viabiliza detectar possíveis acidentes e solucionar de maneira eficiente para que estes acidentes não venham a ocorrer. Justamente por isso, os carros conectados oferecerão maior segurança no trânsito.

Carros, trens e ônibus, juntamente com as estradas e os trilhos, todos equipados com identificadores, sensores e poder de processamento podem fornecer informações importantes ao motorista. Os carros conectados viabilizam, assim, um amplo sistema de prevenção de colisões e monitoramento de transportes de materiais perigosos, por exemplo, o que representa muitas vantagens às pessoas de forma geral, aos governos (que terão mais informações para uma administração eficiente da malha viária) e às empresas, como no caso das transportadoras na medida em que oferece maior segurança e economia.[29]

Neste sentido, Fei Hu[30] explica como a chamada "Internet dos Veículos" (*Internet of Vehicles – IoV*) facilitou a implementação do sistema de transporte inteligente ("Inteligent Transport System" – ITS) na medida em que a *IoV* enseja aos veículos a capacidade avançada de detecção e comunicação com infraestruturas inteligentes na estrada ("Vehicle to Infrastructure" – V2I), bem como com outros veículos ("Vehicle to Vehicle – V2V), a partir de unidades de bordo de veículos ("Onboard Units" – OBUs) e unidades de beira de estrada ("Roadside Units" – RSUs).

Os carros conectados demandam a participação de diversos setores, como o Governo, as empresas do ramo automotivo, os provedores de conexão e os provedores de aplicação, todos com interesses econômicos próprios que precisarão atuar em conjunto para a viabilidade da "Internet dos Carros". Em outras palavras, é necessária a integração entre múltiplas infraestruturas e de um grande conjunto de dispositivos diferentes, tais como semáforos, radares, GPS, bem como o compartilhamento de dados e informações em vários domínios. Portanto, deve-se adotar uma abordagem horizontal da qual participem todos os envolvidos no segmento para se estabelecer um padrão comum de interoperabilidade entre as tecnologias e os protocolos que serão utilizados.

Atualmente, cerca de 90% dos automóveis novos vendidos nos Estados Unidos vêm equipados com um sistema de gravação de eventos ("Event Data Recorder – EDR"), capaz de armazenar as informações sobre a locomoção do

28. HÖLLER, Jan; TSIATSIS, Vlasios; MULLIGAN, Catherine; KARNOUSKOS, Stamatis; AVESAND, Stefan; BOYLE, David. Op. cit., p. 36.
29. ATZORI, Luigi; IERA, Antonio; MORABITO, Giacomo. Op. cit., p. 08.
30. HU, Fei. *Security and Privacy in Internet of Things (IoTs)*: models, algoritms, and implementations. Nova York: CRC Press, 2016. p. 169.

informações coletadas resultando em predições muito eficazes.[28] Levando esta ferramenta para o contexto do tráfego de veículos, esta tecnologia viabiliza detectar possíveis acidentes e solucionar de maneira eficiente para que estes acidentes não venham a ocorrer. Justamente por isso, os carros conectados oferecerão maior segurança no trânsito.

Carros, trens e ônibus, juntamente com as estradas e os trilhos, todos equipados com identificadores, sensores e poder de processamento podem fornecer informações importantes ao motorista. Os carros conectados viabilizam, assim, um amplo sistema de prevenção de colisões e monitoramento de transportes de materiais perigosos, por exemplo, o que representa muitas vantagens às pessoas de forma geral, aos governos (que terão mais informações para uma administração eficiente da malha viária) e às empresas, como no caso das transportadoras na medida em que oferece maior segurança e economia.[29]

Neste sentido, Fei Hu[30] explica como a chamada "Internet dos Veículos" *(Internet of Vehicles – IoV)* facilitou a implementação do sistema de transporte inteligente ("Inteligent Transport System" – ITS) na medida em que a *IoV* enseja aos veículos a capacidade avançada de detecção e comunicação com infraestruturas inteligentes na estrada ("Vehicle to Infrastructure" – V2I), bem como com outros veículos ("Vehicle to Vehicle – V2V), a partir de unidades de bordo de veículos ("Onboard Units" – OBUs) e unidades de beira de estrada ("Roadside Units" – RSUs).

Os carros conectados demandam a participação de diversos setores, como o Governo, as empresas do ramo automotivo, os provedores de conexão e os provedores de aplicação, todos com interesses econômicos próprios que precisarão atuar em conjunto para a viabilidade da "Internet dos Carros". Em outras palavras, é necessária a integração entre múltiplas infraestruturas e de um grande conjunto de dispositivos diferentes, tais como semáforos, radares, GPS, bem como o compartilhamento de dados e informações em vários domínios. Portanto, deve-se adotar uma abordagem horizontal da qual participem todos os envolvidos no segmento para se estabelecer um padrão comum de interoperabilidade entre as tecnologias e os protocolos que serão utilizados.

Atualmente, cerca de 90% dos automóveis novos vendidos nos Estados Unidos vêm equipados com um sistema de gravação de eventos ("Event Data Recorder – EDR"), capaz de armazenar as informações sobre a locomoção do

28. HÖLLER, Jan; TSIATSIS, Vlasios; MULLIGAN, Catherine; KARNOUSKOS, Stamatis; AVESAND, Stefan; BOYLE, David. Op. cit., p. 36.
29. ATZORI, Luigi; IERA, Antonio; MORABITO, Giacomo. Op. cit., p. 08.
30. HU, Fei. *Security and Privacy in Internet of Things (IoTs)*: models, algoritms, and implementations. Nova York: CRC Press, 2016. p. 169.

veículo tais como excesso de velocidade.[31] Muito embora esta tecnologia esteja sendo comercializada em muitos países, algumas questões precisam ser respondidas, como: será possível passar estas informações às seguradoras de veículos?

Apenas dezessete estados norte-americanos enfrentaram a questão, sendo que somente em quatro deles ficou proibido o compartilhamento destas informações com as seguradoras seja para comprovar a culpa do segurado ou de terceiro, seja para aumentar o valor do seguro em função de se identificar a irresponsabilidade do motorista.[32]

Alguns exemplos de uso de sensores em automóveis são: *ZenDrive*,[33] um aplicativo para o *iPhone* que monitora a direção dando um feedback ao motorista, bem como dicas sobre trânsito e atrações nas proximidades; e o *DriveScribe*,[34] que é um aplicativo para o controle parental sobre a direção de seus filhos adolescentes.

No campo da responsabilidade civil, a *Internet dos Carros* traz uma série de questionamentos, notadamente a partir da proteção à privacidade, à proteção dos dados pessoais e à segurança cibernética contra a invasão destes sistemas por pessoas não autorizadas (*hackers*).

Um exemplo foi a primeira ação coletiva sobre *IoT* contra três fabricantes de automóveis, *Ford Motor Company, General Motors* e *Toyota Motor Corporation* nos EUA em março de 2015. O caso ficou conhecido como "Cahen et al. v. Toyota Motor Corporation",[35] julgado pelo Tribunal Distrital do Distrito Norte da Califórnia sobre a vulnerabilidade dos sistemas eletrônicos dos veículos destas gigantes da Indústria Automotiva, pelo possível acesso não autorizado por *hackers* comprometendo a segurança dos passageiros e a proteção de seus dados pessoais. As investigações revelaram que os *hackers* poderiam se apropriar dos controles dos veículos para acelerá-lo inesperadamente, realizar curvas, ativar a buzina, modificar o velocímetro e as leituras do nível de combustível. Todavia, a Corte de Apelações ("Court of Appeals") do 9º Circuito dos Estados Unidos arquivou a ação, pois os requerentes não demonstraram efetivo prejuízo, na medida em

31. PEPPET, Scott R. Op. cit., p. 92.
32. Cf. Privacy of Data from Event Data Recorders: State Statutes. NATIONAL CONFERENCE STATE LEGISLATURES. Disponível em: http://www.ncsl.org/research/telecommunications-and-informationtechnology/privacy-ofdata-from-event-data-recorders.aspx, archived at http://perma.cc/7XRZ-TNZ7. Acesso em: 12 fev. 2020: "Arkansas, California, Colorado, Connecticut, Delaware, Maine, Montana, Nevada, New Hampshire, New Jersey, New York, North Dakota, Oregon, Texas, Utah, Virginia and Washington – have enacted statutes relating to event data recorders and privacy. Among other provisions, these states provide that data collected from a motor vehicle event data recorder may only be downloaded with the consent of the vehicle owner or policyholder, with certain exceptions."
33. Cf. https://zendrive.com/. Acesso em: 13 fev. 2020.
34. Cf. https://techguysmartbuy.com/2014/04/review-drivescribe-the-app-that-will-improve-your-driving-video.html. Acesso em: 13 fev. 2020.
35. 147 F. Supp.3d 955, N.D. Cal.

que a ação foi motivada pela vulnerabilidade do sistema por si só e não diante de invasão por *hackers* de fato. Neste caso, o pedido era por danos morais em função do abalo psíquico dos motoristas ao constatarem estar expostos a estas invasões.

Poucos meses depois, em julho de 2015, outra ação coletiva, "Brian Flynn et al. v. Fiat Chrysler Harman",[36] o Tribunal Distrital de *Southern District of Illinois* determinou o *recall* de 1,4 milhões de carros cujo *software* "Chrysler's UConnect" foi diagnosticado vulnerável a ataques por *hackers*, que poderiam controlar o rádio e ar condicionado do veículo.

Estes casos despertaram nos Estados Unidos a urgência em regulamentar os carros conectados, cabendo à agência norte-americana de segurança de trânsito, "National Highway Traffic Safety Administration" (NHTSA) e pela agência que tem competência em defender os direitos dos consumidores, "Federal Trade Commission", avaliar estas ferramentas.[37] No Brasil, caberá ao CONTRAN e à SENACON verificar a segurança dos sistemas utilizados nos carros conectados, além da ANPD quanto à proteção de dados pessoais e à privacidade.

A inteligência artificial e a Internet das Coisas não são expressão sinônimas, mas são ferramentas tecnológicas que estão muito próximas, seja por parte da IA que utiliza um volume de informações gerado pela IoT; seja a IoT que utiliza ferramentas de aprendizado de máquina para incorporar inteligência nas soluções oferecidas. Portanto, são duas ferramentas utilizadas pela indústria automotiva, notadamente os carros autônomos e os carros conectados.

36. Case No. 15-cv-0855-MJR-DGW.
37. CHIKE, Patrick. The Legal Challenges of Internet of Things. *Technical Report*. Disponível em: https://www.researchgate.net/publication/322628457. Acesso em: 12 jan. 2020.

que a ação foi motivada pela vulnerabilidade do sistema por si só e não diante de invasão por *hackers* de fato. Neste caso, o pedido era por danos morais em função do abalo psíquico dos motoristas ao constatarem estar expostos a estas invasões.

Poucos meses depois, em julho de 2015, outra ação coletiva, "Brian Flynn et al. v. Fiat Chrysler Harman",[36] o Tribunal Distrital de *Southern District of Illinois* determinou o *recall* de 1,4 milhões de carros cujo *software* "Chrysler's UConnect" foi diagnosticado vulnerável a ataques por *hackers,* que poderiam controlar o rádio e ar condicionado do veículo.

Estes casos despertaram nos Estados Unidos a urgência em regulamentar os carros conectados, cabendo à agência norte-americana de segurança de trânsito, "National Highway Traffic Safety Administration" (NHTSA) e pela agência que tem competência em defender os direitos dos consumidores, "Federal Trade Commission", avaliar estas ferramentas.[37] No Brasil, caberá ao CONTRAN e à SENACON verificar a segurança dos sistemas utilizados nos carros conectados, além da ANPD quanto à proteção de dados pessoais e à privacidade.

A inteligência artificial e a Internet das Coisas não são expressão sinônimas, mas são ferramentas tecnológicas que estão muito próximas, seja por parte da IA que utiliza um volume de informações gerado pela IoT; seja a IoT que utiliza ferramentas de aprendizado de máquina para incorporar inteligência nas soluções oferecidas. Portanto, são duas ferramentas utilizadas pela indústria automotiva, notadamente os carros autônomos e os carros conectados.

36. Case No. 15-cv-0855-MJR-DGW.
37. CHIKE, Patrick. The Legal Challenges of Internet of Things. *Technical Report*. Disponível em: https://www.researchgate.net/publication/322628457. Acesso em: 12 jan. 2020.