Internet das Coisas: Privacidade, Marcos Regulatórios e Consumo

James Cleiton de Oliveira Sá[1]
Prof. Dr Luiz Antonio Perrone Ferreira de Brito[2]
Prof. Dr Edson Aparecida Querido[3]

Resumo

O aumento exponencial dos objetos inteligentes com capacidade de sensoriamento, processamento e comunicação tem tido aceleração em progressão geométrica nos últimos anos. Neste cenário, a Internet das Coisas ou, como é mais conhecida a *Internet of Things (IoT*)) conecta estes objetos à Internet e promove a comunicação entre usuários e dispositivos. A IoT possibilita uma grande quantidade de novas aplicações, tais como cidades inteligentes, saúde e automação de ambientes. Por outro lado, existem diversos desafios que devemos enfrentar no âmbito social, jurídico, teórico e prático. Para responder a algumas dessas questões, precisamos vencer alguns desafios como, por exemplo, definir novos conceitos menos ou mais flexíveis para privacidade e segurança de dados ou efetivar marcos regulatórios rígidos e globais que mantenham mínimos éticos aceitáveis para todos os países. Seja qual for a conduta a ser adotada é inevitável que isto trará consequências para uma sociedade pós-moderna caracterizada pelo consumismo que otimiza seus processos de

[1] Formação – Bacharel em Ciências Jurídicas e Sociais pela Universidade de Taubaté (2004), Pós-Graduado na Especialização em Segurança de Aviação e Aeronavegabilidade Continuada – ITA (2009); Pós-Graduado em Direito e Processo do Trabalho pela UNITAU (2018), Elemento Credenciado EC-PREV, EC-MA e tutor nos cursos de segurança de voo do Centro de Investigação e Prevenção de Acidentes Aeronáuticos (CENIPA), Mestrando no Mestrado Profissional em Gestão e Desenvolvimento Regional pela UNITAU, com ênfase em segurança de voo, 2019-2020.

[2] Possui graduação em Engenharia Civil pela Universidade do Vale do Paraíba (1990), Mestrado em Engenharia Aeronáutica e Mecânica pelo Instituto Tecnológico de Aeronáutica, ITA (2000) e doutorado em Engenharia Civil pela Universidade Estadual de Campinas, UNICAMP (2006). Atualmente é professor da UNITAU. Tem experiência na área de Engenharia Civil, com ênfase em Propagação de ruído e vibração industrial ambiental, atuando principalmente nos seguintes temas: acústica, acústica arquitetonica, isolamento acústico, ruído ambiental e meio ambiente (EIA e RIMA), potência sonora e intensimetria vibração devido ao tráfego ferroviário, rodoviário, bate estacas e conforto ambiental em geral.

[3] Graduação em Ciências Econômicas pela Universidade do Vale do Paraíba (1985), Mestrado em Economia do Trabalho e da Tecnologia pela Pontifícia Universidade Católica de São Paulo (1991) e Doutorado em Engenharia Aeronáutica e Mecânica - Área de Organização Industrial pelo Instituto Tecnológico de Aeronáutica (1998). Pós-Doutorado em Gestão da Inovação Tecnológica - Área de Produção pelo Instituto Tecnológico de Aeronáutica (2010). Professor Assistente Doutor da Universidade de Taubaté (UNITAU) - Exerce a função de Coordenador de Programa de Pós-graduação Stricto e Lato Sensu e Pesquisador. Membro do Conselho Editorial da Revista Brasileira de Gestão e Desenvolvimento Regional (ISSN 1809-239X) na função de Editor Chefe. Membro do Conselho Editorial da Revista Latin American Journal of Business Management (ISSN 2178-4833) na função de Editor Chefe. Membro do Conselho Editorial da Revista Árvore (ISSN 0100-6762) na função de Parecerista. Ad-hoc Referees - Besides the participation of Editorial Board, the Journal of Aerospace Technology and Management - JATM(ISSN 2175-9146) É membro do Corpo de Especialistas do Conselho Estadual de Educação do Estado de São Paulo. Tem experiência na área de Gestão, com ênfase em Gestão de Tecnologia; Gestão Sistêmica; Gestão da Produção e Gerenciamento de Projetos. Atua nos seguintes temas: Planejamento, Desenvolvimento Regional, Economia brasileira e Internacional, Gestão de Projetos, Estratégia Tecnológica e Industrial, Indústria Aeroespacial, Indústria Automobilística e Gerenciamento e Formação Executiva.

mercado com a utilização de tais dados, muitas vezes, sem consentimento. O objetivo principal do artigo é apontar as questões decorrentes, não somente jurídicas, da interação da Internet das Coisas (IoT) com o processamento de dados pessoais na economia digital consumista atual. Como metodologia foi realizada uma pesquisa qualitativa com revisão bibliográfica juntamente com pesquisa preliminar das realidades de proteção de dados dos países da América Latina. Com a pesquisa obtivemos o resultado de que apenas seis países latino-americanos aprovaram legislação de proteção de dados e que a Internet das Coisas é um fenômeno destinado a mudar nosso futuro. Concluiu-se que a promulgação de marcos regulatórios locais é relevante, mas com alcance limitado e, com isto, apontou-se a necessidade de consenso entre todos os Estados a nível global para construção de regulação internacional tendo em conta a salvaguarda da segurança dos usuários e a proteção contra risco de divulgação sem consentimento o que vai influenciar no aumento ou não do consumo.

Palavras-chave: Internet das coisas, marco regulatório, privacidade, segurança de dados

Abstract

The exponential increase in the number of intelligent objects capable of sensing, processing and communicating has accelerated in geometric progression in recent years. In this scenario, the Internet of Things or, as the Internet of Things (IoT) is better known, connects these objects to the Internet and promotes communication between users and devices. IoT enables a large number of new applications, such as smart cities, health and automation of environments. On the other hand, there are several challenges that we must face in the social, legal, theoretical and practical spheres. To answer some of these questions, we need to overcome some challenges, such as, for example, defining new less or more flexible concepts for privacy and data security or putting in place rigid and global regulatory frameworks that maintain acceptable ethical minimums for all countries. Whatever the conduct to be adopted, it is inevitable that this will have consequences for a postmodern society characterized by consumerism that optimizes its market processes with the use of such data, often without consent. The main objective of the article is to point out the issues arising, not only legally, from the interaction of the Internet of Things (IoT) with the processing of personal data in the current consumer digital economy. As a methodology, a qualitative research with bibliographic review was carried out together with a preliminary research on the data protection realities of Latin American countries. With the survey, we obtained the result that only six Latin American countries have passed data protection legislation and that the Internet of Things is a phenomenon destined to change our future. It was concluded that the promulgation of local regulatory frameworks is relevant, but with limited scope and, with this, the need for consensus among all States at the global level was pointed out for the construction of international regulation taking into account the safeguarding of user safety. and protection against risk of disclosure without consent, which will influence the increase or not in consumption.

Keywords: Internet of things, regulatory framework, privacy, data security

1Introdução

Na última década a internet tornou-se uma ferramenta presente no cotidiano das pessoas e das organizações e por vez indispensável ao bom funcionamento dos negócios. Com o crescente incremento das infraestruturas de redes e popularização em massa da rede de alta velocidade, emerge um avanço relacionado à utilização da internet tornando-a uma plataforma global para deixar máquinas e objetos inteligentes capazes de comunicarem-se de forma autônoma.

Esta possibilidade permite que conteúdos e serviços estejam em torno das pessoas, sempre disponíveis, facilitando a comunicação e abrindo o caminho para novas aplicações, possibilitando novas formas de trabalho, de interação e de entretenimento, fazendo com que um novo padrão de vida e de trabalho seja desenvolvido. Este novo padrão torna-se possível através dos avanços das Tecnologias da Informação e Comunicação - TIC até uma nova concepção definida como Internet das Coisas - *Internet of Things (IoT)*. Entretanto, com uma variada coleta de dados e informações, para variados fins, no cotidiano das pessoas e das organizações, a coleta autônoma dos dados e das informações torna a privacidade um dos principais desafios em relação à IoT.

Neste contexto o tema é relevante por discutir e fazer refletir sobre bens fisicamente intangíveis, mas juridicamente tutelados como a privacidade dos usuários das tecnologias da Internet das Coisas, diante de sua regulação jurídica e conexão à economia digital modificando os padrões de consumo e explorando possíveis soluções neste cenário ainda em construção.

O objetivo principal do artigo é apontar e refletir sobre as questões decorrentes, não somente jurídicas, da interação da Internet das Coisas (IoT) com o tratamento da privacidade no processamento de dados pessoais na economia digital consumista atual.

Os novos produtos e serviços da internet das coisas nos tornarão mais eficientes, com maior capacidade de ação e compreensão do meio ambiente, haverá novas ajudas técnicas que prolongarão nossa vida ativa e muito mais. Porém, coexistiremos com um grande número de dispositivos que coletarão informações sobre nossas atividades, costumes, preferências, etc., o que poderia ameaçar nossa privacidade.

Desconfiança pode ser uma barreira para o pleno desenvolvimento desses novos produtos e serviços (SERGL, 2019).

A necessidade de realizar este artigo deve-se principalmente ao fato de que o potencial de coleta, processamento e uso de dados pessoais aumentou consideravelmente com o avanço das tecnologias da informação, impactando os modelos regulatórios de proteção de dados pessoais no processo econômico e nas relações comerciais contemporâneas.

Nesse sentido, em um cenário global em que cerca de 122 países não possuem legislação específica sobre o assunto (BANISAR, 2019), a regulamentação se torna cada vez mais inquestionável diante das perdas econômicas e de investimentos para o país geradas pela ausência de leis de proteção. de dados. Também é um requisito essencial para se tornar membro da Organização para Cooperação e Desenvolvimento Econômico (OCDE). A maioria das nações estão apenas com regulamentos que em direito comparado responsabilizam civil e penalmente quando os danos com tratamento dos dados pessoais já foram efetivamente concretizados (BANISAR, 2019).

Para buscar atingir o objetivo de pesquisa este trabalho foi dividido em introdução justificando para a relevância do tema, desenvolvimento que foi subdividido em conceituar os principais aspectos do tema como internet, internet das coisas, privacidade, marco

regulatórios nacionais e de outras regiões do globo e consumo, descrição da metodologia efetuada, discussão dos resultados e conclusão.

2. Referencial teórico

2.1 Breve histórico da Internet

A Internet serviu para favorecer e aprimorar os sistemas de interação social, com grande impacto na esfera econômica, dado o vasto fluxo de dados em escala global que transformou significativamente a velocidade das transações financeiras e, consequentemente, a acumulação de capital.

A expansão dos meios de comunicação fez com que as distâncias encurtassem ainda mais. A partir dos anos 1980, o cenário se ampliou com as novas formas de consumo cultural: fotocopiadora, videocassetes, videoclipes, videojogos, controle remoto, CDs e TV a cabo (SANTAELLA, 2003).

Os primeiros computadores surgiram em 1945, na Inglaterra e nos Estados Unidos, sendo utilizados por militares para cálculos científicos. A partir de 1960, passaram a ser manipulados também para cálculos científicos e para estatísticas das grandes empresas. Segundo Pierre Lévy (2010), "[...] os computadores ainda eram grandes máquinas de calcular, frágeis, isoladas em salas refrigeradas, que cientistas em uniformes brancos alimentavam com cartões perfurados e que de tempos em tempos cuspiam listagens ilegíveis" (LÉVY apud SASTRE, 2010, p.31).

Uma mudança fundamental aconteceu nos anos de 1970, com o desenvolvimento e a comercialização do microprocessador. Com esse progresso, a produção industrial avançou tecnologicamente e aparelhos eletrônicos, computadores e redes de comunicação de dados se tornaram e são até hoje considerados pela indústria recursos essenciais para ampliar a produtividade (LÉVY apud SASTRE, 2010).

A internet surgiu em 1969, a partir da *Arpanet*, rede de computadores constituída pela *Advanced Projects Agency (ARPA)*, formada pelo Departamento de Defesa dos Estados Unidos com o objetivo de mobilizar recursos de pesquisa para os avanços na tecnologia militar frente à União Soviética. O projeto foi fruto do trabalho de um grupo de cientistas da computação, que deu início ao sonho de transformar o mundo por meio de uma nova forma de comunicação (CASTELLS, 2003). tempos em tempos cuspiam listagens ilegíveis" (LÉVY, 2010, p.31).

2.2 Motivação para o aumento da preocupação mundial com a proteção de dados

O uso de dados se torna cada vez mais importante devido ao desenvolvimento de uma economia global cada vez mais digitalizada. A monetização desses dados torna sua proteção necessária para os usuários da rede. Na frente de transações internacionais, se você pensar em modelos regulatórios para resolução de conflitos.

Além disso, permitiu a criação de novos modelos de negócios baseados precisamente no uso desses dados. Embora a preocupação com a proteção de dados pessoais não seja uma questão recente, somente após uma série de episódios de forte impacto ocorrido em todo o mundo, começou a ser gerado um certo consenso sobre a importância dessa proteção (VERONESE et al, 2017).

O que mudou após esses eventos foi o paradigma da proteção, com a adoção de um modelo de abordagem da base de risco, focado não apenas no estabelecimento de medidas preventivas e punitivas após a violação de direitos, mas também na preocupação de incorporar princípios e mecanismos de prestação de contas, entendidos como o monitoramento e controle da sociedade em relação à questão da governança da Internet (VERONESE et al, 2017).

A preocupação com o processamento de dados pessoais pelo poder público também surge após o episódio que envolveu Edward Snowden e a divulgação de dados da NSA - Agência de Segurança Nacional, a Agência de Segurança Nacional dos Estados Unidos da América. Este caso, a partir de 2013, revelou a existência de programas de vigilância utilizados para monitorar a população globalmente.

Mais recentemente, em 2015-2016, a investigação da *Cambridge Analytica* reforçou a relevância de acelerar o processo regulatório, demonstrando como a desproteção de dados pessoais afeta não apenas a vida de um cidadão, mas de toda a comunidade e o que o sistema entende por democrática (SILVEIRA & FROUFE, 2018, p. 14).

A maneira como a proteção à privacidade é implementada depende das diferentes jurisdições e atores sociais que influenciam esse processo, como o mercado e outros reguladores, "a necessidade de buscar um conteúdo comum mínimo para o direito à privacidade" é mais do que um exercício puramente acadêmico, é uma necessidade real devido ao aumento do fluxo de informações nos últimos anos "(DONEDA, 2006, p. 85-86).

2.3 Privacidade

Stefano Rodotá traz a ideia de funcionalidade de privacidade, considerando que hoje não é uma expressão pura de uma necessidade individual, mas sua inserção deve ser inserida no quadro da nova "cidadania eletrônica" e conceitua o direito de privacidade como “o direito de manter controle sobre suas próprias informações” (RODOTÁ apud SASTRE, 2008, p.92).

Mais e mais pessoas são conhecidas como sujeitos públicos por meio dos dados que nos interessam.

A privacidade não deve ser considerada um direito subjetivo. Uma das razões para isso é a dificuldade de enquadrar a privacidade em uma concepção coerente e unitária (DONEDA apud SASTRE, 2006).

Compreender como as normas técnicas, políticas, econômicas e sociais são articuladas é essencial para entender quem são os principais atores desse processo de transformação e como eles interagem (BROUSEEAU, MARZOUKI, MÉADEL apud SASTRE, 2012).

As autoridades nacionais de proteção de dados (APD), atores centrais para garantir essa proteção, enfrentam uma tarefa difícil de cumprir sua missão e agir como responsáveis por esses direitos. A ação dos APD é entendida como instrumentos adequados para permitir o desenvolvimento de diferentes aspectos da economia baseada em dados, como o comércio eletrônico, garantindo a proteção dos dados pessoais dos usuários da Internet e tornando enfrentar o problema da responsabilidade dos intermediários técnicos, a fim de destacar a especificidade da abordagem europeia construída em torno de um objetivo fundamental que é o equilíbrio entre a lógica do mercado e as preocupações dos cidadãos. (BLANDIN apud SASTRE, 2001).

2.4 Privacidade e Segurança na IoT: argumentos para flexibilização

Uma das promessas da implementação da IoT é oferecer maior eficácia tanto no combate à criminalidade quanto na capacidade de prever, prevenir e responder a situações de emergência ou ameaças à ordem pública.

No caso das epidemias, por exemplo, a rápida coleta e análise de dados se faz particularmente relevante. Já com relação à manutenção da ordem pública, dados coletados por câmeras e a partir de dispositivos pessoais dos cidadãos têm sido utilizados para fins de vigilância e monitoramento territorial em situações de grande circulação de pessoas nas cidades, como os megaeventos (CARDOSO apud MAGRANI, 2018), sensores podem reforçar a segurança em edifícios públicos ou privados e a geolocalização pode ajudar a monitorar a dinâmica de certos fenômenos naturais para operações de prevenção e resgate (BORGIA apud MAGRANI, 2018).

Em muitos debates que deveriam ser técnicos o jargão popular "...quem não deve, não teme" é vociferado para impedir qualquer discussão a respeito dos limites desse cotidiano *reality show* digital.

Segurança pública ostensiva e preventiva, concentra importante preocupação quanto a um dos principais desafios técnicos e regulatórios que a emergente realidade da IoT precisará enfrentar: o equilíbrio entre a ampliação da inovação, a busca da ordem pública e a preservação da privacidade.

Com efeito, é no contexto de debates sobre segurança que emergem importantes questionamentos quanto a abusos e restrições indevidas à privacidade dos cidadãos (BARTOLI apud MAGRANI, 2018).

Com a evolução da tecnologia e a possibilidade da coleta e processamento de grandes volumes de dados, a tensão entre segurança e privacidade alcançou novas dimensões. Tanto internacional quanto nacionalmente, o assunto muitas vezes é abordado de forma polarizada e mutuamente excludente: o incremento da privacidade enfraqueceria os esforços de segurança, e vice-versa (MAGRANI, 2018).

2.5 Realidade atual dos marcos regulatórios

O fluxo de dados transfronteiriço, que é o movimento de dados pessoais através das fronteiras nacionais, é essencial para o comércio no mundo eletrônico. Embora seu uso seja cada vez mais comum para o desenvolvimento comercial, há também uma crescente necessidade de cooperação em questões processuais e de pesquisa.

Assim, o mais importante e o desafio das regulamentações transfronteiriças é entender como gerenciar esse fluxo sem enfrentar direitos e garantias protegidos em um determinado país e não regulamentados em outro, ou mesmo com leis que tratam de proteções de maneiras diferentes.

Acima de tudo, um dos obstáculos para garantir esse fluxo é exatamente o regulamento adotado para a proteção de dados, por exemplo, ter autorização da OCDE para exercer relações comerciais que implicam o uso transfronteiriço de dados.

Na América Latina sete países possuem leis nacionais sobre proteção de dados pessoais e autoridades que garantem essa proteção, sendo eles Brasil, México, Argentina, Uruguai, Peru, Colômbia e Panamá. Estes já possuem APD - autoridade de proteção de dados (SASTRE, 2019)

No Brasil, por exemplo, a Lei Geral de Proteção de Dados (LGPD) foi promulgada recentemente em 14 de agosto de 2018, com entrada em vigor prevista para fevereiro de 2020,

18 meses após a sanção. A aprovação da Lei, no entanto, teve alguns vetos, incluindo as disposições voltadas para a criação da Autoridade Nacional de Proteção de Dados (ANPD), o que levou à edição da Medida Provisória n. 869, de 2018, aprovada no Congresso Nacional Brasileiro com uma Autoridade vinculada à Presidência da República.

O direito europeu à proteção de dados pessoais baseia-se em três pilares principais: as obrigações daqueles que lidam com dados privados, os direitos dos usuários e o papel das autoridades de proteção de dados (APD).

Gradualmente, estabeleceu-se uma tendência de regular a Internet em nosso país, liderada inicialmente por vários projetos de lei propostos com o objetivo de regular a rede de maneira punitiva. Assim, em 1999, o PL nº 84/99, conhecido como Projeto de Lei de Azeredo, foi proposto para tipificar comportamentos conduzidos pelo uso de sistemas eletrônicos, digitais ou similares. A proposta foi severamente refutada pelos setores da sociedade e culminou na elaboração de outro projeto, o PLC nº 21/2014, que gerou o MCI, que foi aprovado após intensos debates no Congresso Nacional, com base em uma construção participativa, estabelecendo princípios, garantias, direitos e deveres do uso da Internet no Brasil. Em 2016, também após consulta pública à sociedade, foi estabelecido seu Decreto Regulatório.

Hoje, existem dois modelos existentes de observar a Internet, como Macron aponta em seu discurso de abertura no *Internet Governance Forum 2018*, que ocorreu em Paris: "existe uma forma de Internet na Califórnia e há uma Internet chinesa". Esses dois modelos têm concepções regulatórias diferentes, o primeiro se concentra na autorregulação e nos interesses privados dos grandes players e das empresas globais dominantes. Ele está inserido em um contexto de democracia e, em teoria, existe a possibilidade de controle de dados pessoais por seus usuários, cuja prática e profundidade dessa autodeterminação dos dados podem ser debatidas.

Enquanto isso, segundo Macron, justamente esse modelo não é democrático, justamente pela ausência de controles por vontade das empresas privadas, ataques à democracia e falta de regulamentação estatal.

Contra o modelo californiano, o modelo chinês, onde o Estado tem um forte papel de monitoramento e filtro de conteúdo, com o desenvolvimento de elementos técnicos não orientados à segurança do usuário, mas para aperfeiçoar esse controle estadual. O próprio governo desenha inovações e propõe regulamentos que legitimam essas práticas de controle.

No âmbito da América Latina, o Brasil assumiu um papel de destaque em relação à regulamentação da Internet com a aprovação da Estrutura Civil da Internet (Lei nº 12.965 / 2014) e, posteriormente, com a publicação do Decreto Regulamentar nº 8.771 / 2016. O destaque brasileiro na aprovação do Marco Civil da Internet e o processo participativo de construção dessa lei promoveram o debate entre as diversas partes afetadas pela regulamentação da rede no país (SENADO, 2020)

A proteção de dados pessoais também ocupa a proteção da dignidade da pessoa na qual os direitos à privacidade são direitos fundamentais, tomando como referência o artigo 12 da Declaração Universal dos Direitos Humanos.

Haja vista ser um tratado internacional no qual o Brasil é signatário com a confirmação por parte do Congresso Nacional o direito à privacidade recebeu confirmação como direito fundamental em nosso país.

A superação do direito à privacidade apenas como tutela patrimonial, diante do cenário em que é tratado como direito fundamental, e o estabelecimento de novos

mecanismos e institutos que permitam a proteção efetiva dos interesses da pessoa, ou seja, portanto, a proteção da privacidade de dados pessoais está alçado como cláusula pétrea na lista de direitos fundamentais de nossa Constituição Federal.

Ao falar sobre proteção de dados pessoais, devemos primeiro levar em consideração que vivemos em uma sociedade hiper conectada, na qual os dados são um dos principais ativos para o desenvolvimento de uma economia global cada vez mais digitalizada.

Apesar da consciência de que a vida cotidiana e a personalidade das pessoas são construídas com dados na era digital, no entanto, muitas vezes, isso passa despercebido pelos usuários, que não percebem a trilha digital que produzem em si mesmos.

Os dados produzidos, não raramente, são armazenados por um longo período de tempo. O controle dessa trilha tornou-se um problema tecnológico e social, pois, a partir de sua análise, é possível obter informações sobre o comportamento, preferências e necessidades pessoais de uma determinada pessoa e até antecipar suas ações futuras (MAGRANI, OLIVEIRA, 2019, p.338; SJÖBERG apud SASTRE, 2016).

Isso se reflete no consentimento e em suas políticas, na maioria das vezes expressos em termos e condições anteriores à contratação de um serviço, que nem são lidos pela pessoa que o utiliza. A discussão sobre a validade do consentimento, uma vez que começa com a preocupação com o tratamento dado aos dados, não apenas pelo Poder Público, mas também pelos agentes privados que lucram com esse bem (BIONI apud SATRE, 2019).

A proteção individual dos dados em si é interpretada em muitos regulamentos como autodeterminação informacional e a autonomia da vontade dos indivíduos com seu consentimento informado, livre e expresso, específico ou inequívoco constrói modelos regulatórios nos quais o consentimento é o elemento central de uma regulamentação da privacidade de dados pessoais (MONTELENE, LE MÉTAYER, 2009, SCHARTZ, 1999).

No Brasil, o artigo 18 da Estrutura Civil da Internet atribui como regra a ausência de responsabilidade pelos provedores de conexão (ISP). E para os fornecedores de aplicativos no artigo 19 atribuiu uma responsabilidade subjetiva e permite que a retirada de conteúdo da rede preceda a autorização judicial. Nos parágrafos seguintes desta Lei, há exceções como direitos autorais e direitos relacionados.

Na Argentina, existe um projeto de lei, publicado em 20 de outubro de 2016 pela agenda nº 824 do Congresso, que regula a responsabilidade dos provedores de serviços de Internet, a fim de garantir a liberdade de expressão e o direito de informações, preservando os direitos à honra, privacidade e imagem, com o mesmo modelo de notificação e remoção. Só existe responsabilidade dos fornecedores por ordem judicial (SATRE, 2019).

2.6 Autoridade de Proteção de Dados (APD)

Os APD podem ser considerados como um dos três pilares da proteção de dados, demonstrando sua importância na União Europeia. Assim, os poderes dos APD são definidos apenas de uma maneira geral. Essas competências estão agrupadas em categorias básicas, tais como: poderes de investigação, poderes de intervenção, poderes para se envolver em processos judiciais e ouvir reclamações.

A adoção de um regulamento geral sobre proteção de dados não se destina a coibir a inovação, mas a gerar confiança nos usuários sobre o tratamento dado pelas empresas que coletam seus dados.

2.7 Discussão sobre Intervenção nos processos democráticos com uso de dados pessoais

A responsabilidade dos intermediários provedores de serviços de Internet também é apresentada em momentos eleitorais. O debate passa pela micro direção de gostos e tendências que geram manipulações como estratégia para capturar os eleitores nas eleições.

Os dados dos cidadãos geralmente coletados legalmente nas redes sociais, abordam o caso da *Cambridge Analytica* nas eleições do México e dos Estados Unidos que elegeram Trump.

Ainda há o caso das eleições brasileiras e o papel das redes. A discussão também passou pelo uso de notícias falsas com o envio de mensagens em massa pelo WhatsApp (SANTOS apud MAGRANI, 2018). Foram feitas propostas de leis que podem reduzir a liberdade de expressão, trazendo novos desafios regulatórios que são apresentados ao longo desse cenário.

A coleta para desenhar estratégias eficazes e capturar o cidadão não está apenas nas redes sociais, mas se eles cruzam os dados com bases públicas, como pesquisa de estatísticas populacionais, organizações de consumidores, o que permite o direcionamento dos dados. A psicometria é a nova técnica usada para realizar o marketing político, que utiliza uma avaliação psicológica dos dados para identificar os desejos e o comportamento dos eleitores, o objetivo público da propaganda política, a fim de promover melhorias em seus perfis (SANTOS, et.al. apud SASTRE, 2018, p.57).

O processo de "consumir *insights*", ou seja, o uso de todos os dados gerados pelo consumidor para gerar um endereço e *insights* de *marketing*, realizados pelas empresas e pelos partidos eleitorais, envolvem o enriquecimento do banco de dados e modelagem de dados (SANTOS, et.al. SASTRE, 2018, p.59).

A análise desses anúncios e propagandas permite verificar o escopo e “melhorar” o serviço, realimentando, no entanto, melhorar para quem? Como uma característica do pós modernismo o consumidor não irá escolher o que comprar, mas sim será dito a ele o que este deverá comprar para saciar sua vontade de consumir.

Esse processo tem a ver com o uso e gerenciamento de algoritmos, mas não apenas para fins comerciais, mas também alinhando esse compartilhamento de dados ao processo democrático de tomada de decisão das eleições e à perpetuação de valores de uma sociedade com elementos de cidadania. Esse problema leva a perguntas sobre o poder e as competências que as grandes empresas de manipulação de dados possuem na pós modernidade.

A interferência nos processos democráticos utilizando como fonte primária os dados pessoais ativa ou passivamente coletados estaria ferindo este direito fundamental à privacidade da pessoa?

2.8 Consumo na IoT

A globalização é um dos fenômenos que há mais tempo vêm atuando e moldando nosso mundo. Em termos de impacto, trata-se de fenômeno ainda incipiente e com crescimento presumível exponencial, em função da crescente digitalização e do aumento do tráfego de dados mundial.

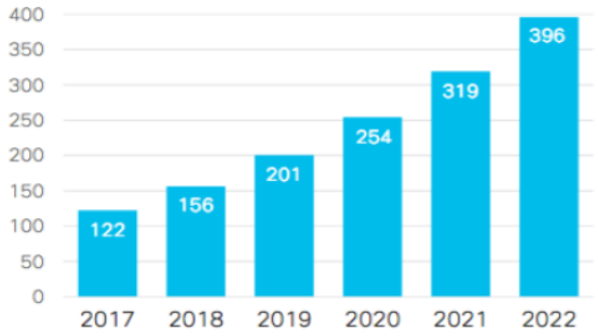
Adrian Wooldridge, da revista The Economist, falando da tendência em 2009, afirmava que estamos só no início da globalização. Em 2009, explicou ele, “apenas 4% do comércio é fora das fronteiras, 3% das marcas são globais e apenas 20% do tráfego da internet

é internacional, mas o balanceamento global é uma força poderosa — e ainda temos muito caminho para percorrer." (ECONOMIST apud MAGRANI, 2018)

A globalização, até recentemente, era algo muito sutil. Hoje, essa sutileza acabou e a aceleração do processo é inegável e inevitável. Ao longo dos últimos 10 anos, o tráfego de dados global cresceu de praticamente zero até bilhões de gigabytes por segundo, lançados à nuvem de todo o planeta. O intercâmbio de dados entre regiões já alcança cerca de um terço do tráfego total mundial.

Dados e informação, hoje, geram mais valor econômico que o comércio internacional de bens, segundo relatório da McKinsey apresentado em 2015 (MC KINSEY apud MAGRANI, 2018).

Figura 1. Crescimento Global de Tráfico IP 2017 – 2022 em exabytes por mês



Fonte: CISCO, 2019

Exabyte é unidade de medida de informação que equivale a 1 EB equivalente a 10^{18} Bytes (CISCO, 2019)

Estima-se que em torno de 900 milhões de pessoas mantenham conexões internacionais via redes sociais e que 360 milhões participem do e-commerce internacional. Plataformas digitais tanto para o emprego tradicional quanto para os contratos de *freelancer* estão começando a criar um mercado de trabalho mais globalizado e flexível (CISCO, 2019).

Os intermediários (provedores de conteúdo) precisam saber cada vez mais sobre seus clientes, a fim de melhorar seu modelo de negócios e obter melhores resultados. Esse maior conhecimento é obtido através da análise exploratória dos dados aos quais eles têm acesso, seja de seus clientes, fornecedores, concorrentes, mas essa análise de dados pode e normalmente invade a privacidade dos envolvidos.

Na economia de dados, existem relacionamentos plurilaterais, nos quais um serviço é oferecido ao usuário de forma que não precise contribuir com uma quantia pecuniária para ele, como os modelos de negócios tradicionais, em um relacionamento binário (consumidor e fornecedor). O acesso "gratuito" deriva da transferência dos dados pessoais desses usuários, consumidores, em troca do uso do serviço, onde o provedor se beneficia da publicidade comportamental direcionada (BIONI, 2019, página 25).

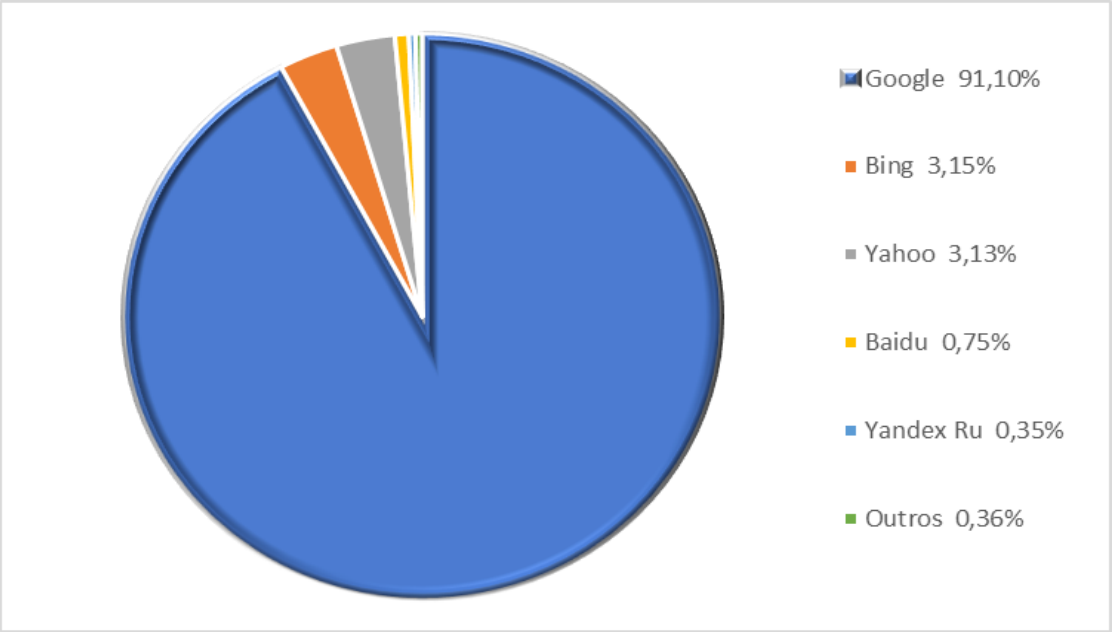
O conceito "modelo de negócios de propaganda de preço zero" usado por Katherine Strandburg (2013, p.86) define esse tipo de modelo de negócios.

Esse modelo de negócios, criado a partir das informações e atividades pessoais do indivíduo, é baseado na mineração de dados, que consiste em extrair conhecimento de dados

brutos, em inteligência de pesquisa e em aprendizado de máquina e o uso de inteligência artificial.

Os dados são alimentados pelos usuários com suas informações pessoais, gostos, preferências, ações. Para tratar dados considerados "brutos", são utilizadas correspondência e segmentação, ou seja, os intermediários processam dados (análise de dados), cruzando informações e direcionando publicidade. (BIONI, 2019, p. 31).

Figura 2. Quota de mercado dos mecanismos de pesquisa no mundo



Fonte: STAT COUNTER, 2019

2.9 Expectativas brasileiras para a Internet das Coisas

As fronteiras e barreiras diariamente estão sendo rompidas, a expansão do conhecimento é imensa e vai levar ao desenvolvimento aqueles segmentos de mercado, indústrias e países que melhor entenderem e aproveitarem a oportunidade para criar o futuro.

O impacto e a aceleração dessa força globalizadora devem gerar um potencial de crescimento enorme, com infinitas oportunidades de intercâmbio de dados sobre inovação e avanços tecnológicos e gerenciais (MAGRANI, 2018)

Mesmo do ponto de vista de uso, e mesmo com o sucesso dos arranjos de governança que temos, a política de internet das pessoas (e instituições) não deu os resultados esperados — o Brasil está perto do centésimo lugar, entre os países do mundo, nos índices de velocidade e qualidade de rede, de prontidão digital, de complexidade de sua economia digital (CISCO, 2019).

A proposição de políticas para a internet das coisas, e de tudo, precisam acentuar esforços não somente em responsabilização civil de danos em caso de uso indevido de dados, mas deve analisar, de maneira crítica e profunda, as causas dessas anomalias e suas consequências, e como elas poderiam vir a ser mitigadas em futuras políticas nacionais, inclusive nesta, das coisas (MAGRANI, 2018)

3. Método

Do ponto de vista metodológico, a pesquisa qualitativa foi realizada com revisão bibliográfica juntamente com pesquisa preliminar das realidades de proteção de dados dos países da América Latina.

Tal pesquisa bibliográfica buscou abranger uma "rede conceitual de atributos legais, cuja realidade depende de indicadores de uma ordem normativa (base legal), de uma ordem específica (implementação da legislação), de uma ordem institucional (papel dos atores envolvidos) e de uma ordem prospectiva (tendência futura) "(SILVA, 2011). Nesse sentido, a preocupação com a dificuldade de desmembramento dos institutos jurídicos em seus efeitos práticos e sua necessária contextualização nacional, ou seja, a preocupação com o "transplante de práticas regulatórias nacionais para órgãos políticos dotados de diferentes modelos socioeconômicos, políticos e jurídicos "(SILVA, 2011, p.4).

4. Resultados e discussão

Os dados trafegados ativa e passivamente pelos dispositivos e plataformas online podem parecer exclusivamente benéficos. No entanto, os dados oriundos desses dispositivos interconectados podem oferecer riscos a direitos fundamentais dos envolvidos, como privacidade e segurança.

Os riscos se agravam pelo fato de que o ambiente regulatório de todo o mundo precisa ajustar-se rapidamente a esse cenário em transformação.

Não há ainda uma regulação específica adequada na área de proteção de dados pessoais e privacidade efetivas para toda a Internet das Coisas, e as propostas em discussão foram desenhadas para um cenário no qual a IoT ainda não era realidade.

Esse fato cria uma janela de oportunidade: é possível aprovar leis que protejam os direitos individuais e favoreçam a inovação ou os conceitos de privacidade e segurança devem ser flexibilizados inevitavelmente?

Nesse cenário, para evitar a perspectiva falaciosa do tudo ou nada e sua influência sobre o próprio processo de elaboração de políticas públicas, é necessário realizar pesquisas para compreender os modelos regulatórios que têm se desenvolvido para subsidiar a evolução da IoT.

A pesquisa no âmbito do eixo horizontal privacidade e segurança deverá ser baseada em um mapeamento compreensivo e uma análise das iniciativas comparadas, contextualizando-os no panorama regulatório brasileiro.

Um dos aspectos salientes do sucesso da internet tradicional, a internet das pessoas (IoP) no mundo, e no Brasil em particular, é o fato de que o Estado teve, e ainda tem, apenas um papel indutor em seu desenvolvimento (MAGRANI, 2018).

A autorregulação exclusiva do setor privado permite que essas empresas criem algoritmos e decidam sobre o conteúdo dos veículos, o uso de dados e a venda para interesses puramente econômicos, sem se preocupar com os dados do usuário.

A troca de dados entre diferentes jurisdições, uma vez que grande parte das empresas são estrangeiras e são realocadas em um país específico, apresenta o dilema de como proteger dados em países com leis, direitos e regulamentos diferentes.

Um exemplo do uso de dados pessoais em diferentes jurisdições da mesma empresa, podemos mencionar as empresas de pedidos de alimentos, que crescem bastante em toda a América Latina, como *IFood, Rappi, Ubereats, Glovo* e *Uber* o mesmo tratamento e o mesmo banco de dados, embora estejam baseadas em um país tendo que importar os dados de seus clientes de outros países. Por um lado, se isso não fosse permitido, os negócios não seriam viáveis, mas devemos garantir, por outro lado, a proteção e segurança de tais dados pessoais de clientes que migram de uma legislação para outra. Esse fluxo deve ser permitido, mas devemos garantir que os dados pessoais sejam protegidos por entidades regionais de harmonização e proteção supranacional e/ou até mesmo a criação de um órgão subordinado às Organização das Nações Unidas – ONU.

Um mercado único latino-americano como o mercado europeu seria uma boa saída após a harmonização das leis, o que seria um passo preliminar para isso. Ainda, para a implementação da proposta, seria necessário adaptar-se ao contexto latino-americano, diante de questões de disparidades socioeconômicas de países, grandes diferenças culturais e dimensões geográficas não tão equivalentes, quando se fala em Brasil, por exemplo. Um passo antes de fazer essa unificação tem a ver com o fortalecimento das leis internas das autoridades de proteção de dados dentro de padrões internacionais, como os da OCDE para o comércio internacional.

5. Considerações finais

Historicamente, na maioria das mudanças com esse potencial e esse tamanho, poucos são os atores que conseguem guiar as transformações e muitos são aqueles interessados nas consequências.

A IoT está sendo guiada pelo setor privado e, particularmente, pelas empresas de tecnologia. Cabe destacar que a produtividade, a inovação e a geração de novos negócios estão sendo lideradas por um grupo muito restrito de multinacionais, ávidas por dados dos usuários.

Os dados pessoais coletados no âmbito da IoT geram enorme riqueza e a coleta, armazenagem e processamento dos dados pessoais de cada pessoa que compre um objeto conectado, ou, talvez, que simplesmente se aproxime dos sensores de tal objeto, é, na verdade, um dos objetivos principais dos jogadores protagonistas da IoT.

As restrições para proteção da privacidade com certeza deverão partir dos Estados, pois ao setor privado não interessa restringir seu próprio negócio. Um marco regulatório com jurisdição global seria a única ação com efetividade e de maior abrangência para proteger a privacidade como direito fundamental da pessoa.

Os dados pessoais já estão sendo coletados, armazenados e processados nos bancos de dados das empresas que desenvolvem os objetos, mas o atual sistema de proteção de dados pessoais não permite aos proprietários das coisas serem proprietários também de seus preciosos dados.

Referências

_____. **Por que é necessária uma Carta de Direitos da Internet?**. Trad. Bernardo Diniz Accioli de Vasconcellos e Chiara Spadaccini de Teffé. Civilistica.com. Rio de Janeiro, a. 4, n. 2, jul. dez./2015. Disponível em: http://civilistica.com/por-que-e-necessaria-uma-carta-de-direitos-da-internet/. Acesso em: 10 fev. 2020.

BOFF, Salete Oro; FORTES, Vinícius Borges. **A privacidade e a proteção dos dados pessoais no ciberespaço como um direito fundamental: perspectivas de construção de um marco regulatório para o Brasil.** Sequência (Florianópolis), Florianópolis, n. 68, p. 109-127, June 2014. DOI: https://doi.org/10.5007/2177-7055.2013v35n68p109. Disponível em: http://www.scielo.br/scielo.php?script=sci_arttext&pid=S217770552014000100006&lng=en&nrmiso. Acesso em: 18 fev. 2020.

CHABRIDON, Sophie et al. ***A survey on addressing privacy together with quality of context for context management in the Internet of Things. annals of telecommunications-annales des télécommunications***, v. 69, n. 1-2, p. 47-62, 2014.

DONEDA, D.; Mendes, L. **Um perfil da nova Lei Geral de Proteção de Dados brasileira *In* Governança e regulações da Internet na América Latina: análise sobre infraestrutura, privacidade, cibe segurança e evoluções tecnológicas em homenagem aos dez anos da *South School on Internet Governance*.** Org.: BELLI, L.; CAVALLI, O. Rio de Janeiro: Escola de Direito do Rio de Janeiro da Fundação Getúlio Vargas, 2019.556 p.

GOMES, G. S., BERGAMO, F. V. M. **Chegou a Era da Internet das Coisas? Um Estudo sobre Adoção de Objetos Inteligentes no Contexto Brasileiro**. Revista Brasileira de Marketing, v. 17, n. 2, p. 251-263, 2018.

MAGGIOLINI, Piercarlo. ***A deep study on the concept of digital ethics***. Rev. adm. empres., São Paulo, v. 54, n. 5, p. 585-591, Oct. 2014. DOI: https://doi.org/10.1590/S0034-759020140511._Disponível em: http://www.scielo.br/scielo.php?script=sci_arttext&pid=S003475902014000500585&lng=en&nr=iso. Acesso em: 25 fev. 2020.

MAGRANI, Eduardo. **A internet das coisas,** FGV Editora, 2018. 192 p.

MARTORELL, Leandro Brambilla; NASCIMENTO, Wanderson Flor do; GARRAFA, Volnei. **Redes sociais, privacidade, confidencialidade e ética: a exposição de imagens de pacientes no *facebook***. Interface (Botucatu), Botucatu, v. 20, n. 56, p. 13-23, mar 2016, E-pub 03-Nov-2015. DOI: https://doi.org/10.1590/1807-57622014.0902. Disponível em: http://www.scielo.br/scielo.php?script=sci_arttext&pid=S141432832016000100013&lng=pt&nrm=iso. Acesso em: 25 fev. 2020.

PACHECO, F., KLEIN, A., RIGHI, R. **Modelos de negócio para produtos e serviços baseados em internet das coisas: uma revisão da literatura e oportunidades de pesquisas**

futuras. REGE Revista De Gestão, 23(1), 41-51. Disponível em DOI: https://doi.org/10.1016/j.rege.2015.12.001. Acesso em: 20 fev. 2020.

PIRES, F. Paulo; **Plataformas para a Internet das Coisas**, v.1, n. 1, jul. 2018, p 5-6.

RODOTÀ, Stéfano. **A vida na sociedade da vigilância – A privacidade hoje.** Rio de Janeiro; São Paulo: Renovar, 2008.

RODRIGUES, G.A.P. ALBUQUERQUE, R. de O.; GOMES F.E.; TIMÓTEO, R.; JUNIOR, G.A.O.; VILLALBA, L.J.G; KIM, T.H**.** ***Cybersecurity and Network Forensics: Analysis of Malicious Traffic towards a Honeynet with Deep Packet Inspection***. Appl. Sci. 2017, 7, 1082. Disponível em DOI: https://doi.org/10.3390/app7101082. Acesso em: 20 fev. 2020.

SASTRE, Andrés; LEMOS, Amanda. ***Acceso, uso y protección de datos personales em América Latina: diseños metodológicos y teóricos*****.** Disponível em: https://www.cprlatam.org/. Acesso em: 20 fev. 2020.

SANTOS, Bruna; VARON, Joana. ***Data and Elections in Brazil 2018 a research by Coding Rights for Tactical Technology Collective, Published as Country Report of the Project 'personal data and political influence', available at "our data, our selves"***. Rio de Janeiro, outubro, 2018.

SANTOS, César Carlos. **O Desafio da Privacidade na Internet das Coisas**. Revista Gestão.Org, v. 13, Edição Especial, 2015. p. 282-290. ISSN 1679-1827. Disponível em: http://www.revista.ufpe.br/gestao.org.br. Acesso em 20 fev. 2020.

SCHARTWZ, Paul M. ***Privacy and democracy in cyberspace*****.** Vanderbilt Law Review, v.52, p.1658, 1999.

SERGL, M. J.; CUNHA, G. **A relação entre o indivíduo pós-moderno, o consumo e a internet das coisas.** R. Tecnol. Soc., Curitiba, v. 16, n. 39, p. 41-56, jan/mar. 2020. Disponível em: https://periodicos.utfpr.edu.br/rts/article/view/8747. Acesso em: 10 fev. 2020.

SILVA, Edima Aranha. **Evolução histórica do método científico: desafios e paradigmas para o século XXI**. Economia e Pesquisa. Araçatuba, v.3, n.3, p. 109-118, mar. 2001

SILVEIRA, Alessandra; FROUFE, Pedro. **Do mercado interno à cidadania de direitos: a proteção de datos pessoais como a questão jus fundamental identitária dos nossos tempos.** UNIO - EU *Law Journal*. Vol. 4, No. 2, jul. 2018, p 4-20.

VERONESE, A.; CUNHA, M. **Desafios do comércio eletrônico no Brasil: integração vertical entre fornecedores e meios de pagamentos, proteção de dados pessoais e cooperação regulatória internacional**. UNIO - EU *Law Journal*. v. 4, n. 2, jul. 2018, p 73-89.